Información avanzada de incorporación de cuentas de AMS

Guía de incorporación avanzada de AMS

Version September 25, 2025

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

Guía de incorporación avanzada de AMS: Información avanzada de incorporación de cuentas de AMS

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

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

Table of Contents

Introducción a la incorporación de AWS Managed Services 1
Más información sobre AMS 1
Términos clave 2
Modos AMS 9
Modos y aplicaciones o cargas de trabajo AMS 10
Guía prescriptiva posterior a la cuenta de AMS 18
Lo que hacemos, lo que no hacemos 18
Gestión del tráfico de salida AMS 19
Roles de usuario de IAM 20
MALZ: Funciones de usuario de IAM predeterminadas 21
SALZ: rol de usuario de IAM predeterminado 34
Reglas de firewall de acceso predeterminadas 42
Puertos de instancias de Linux Stack 43
Puertos de instancias de Windows Stack 43
Administración de servicios 45
Gobierno de cuentas 45
Inicio del servicio 46
Gestión de relaciones con los clientes (CRM) 46
Proceso de CRM 47
Reuniones de CRM 48
Organización de reuniones de CRM 49
Informes mensuales de CRM 50
Optimización de costos 51
Marco de optimización de costos 51
Matriz de responsabilidad de optimización de costes 54
Horas de servicio 56
Obtener ayuda 56
Modos de administración de cambios 57
Descripción general de los modos 58
Tipos de modos y cuentas en AMS 59
Modos y aplicaciones o cargas de trabajo AMS 62
Casos de uso reales para los modos AMS 71
Modo RFC 74
Más información sobre RFCs 75

¿Qué son los tipos de cambios? 116
Solución de problemas de errores de RFC 129
Modo de cambio directo 140
Cómo empezar con el modo Direct Change 141
Seguridad y conformidad 144
Gestión de cambios en el modo Direct Change 149
Creación de pilas mediante el modo de cambio directo 152
Casos de uso del modo de cambio directo 155
Modo desarrollador 156
Cómo empezar con el modo Desarrollador 157
Seguridad y conformidad 159
Administración de cambios 161
Aprovisionamiento de la infraestructura 167
Controles de detección 168
Registro, supervisión y gestión de eventos 168
Administración de incidentes 168
Administración de parches 169
Gestión de la continuidad 169
Gestión de seguridad y acceso 169
Modo de aprovisionamiento de autoservicio en AMS 170
Cómo empezar con el modo SSP en AMS 171
Amazon API Gateway 171
Alexa for Business 172
Amazon AppStream 2.0 174
Amazon Athena 177
Amazon Bedrock 178
Amazon CloudSearch 179
Amazon CloudWatch Synthetics 180
Amazon Cognito 181
Amazon Comprehend 183
Amazon Connect 184
Amazon Data Firehose 187
El DevOps gurú de Amazon 188
Amazon DocumentDB (con compatibilidad con MongoDB) 189
Amazon DynamoDB 190
Amazon Elastic Container Registry 191

EC2 Image Builder 192
Amazon ECS en AWS Fargate 194
Amazon EKS en AWS Fargate 197
Amazon EMR 200
Amazon EventBridge 203
Amazon Forecast 205
Amazon FSx 208
Amazon FSx para OpenZFS 210
Amazon FSx para NetApp ONTAP 212
Amazon Inspector Classic 213
Amazon Kendra 215
Amazon Kinesis Data Streams 215
Amazon Kinesis Video Streams 216
Amazon Lex 217
Amazon MQ 218
Amazon Managed Service para Apache Flink 219
Transmisión gestionada de Amazon para Apache Kafka 221
Servicio administrado por Amazon para Prometheus 222
Amazon Personalize 223
Amazon QuickSight 226
Amazon Rekognition 227
Amazon SageMaker AI 229
Amazon Simple Email Service 232
Amazon Simple Workflow Service 233
Amazon Textract 234
Amazon Transcribe 235
Amazon WorkSpaces 237
Servicios de códigos AMS 239
AWS Amplify 242
AWS AppSync 243
AWS App Mesh 244
AWS Audit Manager 245
AWS Batch 246
AWS Certificate Manager 247
AWS Private Certificate Authority 249
AWS CloudEndure 252

AWS CloudHSM 253
AWS CodeBuild 255
AWS CodeCommit 256
AWS CodeDeploy 258
AWS CodePipeline 259
AWS Compute Optimizer 261
AWS DataSync 262
AWS Device Farm 264
AWS Elastic Disaster Recovery 264
AWS Elemental MediaConvert 266
AWS Elemental MediaLive 267
AWS Elemental MediaPackage 268
AWS Elemental MediaStore 269
AWS Elemental MediaTailor 270
AWS Global Accelerator 271
AWS Glue 272
AWS Lake Formation 273
AWS Lambda 275
AWS License Manager 276
AWS Migration Hub 277
AWS Outposts 278
AWS Resilience Hub 279
AWS Secrets Manager 280
AWS Security Hub CSPM 283
AWS Service Catalog AppRegistry 284
AWS Shield 285
AWS Snowball Edge 286
AWS Step Functions 288
AWS Systems Manager Almacén de parámetros 289
AWS Systems Manager Automation 290
AWS Transfer Family 294
AWS Transit Gateway 295
AWS WAF 296
AWS Well-Architected Tool 297
AWS X-Ray 298
VM Import/Export 299

Modo gestionado por el cliente 301
Cómo empezar con el modo Customer Managed 301
Catálogo de servicios de AMS y AWS 302
Introducción a Service Catalog 302
Service Catalog en AMS antes de empezar 303
Incorporación de AMS Multi-Account Landing Zone (MALZ) 307
Arquitectura de red MALZ 307
Acerca de la arquitectura de red de landing zone multicuenta 307
Elegir un solo MALZ o varios MALZs 310
Cuentas multicuenta de Landing Zone 315
MALZ: Incorporación de cuentas principales 350
Crea una AWS cuenta principal de landing zone con varias cuentas 350
Cree un rol de IAM para que AMS acceda a su cuenta 352
Proteja la nueva cuenta con autenticación multifactor (MFA) para el usuario root 353
Suscríbase AWS Marketplace a EPS 354
Configurar redes 355
Configurar la administración de acceso 358
MALZ: Incorporación de cuentas de aplicaciones 364
Solicitar una nueva cuenta de aplicación 364
Configuración de Active Directory para federar el acceso a las funciones de AMS IAM 366
Configuración de la red con la nueva cuenta de la aplicación 369
Configuración adicional VPCs en la cuenta de la aplicación 371
Apéndice: lista de consideraciones para la incorporación de múltiples cuentas a una zona de landing zone (MALZ) 371
Configuración de la cuenta 372
Alertas de monitoreo de zonas de landing zone con varias cuentas de AMS 373
Configuración de red 373
Configuración de Active Directory 374
Protección de endpoints de Trend Micro (EPS) 374
Acceso: Bastions, SSH y RDP 375
Federación 376
Incorporación de AMS Single-Account Landing Zone (SALZ) 377
Proceso de incorporación de AMS SALZ 377
Arquitectura de red SALZ 378
Servicios compartidos de zona de aterrizaje con una sola cuenta de AMS 379
SALZ: Crea una nueva AWS cuenta para AMS 380

Crea un Cuenta de AWS ... 380
Configure la facturación consolidada: vincule la nueva cuenta a la cuenta del pagador ... 383
Configure su Cuenta de AWS acceso a AMS ... 384
Suscríbase a AWS Marketplace para EPS ... 386
Suscríbase a AWS Marketplace para CentOS 7.6 ... 387
Proteja la nueva cuenta con autenticación multifactor (MFA) para el usuario root ... 387
SALZ: Configurar redes ... 388
Asigne espacio IP para su entorno AMS ... 388
Establezca una conectividad de red privada con AWS ... 389
Configura tu firewall ... 391
Opciones de AMS Bastion durante las migraciones o la incorporación de aplicaciones ... 391
SALZ: configurar la gestión de acceso ... 392
Establecer una confianza en Active Directory (AD) ... 393
Federe su Active Directory con las funciones de AMS AWS Identity and Access Management ... 399
SALZ: configuración predeterminada ... 405
Seguridad de terminales (EPS) ... 406
Grupos de seguridad ... 411
EC2 Perfil de instancia de IAM ... 416
Valores predeterminados de las métricas monitorizadas ... 424
Valores predeterminados de retención y rotación de registros ... 441
Valores predeterminados de administración de continuidad ... 442
Valores predeterminados de aplicación de parches ... 443
Valide el servicio AMS (SALZ) ... 445
Encuentra la configuración de la cuenta ... 445
Buscar un ID de instancia o una dirección IP ... 449
Nombres de bastiones compatibles con DNS ... 452
Búsqueda de direcciones IP de bastión ... 453
EC2 instancias: creación ... 454
Acceso, solicitud ... 463
Otros | Otros RFC, creación (CLI) ... 470
Cualquier pila: eliminar, reiniciar, iniciar, detener ... 473
Ejemplos de acceso ... 485
Reportar un incidente ... 495
Crear una solicitud de servicio ... 498
Pasos posteriores a la incorporación ... 501

Tutoriales 501
Apéndice: Cuestionario de incorporación de SALZ 529
Resumen de despliegue 529
Consideraciones sobre la arquitectura del entorno 530
Alertas de monitoreo de zonas de aterrizaje con una sola cuenta 531
Maintenance Window (Período de mantenimiento) 531
Siguientes pasos 531
Apéndice: Regla de notificación de ActiveDirectory Federation Services (ADFS) y configuración de SAML 533
Configuraciones de reglas de reclamación de ADFS 533
Consola web 534
Acceso a API y CLI con SAML 534
Configuración de scripts 534
Configuración de Windows 534
Configuración de Linux 537
Historial de documentos 538
..... dxli

Introducción a la incorporación de AWS Managed Services

Bienvenido a AWS Managed Services (AMS). AMS es un servicio empresarial que proporciona una administración continua de su infraestructura de AWS. Esta guía está diseñada para ayudarle a empezar a utilizar AMS, y le explicamos cómo configurar una nueva cuenta para AMS, configurar las redes y el acceso a AMS y validar su configuración de incorporación.

Está destinado a los administradores de TI encargados de preparar y llevar a cabo las tareas necesarias para incorporar el servicio AMS a una nueva cuenta de AWS. La incorporación del servicio AMS requiere privilegios especiales para configurar las confianzas de Active Directory y realizar otras tareas a nivel de red. Para obtener ayuda para decidir si usar cuentas de zona de aterrizaje con varias cuentas o cuentas de zona de aterrizaje con una sola cuenta, visita Cómo elegir una MALZ o varias. MALZs

> **Important**
>
> Esta guía se divide en dos partes después de esta introducción: una para las cuentas de landing zone multicuenta y otra para las cuentas de landing zone de una sola cuenta. La incorporación es muy diferente para ambas. Dirígete a la sección de la guía que corresponda a tu situación.

Temas

- Más información sobre AMS
- Términos clave de AMS
- Modos AMS
- Guía prescriptiva posterior a la cuenta de AMS
- Lo que hacemos, lo que no hacemos
- Gestión del tráfico de salida AMS
- Función de usuario de IAM en AMS
- Reglas de firewall de acceso predeterminadas

Más información sobre AMS

Para entender mejor el AMS, consulte estas secciones de la guía del usuario del AMS:

- What Is AWS Managed Services presenta el servicio AMS y describe las características, operaciones e interfaces clave, así como una arquitectura de red típica administrada por AMS. En este capítulo también se proporciona información sobre la gestión del acceso, incluida la forma de acceder a los recursos gestionados por AMS y el uso de los bastiones.
- Key Terms proporciona definiciones y explicaciones de la terminología de AMS.
- Al comprender los valores predeterminados de AMS, se proporcionan los valores predeterminados que utiliza AMS, incluidos los valores predeterminados para los componentes básicos del entorno, la IAM y los proxies EC2, las métricas supervisadas, el registro, la seguridad de los terminales (EPS), las copias de seguridad y los parches.
- La administración de cambios proporciona detalles sobre cómo funcionan las solicitudes de cambio (RFCs) y los tipos de cambio (CTs) e incluye ejemplos del uso de AMS. RFCs
- Varios capítulos adicionales tratan sobre el acceso a la consola de AWS, la CLI de AMS, mediante el sistema de administración de cambios AMS, el AMS SKMS, la seguridad, las solicitudes de servicio, los incidentes, la supervisión, los registros, el EPS, las copias de seguridad y la administración de parches.

Para obtener más información sobre la arquitectura de zonas de aterrizaje multicuenta de AMS, consulte Arquitectura de red de zonas de aterrizaje multicuenta

Para obtener más información sobre la arquitectura de zonas de aterrizaje de cuenta única de AMS, consulte Arquitectura de red de zonas de aterrizaje de cuenta única

Términos clave de AMS

- AMS Advanced: los servicios descritos en la sección «Descripción del servicio» de la documentación avanzada de AMS. Consulte la descripción del servicio.
- Cuentas avanzadas de AMS: AWS cuentas que cumplen en todo momento todos los requisitos de incorporación avanzada de AMS. Para obtener información sobre las ventajas de AMS Advanced, los casos prácticos y ponerse en contacto con un representante de ventas, consulte AWS Managed Services.
- Cuentas AMS Accelerate: AWS cuentas que cumplen en todo momento todos los requisitos de incorporación de AMS Accelerate. Consulte Cómo empezar a utilizar AMS Accelerate.
- AWS Managed Services: AMS o AMS Accelerate.
- Cuentas de AWS Managed Services: las cuentas AMS o las cuentas AMS Accelerate.

- Recomendación fundamental: recomendación emitida AWS mediante una solicitud de servicio en la que se le informa de que es necesario tomar medidas para protegerse de posibles riesgos o interrupciones en sus recursos o en los Servicios de AWS mismos. Si decide no seguir una recomendación crítica antes de la fecha especificada, usted es el único responsable de cualquier daño que se derive de su decisión.
- Configuración solicitada por el cliente: cualquier software, servicio u otra configuración que no esté identificada en:
  - Accelerate: configuraciones compatibles o AMS Accelerate; descripción del servicio.
  - AMS Advanced: configuraciones compatibles o AMS Advanced; descripción del servicio.
- Comunicación de incidentes: AMS le comunica un incidente o usted solicita un incidente a AMS a través de un incidente creado en el Support Center de AMS Accelerate y en la consola de AMS para AMS. La consola AMS Accelerate proporciona un resumen de los incidentes y las solicitudes de servicio en el panel de control y enlaces al Support Center para obtener más información.
- Entorno gestionado: las cuentas AMS Advanced o las cuentas AMS Accelerate gestionadas por AMS.

  En el caso de AMS Advanced, se incluyen las cuentas de zona de aterrizaje multicuenta (MALZ) y de zona de aterrizaje de cuenta única (SALZ).
- Fecha de inicio de la facturación: al día hábil siguiente, AWS recibirá la información solicitada en el correo electrónico de incorporación de AWS Managed Services. El correo electrónico de incorporación de AWS Managed Services hace referencia al correo electrónico que usted envía para recopilar la información necesaria para activar los servicios gestionados de AWS en sus cuentas. AWS

  En el caso de las cuentas que usted inscriba posteriormente, la fecha de inicio de la facturación es el día siguiente al envío por parte de AWS Managed Services de una notificación de activación de AWS Managed Services para la cuenta inscrita. Se produce una notificación de activación de AWS Managed Services cuando:

  1. Concede acceso a una AWS cuenta compatible y se la entrega a AWS Managed Services.
  2. AWS Managed Services diseña y crea la cuenta de AWS Managed Services.
- Finalización del servicio: puede cancelar los servicios gestionados de AWS para todas las cuentas de AWS Managed Services o para una cuenta específica de AWS Managed Services por cualquier motivo avisando con al AWS menos 30 días de antelación mediante una solicitud de servicio. En la fecha de finalización del servicio, puede:

1. AWS le entrega el control de todas las cuentas de AWS Managed Services o de las cuentas de AWS Managed Services especificadas, según corresponda, o
2. Las partes eliminan las AWS Identity and Access Management funciones que dan AWS acceso a todas las cuentas de AWS Managed Services o a las cuentas de AWS Managed Services especificadas, según proceda.

- Fecha de finalización del servicio: la fecha de finalización del servicio es el último día del mes natural siguiente al final del período de preaviso de rescisión obligatorio de 30 días. Si el final del período de notificación de rescisión requerido cae después del día 20 del mes calendario, la fecha de finalización del servicio es el último día del mes calendario siguiente. Los siguientes son ejemplos de escenarios para las fechas de terminación.
  - Si el aviso de rescisión se proporciona el 12 de abril, el aviso de 30 días finaliza el 12 de mayo. La fecha de finalización del servicio es el 31 de mayo.
  - Si se proporciona un aviso de rescisión el 29 de abril, el aviso de 30 días finaliza el 29 de mayo. La fecha de finalización del servicio es el 30 de junio.
- Prestación de AWS Managed Services: AWS pone a su disposición los servicios gestionados de AWS Managed Services y los puede utilizar para cada cuenta de AWS Managed Services a partir de la fecha de inicio del servicio.
- Cancelación de cuentas de AWS Managed Services específicas: puede cancelar los servicios de AWS Managed Services de una cuenta específica de AWS Managed Services por cualquier motivo mediante AWS notificación mediante una solicitud de servicio («Solicitud de cancelación de la cuenta AMS»).

Condiciones de gestión de incidentes:

- Evento: un cambio en su entorno de AMS.
- Alerta: cada vez que un evento de un Servicio de AWS dispositivo compatible supera un umbral y activa una alarma, se crea una alerta y se envía un aviso a tu lista de contactos. Además, se crea un incidente en tu lista de incidentes.
- Incidente: una interrupción no planificada o una degradación del rendimiento de su entorno de AMS o AWS Managed Services que se traduce en un impacto según lo informado por AWS Managed Services o por usted.
- Problema: una causa raíz subyacente compartida de uno o más incidentes.
- Resolución de incidentes o resolución de un incidente:

  - AMS ha restablecido todos los servicios o recursos de AMS no disponibles relacionados con ese incidente a un estado disponible, o
  - AMS ha determinado que las pilas o los recursos no disponibles no se pueden restaurar a un estado disponible, o
  - AMS ha iniciado una restauración de la infraestructura autorizada por usted.
- Tiempo de respuesta ante un incidente: diferencia de tiempo entre el momento en que se crea un incidente y el momento en que AMS proporciona una respuesta inicial a través de la consola, el correo electrónico, el centro de servicio o el teléfono.
- Tiempo de resolución de incidentes: la diferencia de tiempo entre el momento en que AMS o usted crean un incidente y el momento en que se resuelve el incidente.
- Prioridad de incidentes: cómo AMS o usted priorizan los incidentes, ya sea baja, media o alta.
  - Baja: un problema no crítico con su servicio AMS.
  - Medio: hay un servicio de AWS disponible en su entorno gestionado, pero no funciona según lo previsto (según la descripción del servicio correspondiente).
  - Alto: (1) la consola AMS o uno o más AMS de su APIs entorno gestionado no están disponibles; o (2) una o más pilas o recursos de AMS de su entorno gestionado no están disponibles y la falta de disponibilidad impide que la aplicación desempeñe su función.

  AMS puede reclasificar los incidentes de acuerdo con las directrices anteriores.
- Restauración de la infraestructura: volver a implementar las pilas existentes, en función de las plantillas de las pilas afectadas, e iniciar una restauración de datos en función del último punto de restauración conocido, a menos que se especifique lo contrario, cuando no sea posible resolver los incidentes.

Términos de infraestructura:

- Entorno de producción gestionado: una cuenta de cliente en la que residen las aplicaciones de producción del cliente.
- Entorno no productivo gestionado: cuenta de cliente que solo contiene aplicaciones que no son de producción, como aplicaciones de desarrollo y pruebas.
- Pila de AMS: grupo de uno o más AWS recursos que AMS administra como una sola unidad.
- Infraestructura inmutable: modelo de mantenimiento de infraestructura típico de los grupos de Amazon EC2 Auto Scaling (ASGs) en el que los componentes de infraestructura actualizados (en AWS la AMI) se sustituyen en cada implementación, en lugar de actualizarse in situ. La ventaja de

una infraestructura inmutable es que todos los componentes permanecen en un estado sincrónico, ya que siempre se generan a partir de la misma base. La inmutabilidad es independiente de cualquier herramienta o flujo de trabajo para crear la AMI.

- Infraestructura mutable: modelo de mantenimiento de infraestructura típico de las pilas que no son grupos de Amazon EC2 Auto Scaling y que contienen una sola instancia o solo unas pocas instancias. Este modelo es el que más se parece a la implementación de sistemas tradicional, basada en hardware, en la que un sistema se implementa al principio de su ciclo de vida y, posteriormente, las actualizaciones se van añadiendo capas a ese sistema a lo largo del tiempo. Todas las actualizaciones del sistema se aplican a las instancias de forma individual y pueden provocar un tiempo de inactividad del sistema (según la configuración de la pila) debido al reinicio de la aplicación o del sistema.
- Grupos de seguridad: firewalls virtuales para que la instancia controle el tráfico entrante y saliente. Los grupos de seguridad actúan en el ámbito de la instancia, no en el de la subred. Por lo tanto, cada instancia de una subred de la VPC podría tener asignado un conjunto diferente de grupos de seguridad.
- Acuerdos de nivel de servicio (SLAs): parte de los contratos de AMS con usted que definen el nivel de servicio esperado.
- El SLA no está disponible y no está disponible:
  - Una solicitud de API enviada por usted que produce un error.
  - Una solicitud de consola enviada por ti que da como resultado una respuesta HTTP de cinco veces mayor (el servidor no puede ejecutar la solicitud).
  - Cualquiera de las Servicio de AWS ofertas que constituyen pilas o recursos en su infraestructura gestionada por AMS se encuentra en un estado de «interrupción del servicio», como se muestra en el Service Health Dashboard.
  - La falta de disponibilidad que resulte directa o indirectamente de una exclusión de AMS no se tiene en cuenta al determinar la elegibilidad para los créditos de servicio. Los servicios se consideran disponibles a menos que cumplan con los criterios para no estar disponibles.
- Objetivos de nivel de servicio (SLOs): parte de los contratos de AMS con usted que definen objetivos de servicio específicos para los servicios de AMS.

Términos de aplicación de parches:

- Parches obligatorios: actualizaciones de seguridad críticas para abordar problemas que podrían comprometer el estado de seguridad de su entorno o cuenta. Una «actualización de seguridad

crítica» es una actualización de seguridad calificada como «crítica» por el proveedor de un sistema operativo compatible con AMS.

- Parches anunciados frente a parches publicados: los parches se anuncian y publican por lo general según un calendario. Los parches emergentes se anuncian cuando se descubre la necesidad de aplicarlos y, por lo general, poco después de su publicación.
- Complemento de parche: parche basado en etiquetas para instancias de AMS que aprovecha la funcionalidad AWS Systems Manager (SSM) para que pueda etiquetar instancias y parchearlas utilizando una línea base y una ventana que usted configure.
- Métodos de parches:
  - Parcheo in situ: parcheo que se realiza cambiando las instancias existentes.
  - Parcheo de reemplazo de la AMI: aplicación de parches que se realiza cambiando el parámetro de referencia de la AMI de una configuración de lanzamiento de grupo de EC2 Auto Scaling existente.
- Proveedor de parches (proveedores de sistemas operativos, terceros): los parches los proporciona el proveedor o el órgano rector de la aplicación.
- Tipos de parches:
  - Actualización de seguridad crítica (CSU): actualización de seguridad calificada como «crítica» por el proveedor de un sistema operativo compatible.
  - Actualización importante (IU): una actualización de seguridad calificada como «importante» o una actualización no relacionada con la seguridad calificada como «crítica» por el proveedor de un sistema operativo compatible.
  - Otra actualización (OU): actualización realizada por el proveedor de un sistema operativo compatible que no es una CSU ni una IU.
- Parches compatibles: AMS admite parches a nivel de sistema operativo. El proveedor publica actualizaciones para corregir vulnerabilidades de seguridad u otros errores o para mejorar el rendimiento. Para obtener una lista de las configuraciones compatibles actualmente OSs, consulte Support Configurations.

Términos de seguridad:

- Controles de Detective: una biblioteca de monitores creados o habilitados por AMS que proporcionan una supervisión continua de los entornos y las cargas de trabajo gestionados por los clientes para detectar configuraciones que no se ajustan a los controles de seguridad, operativos o

del cliente, y toman medidas al notificar a los propietarios, modificar de forma proactiva o cancelar los recursos.

Condiciones de la solicitud de servicio:

- Solicitud de servicio: una solicitud suya para que AMS tome una medida en su nombre.
- Notificación de alerta: aviso que AMS publica en su página de lista de solicitudes de servicio cuando se activa una alerta de AMS. El contacto configurado para su cuenta también recibe una notificación mediante el método configurado (por ejemplo, el correo electrónico). Si tiene etiquetas de contacto en sus instancias o recursos y ha dado su consentimiento a su administrador de prestación de servicios en la nube (CSDM) para las notificaciones basadas en etiquetas, la información de contacto (valor clave) de la etiqueta también se notificará para recibir alertas de AMS automatizadas.
- Notificación de servicio: una notificación de AMS que se publica en la página de la lista de solicitudes de servicios.

Términos varios:

- Interfaz de AWS Managed Services: para AMS: la consola avanzada de AWS Managed Services, la API CM de AMS y la Soporte API. Para AMS Accelerate: la Soporte consola y la Soporte API.
- Satisfacción del cliente (CSAT): El CSAT de AMS se basa en análisis exhaustivos, que incluyen valoraciones de casos por correspondencia en cada caso o correspondencia, cuando se presentan, encuestas trimestrales, etc.
- DevOps: DevOps es una metodología de desarrollo que aboga firmemente por la automatización y la supervisión en todos los pasos. DevOps tiene como objetivo acortar los ciclos de desarrollo, aumentar la frecuencia de despliegue y ofrecer versiones más fiables, ya que reúne las funciones de desarrollo y operaciones, que tradicionalmente estaban separadas, sobre la base de la automatización. Cuando los desarrolladores pueden gestionar las operaciones y las operaciones sirven de base para el desarrollo, los problemas se descubren y resuelven más rápidamente y los objetivos empresariales se alcanzan más fácilmente.
- ITIL: La biblioteca de infraestructura de tecnología de la información (denominada ITIL) es un marco de ITSM diseñado para estandarizar el ciclo de vida de los servicios de TI. ITIL se organiza en cinco etapas que cubren el ciclo de vida de los servicios de TI: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora del servicio.

- Administración de servicios de TI (ITSM): conjunto de prácticas que alinean los servicios de TI con las necesidades de su empresa.
- Servicios de monitorización gestionados (MMS): AMS opera su propio sistema de monitorización, Managed Monitoring Service (MMS), que consume eventos de AWS salud y agrega datos de CloudWatch Amazon y datos de Servicios de AWS otros, y notifica a los operadores de AMS (en línea las 24 horas del día, los 7 días de la semana) cualquier alarma creada a través de un tema del Amazon Simple Notification Service (Amazon SNS).
- Espacio de nombres: cuando crea políticas de IAM o trabaja con Amazon Resource Names (ARNs), identifica y utiliza un espacio Servicio de AWS de nombres. Los espacios de nombres se utilizan para identificar acciones y recursos.

Modos AMS

Úselo para ayudarle a seleccionar el modo AWS Managed Services (AMS) adecuado para alojar sus aplicaciones, en función de la combinación deseada de flexibilidad y gobierno prescriptivo para lograr sus resultados empresariales.

El público al que va dirigida esta información es:

- Los equipos de clientes son responsables de la estrategia y la gobernanza de su landing zone. Esta información ayudará al equipo a sentar las bases de una landing zone gestionada por AMS, con los modos AMS que les gustaría ofrecer a sus clientes internos y externos.
- Propietarios de empresas y aplicaciones encargados de migrar su aplicación a AMS. Esta información ayudará a planificar la migración de la aplicación, con el modo AMS adecuado para migrate/host su aplicación. Tenga en cuenta que la misma aplicación se puede alojar en más de un modo AMS durante las diferentes fases de su ciclo de vida del ciclo de vida del desarrollo de software (SDLC).
- Los socios de AMS se encargaron de guiar a los clientes sobre las diferentes opciones para crear y migrar a AMS.

Esta información supone que ya ha tomado la decisión de utilizar AMS para acelerar su transición a la nube. Consulte este paper en dos momentos de su proceso de migración a la nube: primero, durante la fase básica de configuración de la plataforma gestionada por AMS. En segundo lugar, cuando está pasando de la fase básica a la de migración de su proceso de adopción de la nube, justo después de completar la incorporación a AMS y centrarse en la gobernanza y las operaciones de las aplicaciones.

Modos y aplicaciones o cargas de trabajo AMS

Tenga en cuenta los requisitos operativos y de gobierno de sus aplicaciones al seleccionar el modo correcto, ya sea solicitando una nueva cuenta de aplicación o alojando la aplicación en una cuenta de aplicación existente. La selección del modo AMS adecuado para cada aplicación o carga de trabajo depende de los siguientes factores:

- El tipo de función del ciclo de vida del SDLC que proporcionará el entorno (por ejemplo, entorno aislado con cambios no moderados, UAT con algunos cambios frecuentes, producción con cambios mínimos y altamente regulada)
- Las políticas de gobierno necesarias (aplicadas a SCPs nivel de unidad organizativa)
- Modelo operativo (si desea asumir la responsabilidad operativa o desea subcontratarla a AMS)
- Los resultados empresariales deseados, como el tiempo necesario para operar en la nube y el coste de las operaciones.

> **Note**
>
> Para obtener una descripción de los tipos de modos por servicio de AMS, consulte Tipos de modos y cuentas en AMS.
> Para ver casos de uso reales de los distintos modos, consulte Casos de uso reales de los modos AMS

En la siguiente tabla se describen las principales consideraciones para que los propietarios de aplicaciones puedan decidir cuál es el modo AMS más adecuado. Los propietarios de las aplicaciones deben incluir una fase de evaluación antes de la migración de la aplicación para comprender completamente qué modo se aplica a su aplicación específica. Ejemplo: en el caso de las aplicaciones basadas en servicios nativos de la nube o en una arquitectura sin servidor, la mejor opción podría ser empezar a crear e iterar en modo desarrollador e implementar la infraestructura como código final mediante el modo AMS Managed (SSP). En este caso, puede ser necesaria una ligera refactorización para garantizar que cualquier CloudFormation plantilla creada para el despliegue automatizado cumpla con las directrices de ingesta establecidas por AMS. Además, cualquier permiso de IAM debe ser aprobado por AMS Security para garantizar que siga el modelo de privilegios mínimos.

El modo AMS seleccionado para alojar la aplicación puede ayudarle a desarrollar el modelo operativo de nube que desee.

> **Note**
>
> Puede existir más de un modelo operativo en la nube en una única zona de aterrizaje gestionada por AMS en función de los distintos modos de AMS seleccionados para alojar las aplicaciones.

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Preparación operativa						
Registro, supervisión y gestión de eventos	AMS es responsable de toda la infraestructura gestionada			El cliente es responsable de los servicios aprovisionados de autoservicio (SSP)	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	El cliente es responsable
Gestión de la continuidad	La responsabilidad de AMS de ejecutar el plan de respaldo seleccionado por el cliente			El cliente es responsable de los servicios aprovisionados de autoservicio (SSP)	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de	

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
					desarrollador ajena al sistema AMS CM	
Administración de acceso a nivel de instancia	Administrado por AMS mediante una confianza unidireccional de AD con dominio local. Requiere una infraestructura gestionada para unirse al dominio AMS			No aplicable	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	
Gestión de la seguridad y gestión del acceso a nivel de cuenta	Responsabilidad de AMS con respecto a todas las cuentas gestionadas			AMS es responsable de todas las cuentas gestionadas	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Administración de parches	Responsabilidad de AMS con respecto a todas las cuentas gestionadas			El cliente es responsable de los servicios aprovisionados de autoservicio (SSP)	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	
Administración de cambios	Responsabilidad de AMS con respecto a todas las cuentas gestionadas			El cliente es responsable de los servicios aprovisionados de autoservicio (SSP)	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Gestión del aprovisionamiento	Prescriptivo y estandarizado para las opciones de aprovisionamiento que se ofrecen en AMS	Flexibilidad para utilizar directamente la API de servicios de AWS para AWS Service Catalog siguiendo los estándares prescriptivos de AMS	Flexibilidad para utilizar directamente la API de servicios de AWS siguiendo los estándares prescriptivos de AMS	Flexibilidad para utilizar directamente el servicio de AWS APIs para los servicios de SSP	Flexibilidad para utilizar directamente la API de servicios de AWS para el aprovisionamiento	

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Gestión y auditoría de incidentes	AMS es responsable de todas las cuentas gestionadas				El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema de gestión de cambios de AMS	
GuardRails y una infraestructura (red) y un marco de seguridad compartidos	Uso prescriptivo y estandarizado de las cuentas principales de AMS					Flexible y personalizado, aprovechando las cuentas principales de AMS
Preparación de las aplicaciones						

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Refactorización de aplicaciones	Es necesaria una refactorización de la luz				Es necesaria una refactorización ligera (si se aprovisiona con AMS Standard CM)	No es necesario refactorizar
Support para los servicios de AWS	Limitado a lo que admite AMS					No limitado
Consideraciones empresariales						
Es hora de estar listo para operar	De tres a seis meses			Más de 6 meses, dependiendo de las competencias operativas de las aplicaciones del cliente		De 6 a 18 meses, según las competencias del cliente en materia de infraestructura y operaciones de aplicaciones
Costos	$$$$			$$$	$$	$

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Ejemplos de aplicaciones	Servidor web con pila de 3 niveles, aplicaciones con requisitos normativos y de conformidad			Servidor web que utiliza API Gateway, aplicación conteneri zada que aprovecha ECS/EKS	Iteración /optimización en la aplicación Data Lake que usa Lambda, Glue, Athena, etc.	Descentralizadas, accounts/ applications como en un entorno sandbox, aplicaciones gestionadas por terceros

* Operations On Demand (OOD) ofrece una oferta para los clientes que utilizan el modo CM estándar para gestionar sus cambios mediante una dotación de recursos específica. Para obtener más información, consulte el catálogo de ofertas de Operations on Demand y hable con su gerente de prestación de servicios en la nube (CSDM).

> **Note**
>
> La comparación de precios entre el modo SSP y el modo desarrollador supone que se aprovisionan los mismos servicios de AWS.

Comparación de los modos AMS con los objetivos empresariales y de TI

Como se muestra, si busca un modelo de gobierno estandarizado y altamente controlado para sus aplicaciones, los modos Standard Change, AWS Service Catalog o Direct Change gestionados por AMS son los más adecuados. Si necesita un modelo de gobierno personalizado que se centre en la innovación de las aplicaciones sin necesidad de contar con una preparación operativa, seleccione el modo gestionado por el cliente. Con el modo gestionado por el cliente, poner en funcionamiento sus aplicaciones podría tardar más tiempo, ya que es responsable de establecer

las personas, los procesos y las herramientas que respalden las capacidades operativas, como la gestión de incidentes, la gestión de la configuración, la gestión del aprovisionamiento, la gestión de la seguridad, la gestión de parches, etc.

Guía prescriptiva posterior a la cuenta de AMS

A medida que las organizaciones adoptan operaciones y DevOps prácticas distribuidas, hay un conjunto básico de capacidades operativas que deben aplicarse a todas las cuentas antes de implementar las cargas de trabajo para cumplir con los pilares de Well Architected.

Este enlace descarga un archivo ZIP que contiene un documento de Word y un archivo ZIP con guiones y ejemplos. La configuración automática de cuentas es un conjunto de scripts para automatizar o iniciar la configuración de una nueva cuenta de aplicación.

Una vez que se vende una cuenta nueva y antes de que se despliegue cualquier carga de trabajo, para que la cuenta esté lista desde el punto de vista operativo, de seguridad y de administración, se configuran planes de respaldo predeterminados, ventanas de parches y cifrado (y mucho más). Para mejorar la agilidad, la coherencia y la capacidad de respuesta de la configuración de las cuentas de las aplicaciones, le ofrecemos el siguiente ejemplo de «Cómo hacerlo» como referencia.

Configuración automática de la cuenta.

Lo que hacemos, lo que no hacemos

AMS le ofrece un enfoque estandarizado para implementar la infraestructura de AWS y proporciona la administración operativa continua necesaria. Para obtener una descripción completa de las funciones, responsabilidades y servicios compatibles, consulte la descripción del servicio.

> **Note**
>
> Para solicitar que AMS proporcione un servicio de AWS adicional, presente una solicitud de servicio. Para obtener más información, consulte Realización de solicitudes de servicio.

- Qué hacemos:

  Una vez completada la incorporación, el entorno AMS estará disponible para recibir solicitudes de cambio (RFCs), incidentes y solicitudes de servicio. Su interacción con el servicio AMS gira en torno al ciclo de vida de una pila de aplicaciones. Las nuevas pilas se ordenan a partir de una lista

preconfigurada de plantillas, se lanzan a subredes de nube privada virtual (VPC) específicas, se modifican durante su vida operativa mediante solicitudes de cambio (RFCs) y se supervisan las 24 horas del día, los 7 días de la semana para detectar eventos e incidentes.

AMS supervisa y mantiene las pilas de aplicaciones activas, incluida la aplicación de parches, y no requieren ninguna otra acción durante la vida útil de la pila, a menos que sea necesario cambiarlas o retirarlas del servicio. Los incidentes detectados por AMS que afecten al estado y al funcionamiento de la pila generan una notificación y es posible que necesites o no que tomes medidas para resolverlos o verificarlos. Puede realizar preguntas prácticas y de otro tipo enviando una solicitud de servicio.

Además, AMS le permite habilitar servicios de AWS compatibles que no están gestionados por AMS. Para obtener información sobre los servicios compatibles con AWS-AMS, consulte Modo de aprovisionamiento de autoservicio.

- Lo que NO hacemos:

  Si bien AMS simplifica la implementación de aplicaciones al proporcionar una serie de opciones manuales y automatizadas, usted es responsable del desarrollo, las pruebas, la actualización y la administración de su aplicación. AMS proporciona asistencia para la resolución de problemas de infraestructura que afectan a las aplicaciones, pero AMS no puede acceder a las configuraciones de las aplicaciones ni validarlas.

Gestión del tráfico de salida AMS

De forma predeterminada, la ruta con un CIDR de destino de 0.0.0.0/0 para las subredes privadas y de aplicaciones de cliente de AMS tiene como destino una puerta de enlace de traducción de direcciones de red (NAT). Los servicios TrendMicro y los parches de AMS son componentes que deben tener acceso de salida a Internet para que AMS pueda prestar su servicio y los sistemas operativos puedan obtener actualizaciones. TrendMicro

AMS permite desviar el tráfico de salida a Internet a través de un dispositivo de salida gestionado por el cliente siempre que:

- Actúa como un proxy implícito (por ejemplo, transparente).

  y

- Permite las dependencias HTTP y HTTPS de AMS (enumeradas en esta sección) para permitir la aplicación continua de parches y el mantenimiento de la infraestructura gestionada por AMS.

Algunos ejemplos son:

- La pasarela de tránsito (TGW) tiene una ruta predeterminada que apunta al firewall local administrado por el cliente a través de la conexión AWS Direct Connect en la cuenta de red de zona de aterrizaje multicuenta.
- El TGW tiene una ruta predeterminada que apunta a un punto de enlace de AWS en la VPC de salida de múltiples cuentas que aprovecha AWS y apunta a un proxy administrado por el cliente en otra cuenta de PrivateLink AWS.
- El TGW tiene una ruta predeterminada que apunta a un firewall administrado por el cliente en otra cuenta de AWS, con una conexión site-to-site VPN adjunta a la TGW de la zona de destino multicuenta.

AMS ha identificado las dependencias HTTP y HTTPS correspondientes de AMS, y las desarrolla y perfecciona de forma continua. Consulte egressMgmt.zip. Junto con el archivo JSON, el ZIP contiene un archivo README.

> **Note**
>
> - Esta información no es exhaustiva; algunos sitios externos obligatorios no aparecen aquí.
> - No utilices esta lista como parte de una lista de rechazados o una estrategia de bloqueo.
> - Esta lista pretende ser un punto de partida para un conjunto de reglas de filtrado de egreso, con la expectativa de que se utilicen herramientas de generación de informes para determinar con precisión dónde se diferencia el tráfico real de la lista.

Para solicitar información sobre cómo filtrar el tráfico de salida, envíe un correo electrónico a su CSDM: ams-csdm@amazon.com.

Función de usuario de IAM en AMS

Una función de IAM es similar a la de un usuario de IAM, en el sentido de que es una AWS identidad con políticas de permisos que determinan lo que la identidad puede y no puede hacer en ella. AWS

No obstante, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite.

Actualmente, `Customer_ReadOnly_Role` hay un rol de usuario predeterminado de AMS para las cuentas de AMS estándar y un rol adicional `customer_managed_ad_user_role` para las cuentas de AMS con Active Directory administrado.

Las políticas de roles establecen los permisos CloudWatch y las acciones de registro de Amazon S3, el acceso a la consola AMS, las restricciones de solo lectura en la mayoría de los casos Servicios de AWS, el acceso restringido a la consola S3 de la cuenta y el acceso mediante cambios de tipo.

Además, `Customer_ReadOnly_Role` tiene permisos mutables de instancias reservadas que le permiten reservar instancias. Tiene algunos valores de ahorro de costes, por lo que, si sabe que va a necesitar un número determinado de EC2 instancias de Amazon durante un período prolongado, puede llamarlas APIs. Para obtener más información, consulte Amazon EC2 Reserved Instances.

> **Note**
>
> El objetivo de nivel de servicio (SLO) de AMS para crear políticas de IAM personalizadas para los usuarios de IAM es de cuatro días hábiles, a menos que se vaya a reutilizar una política existente. Si desea modificar el rol de usuario de IAM existente o añadir uno nuevo, envíe un RFC de IAM: Update Entity o IAM: Create Entity, respectivamente.

Si no está familiarizado con las funciones de Amazon IAM, consulte Funciones de IAM para obtener información importante.

Zona de aterrizaje multicuenta (MALZ): para ver las políticas de rol de usuario predeterminadas y no personalizadas de las zonas de aterrizaje multicuenta de AMS, consulte a continuación. MALZ: Funciones de usuario de IAM predeterminadas

MALZ: Funciones de usuario de IAM predeterminadas

Declaraciones de política de JSON para los roles de usuario multicuenta predeterminados de AMS multicuenta en la zona de landing zone.

> **Note**
>
> Los roles de usuario se pueden personalizar y pueden variar según la cuenta. Se proporcionan instrucciones para encontrar su función.

Estos son ejemplos de los roles de usuario predeterminados de MALZ. Para asegurarse de que ha establecido las políticas que necesita, ejecute el comando AWS `get-role` o inicie sesión en la consola AWS Management -> IAM y seleccione Roles en el panel de navegación.

Funciones principales de la cuenta OU

Una cuenta principal es una cuenta de infraestructura gestionada por Malz. Las cuentas principales de AMS multi-account landing zone incluyen una cuenta de administración y una cuenta de red.

Cuenta principal de OU: funciones y políticas comunes

Rol	Política o políticas
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Política gestionada pública de AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAcceso (política gestionada pública de AWS).
AWSManagedServicesChangeManagementRole (Versión de la cuenta principal)	ReadOnlyAccess
	AWSSupportAcceso
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

Cuenta principal de OU: funciones y políticas de la cuenta de administración

Rol	Política o políticas
AWSManagedServicesBillingRole	AMSBillingPolítica (AMSBillingPolítica).

Rol	Política o políticas
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Política gestionada pública de AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAcceso (política gestionada pública de AWS).
AWSManagedServicesChangeManagementRole (Versión de cuenta de administración)	ReadOnlyAccess
	AWSSupportAcceso
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

Cuenta principal de OU: funciones y políticas de las cuentas de red

Rol	Política o políticas
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Política gestionada pública de AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAcceso (política gestionada pública de AWS).
AWSManagedServicesChangeManagementRole (Versión de cuenta de red)	ReadOnlyAccess
	AWSSupportAcceso
	AMSChangeManagementReadOnlyPolicy

Rol	Política o políticas
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

Funciones de la cuenta de la aplicación

Los roles de la cuenta de la aplicación se aplican a las cuentas específicas de la aplicación.

Cuenta de aplicación: funciones y políticas

Rol	Política o políticas
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Política gestionada pública de AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAcceso (política gestionada pública de AWS). Esta política proporciona acceso a todas las operaciones y recursos de soporte. Para obtener más información, consulte Introducción a AWS Support.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess
	AWSSupportEjemplo de acceso Esta política proporciona acceso a todas las operaciones y recursos de soporte.
	AWSCertificateManagerFullAccess información, (Política pública gestionada de AWS)

Rol	Política o políticas
	AWSWAFFullAccess información (política pública gestionada por AWS). Esta política otorga acceso total a los recursos de AWS WAF.
	AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (Versión de la cuenta de la aplicación)	ReadOnlyAccess
	AWSSupportAcceso (política gestionada pública de AWS). Esta política proporciona acceso a todas las operaciones y recursos de soporte. Para obtener más información, consulte Introducción a AWS Support.
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Política
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupportAcceso
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess

Rol	Política o políticas
	AWSWAFFullAcceso
	AMSS3Política
	AMSReservedInstancesPolicy

Ejemplos de política

Se proporcionan ejemplos de la mayoría de las políticas utilizadas. Para ver la ReadOnlyAccess política (que tiene una extensión de páginas, ya que proporciona acceso de solo lectura a todos los AWS servicios), puede utilizar este enlace si tiene una cuenta de AWS activa:. ReadOnlyAccess Además, aquí se incluye una versión resumida.

AMSBillingPolítica

`AMSBillingPolicy`

El departamento de contabilidad puede utilizar la nueva función de facturación para ver y cambiar la información de facturación o la configuración de la cuenta de gestión. Para acceder a información como los contactos alternativos, ver el uso de los recursos de la cuenta, controlar tu facturación o incluso modificar tus métodos de pago, utilizas esta función. Esta nueva función incluye todos los permisos que figuran en la página web de acciones de IAM sobre facturación de AWS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToBilling"
        },
        {
```

```
            "Action": [
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountSettings"
        },
        {
            "Action": [
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountBudget"
        },
        {
            "Action": [
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPaymentMethods"
        },
        {
            "Action": [
                "aws-portal:ViewUsage"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToUsage"
        },
        {
            "Action": [
                "cur:DescribeReportDefinitions",
                "cur:PutReportDefinition",
                "cur:DeleteReportDefinition",
                "cur:ModifyReportDefinition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostAndUsageReport"
```

```
        },
        {
            "Action": [
                "pricing:DescribeServices",
                "pricing:GetAttributeValues",
                "pricing:GetProducts"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPricing"
        },
        {
            "Action": [
                "ce:*",
                "compute-optimizer:*"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostExplorerComputeOptimizer"
        },
        {
            "Action": [
                "purchase-orders:ViewPurchaseOrders",
                "purchase-orders:ModifyPurchaseOrders"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPurchaseOrders"
        },
        {
            "Action": [
                "redshift:AcceptReservedNodeExchange",
                "redshift:PurchaseReservedNodeOffering"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToRedshiftAction"
        },
        {
            "Action": "savingsplans:*",
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AWSSavingsPlansFullAccess"
        }
```

```
    ]
}
```

AMSChangeManagementReadOnlyPolicy

`AMSChangeManagementReadOnlyPolicy`

Permisos para ver todos los tipos de cambios de AMS y el historial de los tipos de cambios solicitados.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

`AMSMasterAccountSpecificChangeManagementInfrastructurePolicy`

Permisos para solicitar el tipo de cambio de despliegue | Managed landing zone | Cuenta de administración | Crear cuenta de aplicación (con VPC).

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

`AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy`

Permisos para solicitar el tipo de cambio de implementación | Managed landing zone | Cuenta de red | Crear tabla de rutas de aplicaciones.

AMSChangeManagementInfrastructurePolicy

`AMSChangeManagementInfrastructurePolicy`(para administración | Otros | Otros CTs)

Permisos para solicitar los tipos de cambio de administración | Otros | Otros | Otros | Otros | Otros | Actualizar tipos de cambios.

AMSSecretsManagerSharedPolicy

`AMSSecretsManagerSharedPolicy`

Permisos para ver los datos secretos passwords/hashes compartidos por AMS AWS Secrets Manager (por ejemplo, las contraseñas de la infraestructura para su auditoría).

Permisos para crear un secreto password/hashes para compartirlo con AMS. (por ejemplo, las claves de licencia de los productos que se deben implementar).

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
   "Sid": "AllowAccessToSharedNameSpaces",
   "Effect": "Allow",
   "Action": "secretsmanager:*",
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
   ]
  },
  {
   "Sid": "DenyGetSecretOnCustomerNamespace",
   "Effect": "Deny",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
   "Sid": "AllowReadAccessToAMSNameSpace",
   "Effect": "Deny",
   "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
 ]
}
```

AMSChangeManagementPolicy

`AMSChangeManagementPolicy`

Permisos para solicitar y ver todos los tipos de cambios de AMS y el historial de los tipos de cambios solicitados.

AMSReservedInstancesPolicy

`AMSReservedInstancesPolicy`

Permisos para gestionar las instancias EC2 reservadas de Amazon; para obtener información sobre los precios, consulte Amazon EC2 Reserved Instances.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Sid": "AllowReservedInstancesManagement",
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
   "*"
  ]
 }]
}
```

AMSS3Política

`AMSS3Policy`

Permisos para crear y eliminar archivos de buckets de Amazon S3 existentes.

> **Note**
>
> Estos permisos no permiten crear buckets de S3; esto debe hacerse con el tipo de cambio Deployment | Advanced stack components | S3 storage | Create.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSSupportAcceso

`AWSSupportAccess`

Acceso completo a Soporte. Para obtener información, consulte Cómo empezar con Soporte. Para obtener información sobre Premium Support, consulte Soporte.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "support:*"
  ],
  "Resource": "*"
 }]
}
```

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions`(Política de AWS gestión pública)

Permisos para suscribirse, cancelar la suscripción y ver AWS Marketplace las suscripciones.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
```

```
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`

Acceso completo a AWS Certificate Manager. Para obtener más información, consulte AWS Certificate Manager.

`AWSCertificateManagerFullAccess`información (Política pública gestionada de AWS).

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "acm:*"
  ],
  "Resource": "*"
 }]
}
```

AWSWAFFullAcceso

`AWSWAFFullAccess`

Acceso completo a AWS WAF. Para obtener más información, consulte AWS WAF : Web Application Firewall.

`AWSWAFFullAccess`información, (política de AWS gestión pública). Esta política otorga acceso total a AWS WAF los recursos.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

ReadOnlyAccess

`ReadOnlyAccess`

Acceso de solo lectura a todos los AWS servicios y recursos de la AWS consola. Cuando AWS lanza un nuevo servicio, AMS actualiza la ReadOnlyAccess política para añadir permisos de solo lectura al nuevo servicio. Los permisos actualizados se aplican a todas las entidades principales a las que la política está asociada.

Esto no permite iniciar sesión en los hosts o en los EC2 hosts de bases de datos.

Si tienes una política activa Cuenta de AWS, puedes usar este enlace ReadOnlyAccesspara ver la ReadOnlyAccess política completa. Toda la ReadOnlyAccess política es muy larga, ya que proporciona acceso de solo lectura para todos. Servicios de AWS El siguiente es un extracto parcial de la política. ReadOnlyAccess

Zona de aterrizaje de cuenta única (SALZ): para ver las políticas de rol de usuario predeterminadas y no personalizadas de la zona de aterrizaje de cuenta única de AMS, consulte a continuación. SALZ: rol de usuario de IAM predeterminado

SALZ: rol de usuario de IAM predeterminado

Declaraciones de política de JSON para el rol de usuario predeterminado de AMS con una sola cuenta en la zona de landing zone.

> **Note**
>
> El rol de usuario predeterminado de SALZ se puede personalizar y puede variar según la cuenta. Se proporcionan instrucciones para encontrar su función.

El siguiente es un ejemplo del rol de usuario de SALZ predeterminado. Para asegurarse de que tiene las políticas definidas para usted, ejecute el `get-role`comando. O bien, inicie sesión en la AWS Identity and Access Management consola en y https://console.aws.amazon.com/iam/, a continuación, seleccione Roles.

La función de cliente de solo lectura es una combinación de varias políticas. A continuación se presenta un desglose del rol (JSON).

Política de auditoría de Managed Services:

Política de IAM ReadOnly de Managed Services

Política de usuario de Managed Services

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "AllowCustomerToListTheLogBucketLogs",
     "Effect": "Allow",
     "Action": [
       "s3:ListBucket"
     ],
     "Resource": [
       "arn:aws:s3:::mc-a*-logs-*"
     ],
     "Condition": {
       "StringLike": {
         "s3:prefix": [
           "aws/*",
           "app/*",
           "encrypted",
           "encrypted/",
           "encrypted/app/*"
         ]
```

```
        }
      }
    },
    {
      "Sid": "BasicAccessRequiredByS3Console",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "AllowCustomerToGetLogs",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
      ]
    },
    {
      "Sid": "AllowAccessToOtherObjects",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCustomerToListTheLogBucketRoot",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
```

```
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:prefix": [
            "",
            "/"
          ]
        }
      }
    },
    {
      "Sid": "AllowCustomerCWLConsole",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "AllowCustomerCWLAccessLogs",
      "Effect": "Allow",
      "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
      ]
    },
    {
      "Sid": "AWSManagedServicesFullAccess",
      "Effect": "Allow",
      "Action": [
        "amscm:*",
        "amsskms:*"
      ],
```

```
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ModifyAWSBillingPortal",
      "Effect": "Allow",
      "Action": [
        "aws-portal:Modify*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "DenyDeleteCWL",
      "Effect": "Deny",
      "Action": [
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "DenyMCCWL",
      "Effect": "Deny",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
      ]
    },
    {
      "Sid": "DenyS3MCNamespace",
      "Effect": "Deny",
      "Action": [
```

```
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*-audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
      ]
    },
    {
      "Sid": "ExplicitDenyS3CfnBucket",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::cf-templates-*"
      ]
    },
    {
      "Sid": "DenyListBucketS3LogsMC",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
          ]
        }
      }
    },
    {
      "Sid": "DenyS3LogsDelete",
      "Effect": "Deny",
      "Action": [
        "s3:Delete*",
```

```
        "s3:Put*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
      ]
    },
    {
      "Sid": "DenyAccessToKmsKeysStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
      ]
    },
    {
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
      ],
```

```
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Política compartida de Customer Secrets Manager

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
   {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ],
```

```
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}
```

Política de suscripción a Customer Marketplace

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Reglas de firewall de acceso predeterminadas

Estas son las reglas de firewall predeterminadas que se requieren para acceder a las instancias.

> **Note**
>
> Para obtener información sobre las reglas de firewall y los puertos necesarios para establecer una confianza unidireccional de AD, consulte la Guía de seguridad de AMS en la consola AWS Artifact -> pestaña Informes y busque AWS Managed Services.

Puertos de instancias de Linux Stack

Estas reglas son necesarias para la autenticación en las pilas de AMS Linux.

La instancia de Linux transfiere las reglas de: instancia de Linux Stack A: controlador de dominio CORP

Puerto	Protocolo	Servicio	Dirección
389	TCP	LDAP	Ingreso
389	UDP	LDAP	Ingreso
88	TCP	Kerberos	Ingreso
88	UDP	Kerberos	Ingreso

Puertos de instancias de Windows Stack

Estas reglas son necesarias para la autenticación en las pilas de Windows de AMS.

DESDE: Windows Stack Instance HASTA: CORP Domain Controller

Puerto	Protocolo	Servicio	Dirección
88	TCP | UDP	Kerberos	Entrada y salida
135	TCP | UDP	Servicio de localización DCE/RPC	Entrada y salida
389	TCP | UDP	LDAP	Entrada y salida
3268	TCP | UDP	msft-gc, Catálogo global de Microsoft (servicio LDAP que contiene datos de bosques de Active Directory)	Entrada y salida
445	TCP	Microsoft-DS Active Directory, recursos compartidos de Windows	Entrada y salida
49152 - 65535	TCP	Puertos dinámicos o privados que no se pueden registrar en la IANA. Este rango se utiliza para servicios	Entrada y salida

Puerto	Protocolo	Servicio	Dirección
		privados o personalizados o con fines temporales y para la asignación automática de puertos efímeros.	

Administración de servicios en AWS Managed Services

Temas

- Gestión de cuentas en AWS Managed Services
- Inicio del servicio en AWS Managed Services
- Gestión de relaciones con los clientes (CRM)
- Optimización de costos en AWS Managed Services
- Horas de servicio en AWS Managed Services
- Obtener ayuda en AWS Managed Services

Cómo funciona el servicio AMS para usted.

Gestión de cuentas en AWS Managed Services

En esta sección se describe la gobernanza de las cuentas de AMS.

Se le designa como administrador de prestación de servicios en la nube (CSDM), que proporciona asesoramiento en todo AMS y tiene un conocimiento detallado de su caso de uso y de la arquitectura tecnológica para el entorno gestionado. CSDMs colabore con los administradores de cuentas, los administradores técnicos de cuentas, los arquitectos de nube de AWS Managed Services (CAs) y los arquitectos de soluciones de AWS (SAs), según proceda, para ayudar a lanzar nuevos proyectos y ofrecer recomendaciones sobre las mejores prácticas a lo largo de los procesos de desarrollo y operaciones del software. El CSDM es el principal punto de contacto de AMS. Las principales responsabilidades de su CSDM son:

- Organice y dirija reuniones mensuales de revisión del servicio con los clientes.
- Proporcione detalles sobre la seguridad, las actualizaciones de software para el entorno y las oportunidades de optimización.
- Defienda sus requisitos, incluidas las solicitudes de funciones para AMS.
- Responda y resuelva las solicitudes de informes de facturación y servicio.
- Proporcione información para recomendaciones de optimización financiera y de capacidad.

Inicio del servicio en AWS Managed Services

Inicio del servicio: la fecha de inicio del servicio de una cuenta de AWS Managed Services es el primer día del primer mes natural después del cual AWS le notifica que se han completado las actividades establecidas en los requisitos de incorporación de esa cuenta de AWS Managed Services; siempre que si AWS realiza dicha notificación después del día 20 de un mes natural, la fecha de inicio del servicio será el primer día del segundo mes natural siguiente a la fecha de dicha notificación.

Inicio del servicio

- R significa parte responsable que hace el trabajo para lograr la tarea.
- La letra I significa «informado»: una parte que recibe información sobre el progreso, a menudo solo una vez finalizada la tarea o el producto final.

Inicio del servicio

N.° de paso	Título del paso	Descripción	Cliente	AMS
1.	Entrega de la cuenta de AWS al cliente	El cliente crea una nueva cuenta de AWS y se la entrega a AWS Managed Services	R	I
2.	Cuenta AWS Managed Services: diseño	Finalice el diseño de la cuenta de AWS Managed Services	I	R
3.	Cuenta AWS Managed Services: creación	Se crea una cuenta de AWS Managed Services según el diseño del paso 2	I	R

Gestión de relaciones con los clientes (CRM)

AWS Managed Services (AMS) proporciona un proceso de administración de las relaciones con los clientes (CRM) para garantizar que se establezca y mantenga una relación bien definida con

usted. La base de esta relación se basa en el conocimiento que AMS tiene de las necesidades de su empresa. El proceso de CRM facilita una comprensión precisa y completa de:

- Las necesidades de su empresa y cómo satisfacerlas
- Sus capacidades y limitaciones
- AMS y sus diferentes responsabilidades y obligaciones

El proceso de CRM permite a AMS utilizar métodos coherentes para prestarle servicios y gestionar su relación con AMS. El proceso de CRM incluye:

- Identificar a las partes interesadas clave
- Establecer un equipo de gobierno
- Realización y documentación de reuniones de revisión del servicio con usted
- Proporcionar un procedimiento formal de quejas de servicio con un procedimiento de escalamiento
- Implementar y monitorear su proceso de satisfacción y comentarios
- Gestionar su contrato

Proceso de CRM

El proceso de CRM incluye las siguientes actividades:

- Identificar y comprender los procesos y necesidades de su negocio. Su acuerdo con AMS identifica a sus partes interesadas.
- Definir los servicios que se prestarán para satisfacer sus necesidades y requisitos.
- Reunirnos con usted durante las reuniones de revisión del servicio para analizar cualquier cambio en el alcance del servicio de AMS, el SLA, el contrato y las necesidades de su empresa. Es posible que se celebren reuniones provisionales con usted para analizar el desempeño, los logros, los problemas y los planes de acción.
- Controle su satisfacción mediante nuestra encuesta de satisfacción del cliente y los comentarios proporcionados en las reuniones.
- Informar sobre el rendimiento mediante informes mensuales de rendimiento medidos internamente.
- Revisar el servicio con usted para determinar las oportunidades de mejora. Esto incluye una comunicación frecuente con usted en relación con el nivel y la calidad del servicio de AMS prestado.

Reuniones de CRM

Los gerentes de prestación de servicios en la nube de AMS (CSDMs) se reúnen con usted periódicamente para hablar sobre las áreas de servicio (operaciones, seguridad e innovaciones de productos) y ejecutivas (informes de acuerdos de nivel de servicio, medidas de satisfacción y cambios en las necesidades de su empresa).

Reunión	Finalidad	Mode	Participantes
Revisión de estado semanal (opcional)	Problemas o incidentes pendientes, parches, eventos de seguridad, registros de problemas Tendencia operativa de 12 semanas (+/- 6) Dudas del operador de la aplicación Horario de fin de semana	Cliente presencial location/ Telecom/Chime	AMS: CSDM y arquitecto de nube (CA) Miembros del equipo asignados por el cliente (p. ej.: equipos de Cloud/ Infrastructure, Application Support, Architecture, etc.)
Revisión empresarial mensual	Revise el rendimiento del nivel de servicio (informes, análisis y tendencias) Análisis financiero Hoja de ruta del producto ELENCO	Cliente presencial location/ Telecom/Chime	AMS: CSDM, arquitecto de nube (CA), equipo de cuentas de AMS, gerente de productos técnicos de AMS (TPM) (opcional), gerente de OPS de AMS (opcional)

Reunión	Finalidad	Mode	Participantes
			Usted: representante del operador de aplicaciones
Revisión comercial trimestral	Rendimiento y tendencias del cuadro de mando y del acuerdo de nivel de servicio (SLA) (6 meses) Planes o migraciones para los próximos 3, 6 y 9 meses Riesgos y mitigaciones de riesgos Iniciativas clave de mejora Elementos de la hoja de ruta del producto Oportunidades alineadas con la dirección futura Finanzas Iniciativas de ahorro de costos Optimización empresarial	Ubicación in situ del cliente	AMS: CSDM, arquitecto de la nube, equipo de cuentas de AMS, director de servicios de AMS, gerente de operaciones de AMS Usted: representante del operador de aplicaciones, representante de servicio, director de servicio

Organización de reuniones de CRM

El CSDM de la AMS es responsable de documentar la reunión, lo que incluye:

- Crear la agenda, incluidos los puntos de acción, los temas y la lista de asistentes.
- Crear la lista de puntos de acción revisados en cada reunión para garantizar que los puntos se completen y se resuelvan según lo programado.
- Distribuir las actas de la reunión y la lista de elementos de acción a los asistentes a la reunión por correo electrónico en el plazo de un día hábil después de la reunión.

- Almacenar las actas de las reuniones en el repositorio de documentos correspondiente.

En ausencia del CSDM, el representante de la AMS que dirige la reunión crea y distribuye las actas.

> **Note**
>
> Su CSDM trabaja con usted para establecer el gobierno de su cuenta.

Informes mensuales de CRM

Su AMS CSDM prepara y envía presentaciones mensuales sobre el rendimiento del servicio. Las presentaciones incluyen información sobre lo siguiente:

- Fecha del informe
- Resumen e información:
  - Información clave: recuento total y activo de las pilas, estado de las actualizaciones en las pilas, estado de incorporación de la cuenta (solo durante la incorporación), resúmenes de los problemas específicos de los clientes
  - Rendimiento: estadísticas sobre la resolución de incidentes, las alertas, la aplicación de parches, las solicitudes de cambio (RFCs), las solicitudes de servicio y la disponibilidad de la consola y la API
  - Problemas, desafíos, inquietudes y riesgos: estado de los problemas específicos del cliente
  - Próximos temas: planes de incorporación o resolución de incidentes específicos para cada cliente
- Recursos gestionados: gráficos y diagramas circulares de pilas
- Métricas de AMS: métricas de monitoreo y eventos, métricas de incidentes, métricas de cumplimiento de los SLA de AMS, métricas de solicitudes de servicio, métricas de administración de cambios, métricas de almacenamiento, métricas de continuidad, métricas de Trusted Advisor y resúmenes de costos (presentados de varias maneras). Solicitudes de funciones. Información de contacto.

> **Note**
>
> Además de la información descrita, su CSDM también le informa de cualquier cambio sustancial en el alcance o las condiciones, incluido el uso de subcontratistas por parte de AMS para actividades operativas.
> AMS genera informes sobre la aplicación de parches y las copias de seguridad que su CSDM incluye en su informe mensual. Como parte del sistema de generación de informes, AMS añade cierta infraestructura a tu cuenta a la que no puedes acceder:
>
> - Un bucket de S3, con los datos sin procesar informados
> - Una instancia de Athena, con definiciones de consulta para consultar los datos
> - Un Glue Crawler para leer los datos sin procesar del depósito S3

Optimización de costos en AWS Managed Services

AWS Managed Services le proporciona informes detallados de costos, utilización y ahorros todos los meses durante las revisiones empresariales mensuales (MBRs).

AMS sigue un conjunto estándar de procesos y mecanismos para identificar vías de ahorro de costes en sus cuentas gestionadas y ayudarle a planificar e implementar los cambios para optimizar su gasto en AWS.

> **Note**
>
> AMS está desarrollando un vídeo para ayudar a optimizar los costes. El primer paso es proporcionarle una hoja de cálculo en PDF y Excel con las mejores prácticas de optimización de costes. Para acceder a estos recursos, abra el archivo ZIP de la guía rápida para la optimización de costos.

Marco de optimización de costos

AMS sigue un enfoque de tres etapas con usted para optimizar sus costos de AWS:

1. Identifique las vías de optimización de costes en su entorno gestionado
2. Preséntele un plan de optimización de costos
3. Ayude a lograr la optimización de costos de una manera mensurable

Identifique las vías de optimización de costos en el entorno gestionado

AMS utiliza herramientas AWS nativas, como Cost Explorer y Trusted Advisor, a la vez que aprovecha más de 20 patrones de ahorro de costos en la optimización de la arquitectura, las optimizaciones AWS centradas en las EC2 instancias y las cuentas para crear recomendaciones de ahorro de costos personalizadas para usted.

Algunas de las recomendaciones de optimización incluyen las siguientes.

Recomendaciones de optimización arquitectónica:

- Uso óptimo de la clase de almacenamiento S3: Amazon S3 ofrece una variedad de clases de almacenamiento para cumplir con varios requisitos de carga de trabajo en función del acceso a los datos, la resiliencia y el costo. Los análisis de las clases de almacenamiento S3 Intelligent-Tiering y S3 basados en las necesidades de carga de trabajo le permiten administrar los costos de S3 de manera eficiente.
- Uso de arquitecturas de almacenamiento en caché: aprovechar las instancias de caché, cuando proceda, puede ayudarlo a reemplazar algunas instancias de bases de datos y, al mismo tiempo, cumplir con sus requisitos de IOPS.
- Ahorros en la actualización de EBS: la migración de sus volúmenes de EBS de gp2 a gp3 proporciona un ahorro de costos de hasta un 20% y puede aprovechar un rendimiento básico predecible de 3000 IOPS y 125 MiB/s, independientemente del tamaño del volumen.
- Uso de la elasticidad: las capacidades de autoescalado que AWS proporciona permiten una utilización eficaz de los recursos y vías para la optimización de los costos. Revisar y actualizar las políticas de escalado de instancias con regularidad en función de las necesidades también permite ahorrar costos.

EC2 recomendaciones centradas en las instancias

- Ajuste del tamaño de las instancias: las recomendaciones se centraron en el tamaño de las instancias y en las configuraciones óptimas en función del uso. Las recomendaciones también incluyen el uso de la función Amazon EC2 Auto Scaling y la sustitución de las EC2 instancias, cuando proceda, por contenido web estático en Amazon S3, etc. AWS Lambda
- Programación de instancias: el uso del programador de recursos de AMS para iniciar y detener automáticamente las instancias en función de un cronograma ayuda a reducir los costos, especialmente en el caso de las instancias que no son de producción y que no se utilizan fuera del horario laboral.

- Suscribirse a planes de ahorro: el plan de ahorro es la forma más fácil de ahorrar en el consumo. AWS Los EC2 Instance Savings Plans ofrecen hasta un 72% de ahorro en comparación con los precios bajo demanda en el uso de EC2 instancias de Amazon. Los Amazon SageMaker AI Savings Plans ofrecen hasta un 64% de ahorro en el uso de los servicios de Amazon SageMaker AI. AMS ofrece las recomendaciones adecuadas sobre los planes de ahorro en función del uso AWS de los recursos.
- Guía de uso y consumo de instancias reservadas (RI): las instancias EC2 reservadas (RI) de Amazon ofrecen un descuento significativo (hasta un 75%) en comparación con los precios bajo demanda y ofrecen una reserva de capacidad cuando se utilizan en una zona de disponibilidad específica.
- Uso de instancias puntuales: las cargas de trabajo tolerantes a errores pueden utilizar instancias puntuales y reducir los precios hasta un 90%.
- Terminación de instancias inactivas: identificar e informar sobre las instancias que están inactivas o de baja utilización y que se pueden cerrar.

Recomendaciones centradas en las cuentas

- Limpieza de cuentas: a nivel de cuentas, AMS también identifica los volúmenes de EBS no utilizados, los registros duplicados CloudTrail , las cuentas vacías con recursos no utilizados, etc., y ofrece recomendaciones para la limpieza.
- Recomendaciones de SLA: Además, AMS revisa periódicamente sus cuentas Plus y Premium y recomienda elegir el nivel de SLA adecuado para las cuentas.
- Optimización de la automatización de AMS: AMS optimiza continuamente la automatización y la infraestructura de AMS utilizadas para proporcionar los servicios de AMS.

Preséntelo a los clientes y ayúdeles en la planificación

AMS realiza revisiones comerciales mensuales (MBRs) con las principales partes interesadas de los clientes y presenta las vías, los mecanismos y las recomendaciones de ahorro de costos identificadas, junto con los posibles ahorros de costos. Seguiremos trabajando con usted para planificar los cambios necesarios.

Ayudamos en la implementación de las recomendaciones y medimos el impacto en los costos

El AMS ayuda a lograr y medir los impactos en los costos y los cambios de optimización.

Usted evalúa el impacto en la aplicación, el riesgo y los criterios de éxito de los cambios recomendados y formula las solicitudes de cambio adecuadas (RFCs) a través de la consola AMS. AMS colabora con usted e implementa los cambios relacionados con la optimización de costes en sus cuentas gestionadas. AMS mide el impacto en los costes e incluye los ahorros obtenidos en las revisiones empresariales mensuales (MBRs).

Matriz de responsabilidad de optimización de costes

Responsabilidades en la optimización de costes de AMS.

Optimización de costes (RACI)

Actividad	Cliente	AMS
Compilación de recomendaciones de ahorro de costes y preparación del informe	I	R
Presentación del informe de ahorro de costos	C	R
Planificar los cambios asociados al ahorro de costes	R	C
Evaluar el	R	C

Actividad	Cliente	AMS
impacto y el riesgo del cambio		
Recaudar RFCs para implementar los cambios	R	C
Revisar RFCs e implementar los cambios	C	R
Probar la aplicación y validar la implementación del cambio	R	C
Medir el impacto en los costos después del cambio y presentarlo al cliente	I	R

Horas de servicio en AWS Managed Services

Característica	AMS Advanced
	Nivel premium
Solicitud de servicio	24/7
Gestión de incidentes (P2-P3)	24/7
Copia de seguridad y recuperación	24/7
Administración de parches	24/7
Monitorización y alertas	24/7
Solicitud de cambio automatizada (RFC)	24/7
Solicitud de cambio no automatizada (RFC)	24/7
Gestor de prestación de servicios en la nube (CSDM)	De lunes a viernes: de 08:00 a 17:00, horario comercial local

Obtener ayuda en AWS Managed Services

AMS lo apoya en la gestión de incidentes, solicitudes de servicio y cambios las 24 horas del día, los 7 días de la semana y los 365 días del año (de conformidad con el acuerdo de nivel de servicio de AMS que se aplique a la cuenta).

Para informar de un problema de rendimiento de los servicios de AWS o AMS que afecte a su entorno gestionado, utilice la consola AMS y envíe un informe de incidente. Para obtener más información, consulte Notificación de un incidente. Para obtener información general sobre la gestión de incidentes de AMS, consulte Respuesta a incidentes.

Para solicitar información o consejos, o para solicitar servicios adicionales a AMS, utilice la consola de AMS y envíe una solicitud de servicio. Para obtener más información, consulte Creación de una solicitud de servicio. Para obtener información general sobre las solicitudes de servicio de AMS, consulte Administración de solicitudes de servicio.

Modos de administración de cambios

AWS Managed Services (AMS) utiliza el modo de administración de cambios para proteger los cambios en AMS Advanced. Los modos de administración de cambios le ayudan a mantener altos estándares operativos para el entorno y a controlar los riesgos y evitar los impactos adversos. El AMS Advanced tiene diferentes modos que proporcionan distintos niveles de control y riesgo. AMS gestiona todos los modos, excepto el modo gestionado por el cliente. Los modos de gestión de cambios disponibles son los siguientes:

- Modo RFC (anteriormente modo CM estándar): proporciona un sistema de «solicitud de cambio» (RFC) y tipos de cambio personalizados por AMS () CTs
- Modo Direct Change: igual que el modo RFC, además del uso de AWS APIs y consolas para crear recursos administrados por AMS
- AWS Service Catalog en AMS: similar al modo Direct Change, pero en lugar de utilizar el sistema de administración de cambios AMS (RFCs), se utiliza AWS Service Catalog para crear recursos que luego administra AMS.
- Modo desarrollador: igual que en el modo Direct Change, solo que los recursos que cree con AWS APIs y las consolas no están administrados por AMS; usted es responsable de su administración
- Modo de autoaprovisionamiento (SSP): igual que el modo desarrollador, excepto que no hay acceso al sistema de gestión de cambios AMS (no) RFCs
- Modo gestionado por el cliente: AMS te proporciona una zona de aterrizaje con varias cuentas, pero toda la gestión de los recursos es tu responsabilidad

El sistema de gestión de cambios de AWS Managed Services (AMS), que utiliza la API de gestión de cambios (CM), proporciona operaciones para crear y gestionar solicitudes de cambio (RFCs) tanto para cuentas de zona de aterrizaje multicuenta (MALZ) como de zona de aterrizaje de cuenta única (SALZ).

Una solicitud de cambio (RFC) es una solicitud creada por usted o por AMS a través de la interfaz de AMS para realizar un cambio en el entorno gestionado e incluye un identificador de tipo de cambio (CT) para una operación concreta.

La API de gestión de cambios (CM) de AMS proporciona operaciones para crear y gestionar las solicitudes de cambio (RFCs). Puede crear, actualizar, enviar, aprobar, rechazar y cancelar RFCs. Los operadores de AMS pueden crear, actualizar, enviar, aprobar, rechazar, cancelar y marcar RFCs como cerrados.

Para obtener una lista de los prefijos reservados del AMS que no deben usarse en nombres de etiquetas o de otro tipo, consulte Prefijos reservados.

Para obtener información sobre cada tipo de cambio, incluidos esquemas y ejemplos, consulte la Referencia de tipos de cambio de AMS.

> **Note**
>
> Todas las llamadas a la API de administración de cambios se graban en AWS CloudTrail. Para obtener más información, consulte Acceder a sus registros.

Descripción general de los modos

Utilice esta información como ayuda para seleccionar el modo de AWS Managed Services (AMS) adecuado para alojar sus aplicaciones, en función de la combinación deseada de flexibilidad y gobierno prescriptivo para lograr sus resultados empresariales.

El público al que va dirigida esta información es:

- Los equipos de clientes son responsables de la estrategia y la gobernanza de su landing zone. Esta información ayudará al equipo a sentar las bases de una landing zone gestionada por AMS, con los modos AMS que les gustaría ofrecer a sus clientes internos y externos.
- Propietarios de empresas y aplicaciones encargados de migrar su aplicación a AMS. Esta información ayudará a planificar la migración de la aplicación, con el modo AMS adecuado para migrate/host su aplicación. Tenga en cuenta que la misma aplicación se puede alojar en más de un modo AMS durante las diferentes fases de su ciclo de vida del ciclo de vida del desarrollo de software (SDLC).
- Los socios de AMS se encargaron de guiar a los clientes sobre las diferentes opciones para crear y migrar a AMS.

Esta información resulta especialmente útil durante la fase inicial de la configuración de la plataforma gestionada por AMS y cuando se está pasando de la fase básica a la de migración de la transición a la fase de adopción de la nube, justo después de que se haya completado la incorporación a AMS y se esté centrando en la gobernanza y las operaciones de las aplicaciones.

Tipos de modos y cuentas en AMS

Los modos AWS Managed Services (AMS) se pueden definir como las formas de interactuar con el servicio AMS en el marco de gobierno específico de cada modo. Se anotan las diferencias de zona de aterrizaje, zona de aterrizaje multicuenta o MALZ y zona de aterrizaje de cuenta única o SALZ.

> **Note**
>
> Para obtener más información sobre la implementación de aplicaciones y la elección del modo AMS correcto, consulte Modos AMS y aplicaciones o cargas de trabajo.
> Para ver casos de uso reales de los distintos modos, consulte Casos de uso reales de los modos AMS

La siguiente tabla proporciona descripciones de los modos por servicio AMS.

Función AMS	Modo RFC (anteriormente modo CM estándar)/ OOD *	Modo de cambio directo	AWS Service Catalog	Aprovisionamiento de autoservicio/modo de desarrollador	Gestionado por el cliente
Configuración de la zona de aterrizaje	MALZ y SALZ	MALZ y SALZ	MALZ y SALZ		
Administración de cambios	Programación de cambios, revisión de los cambios manuales y registro de cambios	Igual que el modo RFC para cambios de alto riesgo, como los de IAM o los grupos de seguridad	Ninguno		

Función AMS	Modo RFC (anteriormente modo CM estándar)/ OOD *	Modo de cambio directo	AWS Service Catalog	Aprovisionamiento de autoservicio/modo de desarrollador	Gestionado por el cliente
Registro, supervisión, barandas y gestión de eventos	Sí (recursos compatibles)			No	
Gestión de la continuidad	Sí (recursos compatibles)			No aplicable/No	No
Administración de la seguridad	Controles de seguridad a nivel de instancia y controles a nivel de cuenta			Controles a nivel de cuenta	Controles a nivel de organización de AWS
Administración de parches	Sí			No aplicable/No	No
Administración de incidentes y problemas	SLA de respuesta y resolución para los recursos compatibles con AMS			SLA de respuesta para los recursos resultantes	No
Informes	Sí			No	
Gestión de solicitudes de servicio	Sí			Solo solicitudes de soporte	No

* Operations On Demand (OOD) ofrece a los clientes que utilizan el modo RFC para gestionar sus cambios mediante una dotación de recursos específica. Para obtener más información, consulte el

catálogo de ofertas de Operations on Demand y hable con su gerente de prestación de servicios en la nube (CSDM).

> **Note**
>
> Modo de aprovisionamiento de autoservicio en AMSy ambos Modo AMS Advanced Developer pueden parecer adecuados para una aplicación que tiene una arquitectura compleja basada en los servicios nativos de AWS. Al diseñar la arquitectura de las cargas de trabajo, debe hacer concesiones entre la excelencia operativa y la agilidad, en función del contexto empresarial. Esta es una buena forma de pensar en seleccionar el modo SSP o el modo Desarrollador para su aplicación. La selección también puede cambiar en función de la fase de SDLC de la aplicación. Por ejemplo: cuando la aplicación esté lista para la producción, el modo SSP puede ser una opción más adecuada debido a que las barandillas AMS son más estrictas en este modo. Las barreras se imponen en forma de controles preventivos, como el control de cambios basado en RFC para las actualizaciones de IAM, y a nivel de la unidad organizativa de la aplicación. SCPs Estas decisiones de negocio puede impulsar sus prioridades de diseño. Se puede optimizar para aumentar la flexibilidad de los propietarios de las aplicaciones en la fase «previa a la producción», en detrimento de la gobernanza y el soporte operativo.

Arquitectura MALZ y modos AMS asociados

La zona de aterrizaje multicuenta (MALZ) de AMS le ofrece la opción de aprovisionar automáticamente cuentas de aplicaciones (o cuentas de recursos) en las unidades organizativas (OU) predeterminadas: OU gestionada por el cliente, OU gestionada o OU de desarrollo. La infraestructura aprovisionada en las cuentas de aplicación creadas en cada una de ellas OUs está sujeta al modo AMS específico que ofrecen esas cuentas fundamentales. OUs Es habitual encontrar una combinación de dos o más modos en la misma cuenta de aplicación. Por ejemplo: el modo RFC y el modo SSP pueden coexistir en una cuenta gestionada por AMS que aloje una arquitectura de canalización compuesta por API Gateway y Lambda para las funciones de activación EC2, y S3 y SQS para la ingesta y la organización. En este caso, el modo SSP se aplicaría a Lambda y API Gateway.

La figura 1 presenta cómo se ofrecen los diferentes modos a través de los fundamentos de AMS. OUs Al solicitar una nueva cuenta de aplicación en AMS, debe seleccionar la OU de la cuenta.

Arquitectura MALZ y modos AMS asociados

AMS aprovecha las bases OUs basadas en las mejores prácticas de AWS para gestionar las cuentas de forma lógica mediante políticas de control de servicios (). SCPs Esto sirve como una forma de reforzar el marco de gobierno en cada modo de AMS. Cualquier barrera de control y seguridad (en forma de SCPs) que se aplique a la base OUs también se aplica automáticamente. custom/child OUs Se SCPs puede solicitar un suplemento para el niño. OUs Es importante entender que las cuentas de las aplicaciones no son lo mismo que los modos. Los modos se aplican a la infraestructura aprovisionada en las cuentas y definen las responsabilidades operativas entre AMS y los clientes.

Figura 1: Arquitectura MALZ y modos AMS asociados

> **Note**
>
> El término «restrictivo» implica que puede solicitar políticas personalizadas para ellos OUs. AMS las aprueba para case-by-case garantizar que no interfieran en la capacidad de AMS de ofrecer excelencia operativa. Para obtener una lista detallada de las barandillas AMS, consulte las barandillas AMS en la guía del usuario.

Modos y aplicaciones o cargas de trabajo AMS

Tenga en cuenta los requisitos operativos y de gobierno de sus aplicaciones al seleccionar el modo correcto, ya sea solicitando una nueva cuenta de aplicación o alojando la aplicación en una cuenta de aplicación existente. La selección del modo AMS adecuado para cada aplicación o carga de trabajo depende de los siguientes factores:

- El tipo de función del ciclo de vida del SDLC que proporcionará el entorno (por ejemplo, entorno aislado con cambios no moderados, UAT con algunos cambios frecuentes, producción con cambios mínimos y altamente regulada)
- Las políticas de gobierno necesarias (aplicadas a SCPs nivel de unidad organizativa)
- Modelo operativo (si desea asumir la responsabilidad operativa o desea subcontratarla a AMS)
- Los resultados empresariales deseados, como el tiempo necesario para operar en la nube y el coste de las operaciones.

> **Note**
>
> Para obtener una descripción de los tipos de modos por servicio de AMS, consulte Tipos de modos y cuentas en AMS.
> Para ver casos de uso reales de los distintos modos, consulte Casos de uso reales de los modos AMS

En la siguiente tabla se describen las principales consideraciones para que los propietarios de aplicaciones puedan decidir cuál es el modo AMS más adecuado. Los propietarios de las aplicaciones deben incluir una fase de evaluación antes de la migración de la aplicación para comprender completamente qué modo se aplica a su aplicación específica. Ejemplo: en el caso de las aplicaciones basadas en servicios nativos de la nube o en una arquitectura sin servidor, la mejor opción podría ser empezar a crear e iterar en modo desarrollador e implementar la infraestructura como código final mediante el modo AMS Managed (SSP). En este caso, puede ser necesaria una ligera refactorización para garantizar que cualquier CloudFormation plantilla creada para el despliegue automatizado cumpla con las directrices de ingesta establecidas por AMS. Además, cualquier permiso de IAM debe ser aprobado por AMS Security para garantizar que siga el modelo de privilegios mínimos.

El modo AMS seleccionado para alojar la aplicación puede ayudarle a desarrollar el modelo operativo de nube que desee.

> **Note**
>
> Puede existir más de un modelo operativo en la nube en una única zona de aterrizaje gestionada por AMS en función de los distintos modos de AMS seleccionados para alojar las aplicaciones.

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Preparación operativa						

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Registro, supervisión y gestión de eventos	AMS es responsable de toda la infraestructura gestionada			El cliente es responsable de los servicios aprovisionados de autoservicio (SSP)	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	El cliente es responsable
Gestión de la continuidad	La responsabilidad de AMS de ejecutar el plan de respaldo seleccionado por el cliente			El cliente es responsable de los servicios aprovisionados de autoservicio (SSP)	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Administración de acceso a nivel de instancia	Administrado por AMS mediante una confianza unidireccional de AD con dominio local. Requiere una infraestructura gestionada para unirse al dominio AMS			No aplicable	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	
Gestión de la seguridad y gestión del acceso a nivel de cuenta	Responsabilidad de AMS con respecto a todas las cuentas gestionadas			AMS es responsable de todas las cuentas gestionadas	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Administración de parches	Responsabilidad de AMS con respecto a todas las cuentas gestionadas			El cliente es responsable de los servicios aprovisionados de autoservicio (SSP)	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	
Administración de cambios	Responsabilidad de AMS con respecto a todas las cuentas gestionadas			El cliente es responsable de los servicios aprovisionados de autoservicio (SSP)	El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema AMS CM	

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Gestión del aprovisionamiento	Prescriptivo y estandarizado para las opciones de aprovisionamiento que se ofrecen en AMS	Flexibilidad para utilizar directamente la API de servicios de AWS para AWS Service Catalog siguiendo los estándares prescriptivos de AMS	Flexibilidad para utilizar directamente la API de servicios de AWS siguiendo los estándares prescriptivos de AMS	Flexibilidad para utilizar directamente el servicio de AWS APIs para los servicios de SSP	Flexibilidad para utilizar directamente la API de servicios de AWS para el aprovisionamiento	

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Gestión y auditoría de incidentes	AMS es responsable de todas las cuentas gestionadas				El cliente es responsable de los recursos aprovisionados mediante la función de IAM de desarrollador ajena al sistema de gestión de cambios de AMS	
GuardRails y una infraestructura (red) y un marco de seguridad compartidos	Uso prescriptivo y estandarizado de las cuentas principales de AMS					Flexible y personalizado, aprovechando las cuentas principales de AMS
Preparación de las aplicaciones						

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Refactorización de aplicaciones	Es necesaria una refactorización de la luz				Es necesaria una refactorización ligera (si se aprovisiona con AMS Standard CM)	No es necesario refactorizar
Support para los servicios de AWS	Limitado a lo que admite AMS					No limitado
Consideraciones empresariales						
Es hora de estar listo para operar	De tres a seis meses			Más de 6 meses, dependiendo de las competencias operativas de las aplicaciones del cliente		De 6 a 18 meses, según las competencias del cliente en materia de infraestructura y operaciones de aplicaciones
Costos	$$$$			$$$	$$	$

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisionamiento de autoservicio	Modo de desarrollador	Gestionado por el cliente
Ejemplos de aplicaciones	Servidor web con pila de 3 niveles, aplicaciones con requisitos normativos y de conformidad			Servidor web que utiliza API Gateway, aplicación conteneri zada que aprovecha ECS/EKS	Iteración /optimización en la aplicación Data Lake que usa Lambda, Glue, Athena, etc.	Descentralizadas, accounts/ applications como en un entorno sandbox, aplicaciones gestionadas por terceros

* Operations On Demand (OOD) ofrece una oferta para los clientes que utilizan el modo CM estándar para gestionar sus cambios mediante una dotación de recursos específica. Para obtener más información, consulte el catálogo de ofertas de Operations on Demand y hable con su gerente de prestación de servicios en la nube (CSDM).

> **Note**
>
> La comparación de precios entre el modo SSP y el modo desarrollador supone que se aprovisionan los mismos servicios de AWS.

Comparación de los modos AMS con los objetivos empresariales y de TI

Como se muestra, si busca un modelo de gobierno estandarizado y altamente controlado para sus aplicaciones, los modos Standard Change, AWS Service Catalog o Direct Change gestionados por AMS son los más adecuados. Si necesita un modelo de gobierno personalizado que se centre en la innovación de las aplicaciones sin necesidad de contar con una preparación operativa, seleccione el modo gestionado por el cliente. Con el modo gestionado por el cliente, poner en funcionamiento sus aplicaciones podría tardar más tiempo, ya que es responsable de establecer

las personas, los procesos y las herramientas que respalden las capacidades operativas, como la gestión de incidentes, la gestión de la configuración, la gestión del aprovisionamiento, la gestión de la seguridad, la gestión de parches, etc.

Casos de uso reales para los modos AMS

Examínelos para ayudar a determinar cómo utilizar los modos AMS.

- Caso de uso 1: el imperativo empresarial de reducir los costes con una salida urgente del centro de datos: una empresa que se enfrenta a un acontecimiento empresarial convincente, como la salida de un centro de datos, está interesada en realojar sus aplicaciones locales en la nube. La mayor parte del inventario local consiste en servidores Windows y Linux con una combinación de versiones de sistemas operativos. De este modo, el cliente también quiere aprovechar los ahorros de costes que ofrece la migración a la nube y mejorar el aspecto técnico y de seguridad de sus aplicaciones. El cliente quiere avanzar con rapidez, pero aún no cuenta con la experiencia interna necesaria en operaciones en la nube. El cliente debe encontrar un equilibrio entre la refactorización, ya que una refactorización excesiva puede resultar arriesgada si se tiene en cuenta un plazo ajustado. Sin embargo, con algunas refactorizaciones, como la actualización de las versiones del sistema operativo y la optimización de las bases de datos, las aplicaciones pueden alcanzar el siguiente nivel de rendimiento. En este ejemplo, el cliente puede seleccionar el modo RFC administrado por AMS para volver a alojar la mayoría de sus aplicaciones. AMS proporciona operaciones de infraestructura y, al mismo tiempo, orienta a los equipos de operaciones del cliente sobre las mejores prácticas para operar de forma segura en la nube.

  El AWS Service Catalog administrado por AMS y el modo Direct Change administrado por AMS ofrecen al cliente una flexibilidad adicional y, al mismo tiempo, logran los mismos resultados y objetivos empresariales. Además, el cliente puede utilizar la oferta Operations On Demand (OOD) de AMS para contar con ingenieros de operaciones de AMS dedicados a priorizar la ejecución de las solicitudes de cambio (). RFCs

  Además de delegar las tareas operativas indiferenciadas de la infraestructura (aplicación de parches, copias de seguridad, administración de cuentas, etc.) a AMS, el cliente puede seguir centrándose en optimizar su aplicación y en ampliar sus equipos internos a las operaciones en la nube. AMS proporciona informes mensuales al cliente sobre el ahorro de costes y hace recomendaciones sobre la optimización de los recursos. En este caso de uso, si había end-of-life aplicaciones alojadas en versiones antiguas del sistema operativo, como Windows 2003 y 2008,

que el cliente decidió no volver a factorizar, también se pueden migrar a AMS y alojarse en una cuenta que utilice el modo administrado por el cliente.

- Caso de uso 2: creación de un lago de datos con Lambda, Glue y Athena dentro del límite seguro de AMS: una empresa busca configurar un lago de datos para satisfacer las necesidades de informes de múltiples aplicaciones en AMS. El cliente quiere usar depósitos de S3 para el almacenamiento de conjuntos de datos y AWS Athena para realizar consultas en el conjunto de datos de cada informe. S3 y AWS Athena se implementarán en cuentas administradas por AMS independientes. La cuenta de S3 también incluye otros servicios, como Glue, Lambda y Step Functions, para crear una canalización de ingesta de datos. En este caso, Glue, Lambda, Athena y Step Functions se consideran servicios de autoservicio (SSP). El cliente también implementó una EC2 instancia en la cuenta que actúa como servidor ad hoc. tooling/scripting El cliente comienza por solicitar a AMS que habilite los servicios SSP en su cuenta gestionada por AMS. AMS proporciona una función de IAM para cada servicio que el cliente puede asumir, una vez que la función se ha incorporado a la solución de federación del cliente. Para facilitar la administración, el cliente también puede combinar las políticas de las distintas funciones de IAM en una sola función personalizada, lo que reduce la necesidad de cambiar de función al trabajar entre los servicios de AWS. Una vez que la función esté habilitada en la cuenta, el cliente podrá configurar los servicios según sus necesidades. Sin embargo, el cliente debe trabajar con el sistema de gestión de cambios AMS para solicitar permisos adicionales, según su caso de uso.

  Por ejemplo, para acceder a Glue Crawlers, Glue necesita permisos adicionales. También se necesitarán permisos adicionales para crear fuentes de eventos para Lambda. El cliente trabajará con AMS para actualizar las funciones de IAM y permitir el acceso entre cuentas para que Athena consulte los buckets de S3. También será necesario actualizar las funciones de servicio o las funciones vinculadas a servicios mediante la administración de cambios de AMS para que Lambda llame al servicio Step Functions y Glue para leer y escribir en todos los buckets de S3. AMS trabaja con los clientes para garantizar que se siga el modelo de acceso con menos privilegios y que los cambios de IAM solicitados no sean excesivamente permisivos y expongan el entorno a riesgos innecesarios. El equipo del lago de datos del cliente dedica tiempo a planificar todos los permisos de IAM necesarios para los servicios específicos de la arquitectura del cliente y solicita a AMS que los habilite. Esto se debe a que todos los cambios de IAM se procesan manualmente y son revisados por el equipo de seguridad de AMS. El tiempo necesario para procesar estas solicitudes debe tenerse en cuenta en el cronograma de implementación de la aplicación.

  Como los servicios del SSP están operativos en la cuenta, el cliente puede solicitar asistencia e informar de problemas mediante la gestión de incidentes y las solicitudes de servicio de AMS. Sin embargo, AMS no supervisará activamente las métricas de rendimiento y simultaneidad de

Lambda ni las métricas de trabajo de Glue. Es responsabilidad del cliente asegurarse de que los servicios de SSP estén habilitados para el registro y la supervisión adecuados. AMS administra completamente la EC2 instancia y el bucket de S3 de la cuenta.

- Caso de uso 3: configuración rápida y flexible de una canalización de implementación de CICD en AMS: un cliente quiere configurar una canalización de CICD basada en Jenkins para implementar una canalización de código en todas las cuentas de aplicaciones de AMS. El cliente puede considerar más adecuado alojar esta canalización de CICD en el modo Direct Change (DCM) administrado por AMS o en el modo Desarrollador administrado por AMS, ya que le da la flexibilidad de configurar el servidor Jenkins con la configuración personalizada requerida EC2, con los permisos de acceso de IAM deseados CloudFormation y los depósitos S3 que alojan el repositorio de artefactos. Si bien esto también se puede hacer en el modo RFC administrado por AMS, el equipo del cliente tendría que crear varios manuales RFCs para que las funciones de IAM se basen en el conjunto de permisos aprobados menos permisivo, que AMS revisa manualmente. DCM permite a los clientes alcanzar sus objetivos operativos en AWS y, al mismo tiempo, evitar la necesidad de crear varios manuales RFCs para las funciones de IAM, cuando utilizan el modo RFC administrado por AMS, a fin de utilizar el conjunto menos permisivo de permisos aprobados, que AMS revisa manualmente. Impulsar los procesos y las herramientas de AMS requeriría tiempo y formación por parte del cliente. Al trabajar con el modo Desarrollador, el cliente puede empezar con un «rol de desarrollador» para aprovisionar la infraestructura mediante AWS nativo APIs. La forma más rápida y flexible de configurar esta canalización sería utilizar el modo AMS Managed-Developer. El modo desarrollador ofrece la forma más rápida y sencilla, al tiempo que compromete la integración operativa, mientras que el DCM es menos flexible, pero proporciona el mismo nivel de soporte operativo que el modo RFC.
- Caso de uso 4, un modelo operativo personalizado dentro de la base de AMS: un cliente está pensando en dejar su centro de datos dentro de unos plazos y una de sus aplicaciones empresariales está gestionada íntegramente por un MSP externo, lo que incluye las operaciones de aplicaciones y las operaciones de infraestructura. Suponiendo que el cliente no tenga tiempo previsto para rediseñar esta aplicación de forma que pueda ser gestionada por AMS, el modo Customer Managed es una opción adecuada. El cliente puede aprovechar la configuración rápida y automática de la zona de aterrizaje gestionada por AMS. Pueden aprovechar la administración centralizada de cuentas que controla la venta y la conectividad de las cuentas a través de la cuenta de red centralizada. También simplifica su facturación al consolidar los cargos de todas las cuentas administradas por los clientes a través de la cuenta AMS Payer. El cliente tiene la flexibilidad de configurar su modelo de gestión de acceso personalizado con el MSP, de forma independiente de la gestión de acceso estándar que se utiliza en las cuentas gestionadas por AMS. De esta forma, al utilizar el modo gestionado por el cliente, puede configurar un entorno

gestionado por AMS y, al mismo tiempo, cumplir con el requisito empresarial de dejar vacante su entorno local. En este caso, si el cliente también tiene aplicaciones basadas en Windows que va a migrar a la nube y decide pasarlas a una cuenta gestionada por el cliente, el cliente es responsable de crear un modelo operativo en la nube. Esto puede resultar complejo, costoso y llevar mucho tiempo, según la capacidad del cliente para transformar los procesos de TI tradicionales y capacitar a las personas. El cliente puede ahorrar tiempo y costes al «transferir» dichas cargas de trabajo a una cuenta gestionada por AMS y delegar las operaciones de infraestructura a AMS.

> **Note**
>
> A veces, los clientes pueden sentir la necesidad de cambiar las cuentas de las aplicaciones entre el marco de gobierno del modo RFC o SSP y el modo desarrollador. Por ejemplo, los clientes pueden alojar una aplicación en modo gestionado por AMS como parte de la migración inicial de tipo lift and shift, pero con el tiempo quieren volver a escribir la aplicación para optimizarla para los servicios de AWS nativos de la nube. Podrían cambiar el modo de la cuenta previa a la producción, de RFC gestionada por AMS a un modo de desarrollador gestionado por AMS, lo que les proporcionaría la flexibilidad y la agilidad necesarias para aprovisionar la infraestructura. Sin embargo, una vez que se hayan realizado los cambios en el aprovisionamiento de la infraestructura utilizando la «función de desarrollador», la misma infraestructura no podrá volver al modo RFC administrado por AMS. Esto se debe a que AMS no puede garantizar las operaciones de la infraestructura que se aprovisionó fuera del sistema de gestión de cambios de AMS. Es posible que los clientes tengan que crear una nueva cuenta de aplicación que ofrezca el modo RFC gestionado por AMS y, a continuación, volver a implementar la configuración de infraestructura «optimizada» mediante CloudFormation plantillas o incorporadas de forma personalizada AMIs en una cuenta gestionada por AMS. Esta es una forma sencilla de implementar una configuración lista para producción. Una vez implementada, la aplicación estará sujeta al gobierno y las operaciones prescriptivas de AMS. Lo mismo se aplica al cambio de modo entre el modo gestionado por el cliente y el gestionado por AMS.

Modo RFC

El modo RFC es el modo predeterminado para los clientes del plan de operaciones AMS Advanced. Incluye un sistema de gestión de cambios con solicitudes de cambio o RFCs un catálogo de tipos de cambios que puede utilizar para solicitar la adición o el cambio que necesite en sus cuentas.

Este sistema de administración de cambios proporciona un nivel de seguridad al limitar quién puede realizar cambios en sus cuentas.

Para obtener más información sobre los tipos de cambios de AMS Advanced, consulta ¿Qué son los tipos de cambios de AMS? .

Para obtener más información sobre la incorporación a AMS Advanced, consulte Introducción a la incorporación de AWS Managed Services.

Para ver ejemplos de tipos de cambio, consulte la sección «Información adicional» para ver el tipo de cambio correspondiente en la sección de AMS Advanced Change Type Reference Change Types Change Types by Classification.

> **Note**
>
> El modo RFC se denominaba anteriormente «modo de gestión de cambios» o «modo CM estándar».

Temas

- Más información sobre RFCs
- ¿Qué son los tipos de cambios?
- Solución de problemas de errores de RFC en AMS

Más información sobre RFCs

Las solicitudes de cambio, o bien RFCs, funcionan de forma doble. En primer lugar, hay parámetros necesarios para la propia RFC. Estas son las opciones de la `CreateRfc` API. Y, en segundo lugar, hay parámetros necesarios para la acción del RFC (los parámetros de ejecución). Para obtener más información sobre las `CreateRfc` opciones, consulte la CreateRfcsección de referencia de la API de AMS. Estas opciones suelen aparecer en el área de configuraciones adicionales de las páginas de creación de RFC.

Puede crear y enviar un RFC con la `CreateRfc` API, la `aws amscm create-rfc` CLI o mediante las páginas Crear RFC de la consola AMS. Para ver un tutorial sobre la creación de un RFC, consulte. Crear un RFC

Temas

- ¿Qué son RFCs?
- Autenticarse al utilizar la API/CLI de AMS
- Comprenda las revisiones de seguridad de RFC
- Comprenda las clasificaciones de tipos de cambio de RFC
- Comprenda los estados de acción y actividad del RFC
- Comprenda los códigos de estado RFC
- Comprenda la actualización de RFC CTs y la detección CloudFormation de desviaciones de plantillas
- Programar RFCs
- Aprobar o rechazar RFCs
- Solicita periodos de ejecución restringidos por RFC
- Crear, clonar, actualizar, buscar y cancelar RFCs
- Utilice la consola AMS con RFCs
- Más información sobre los parámetros de RFC comunes
- Suscríbase al correo electrónico diario del RFC

¿Qué son RFCs?

Una solicitud de cambio, o RFC, es la forma de realizar un cambio en el entorno gestionado por AMS o de pedirle a AMS que realice un cambio en su nombre. Para crear una RFC, debe elegir entre los tipos de cambio de AMS, elegir los parámetros de la RFC (como la programación) y, a continuación, enviar la solicitud mediante la consola AMS o los comandos de la API y. CreateRfcSubmitRfc

Una RFC contiene dos especificaciones, una para la propia RFC y otra para los parámetros del tipo de cambio (CT). En la línea de comandos, puede utilizar un comando RFC integrado o una CreateRfc plantilla estándar en formato JSON, que debe rellenar y enviar junto con el archivo de esquema CT JSON que cree (basado en los parámetros de CT). El nombre del CT es una descripción informal del CT. Un CSIO (categoría, subcategoría, elemento, operación) es una descripción más formal de una tomografía computarizada. Al crear una RFC, solo se debe especificar el ID de CT.

AMS le notifica cuando el cambio se ha realizado correctamente (éxito) o no (error).

> **Note**
>
> Para obtener información sobre la solución de problemas de errores de RFC, consulte. Solución de problemas de errores de RFC en AMS

El siguiente gráfico muestra el flujo de trabajo de una RFC enviada por usted.

Autenticarse al utilizar la API/CLI de AMS

Al utilizar la API/CLI de AMS, debe autenticarse con credenciales temporales.
Para solicitar credenciales de seguridad temporales para usuarios federados, cal GetFederationTokenAssumeRole, AssumeRoleWithSAML o AssumeRoleWithWebIdentityAWS security token service (STS). APIs

Una opción habitual es SAML. Tras la configuración, se añade un argumento a cada operación a la que se llame. Por ejemplo: `aws --profile saml amscm list-change-type-categories`.

Un método abreviado para los perfiles de SAML 2.0 consiste en establecer la variable de perfil al principio de cada uno API/CLI con `set AWS_DEFAULT_PROFILE=saml` (en Windows, sería en Linux`export AWS_DEFAULT_PROFILE=saml`). Para obtener información sobre la configuración de las variables de entorno CLI, consulte Configuración de la interfaz de línea de comandos de AWS, variables de entorno.

Comprenda las revisiones de seguridad de RFC

El proceso de aprobación de la administración de cambios de AWS Managed Services (AMS) garantiza que realicemos una revisión de seguridad de los cambios que realicemos en sus cuentas.

AMS evalúa todas las solicitudes de cambio (RFCs) en función de las normas técnicas de AMS. Cualquier cambio que pueda reducir el nivel de seguridad de tu cuenta al apartarse de los estándares técnicos pasa por una revisión de seguridad. Durante la revisión de seguridad, AMS destaca los riesgos relevantes y, en casos de riesgo de seguridad alto o muy alto, el personal de seguridad autorizado acepta o rechaza la RFC. Todos los cambios también se evalúan para determinar si tienen un impacto adverso en la capacidad operativa de AMS. Si se detectan posibles impactos adversos, se requieren revisiones y aprobaciones adicionales por parte de AMS.

Normas técnicas de la AMS

Los estándares técnicos de AMS definen los criterios de seguridad, las configuraciones y los procesos mínimos para establecer la seguridad básica de sus cuentas. Tanto usted como AMS deben seguir estos estándares.

Cualquier cambio que pueda reducir la seguridad de tu cuenta al no cumplir con las normas técnicas pasa por un proceso de aceptación del riesgo, en el que AMS resalta el riesgo relevante y el personal de seguridad autorizado por tu parte lo acepta o rechaza. Todos estos cambios también se evalúan para determinar si podrían repercutir negativamente en la capacidad de AMS para gestionar la cuenta y, de ser así, AMS deberá realizar revisiones y aprobaciones adicionales.

Proceso de gestión de riesgos para la seguridad del cliente (CSRM) de RFC

Cuando alguien de su organización solicita un cambio en su entorno gestionado, AMS revisa el cambio para determinar si la solicitud podría deteriorar la seguridad de su cuenta al incumplir los estándares técnicos. Si la solicitud reduce la postura de seguridad de la cuenta, AMS notifica a su contacto del equipo de seguridad el riesgo correspondiente y ejecuta el cambio; o, si el cambio introduce un riesgo de seguridad alto o muy alto en el entorno, AMS solicita la aprobación explícita del contacto de su equipo de seguridad en forma de aceptación del riesgo (se explica a continuación). El proceso de aceptación de riesgos por parte de los clientes de AMS está diseñado para:

- Asegúrese de que los riesgos estén claramente identificados y comunicados a los propietarios correctos
- Minimice los riesgos identificados para su entorno
- Obtenga y documente la aprobación de los contactos de seguridad designados que entiendan el perfil de riesgo de su organización
- Reduzca la sobrecarga operativa continua en relación con los riesgos identificados

¿Cómo acceder a los estándares técnicos y a los riesgos altos o muy altos

Hemos puesto a su disposición la documentación sobre las normas técnicas de AMS para su consulta en https://console.aws.amazon.com/artifact/forma de informe. Utilice la documentación de normas técnicas de AMS para saber si un cambio requeriría la aceptación por parte de su contacto de seguridad autorizado por parte de su contacto de seguridad autorizado antes de enviar una solicitud de cambio (RFC).

Para encontrar el informe de normas técnicas, busque «Normas técnicas de AWS Managed Services (AMS)» en la barra de búsqueda de la pestaña AWS Artifact Informes tras iniciar sesión con la configuración predeterminada AWSManagedServicesChangeManagementRole.

> **Note**
>
> El Cliente_ ReadOnly _Role in single account landing zone puede acceder al documento estándar técnico de AMS. En la zona de aterrizaje multicuenta, se puede AWSManaged ServicesAdminRole utilizar la que AWSManaged ServicesChangeManagementRole utilizan los administradores de seguridad y los equipos de aplicaciones para acceder al documento. Si tu equipo usa un rol personalizado, crea una RFC Otros | Otros para solicitar el acceso y actualizaremos el rol personalizado especificado.

Comprenda las clasificaciones de tipos de cambio de RFC

Los tipos de cambios que se utilizan al enviar una RFC se dividen en dos categorías amplias:

- Implementación: esta clasificación sirve para crear recursos.
- Administración: esta clasificación sirve para actualizar o eliminar recursos. La categoría Administración también contiene los tipos de cambios para acceder a las instancias, cifrarlas o compartirlas AMIs, e iniciar, detener, reiniciar o eliminar pilas.

Comprenda los estados de acción y actividad del RFC

`RfcActionState`(API) o Activity State (consola) le ayudan a comprender el estado de la intervención o acción humana en una RFC. Se utiliza principalmente de forma manual RFCs, y le `RfcActionState` ayuda a entender si es necesario que usted o las operaciones de AMS tomen alguna medida, y le ayuda a ver si AMS Operations está trabajando activamente en su RFC. Esto proporciona una mayor transparencia sobre las medidas que se toman en relación con una RFC durante su ciclo de vida.

`RfcActionState`Definiciones (API) o estado de actividad (consola):

- AwsOperatorAssigned: Un operador de AWS está trabajando activamente en su RFC.
- AwsActionPending: Se espera una respuesta o acción de AWS.
- CustomerActionPending: Se espera una respuesta o acción del cliente.

- NoActionPending: No es necesario que AWS ni el cliente realicen ninguna acción.
- NotApplicable: Los operadores o los clientes de AWS no pueden establecer este estado y solo se usa RFCs cuando se creó antes del lanzamiento de esta funcionalidad.

Los estados de acción de la RFC varían en función de si el tipo de cambio presentado requiere una revisión manual y si la programación se ha establecido lo antes posible o no.

- La RFC ActionStatecambia durante la revisión, la aprobación y el inicio de un tipo de cambio manual con programación diferida:
  - Después de enviar una RFC manual, programada, la RFC cambia ActionStateautomáticamente AwsActionPendinga para indicar que un operador debe revisar y aprobar la RFC.
  - Cuando un operador comienza a revisar activamente su RFC, cambia a. ActionStateAwsOperatorAssigned
  - Cuando el operador aprueba su RFC, el estado de la RFC cambia a Programado y, automáticamente, a. ActionStateNoActionPending
  - Cuando se alcanza la hora de inicio programada de la RFC, el estado de la RFC cambia a InProgress, y ActionStateautomáticamente cambia AwsActionPendinga, para indicar que es necesario asignar un operador para que revise la RFC.
  - Cuando un operador comienza a ejecutar activamente la RFC, la cambia a. ActionStateAwsOperatorAssigned
  - Una vez completada, el operador cierra la RFC. Esto cambia automáticamente el ActionStatea. NoActionPending

⚠ Important

- Usted no puede establecer los estados de acción. Los configuran automáticamente en función de los cambios en la RFC o los configuran manualmente los operadores de AMS.
- Si añade correspondencia a un RFC, ActionStatese establece automáticamente en. AwsActionPending
- Cuando se crea un RFC, ActionStatese establece automáticamente en. NoActionPending
- Cuando se envía un RFC, ActionStatese establece automáticamente en. AwsActionPending

- Cuando una RFC es rechazada, cancelada o completada con un estado de éxito o error, ActionStatese restablece automáticamente a. NoActionPending
- Los estados de acción están habilitados tanto para los automáticos como para los manuales RFCs, pero son más importantes para los manuales, RFCs ya que estos tipos de estados RFCs suelen requerir comunicaciones.

Revise los ejemplos de casos de uso de los estados de acción de la RFC

Caso de uso: visibilidad en el proceso manual de RFC

- Una vez que envíes una RFC manual, el estado de acción de la RFC cambia automáticamente `AwsActionPending` para indicar que un operador debe revisar y aprobar la RFC. Cuando un operador comienza a revisar activamente tu RFC, el estado de acción de la RFC cambia a. `AwsOperatorAssigned`
- Considere una RFC manual que haya sido aprobada y programada y que esté lista para empezar a ejecutarse. Una vez que el estado de la RFC cambia a`InProgress`, el estado de acción de la RFC cambia automáticamente a. `AwsActionPending` Cambia de nuevo a `AwsOperatorAssigned` una vez que un operador comienza a ejecutar activamente la RFC.
- Cuando se completa una RFC manual (cerrada como «correcta» o «fallida»), el estado de la acción de la RFC cambia `NoActionPending` para indicar que no es necesario que el cliente ni el operador realicen ninguna otra acción.

Caso de uso: correspondencia de RFC

- Cuando se trata de una RFC manual`Pending Approval`, es posible que un operador de AMS necesite más información por su parte. Los operadores enviarán una correspondencia a la RFC y cambiarán el estado de acción de la RFC a. `CustomerActionPending` Cuando respondes añadiendo una nueva correspondencia de RFC, el estado de acción de la RFC cambia automáticamente a. `AwsActionPending`
- Cuando se produce un error en una RFC automática o manual, puede añadir una correspondencia a los detalles de la RFC y preguntar al operador del AMS por qué ha fallado la RFC. Cuando añada su correspondencia, el estado de acción de la RFC se establece automáticamente en. `AwsActionPending` Cuando el operador del AMS coja la RFC para ver su correspondencia, el estado de acción de la RFC cambiará a. `AwsOperatorAssigned` Cuando el operador responde añadiendo una nueva correspondencia de RFC, el estado de acción de la RFC puede configurarse

en`CustomerActionPending`, lo que indica que se espera otra respuesta del cliente, o en, que indica que no se necesita ni se espera ninguna respuesta del cliente. `NoActionPending`

Comprenda los códigos de estado RFC

Los códigos de estado RFC le ayudan a realizar un seguimiento de sus solicitudes. Puede observar estos códigos de estado durante la ejecución de una RFC en la salida de la CLI o actualizando la página de lista de RFC en la consola.

También puedes ver los códigos de una RFC en la página de detalles de esa RFC, que podría tener este aspecto:

Es posible que veas un RFC en tu lista que no hayas enviado. Cuando los operadores de AMS utilizan un CT solo interno, lo envían en una RFC y aparece en la lista de RFC. Para obtener más información, consulte Tipos de cambios solo internos.

> **Important**
>
> Puede solicitar notificaciones de los cambios de estado de la RFC. Para obtener más información, consulte Notificaciones de cambio de estado del RFC.

Códigos de estado RFC

Success	Failure
Edición: el RFC se creó pero no se envió PendingApproval /Enviado: El RFC se ha enviado y el sistema está determinando si requiere aprobación y obteniendo esa aprobación, si es necesaria Aprobado por AWS o aprobado por el cliente: el RFC ha sido aprobado. RFCs Los automatizados están aprobados por AWS, RFCs los manuales los aprueban los operadores y, a veces, los clientes	Rechazados: RFCs se rechazan normalmente porque no se validan; por ejemplo, se especific a un recurso inutilizable, es decir, una subred Cancelados: RFCs se cancelan normalmente porque no pasan la validación antes de que haya transcurrido la hora de inicio configurada Fallo: el RFC ha fallado; consulte el StatusRea son resultado para ver los motivos del error y AMS Operations generará automáticamente

Success	Failure
Programado: el RFC ha superado las comprobaciones de sintaxis y requisitos y su ejecución está programada InProgress: el RFC se está ejecutando, tenga en cuenta RFCs que si aprovisiona varios recursos o tiene una ejecución prolongada UserData, tarda más en ejecutarse Ejecutado: se ha ejecutado el RFC Éxito o éxito: el RFC se completó correctam ente	una alerta de avería y se comunicará con usted según sea necesario

> **Note**
>
> Las solicitudes canceladas o rechazadas se RFCs pueden volver a enviar utilizando UpdateRfc; consulte también. Actualización RFCs

Si la RFC cumple todas las condiciones necesarias (por ejemplo, se especifican todos los parámetros necesarios), el estado cambia a `PendingApproval` (incluso las automatizadas CTs requieren aprobación, lo que ocurre automáticamente si se aprueban las comprobaciones de sintaxis y parámetros). Si no se aprueba, el estado cambia a`Rejected`. `StatusReason`Proporciona información sobre los rechazos; los `ExecutionOutput` campos proporcionan información sobre la aprobación y la finalización. Los códigos de error incluyen:

- InvalidRfcStateException: El RFC está en un estado que no permite la operación a la que se ha llamado. Por ejemplo, si el RFC ha pasado al estado Enviado, ya no se puede modificar.
- InvalidRfcScheduleException: Se han infringido TimeoutInMinutes los parámetros EndTime, o. StartTime
- InternalServerError: Se encontró un problema con el sistema.
- InvalidArgumentException: un parámetro se ha especificado de forma incorrecta; por ejemplo, se ha utilizado un valor inaceptable.
- ResourceNotFoundException: no se encuentra un valor, como el ID de la pila.

Si las horas de inicio y finalización programadas solicitadas (también conocidas como ventana de ejecución del cambio) se producen antes de que se apruebe el cambio, el estado de la RFC cambia a`Canceled`. Si se aprueba el cambio, el estado de la RFC cambia a. `Scheduled` La ventana de ejecución de cambios para ASAP RFCs es la hora de envío más el `ExpectedExecutionDuration` valor del CT.

En cualquier momento antes de la llegada de la ventana de ejecución de cambios, se puede modificar o cancelar un cambio programado (enviado con un `RequestedStartTime` en la CLI). Si se modifica el cambio programado, se debe volver a enviar.

Cuando llegue la hora de inicio del cambio (programada o lo antes posible) y una vez finalizadas las aprobaciones, el estado cambiará `InProgress` y no se podrá realizar ninguna modificación. Si el cambio se completa dentro del período de ejecución de cambios especificado, el estado cambia a. `Success` Si se produce un error en alguna parte del cambio o si el cambio sigue en curso al finalizar la ventana de ejecución de cambios, el estado cambia a`Failure`.

> **Note**
>
> Durante los estados o `Failure` cambios `InProgressSuccess`, la RFC no se puede modificar ni cancelar.

El siguiente diagrama ilustra los estados de la RFC desde la llamada a CreateRFC hasta la resolución.

Comprenda la actualización de RFC CTs y la detección CloudFormation de desviaciones de plantillas

Los recursos aprovisionados en AMS utilizan una plantilla modificada CloudFormation . Si un parámetro de un recurso ha cambiado directamente a través de la consola de AWS administración de un servicio, el registro de CloudFormation creación de ese recurso deja de estar sincronizado. Si esto ocurre e intenta utilizar un tipo de cambio de actualización de AMS para actualizar el recurso en AMS, AMS hará referencia a la configuración de recursos original y, posiblemente, restablecerá los parámetros modificados. Este restablecimiento puede ser perjudicial, por lo que AMS no permite realizar cambios en RFCs los tipos de actualización si se detecta algún cambio adicional en la configuración de AMS.

Para obtener una lista de los tipos de cambios de actualización, usa el filtro de consola.

Corrección de desviaciones FAQs

Preguntas y respuestas sobre la remediación de las derivas del AMS. Hay dos tipos de cambios que puede utilizar para iniciar la corrección de errores: uno es el modo de ejecución manual o «se requiere revisión» y el otro es el modo de ejecución = automatizado.

Recursos compatibles con la corrección de desviaciones (ct-3kinq0u4l33zf)

Estos son los recursos que admite el tipo de cambio de remediación de desviaciones (ct-3kinq0u4l33zf). Para corregir cualquier recurso, utilice en su lugar el tipo de cambio «es necesario revisar» (ct-34sxfo53yuzah).

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

Tipos de cambios de remediación de la deriva

Preguntas y respuestas sobre el uso de los tipos de cambios de corrección de desviaciones del AMS.

Para obtener una lista de los recursos compatibles con la función de corrección de desviaciones, consulte. Recursos compatibles con la corrección de desviaciones (ct-3kinq0u4l33zf)

> **Important**
>
> La corrección de errores modifica and/or los parámetros de las plantillas de pila y es obligatorio actualizar los repositorios de plantillas locales o cualquier automatización que actualice estas pilas para utilizar la plantilla y los parámetros de pila más recientes. El uso de and/or parámetros de plantillas antiguas sin sincronizarlos puede provocar cambios perjudiciales en los recursos subyacentes.
> El CT (ct-3kinq0u4l33zf), automatizado y que no requiere revisión, solo permite corregir 10 recursos por RFC. Para corregir los recursos restantes en lotes de 10, cree nuevos hasta que se hayan corregido todos los recursos. RFCs

¿Qué tipo de cambio de remediación de desviaciones debo utilizar?

Recomendamos utilizar la tomografía computarizada automática (ct-3kinq0u4l33zf) que no requiere revisión cuando:

- Al intentar realizar una actualización de un recurso de pila existente mediante un CT automatizado, la RFC se rechaza tal como está la pila. `DRIFTED`
- Utilizaste un CT de actualización en el pasado y falló porque la pila estaba a la deriva. No es necesario que intentes realizar una actualización de nuevo y, en su lugar, puedes utilizar la revisión manual o CT requerida.

Recomendamos utilizar la revisión manual obligatoria (ct-34sxfo53yuzah) solo cuando los tipos de recursos desviados no sean compatibles con la corrección de la desviación (no sea necesaria una revisión), automática, CT (ct-3kinq0u4l33zf) o cuando la corrección de la deriva no requiera revisión, automática o CT falle.

¿Qué cambios se realizan en la pila durante la remediación?

La corrección requiere actualizar los and/or parámetros de la plantilla de la pila en función de las propiedades que estén desviadas. La corrección también actualiza la política de pila de la pila durante la corrección y restaura la política de pila a su valor anterior una vez finalizada la corrección.

¿Cómo podemos ver los cambios realizados en los parámetros de la plantilla de pila? and/or

En la respuesta a la RFC, se proporciona un resumen de los cambios con la siguiente información:

- `ChangeSummaryJson`: Contiene un resumen de los cambios de los and/or parámetros de la plantilla de pila como parte de la corrección de errores. La remediación se lleva a cabo en varias fases. Este resumen de cambios consiste en los cambios de las fases individuales. Si la remediación se ha realizado correctamente, compruebe los cambios de la última fase. Consulte ExecutionPlan en el JSON las fases ejecutadas en orden. Por ejemplo, RestoreReferences la sección cuando está presente siempre se ejecuta al final y contiene JSON para los cambios posteriores a la corrección. Si la corrección se ejecuta en DryRun modo, ninguno de estos cambios se habría aplicado a la pila.
- `PreRemediationStackTemplateAndConfigurationJson`: Contiene una instantánea de la configuración de la CloudFormation pila, que incluye la plantilla, los parámetros y los resultados, StackPolicyBody antes de que se activara la corrección en la pila.

¿Qué debo hacer una vez que se haya realizado la corrección?

> **Important**
>
> Debe actualizar sus repositorios de plantillas locales, o cualquier automatización, que implique actualizar la pila corregida, con la plantilla y los parámetros más recientes que se proporcionan en el resumen de la RFC. Es muy importante hacerlo porque el uso de los and/or parámetros de la plantilla anterior puede provocar nuevos cambios destructivos en los recursos de la pila.

¿Mi solicitud se verá afectada durante esta corrección?

La corrección es un proceso fuera de línea que se realiza únicamente en la CloudFormation configuración de pila. No se realiza ninguna actualización en el recurso subyacente.

¿Puedo seguir utilizando Management | Other | Other RFCs para realizar actualizaciones en los recursos tras la corrección?

Le recomendamos que siempre actualice los recursos de la pila mediante la actualización CTs automática disponible. Si la actualización disponible CTs no es compatible con su caso de uso, utilice Gestión | Otras | Otras solicitudes.

¿La remediación crea nuevos recursos en la pila?

La remediación no crea ningún recurso nuevo en la pila. Sin embargo, la corrección crea nuevos resultados y actualiza la sección de metadatos de la plantilla de pila para almacenar el resumen de la corrección como referencia.

¿La remediación siempre tendrá éxito?

La remediación requiere un análisis y una validación cuidadosos de la configuración de la plantilla para determinar si se puede llevar a cabo. En los casos en los que estas validaciones fallan, el proceso de corrección se detiene y no se realiza ningún cambio en la plantilla ni en los parámetros de la pila. Además, la corrección solo se puede realizar en los tipos de recursos compatibles.

¿Cómo puedo realizar actualizaciones para apilar los recursos si la remediación no se realiza correctamente?

Puede utilizar el CT Management | Other | Other | Update (ct-0xdawir96cy7k) para solicitar cambios. AMS monitorea estos escenarios y trabaja para mejorar la solución de remediación.

¿Puedo corregir las pilas que tienen tipos de recursos compatibles y no compatibles?

Sí. Sin embargo, la corrección solo se lleva a cabo si los tipos de recursos admitidos se encuentran dispersos en la pila. Si se desvía algún tipo de recurso no compatible, la remediación no continúa.

¿Puedo solicitar la reparación de las pilas creadas mediante una ingesta que no sea de CFN? CTs

Sí. La corrección se puede realizar en las pilas independientemente del tipo de cambio utilizado para crear la pila.

¿Puedo saber los cambios que se realizarían en la pila antes de la corrección?

Sí. Ambos tipos de cambios ofrecen una DryRunopción que puede utilizar para solicitar los cambios que se realizarían si se corrigiera la pila. Sin embargo, los cambios de corrección finales pueden variar en función de la desviación presente en la pila en el momento de la corrección.

Programar RFCs

La función de programación le permite elegir una hora de inicio para RFCs. Las siguientes opciones están disponibles en la función de programación:

- Ejecute este cambio lo antes posible: AMS ejecuta la RFC en cuanto se aprueba. La mayoría CTs se aprueban automáticamente. Use esta opción si no desea que la RFC comience a una hora específica.
- Programa este cambio: establece un día, una hora y una zona horaria para que se ejecute la RFC. En el caso de los tipos de cambios automatizados, se recomienda solicitar una hora de inicio

al menos 10 minutos después de la fecha prevista para enviar la RFC. Para revisar los tipos de cambios obligatorios, es obligatorio que solicites una hora de inicio que sea, como mínimo, 24 horas después de la fecha en que planeas enviar la RFC. Si la RFC no se aprueba a la hora de inicio configurada, se rechaza la RFC.

Establezca un cronograma de RFC

Para programar una RFC, utilice uno de los métodos siguientes:

Ejecute este cambio lo antes posible:

- Consola: no haga nada. Utiliza la programación de RFC predeterminada.
- API o CLI: elimine las `RequestedEndTime` opciones `RequestedStartTime` y de la operación Crear RFC.

Las «revisiones obligatorias» de ASAP se RFCs rechazan automáticamente si no se aprueban dentro de los treinta días posteriores a su presentación.

Programa este cambio:

- Consola: selecciona el botón de opción Programar este cambio. Se abre un área de hora de inicio. Escribe un día manualmente o usa el widget de calendario para elegir un día. Introduzca una hora, en UTC, expresada en formato ISO 8601 y utilice la lista desplegable para elegir una ubicación. De forma predeterminada, AMS utiliza el formato ISO 8601 YYYYMMDDThhmmss Z YYYY-MM-DDThh o:MM:SSZ, se acepta cualquiera de los dos formatos.

  > **Note**
  >
  > La hora de finalización predeterminada es de 4 horas a partir de la hora de inicio que introduzca. Para establecer la hora de finalización del cambio programado en más de 4 horas, utilice la API o la CLI para ejecutar el cambio.

- API o CLI: envíe valores para los `RequestedEndTime` parámetros `RequestedStartTime` y de la operación Crear RFC. Pasar una configuración `RequestedEndTime` no detiene la ejecución de un tipo de cambio automatizado que ya se ha iniciado. En el caso de un tipo de cambio que «requiere revisión», si `RequestedEndTime` se realiza mientras la investigación de operaciones de AMS aún está en curso y estás en contacto con AMS, puedes solicitar una prórroga o se te puede pedir que vuelvas a enviar la RFC.

> **Tip**
>
> Para ver un ejemplo de lectura de la hora UTC, consulta UTC en el sitio web de Time-IS. Ejemplo de formato ISO 8601 para un date/time valor del 5 de diciembre de 2016 a las 14:20 horas: 2016-12-05T 14:20:00 Z o 20161205T142000Z.

Si proporciona...

- solo a`RequestedStartTime`, la RFC se considera programada y `RequestedEndTime` se rellena con el `ExecutionDurationInMinutes` valor.
- solo a`RequestedEndTime`, lanzamos un InvalidArgumentException.
- ambos `RequestedStartTime` y`RequestedEndTime`, sobrescribimos el `RequestedEndTime` con la hora de inicio especificada más el `ExecutionDurationInMinutes` valor.
- `RequestedStartTime`ni tampoco`RequestedEndTime`, mantenemos esos valores como nulos y el RFC se trata como un RFC ASAP.

> **Note**
>
> Para todo lo programado RFCs, se escribe una hora de finalización no especificada como la hora especificada `RequestedStartTime` más el `ExpectedExecutionDurationInMinutes` atributo del tipo de cambio enviado. Por ejemplo, si `ExpectedExecutionDurationInMinutes` es «60» (minutos) y la especificada `RequestedStartTime` es `2016-12-05T14:20:00Z` (5 de diciembre de 2016 a las 4:20 a.m.), la hora de finalización real se establecerá en el 5 de diciembre de 2016 a las 5:20 a.m. Para `ExpectedExecutionDurationInMinutes` buscar el tipo de cambio específico, ejecute este comando:
>
> ```
> aws amscm --profile saml get-change-type-version --
> change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
> {ExpectedDuration:ExpectedExecutionDurationInMinutes}"
> ```

Utilice la opción de prioridad RFC

Utilice la opción Prioridad en los tipos de `execution mode = manual` cambio para alertar a AMS Operations de la urgencia de la solicitud.

Opción de prioridad en`execution mode = manual`:

Especifique la prioridad de un RFC manual como Alta, Media o Baja. RFCs Los clasificados como altos se revisan y aprueban antes de RFCs clasificarse como medios, con sujeción a los objetivos de nivel de servicio (SLOs) de la RFC y a sus tiempos de presentación. RFCs con prioridad baja o sin prioridad especificada, se procesan en el orden en que se envían.

Aprobar o rechazar RFCs

RFCs presentadas con aprobación obligatoria (manual) CTs deben ser aprobadas por usted o por AMS. Las preaprobadas se procesan automáticamente CTs . Para obtener más información, consulte Requisitos de aprobación CT.

> **Note**
>
> Cuando utilice la opción «revisión obligatoria» CTs, AMS recomienda que utilice la opción de programación lo antes posible (elija ASAP en la consola y deje en blanco la hora de inicio y finalización en la API/CLI), ya que CTs requiere que un operador de AMS examine la RFC y, posiblemente, se comunique con usted antes de que pueda aprobarse y ejecutarse. Si las programa RFCs, asegúrese de esperar al menos 24 horas. Si la aprobación no se produce antes de la hora de inicio programada, la RFC se rechaza automáticamente.

Si AMS ha enviado correctamente un RFC que requiere aprobación, usted debe aprobarlo de forma explícita. O bien, si envía un RFC que requiere aprobación, AMS debe aprobarlo. Si tienes que aprobar un RFC enviado por AMS, se te enviará un correo electrónico u otra comunicación predeterminada solicitando la aprobación. La comunicación incluye el identificador de RFC. Una vez enviada la comunicación, realice una de las siguientes acciones:

- Aprobación o rechazo de la consola: utilice la página de detalles del RFC para ver el RFC correspondiente:

- Aprobación de API/CLI: ApproveRfcmarca un cambio como aprobado. La acción debe ser realizada tanto por el propietario como por el operador, si ambas son necesarias. A continuación,

se muestra un ejemplo de comando CLI approved. En el siguiente ejemplo, sustituya el RFC_ID por el ID de RFC adecuado.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- Rechazo de API/CLI: RejectRfcmarca un cambio como rechazado. El siguiente es un ejemplo de comando de rechazo de CLI. En el siguiente ejemplo, sustituya el RFC_ID por el ID de RFC adecuado.

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

Solicita periodos de ejecución restringidos por RFC

Conocidos anteriormente como días restringidos, puedes solicitar que se restrinjan determinados períodos de tiempo. No se pueden realizar cambios durante esos períodos.

Para establecer un período de ejecución restringido, usa la operación de la UpdateRestrictedExecutionTimesAPI y establece un período de tiempo específico, en UTC. El período que especifiques anula cualquier período anterior que se haya especificado. Si envía un RFC durante el tiempo de ejecución restringido especificado, el envío no se realizará correctamente y aparecerá el error Programa de RFC no válido. Puede especificar hasta 200 períodos de tiempo restringidos. De forma predeterminada, no se establece ningún período restringido. El siguiente es un ejemplo de comando de solicitud (con la autenticación SAML configurada):

```
aws amscm  --profile saml update-restricted-execution-times --restricted-execution-
times="[{\"TimeRange\":{\"StartTime\":\"2018-01-01T12:00:00Z\",\"EndTime\":
\"2018-01-01T12:00:01Z\"}}]"
```

También puedes ver tu RestrictedExecutionTimes configuración actual ejecutando la operación de ListRestrictedExecutionTimesAPI. Ejemplo:

```
aws amscm  --profile saml list-restricted-execution-times
```

Si quieres enviar una RFC durante un tiempo de ejecución restringido específico, añade la RestrictedExecutionTimesOverrideIdcon el valor de OverrideRestrictedTimeRangesy envía la RFC como lo harías normalmente. Se recomienda utilizar este método únicamente para una RFC crítica o de emergencia. Para obtener más información, consulta la referencia de la API de SubmitRfc.

Crear, clonar, actualizar, buscar y cancelar RFCs

En los ejemplos siguientes se explican varias operaciones de RFC.

Temas

- Crear un RFC
- Clona RFCs (recrea) con la consola AMS
- Actualización RFCs
- Encuentra RFCs
- Cancelar RFCs

Crear un RFC

Crear un RFC con la consola

La siguiente es la primera página del proceso de creación de un RFC en la consola AMS, con las tarjetas rápidas abiertas y la opción Buscar tipos de cambios activa:

La siguiente es la primera página del proceso de creación de RFC en la consola AMS, con la opción Seleccionar por categoría activa:

Cómo funciona:

1. Vaya a la página Crear RFC: en el panel de navegación izquierdo de la consola AMS, haga clic RFCspara abrir la página de RFCs listas y, a continuación, haga clic en Crear RFC.
2. Elija un tipo de cambio (CT) popular en la vista predeterminada de búsqueda de tipos de cambios o seleccione un CT en la vista Elegir por categoría.
   - Busque por tipo de cambio: puede hacer clic en un CT popular del área de creación rápida para abrir inmediatamente la página Ejecutar RFC. Tenga en cuenta que no puede elegir una versión antigua de CT con Quick Create.

     Para ordenar CTs, utilice el área Todos los tipos de cambios en la vista de tarjeta o de tabla. En cualquiera de las vistas, seleccione una CT y, a continuación, haga clic en Crear RFC para abrir la página Ejecutar RFC. Si corresponde, aparece la opción Crear con una versión anterior junto al botón Crear RFC.

- Elegir por categoría: seleccione una categoría, una subcategoría, un elemento y una operación, y se abrirá el cuadro de detalles del CT con la opción Crear con una versión anterior, si corresponde. Haga clic en Crear RFC para abrir la página Ejecutar RFC.

3. En la página Ejecutar RFC, abra el área del nombre del CT para ver el cuadro de detalles del CT. Se requiere un asunto (lo rellena automáticamente si elige su CT en la vista Buscar tipos de cambios). Abra el área de configuración adicional para añadir información sobre la RFC.

   En el área de configuración de ejecución, utilice las listas desplegables disponibles o introduzca valores para los parámetros necesarios. Para configurar los parámetros de ejecución opcionales, abra el área de configuración adicional.
4. Cuando haya terminado, haga clic en Ejecutar. Si no hay errores, aparecerá la página de la RFC creada correctamente con los detalles de la RFC enviada y el resultado inicial de la ejecución.
5. Abra el área de parámetros de ejecución para ver las configuraciones que envió. Actualice la página para actualizar el estado de ejecución de la RFC. Si lo desea, cancele la RFC o cree una copia de la misma con las opciones de la parte superior de la página.

Creación de un RFC con la CLI

Cómo funciona:

1. Utilice la función de creación en línea (se emite un `create-rfc` comando con todos los parámetros de ejecución y RFC incluidos) o la de plantilla (se crean dos archivos JSON, uno para los parámetros de RFC y otro para los parámetros de ejecución) y ejecute el `create-rfc` comando con los dos archivos como entrada. Ambos métodos se describen aquí.
2. Envíe el `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con el ID de RFC devuelto.

   Supervise el comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando

cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a la parte de los parámetros de la RFC de la solicitud (no a los parámetros de ejecución). Para ver una lista de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

CREACIÓN EN LÍNEA:

Ejecute el comando create RFC con los parámetros de ejecución incluidos en línea (comillas de escape al proporcionar los parámetros de ejecución en línea) y, a continuación, envíe el ID de RFC devuelto. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

CREACIÓN DE PLANTILLA:

> **Note**
>
> En este ejemplo de creación de una RFC, se utiliza el tipo de cambio de pila Load Balancer (ELB).

1. Busca el CT correspondiente. El siguiente comando busca en los resúmenes de las clasificaciones de CT aquellas que contengan «ELB» en el nombre del elemento y crea un resultado con la categoría, el artículo, la operación y el ChangeType identificador en forma de tabla (la subcategoría para ambos es). `Advanced stack components`

   ```
   aws amscm list-change-type-classification-summaries --query
    "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
   [Category,Item,Operation,ChangeTypeId]" --output table
   ```

   ```
   ----------------------------------------------------------------------
   |                            CtSummaries                             |
   +-----------+--------------------------+--------------------------+
   | Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
   | Management| Load balancer (ELB) stack | Update | ct-0ltm873rsebx9 |
   ```

```
+-----------+---------------------------+--------------------------+
```

2. Busque la versión más reciente del CT:

   `ChangeTypeIdyChangeTypeVersion`: El identificador de tipo de cambio para este tutorial es `ct-123h45t6uz7jl` (crear ELB). Para encontrar la última versión, ejecute este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. Conozca las opciones y los requisitos. El siguiente comando envía el esquema a un archivo JSON denominado CreateElbParams .json.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. Modifique y guarde los parámetros de ejecución en el archivo JSON. En este ejemplo, el archivo se denomina CreateElbParams .json.

   En el caso de un CT de aprovisionamiento, StackTemplateId se incluye en el esquema y se debe enviar en los parámetros de ejecución.

   TimeoutInMinutesEn cuanto al número de minutos necesarios para crear la pila antes de que se produzca un error en la RFC, esta configuración no retrasará la ejecución de la RFC, pero debes disponer de tiempo suficiente (por ejemplo, no especifiques «5"). Los valores válidos van desde «60» hasta «360», para CTs los de larga duración UserData: Create and Create EC2 ASG. Recomendamos el máximo permitido de «60" para todos los demás aprovisionamientos. CTs

   Proporcione el ID de la VPC en la que desea que se cree la pila; puede obtener el ID de la VPC con el comando CLI. `aws amsskms list-vpc-summaries`

```
{
"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv00000000000",
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters":   {
    "ELBSubnetIds":                     ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold":   4,
```

```
    "ELBHealthCheckInterval":           5,
    "ELBHealthCheckTarget":             "HTTP:80/",
    "ELBHealthCheckTimeout":            60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":                        false
    }
}
```

5. Envía la plantilla JSON de RFC a un archivo de tu carpeta actual denominado .json: CreateElbRfc

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. Modifica y guarda el CreateElbRfc archivo.json. Como creó los parámetros de ejecución en un archivo independiente, elimine la `ExecutionParameters` línea. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
{
"ChangeTypeVersion":    "2.0",
"ChangeTypeId":         "ct-123h45t6uz7jl",
"Title":                "Create ELB"
}
```

7. Crea el RFC. El siguiente comando especifica el archivo de parámetros de ejecución y el archivo de plantilla RFC:

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.json
```

Recibirá el ID de la nueva RFC en la respuesta y podrá utilizarla para enviar y supervisar la RFC. Hasta que la envíe, la RFC permanece en estado de edición y no se inicia.

Consejos

> **Note**
>
> Puede usar el AMS API/CLI para crear un RFC sin crear un archivo JSON de RFC o un archivo JSON de parámetros de ejecución de CT. Para ello, utilice el `create-rfc` comando y añada el RFC y los parámetros de ejecución necesarios al comando, lo que se denomina «Inline Create». Tenga en cuenta que todos los CTs aprovisionamientos contienen dentro del

`execution-parameters` bloque una `Parameters` matriz con los parámetros del recurso. Los parámetros deben tener comillas separadas por una barra invertida (\).
El otro método documentado para crear un RFC se denomina «Creación de plantillas». Aquí se crea un archivo JSON para los parámetros de la RFC y otro archivo JSON para los parámetros de ejecución, y se envían los dos archivos con el `create-rfc` comando. Estos archivos pueden servir como plantillas y reutilizarse para el futuro. RFCs
Al crear RFCs con plantillas, puede usar un comando para crear el archivo JSON con el contenido que desee emitiendo un comando como se muestra. Los comandos crean un archivo denominado «parameters.json» con el contenido mostrado; también puedes usar estos comandos para crear el archivo RFC JSON.

Clona RFCs (recrea) con la consola AMS

Puede utilizar la consola AMS para clonar un RFC existente.

Para clonar o volver a crear un RFC mediante la consola AMS, siga estos pasos:

1. Busque el RFC correspondiente. En el panel de navegación de la izquierda, haga clic en RFCs.

   Se abre el RFCs panel de control.
2. Desplázate por las páginas hasta encontrar el RFC que deseas clonar. Utilice la opción Filtrar para reducir la lista. Elija el RFC que desee clonar.

   Se abre la página de detalles del RFC.
3. Haga clic en Crear una copia.

   Se abre la página Crear una solicitud de cambio con todas las opciones configuradas como en la RFC original.
4. Realice los cambios que desee. Para configurar opciones adicionales, cambie la opción Básica a Avanzada. Una vez configuradas todas las opciones, seleccione Enviar.

   La página de detalles del RFC activo se abre con un nuevo ID de RFC para el RFC clonado y el RFC clonado aparece en el panel de control del RFC.

Actualización RFCs

Puede volver a enviar una RFC que haya sido rechazada o que aún no se haya enviado; para ello, debe actualizar la RFC y, a continuación, enviarla o volver a enviarla. Tenga en cuenta que la

mayoría RFCs se rechazan porque lo especificado `RequestedStartTime` se aprobó antes del envío o no TimeoutInMinutes es adecuado para ejecutar la RFC (dado que TimeoutInMinutes no prolonga una RFC exitosa, recomendamos establecerla siempre en al menos «60" y en «360" para un grupo de Amazon EC2 o Amazon EC2 Auto Scaling con una ejecución prolongada). UserData
En esta sección se describe cómo usar la versión CLI del `UpdateRfc` comando para actualizar una RFC con un nuevo parámetro de RFC, o nuevos parámetros mediante JSON en cadena o un archivo de parámetros actualizado.

En este ejemplo, se describe el uso de la versión CLI de la UpdateRfc API AMS (consulte Actualizar RFC). Si bien existen tipos de cambios para actualizar algunos recursos (el DNS público y privado, las pilas del balanceador de carga y la configuración de parches de las pilas), no existe ningún CT para actualizar una RFC.

Le recomendamos que envíe una UpdateRfc operación a la vez. Si envías varias actualizaciones, por ejemplo, en una pila de DNS, es posible que las actualizaciones fallen al intentar actualizar el DNS al mismo tiempo.

DATOS OBLIGATORIOS`RfcId`: El RFC que estás actualizando.

DATOS OPCIONALES`ExecutionParameters`: A menos que esté actualizando un campo no obligatorio, por ejemplo`Description`, debería enviar parámetros de ejecución modificados para solucionar los problemas que provocaron el rechazo o la cancelación de la RFC. Todos los valores no nulos enviados sobrescriben esos valores en la RFC original.

1. Busque el RFC rechazado o cancelado correspondiente, puede usar este comando (puede sustituir el valor por): `Canceled`

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
   ```

2. Puede modificar cualquiera de los siguientes parámetros del RFC:

   ```
   {
       "Description": "string",
       "ExecutionParameters": "string",
       "ExpectedOutcome": "string",
       "ImplementationPlan": "string",
       "RequestedEndTime": "string",
       "RequestedStartTime": "string",
       "RfcId": "string",
       "RollbackPlan": "string",
       "Title": "string",
   ```

```
    "WorstCaseScenario": "string"}
```

Ejemplo de comando que actualiza el campo Descripción:

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
 --region us-east-1
```

Ejemplo de comando que actualiza el ExecutionParameters VpcId campo:

```
aws amscm update-rfc  --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
 "RFC_ID" --region us-east-1
```

Ejemplo de comando que actualiza la RFC con un archivo de parámetros de ejecución que contiene las actualizaciones; consulte el ejemplo de archivo de parámetros de ejecución en el paso 2 de: EC2 stack | Create:

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. Vuelva a enviar la RFC con `submit-rfc` el mismo ID de RFC que tenía cuando se creó la RFC por primera vez:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Si la RFC es correcta, no recibirá mensajes de confirmación ni de error en la línea de comandos.

4. Para supervisar el estado de la solicitud y ver el resultado de la ejecución, ejecute el siguiente comando.

```
aws amscm get-rfc --rfc-id RFC_ID
```

Encuentra RFCs

Busque una solicitud de cambio (RFC) en la consola

Para buscar un RFC mediante la consola AMS, sigue estos pasos.

> **Note**
>
> Este procedimiento solo se aplica a los programados RFCs, es decir, a los RFCs que no utilizaron la opción ASAP.

1. En el panel de navegación de la izquierda, pulse RFCs.

   Se abre el RFCs panel de control.
2. Desplácese por la lista o utilice la opción Filtro para afinar la lista.

   La lista de RFC cambia según los criterios de filtro.
3. Elija el enlace Asunto de la RFC que desee.

   Se abre la página de detalles de esa RFC con información que incluye el ID de la RFC.
4. Si hay muchas RFCs en el panel de control, puede utilizar la opción de filtro para buscar por RFC:

   - Asunto: la línea de asunto o el título (en la API/CLI) que se le dio al RFC cuando se creó.
   - ID de RFC: el identificador de la RFC.
   - Estado de actividad: si conoce el estado de la RFC, puede elegir entre AwsOperatorAssignedindicar que un operador está consultando la RFC en ese momento, es AwsActionPendingdecir, que un operador de AMS debe realizar algo antes de que la ejecución de la RFC pueda continuar o CustomerActionPendingque debe realizar alguna acción antes de que la ejecución de la RFC pueda continuar.
   - Estado: si conoce el estado de la RFC, puede elegir entre:
     - Programado: RFCs que estaban programados.
     - Cancelados: RFCs que fueron cancelados.
     - En curso: RFCs en progreso.
     - Éxito: RFCs que se ejecutó con éxito.
     - Rechazados: RFCs que fueron rechazados.
     - Edición: RFCs que se están editando.
     - Fallo: RFCs eso falló.

    - Aprobación pendiente: RFCs eso no puede continuar hasta que AMS o usted lo aprueben. Por lo general, esto indica que debe aprobar la RFC. Habrás recibido una notificación de servicio al respecto en tu lista de solicitudes de servicio.
  - Tipo de cambio: seleccione la categoría, la subcategoría, el artículo y la operación y obtendrá automáticamente el identificador del tipo de cambio.
  - Hora de inicio solicitada o hora de finalización solicitada: esta opción de filtro le permite elegir Antes o Después y, a continuación, introducir una fecha y, opcionalmente, una hora (hh:mm y zona horaria). Este filtro solo funciona correctamente según lo programado RFCs (no lo antes posible RFCs).
  - Estado: programado, cancelado, en curso, exitoso, rechazado, editado o fallido.
  - Asunto: el asunto (o el título, si el RFC se creó con la API/CLI) que le diste al RFC.
  - ID del tipo de cambio: utilice el identificador del tipo de cambio enviado con la RFC.

  La búsqueda le permite añadir los filtros, como se muestra en la siguiente captura de pantalla.

5. Haga clic en el enlace del asunto del RFC que desee.

   Se abre la página de detalles de esa RFC con información que incluye el ID de la RFC.

Búsqueda de una solicitud de cambio (RFC) con la CLI

Puede usar varios filtros para buscar una RFC.

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a los parámetros de la RFC que forman parte de la solicitud (no a los parámetros de ejecución). Para ver una lista

de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

Si no anotas el identificador de RFC y necesitas encontrarlo más tarde, puedes usar el sistema de gestión de cambios (CM) de AMS para buscarlo y restringir los resultados con un filtro o una consulta.

1. La ListRfcSummariesoperación de la API CM tiene filtros. Puede filtrar los resultados en función de un `Attribute` y `Value` combinados en una operación AND lógica, o en función de un `AttributeCondition`, un y`Values`.

   Filtrado RFC

Atributo	Valores válidos	Condiciones válidas	Condición predeterminada	Notas
ActualEndTime	Cualquier cadena que represente una fecha y hora del ISO86 01 (por ejemplo, «20170101 T000000Z»)	Antes, después, entre	Ninguno	La condición Antes o Después solo acepta un valor en el campo Valores. La condición Entre debe tener exactamente dos valores en el campo Valores, donde el primer valor debe representar una fecha anterior al segundo valor
ActualStartTime	Cualquier cadena que represente una fecha y hora del ISO86 01 (por ejemplo, «20170101 T000000Z»)	Antes, después, entre	Ninguno	La condición Antes o Después solo acepta un valor en el campo Valores. La condición Entre debe tener exactamente dos valores en

Atributo	Valores válidos	Condiciones válidas	Condición predeterminada	Notas
				el campo Valores, donde el primer valor debe representar una fecha anterior al segundo valor
AutomationStatusId	Manual, automatizado	Igual a	Igual a	Solo hay dos estados de automatización
ChangeTypeId	Cualquier identificador de tipo de cambio válido; por ejemplo, ct-123h45t6uz7jl	Igual a	Igual a	Búsqueda de un tipo de cambio o CSIO
ChangeTypeVersion	Cualquier identificador de tipo de cambio válido; por ejemplo, 1.0	Igual a	Igual a	Búsqueda de un tipo de cambio o CSIO
CreatedBy	Cualquier cadena (la longitud máxima permitida es de 2048 caracteres)	Contiene	Contiene	El CreatedBy campo del RFC contiene el ARN del usuario que lo creó

Atributo	Valores válidos	Condiciones válidas	Condición predeterminada	Notas
CreatedTime	Cualquier cadena que represente una fecha y hora del ISO86 01 (por ejemplo, «20170101 T000000Z»)	Antes, después, entre	Ninguno	La condición Antes o Después solo acepta un valor en el campo Valores. La condición Entre debe tener exactamente dos valores en el campo Valores, donde el primer valor debe representar una fecha anterior al segundo valor
LastModifiedTime	Cualquier cadena que represente una fecha y hora del ISO86 01 (por ejemplo, «20170101 T000000Z»)	Antes, después, entre	Ninguno	La condición Antes o Después solo acepta un valor en el campo Valores. La condición Entre debe tener exactamente dos valores en el campo Valores, donde el primer valor debe representar una fecha anterior al segundo valor

Atributo	Valores válidos	Condiciones válidas	Condición predeterminada	Notas
LastSubmittedTime	Cualquier cadena que represente una fecha y hora del ISO86 01 (por ejemplo, «20170101 T000000Z»)	Antes, después, entre	Ninguno	La condición Antes o Después solo acepta un valor en el campo Valores. La condición Entre debe tener exactamente dos valores en el campo Valores, donde el primer valor debe representar una fecha anterior al segundo valor
RequestedEndTime	Cualquier cadena que represente una fecha y hora del ISO86 01 (por ejemplo, «20170101 T000000Z»)	Antes, después, entre	Ninguno	La condición Antes o Después solo acepta un valor en el campo Valores. La condición Entre debe tener exactamente dos valores en el campo Valores, donde el primer valor debe representar una fecha anterior al segundo valor

Atributo	Valores válidos	Condiciones válidas	Condición predeterminada	Notas
RequestedStartTime	Cualquier cadena que represente una fecha y hora del ISO86 01 (por ejemplo, «20170101 T000000Z»)	Antes, después, entre	Ninguno	La condición Antes o Después solo acepta un valor en el campo Valores. La condición Entre debe tener exactamente dos valores en el campo Valores, donde el primer valor debe representar una fecha anterior al segundo valor
RfcStatusId	Cancelada, editada, InProgress fallida PendingApproval, rechazada, programada, correcta	Igual a	Igual a	Actualice la lista de RFC en la consola AMS o ejecute GetRfc
Título	Cualquier título de RFC válido	Contiene	Contiene	No se admiten las expresiones regulares en cada campo individual. Búsqueda sin distinción de mayúsculas y minúsculas

Ejemplos:

Para encontrar todo lo RFCs relacionado con SQS (donde SQS está contenido en la parte de objetos del CT), puedes usar este comando: IDs

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

Lo que devuelve algo como esto:

```
-------------------------------------------------------------------------
|                          ListRfcSummaries                             |
+----------+--------------------------------+-------+-------+----------------+
|Deployment| Advanced Stack Components      |SQS    |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+--------------------------------+-------+-------+----------------+
```

Otro filtro para el que disponemos `list-rfc-summaries` es`AutomationStatusId`, para buscar RFCs que sean automáticos o manuales:

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

Otro filtro disponible `list-rfc-summaries` es `Title` (Asunto en la consola):

```
 Attribute=Title,Value=RFC-TITLE
```

Ejemplo de la nueva estructura de solicitudes en JSON que devuelve RFCs dónde:

- (El título CONTIENE la frase «Windows 2012" O «Amazon Linux») Y
- (RfcStatusId ES IGUAL A «Éxito» O «InProgress«) Y
- (20170101T000000Z <= <= 20170103T000000Z) Y (RequestedStartTime <= 20170103T000000Z) ActualEndTime

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
```

```
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

> **Note**
>
> Con una versión más avanzada, `Filters` AMS pretende dejar de utilizar los siguientes campos en una próxima versión:
>
> - Valor: el campo Valor forma parte del campo Filtros. Utilice el campo Valores que admite funciones más avanzadas.
> - RequestedEndTimeRange: Utilice el campo RequestedEndTime interno de filtros que admite funciones más avanzadas
> - RequestedStartTimeRange: Utilice el campo RequestedStartTime interno de filtros que admite funciones más avanzadas.

Para obtener información sobre el uso de consultas CLI, consulte Cómo filtrar la salida con la opción --query y la referencia del lenguaje de consulta, JMESPath Especificación.

2. Si utilizas la consola AMS:

Ve a la página RFCsde la lista. Si es necesario, puedes filtrar por el asunto de la RFC, que es lo que ingresaste como RFC `Title` cuando la creaste.

Consejos

> **Note**
>
> Este procedimiento solo se aplica a las personas programadas RFCs, es decir, RFCs que no utilizaron la opción ASAP.

Cancelar RFCs

Puede cancelar un RFC mediante la consola o la API/CLI de AMS.

Para cancelar una RFC con la consola, busque la RFC en su lista de RFC, ábrala y haga clic en Cancelar.

Datos necesarios:

- `Reason`: Por qué cancelas la RFC.
- `RfcId`: El RFC que vas a cancelar.

1. Por lo general, cancelas una RFC justo después de enviarla (por lo que debes tener a mano el identificador de la RFC); de lo contrario, no podrás cancelarla a menos que la hayas programado y sea antes de la hora de inicio especificada. Si necesitas encontrar el ID de la RFC, puedes usar este comando (puedes sustituir la `Value` RFC `PendingApproval` por una RFC que se apruebe manualmente):

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
   ```

2. Ejemplo de comando para cancelar una RFC:

   ```
   aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --
   region us-east-1
   ```

Utilice la consola AMS con RFCs

La consola AMS ofrece funciones que le ayudarán a crear y enviar archivos con éxito RFCs.

Utilice la página de listas de RFC (consola)

La página de RFCslista de consolas AMS le proporciona las siguientes opciones:

- Búsqueda avanzada de RFC a través de un filtro. Para obtener información, consulte Encuentra RFCs.
- Buscar la última vez que se modificó el RFC. Este valor representa la última vez que se cambió el estado de la RFC.
- Visualización de los detalles de la RFC con el asunto de la RFC. Al elegir este enlace, se abre la página de detalles de esa RFC.
- Visualización del estado del RFC. Para obtener información, consulte Comprenda los códigos de estado RFC

Utilice la creación rápida de RFC (consola)

Utilice las tarjetas de creación rápida o la tabla de listas de la RFC, o elija los tipos de cambio RFCs por clasificación.

Para obtener más información, consulte Crear un RFC.

Agregue la correspondencia y los archivos adjuntos del RFC (consola)

Puede añadir correspondencia a una RFC después de haberla enviado y antes de que se apruebe; por ejemplo, cuando tenga el estado «»PendingApproval. Una vez aprobada una RFC (en estado «Programado» o «»), no se puede añadir la correspondencia, ya que podría interpretarse como un cambio en la solicitud. InProgress Una vez completada una RFC (en estado «Cancelada», «Rechazada», «Aceptada» o «Fallo»), la correspondencia se vuelve a activar, aunque la correspondencia se desactiva cuando una RFC permanece cerrada durante más de 30 días.

> **Note**
>
> Cada correspondencia está limitada a 5000 caracteres.

Limitaciones de los archivos adjuntos:

- Solo tres archivos adjuntos por correspondencia.

- Límite de cincuenta archivos adjuntos por RFC.
- Cada archivo adjunto debe tener un tamaño inferior a 5 MB.
- Solo se aceptan archivos de texto, como texto plano (`.txt`), valores separados por comas (`.csv`), JSON () o YAML (`.json`). `.yaml` En el caso del formato YAML, el archivo debe adjuntarse con la extensión de archivo. `.yaml`

> **Note**
>
> Se prohíben los archivos de texto con contenido XML. Si tiene contenido XML para compartir con AMS, utilice una solicitud de servicio.

- Los nombres de los archivos están limitados a 255 caracteres y solo incluyen números, letras, espacios, guiones (-), guiones bajos (_) y puntos (.).
- Actualmente, no se admite la actualización y eliminación de archivos adjuntos en un RFC.

Para añadir correspondencia y archivos adjuntos a una RFC, sigue estos pasos:

1. En la consola AMS, en la página de detalles de una RFC, busca la sección Correspondencia en la parte inferior de la página.

   Antes de cualquier correspondencia:

   Después de un poco de correspondencia:

2. Para añadir una nueva correspondencia, escriba su mensaje en el cuadro de texto Responder. Para adjuntar archivos relacionados con la correspondencia, seleccione Añadir adjunto y, a continuación, elija los archivos que desee.

3. Cuando hayas terminado, selecciona Enviar.

   La nueva correspondencia, junto con los enlaces a los archivos adjuntos, aparecen en la lista de correspondencia de la página de detalles de la RFC.

Configurar las notificaciones por correo electrónico de RFC (consola)

La página de creación de solicitudes de cambio de la consola AMS ofrece la opción de añadir direcciones de correo electrónico para recibir notificaciones de los cambios de estado de los RFC:

Además, puede añadir direcciones de correo electrónico para las notificaciones de cualquier tipo de cambio, por ejemplo:

```
aws amscm create-rfc --change-type-id <Change type ID>
                     --change-type-version 1.0 --title "TITLE"
                     --notification "{\"Email\": {\"EmailRecipients\" :
 [\"email@example.com\"]}}"
```

Agregue una línea similar (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`) a cualquier solicitud de cambio de tipo, en línea o de plantilla, en la parte de parámetros de RFC de la solicitud, no en la parte de parámetros.

Más información sobre los parámetros de RFC comunes

Los siguientes son los parámetros de RFC que debe enviar y los parámetros que se utilizan habitualmente en: RFCs

- Información sobre el tipo de cambio: ChangeTypeId y. ChangeTypeVersion Para obtener una lista del tipo de cambio IDs y los números de versión, consulte la Referencia de tipos de cambio.

  Ejecute `list-change-type-classification-summaries` en la CLI con el `query` argumento para limitar los resultados. Por ejemplo, restrinja los resultados para cambiar los tipos que contienen «Access» en el `Item` nombre.

  ```
  aws amscm list-change-type-classification-summaries --query
   "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
  ```

  Ejecute `get-change-type-version` y especifique el ID del tipo de cambio. El siguiente comando obtiene la versión CT de ct-2tylseo8rxfsc.

  ```
  aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
  ```

- Título: nombre del RFC; pasa a ser el asunto del RFC en la lista de RFC de la consola AMS y puede buscarlo con el comando y el filtro activados `GetRfc` `Title`
- Programación: si desea programar una RFC, debe incluir los `RequestedEndTime` parámetros `RequestedStartTime` y, o bien utilizar la opción de consola Programar este cambio. Para un RFC ASAP (que se ejecuta tan pronto como se aprueba), cuando utilice la CLI, deje `RequestedStartTime` y `RequestedEndTime` nulo. Cuando utilice la consola, acepte la opción ASAP.

  Si `RequestedStartTime` se omite, se rechaza el RFC.
- Aprovisionamiento CTs: los parámetros de ejecución o `Parameters` los ajustes específicos necesarios para aprovisionar el recurso. Varían mucho según el CT.
- No aprovisionamiento CTs: CTs aquellos que no aprovisionan un recurso, como Access CTs u Other | Other, o eliminan una pila, tienen parámetros de ejecución mínimos y no `Parameters` se bloquean.
- Algunas RFCs también requieren que especifiques unos `TimeoutInMinutes` minutos o cuántos minutos se permiten para crear la pila antes de que se produzca un error en la RFC. Los valores válidos van desde 60 (minutos) hasta 360, si se trata de una ejecución prolongada UserData. Si la ejecución no se puede completar antes de que `TimeoutInMinutes` se supere, la RFC fallará. Sin embargo, esta configuración no retrasa la ejecución de la RFC.
- RFCs Las que crean instancias, como un bucket de S3 o un ELB, suelen proporcionar un esquema que permite añadir hasta siete etiquetas (pares clave/valor). Para añadir más etiquetas a su bucket de S3, envíe una RFC mediante el tipo de cambio Deployment | Advanced stack components | Tag | Create (ct-3cx7we852p3af). EC2, EFS, RDS y los esquemas de varios niveles (HA de dos niveles y HA de un nivel) permiten hasta cincuenta etiquetas. Las etiquetas se especifican en la parte del esquema. `ExecutionParameters` Proporcionar etiquetas puede ser de gran valor. Para obtener más información, consulta Cómo etiquetar tus EC2 recursos de Amazon.

  Cuando utilice la consola AMS, debe abrir el área de configuración adicional para poder añadir etiquetas.

> **Tip**
>
> Muchos esquemas CT tienen un `Name` campo `Description` y cerca de la parte superior del esquema. Estos campos se utilizan para nombrar la pila o el componente de la pila, no para nombrar el recurso que se está creando. Algunos esquemas ofrecen un parámetro para nombrar el recurso que se está creando y otros no. Por ejemplo, el esquema CT de

Create EC2 stack no ofrece un parámetro para nombrar la EC2 instancia. Para ello, debes crear una etiqueta con la clave «Nombre» y el valor del nombre que quieres que tenga. Si no creas una etiqueta de este tipo, la EC2 instancia se mostrará en la EC2 consola sin el atributo de nombre.

Usa la opción AWS Región RFC

Los puntos finales de la API y la CLI (`amscmyamsskms`) de AMS están incluidos. `us-east-1` Si te federas con Security Assertion Markup Language (SAML), recibirás scripts en el momento de la incorporación que configurarán tu región como us-east-1. AWS Si utilizas SAML, no necesitas especificar la opción al emitir un comando. `--region` Si tu SAML está configurado para usar us-east-1 pero tu cuenta no se encuentra en AWS esa región, debes especificar la región en la que está incorporada la cuenta cuando emitas otros comandos (por ejemplo,). AWS `aws s3`

Note

La mayoría de los ejemplos de comandos que se proporcionan en esta guía no incluyen la opción. `--region`

Suscríbase al correo electrónico diario del RFC

Puedes suscribirte a un correo electrónico diario en el que se resuma la actividad de tu cuenta en las últimas 24 horas mediante la función de resumen de RFC. La función de resumen de RFC es un proceso simplificado que reduce la cantidad de notificaciones por correo electrónico relacionadas con la cuenta. RFCs El resumen de la RFC puede reducir la probabilidad de que te saltes alguna acción que esté pendiente de respuesta.

Para activar la función de resumen de RFC, póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) de AMS. El CSDM te suscribe. Puede solicitar hasta 20 direcciones de correo electrónico (o alias) para incluirlas en su lista de correo electrónico resumida de RFC. El horario de correo electrónico actual está fijado a las 09:00 UTC-8.

Para desactivar la función de resumen de RFC, comunícate con tu CSDM y envíale tu solicitud.

Si no has configurado el resumen de la RFC y quieres recibir notificaciones sobre la tuya RFCs, o si deseas obtener información más detallada sobre la RFCs que se proporciona en el resumen de la RFC, utiliza el sistema de gestión de cambios para configurar las notificaciones de CloudWatch

eventos o las notificaciones por correo electrónico para cada RFC individual sobre la que desees obtener información. Para obtener información sobre cómo configurar las notificaciones de RFC, consulta las notificaciones de cambio de estado de las RFC.

Entre los temas incluidos en el resumen de la RFC se incluyen los siguientes:

- Pendiente de aprobación por parte del cliente: listas RFCs que están en PendingApprovalestado pendientes de aprobación por parte del cliente
- Respuesta pendiente del cliente: listas RFCs que están esperando su respuesta en la correspondencia de RFC
- Aprobación o respuesta de AWS pendientes: listas RFCs que están esperando la respuesta o aprobación de AMS
- Completado: listas con RFCs los estados correcto, fallido, cancelado o rechazado

El siguiente es un ejemplo de resumen de RFC:

¿Qué son los tipos de cambios?

El tipo de cambio se refiere a la acción que realiza una solicitud de cambio (RFC) de AWS Managed Services (AMS) y abarca la acción de cambio en sí misma y el tipo de cambio: manual o automatizado. AMS tiene una amplia colección de tipos de cambios que no utilizan otros servicios web de Amazon. Estos tipos de cambios se utilizan al enviar una solicitud de cambio (RFC) para implementar, gestionar o acceder a los recursos.

Temas

- Automatizado y manual CTs
- Requisitos de aprobación CT
- Cambiar las versiones de los tipos
- Crear tipos de cambios
- Actualizar tipos de cambios
- Tipos de cambios solo internos
- Esquemas de tipos de cambio
- Administrar los permisos para los tipos de cambios
- Redacción de información confidencial de los tipos de cambios

- Búsqueda de un tipo de cambio mediante la opción de consulta

Automatizado y manual CTs

Una limitación de los tipos de cambio es si son automáticos o manuales; se trata del `AutomationStatusId` atributo del tipo de cambio, denominado modo de ejecución en la consola AMS.

Los tipos de cambios automatizados tienen los resultados y los tiempos de ejecución esperados y se ejecutan en el sistema automatizado AMS, generalmente en una hora o menos (esto depende en gran medida de los recursos que aprovisione el CT). Los tipos de cambios manuales son poco frecuentes, pero se tratan de forma diferente porque requieren que un operador de AMS actúe en función de la RFC antes de poder ejecutarla. A veces, esto implica comunicarse con el remitente de la RFC, por lo que los tipos de cambios manuales requieren períodos de tiempo variables para completarse.

Para todos los programados RFCs, se escribe una hora de finalización no especificada como la hora especificada `RequestedStartTime` más el `ExpectedExecutionDurationInMinutes` atributo del tipo de cambio enviado. Por ejemplo, si `ExpectedExecutionDurationInMinutes` es «60» (minutos) y la especificada `RequestedStartTime` es `2016-12-05T14:20:00Z` (5 de diciembre de 2016 a las 4:20 a.m.), la hora de finalización real se establecerá en el 5 de diciembre de 2016 a las 5:20 a.m. Para `ExpectedExecutionDurationInMinutes` buscar el tipo de cambio específico, ejecute este comando:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

> **Note**
>
> Programado RFCs con modo de ejecución = Manual, en la consola, debe configurarse para que se ejecute al menos 24 horas en el futuro. Esta advertencia no se aplica a la API/CLI de AMS, pero aun así es importante programar el manual con al RFCs menos 8 horas de anticipación.

> **Note**
>
> Cuando utilice la opción «revisión obligatoria» CTs, AMS recomienda que utilice la opción de programación lo antes posible (elija ASAP en la consola y deje en blanco la hora de inicio y finalización en la API/CLI), ya que CTs requiere que un operador de AMS examine la RFC y, posiblemente, se comunique con usted antes de que pueda aprobarse y ejecutarse. Si las programa RFCs, asegúrese de esperar al menos 24 horas. Si la aprobación no se produce antes de la hora de inicio programada, la RFC se rechaza automáticamente.

El objetivo de AMS es responder a una tomografía computarizada manual en un plazo de cuatro horas y se comunicará con ella lo antes posible, pero la RFC podría tardar mucho más en ejecutarse realmente.

Para ver una lista de las CTs que son manuales y requieren una revisión por parte de AMS, consulta el archivo CSV de tipo de cambio, disponible en la página de recursos para desarrolladores de la consola.

YouTube Vídeo: ¿Cómo puedo encontrar los tipos de cambios automatizados para AMS RFCs?

Para encontrar el modo de ejecución de un CT en la consola AMS, debe utilizar la opción de búsqueda Buscar tipos de cambios. Los resultados muestran el modo de ejecución del tipo o los tipos de cambio coincidentes.

Para buscar un tipo de cambio específico mediante la CLI de AMS, ejecute este comando: `AutomationStatus`

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

También puede buscar los tipos de cambio en la Referencia de tipos de cambios de AMS, que proporciona información sobre todos los tipos de cambios de AMS.

> **Note**
>
> ActualmenteAPI/CLI. To access the AMS API/CLI, API/CLI los AMS no forman parte de AWS; puede descargar el SDK de AMS a través de la consola de AMS.

Requisitos de aprobación CT

Los AMS CTs siempre tienen dos condiciones de aprobación, AwsApprovalIdCustomerApprovalIdque indican si la RFC exige que AMS, usted o alguien más apruebe la ejecución.

La condición de aprobación está relacionada en cierta medida con el modo de ejecución; para obtener más información, consulteAutomatizado y manual CTs.

Para averiguar la condición de aprobación de un CT, puede consultar la referencia de cambio de tipo del AMS o correr GetChangeTypeVersion. Ambos también le ofrecerán el modo CT `AutomationStatusId` o modo de ejecución.

Puede aprobarlo RFCs mediante la consola AMS o con el siguiente comando:

```
aws amscm approve-rfc --rfc-id RFC_ID
```

Condición de aprobación CT

Si la condición de aprobación por TC es	Requiere la aprobación de	Y
`AwsApprovalId: Required`	El sistema de cambio de tipos AMS,	No hay que hacer nada más. Esta condición es típica de los sistemas automatizados CTs.
`AwsApprovalId: NotRequiredIfSubmitter`	El AMS cambia el tipo de sistema y nadie más, si el RFC enviado es para la cuenta en la que se presentó,	No hay que hacer nada más. Esta condición es típica de los manuales, CTs ya que siempre los revisan los operadores del AMS.
`CustomerApprovalId: NotRequired`	El sistema de cambio de tipos AMS,	Si el RFC pasa las comprobaciones de sintaxis y parámetros, se aprueba automáticamente.

Si la condición de aprobación por TC es	Requiere la aprobación de	Y
`CustomerApprovalId: Required`	El AMS cambia el sistema de tipos y usted,	Se le envía una notificación y debe aprobar la RFC de forma explícita, ya sea respondiendo a la notificación o ejecutando la ApproveRfcoperación.
`CustomerApprovalId: NotRequiredIfSubmitter`	El AMS cambia el tipo de sistema y nadie más, si has enviado la RFC.	Si el RFC pasa las comprobaciones de sintaxis y parámetros, se aprueba automáticamente.
Incidente o parche de seguridad urgente	AMS	Está aprobado e implementado automáticamente.

Cambiar las versiones de los tipos

Los tipos de cambio se versionan y la versión cambia cuando se realiza una actualización importante del tipo de cambio.

Tras seleccionar un tipo de cambio mediante la consola AMS, tiene la opción de abrir el área de configuración adicional y seleccionar una versión del tipo de cambio. También puede especificar una versión del tipo de cambio en la línea de API/CLI comandos. Es posible que desee hacerlo por varios motivos, entre los que se incluyen los siguientes:

- Sabe que la versión del tipo de cambio de actualización que desea debe coincidir con la versión del tipo de cambio de creación que utilizó para crear el recurso que ahora desea actualizar. Por ejemplo, puede que tengas una instancia de Elastic Load Balancer (ELB) que hayas creado con la versión 1 de ELB Create tipo cambio. Para actualizarla, elija la versión 1 de ELB Update.
- Desea utilizar una versión de tipo de cambio que tenga opciones diferentes a las del tipo de cambio más reciente. No lo recomendamos porque las actualizaciones de AMS cambian de tipo principalmente por motivos de seguridad y te recomendamos que elijas siempre la versión más reciente.

Crear tipos de cambios

Los tipos de cambios de creación coinciden version-to-version con los tipos de cambios de actualización. Es decir, la versión del tipo de cambio que utilice para aprovisionar un recurso debe coincidir con la versión del tipo de cambio de actualización que utilizaría más adelante para modificar ese recurso. Por ejemplo, si crea un depósito de S3 con la versión 2.0 de Create S3 Bucket y, posteriormente, desea enviar una RFC para modificar ese depósito de S3, también debe utilizar la versión 2.0 de Update S3 Bucket, incluso si hay un tipo de cambio de tipo de depósito de S3 de Update S3 con la versión 3.0.

Te recomendamos mantener un registro del ID de tipo de cambio y la versión que utilizas al aprovisionar un recurso con el tipo Crear cambio en caso de que más adelante desees utilizar un tipo de cambio Actualizar para modificarlo.

Actualizar tipos de cambios

AMS proporciona tipos de cambios de actualización para actualizar los recursos que se crearon con Create change types. Los tipos de cambios de actualización deben coincidir version-to-version con el tipo de cambio de creación que se utilizó originalmente para aprovisionar el recurso.

Se recomienda llevar un registro del identificador del tipo de cambio y de la versión que se utiliza al aprovisionar un recurso para facilitar su actualización.

YouTube Vídeo: ¿Cómo utilizo la actualización CTs para cambiar los recursos de una cuenta de AWS Managed Services (AMS)?

Tipos de cambios solo internos

Puedes ver los tipos de cambios que son solo para uso interno. Esto sirve para que sepa qué acciones puede o toma AMS. Si hay un tipo de cambio solo interno que le gustaría tener disponible para su uso, envíe una solicitud de servicio.

Por ejemplo, hay un CT de administración, monitoreo y notificación, supresión de CloudWatch alarmas, actualización, que es solo interno. AMS lo utiliza para implementar actualizaciones de infraestructura (como la aplicación de parches) a fin de desactivar las notificaciones de alarma que las actualizaciones podrían activar por error. Cuando envíe este CT, verá el RFC del CT en su lista de RFC. Cualquier CT solo interno que esté desplegado en una RFC aparecerá en su lista de RFC.

Esquemas de tipos de cambio

Todos los tipos de cambios proporcionan un esquema JSON para que los introduzcas en la creación, modificación o acceso a los recursos. El esquema proporciona los parámetros y sus descripciones para que pueda crear una solicitud de cambio (RFC).

La ejecución correcta de una RFC da como resultado el resultado de la ejecución. Para el aprovisionamiento RFCs, el resultado de la ejecución incluye un «stack_id» que representa la pila CloudFormation y se puede buscar en la consola. CloudFormation El resultado de la ejecución a veces incluye el resultado del ID de la instancia creada y ese ID se puede usar para buscar la instancia en la consola de AWS correspondiente. Por ejemplo, el resultado de ejecución de Create ELB CT incluye un «stack_id» que se puede buscar CloudFormation y genera un valor Key=ELB value= que <stack-xxxx>se puede buscar en la consola de Amazon para Elastic Load Balancing. EC2

Examinemos un esquema CT. Este es el esquema de CodeDeploy Application Create, un esquema bastante pequeño. Algunos esquemas tienen `Parameter` áreas muy grandes.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
  resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
 vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv00000000000",
      "type": "string",
```

La primera parte del esquema proporcio na información a AMS sobre el tipo de cambio solicitado.

```
      "enum": ["stm-sft6rv00000000000"]
    },
    "Name":{
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
      categorize the resource.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
            "maxLength": 127
          },
          "Value": {
            "type": "string",
            "minLength": 1,
            "maxLength": 255
          }
        },
        "additionalProperties": false,
        "required": [
          "Key",
          "Value"
        ]
      },
      "minItems": 1,
      "maxItems": 7
    },
    "TimeoutInMinutes": {
      "description": "The maximum amount of time, in minutes,
 to
      allow for execution of the change. This will not prolong
 execution,
```

El TimeoutInMinutes parámetro permite indicar un tiempo límite para ejecutar el tipo de cambio. Los valores válidos oscilan entre 60 y 360 si se trata de una ejecución prolongada UserData.

En la sección de parámetros se especifican los ajustes del recurso que se está creando o de la acción que se solicita.

```
      but the RFC fails if the change is not completed in the
 specified time.
      Valid values are 60 up to 360, for long-running
 UserData.",
      "type": "number",
      "minimum": 0,
      "maximum": 60
    },
    "Parameters": {
      "description": "Specifications for the stack.",
      "type": "object",
      "properties": {
        "CodeDeployApplicationName": {
          "description": "The name of an AWS CodeDeploy
 application.",
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
      },
      "additionalProperties": false,
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

Las secciones de «propiedades adicionales» le permiten saber qué parámetros son obligatorios y cuáles son opcionales.

> **Note**
>
> Este esquema permite hasta siete etiquetas; sin embargo, EFS EC2, RDS y los esquemas de creación de varios niveles permiten hasta 50 etiquetas.

Administrar los permisos para los tipos de cambios

Puede usar una política personalizada para restringir los tipos de cambio (CTs) que están disponibles para los distintos grupos o usuarios.

Para obtener más información sobre cómo hacerlo, consulte la sección Configuración de permisos de la Guía del usuario de AMS.

Redacción de información confidencial de los tipos de cambios

Los esquemas de tipos de cambio de AMS ofrecen un atributo de parámetro, `"metadata":"ams:sensitive":"true"` que se utiliza para los parámetros que contienen información confidencial, como una contraseña. Cuando se establece este atributo, la entrada proporcionada se oculta. Tenga en cuenta que no puede establecer este atributo de parámetro; sin embargo, si está trabajando con AMS para crear un tipo de cambio y desea ocultar un parámetro al introducirlo, puede solicitarlo.

Búsqueda de un tipo de cambio mediante la opción de consulta

En este ejemplo se muestra cómo utilizar la consola AMS para encontrar el tipo de cambio adecuado para la RFC que desea enviar.

Puede utilizar la consola o la API/CLI para buscar un identificador de tipo de cambio (CT) o una versión. Existen dos métodos: buscar o seleccionar la clasificación. Para ambos tipos de selección, puede ordenar la búsqueda eligiendo Usado con más frecuencia, Usado más recientemente o Alfabético.

YouTube Vídeo: ¿Cómo creo un RFC mediante la CLI de AWS Managed Services y dónde puedo encontrar el esquema CT?

En la consola AMS, en la página RFCs-> Crear RFC:

- Con la opción Buscar por tipo de cambio seleccionada (opción predeterminada), puede hacer lo siguiente:

- Usa el área de creación rápida para seleccionar una de las más populares de AMS CTs. Haga clic en una etiqueta y se abrirá la página Ejecutar RFC con la opción Asunto rellenada automáticamente. Complete las opciones restantes según sea necesario y haga clic en Ejecutar para enviar la RFC.
- O bien, desplácese hacia abajo hasta el área Todos los tipos de cambios y comience a escribir un nombre de CT en el cuadro de opciones; no es necesario que tenga el nombre exacto o completo del tipo de cambio. También puede buscar una tomografía computarizada por ID de tipo de cambio, clasificación o modo de ejecución (automática o manual) introduciendo las palabras correspondientes.

  Con la vista de tarjetas predeterminada seleccionada, las tarjetas CT coincidentes aparecen a medida que escribes, seleccionas una carta y haces clic en Crear RFC. Con la vista de tabla seleccionada, elige el CT correspondiente y haz clic en Crear RFC. Ambos métodos abren la página Ejecutar RFC.

- Como alternativa, y para explorar las opciones de tipos de cambio, haga clic en Elegir por categoría en la parte superior de la página para abrir una serie de cuadros de opciones desplegables.
- Elija una categoría, una subcategoría, un elemento y una operación. Aparece el cuadro de información para ese tipo de cambio y aparece un panel en la parte inferior de la página.
- Cuando esté listo, presione Entrar y aparecerá una lista de los tipos de cambios coincidentes.
- Elige un tipo de cambio de la lista. El cuadro de información para ese tipo de cambio aparece en la parte inferior de la página.
- Una vez que tenga el tipo de cambio correcto, elija Crear RFC.

> **Note**
>
> La CLI de AMS debe estar instalada para que estos comandos funcionen. Para instalar la API o CLI de AMS, vaya a la página de recursos para desarrolladores de la consola AMS. Para obtener material de referencia sobre la API AMS CM o la API AMS SKMS, consulte la sección Recursos de información de AMS en la Guía del usuario. Puede que necesite añadir una `--profile` opción de autenticación; por ejemplo,`aws amsskms` *`ams-cli-command`* `--profile SAML`. Es posible que también tengas que añadir la `--region` opción, ya que todos los comandos de AMS se ejecutan desde us-east-1, por ejemplo. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

> **Note**
>
> Los puntos de enlace AMS API/CLI (amscm y amsskms) se encuentran en la región de AWS del Norte de Virginia,. `us-east-1` En función de cómo esté configurada su autenticación y de la región de AWS en la que se encuentren su cuenta y sus recursos, es posible que tenga que `--region us-east-1` añadirlos al emitir comandos. Es posible que también necesite añadirlo`--profile saml`, si ese es su método de autenticación.

Para buscar un tipo de cambio mediante la API CM de AMS (consulte ListChangeTypeClassificationSummaries) o la CLI:

Puede utilizar un filtro o una consulta para realizar la búsqueda. La ListChangeTypeClassificationSummaries operación tiene opciones de filtros para `CategorySubcategory`,`Item`, y`Operation`, pero los valores deben coincidir exactamente con los valores existentes. Para obtener resultados más flexibles al usar la CLI, puede usar la `--query` opción.

Cambie el tipo de filtrado con la API/CLI AMS CM

Atributo	Valores válidos	Condición válida/predeterminada	Notas
ChangeTypeId	Cualquier cadena que represente a ChangeTypeId (por ejemplo: ct-abc123 xyz7890)	Igual a	Para ver el tipo de cambio, consulte la Referencia del tipo de cambio. IDs Para ver el tipo de cambio IDs, consulte Búsqueda de un tipo de cambio o CSIO.
Categoría	Cualquier texto de formato libre	Contiene	No se admiten las expresiones regulares en cada campo individual. Búsqueda sin distinció
Subcategory			
Elemento			
Operation			

Atributo	Valores válidos	Condición válida/predeterminada	Notas
			n de mayúsculas y minúsculas

1. Estos son algunos ejemplos de clasificaciones de tipos de cambio de listas:

   El siguiente comando muestra todas las categorías de tipos de cambio.

   ```
   aws amscm list-change-type-categories
   ```

   El siguiente comando muestra las subcategorías que pertenecen a una categoría específica.

   ```
   aws amscm list-change-type-subcategories --category CATEGORY
   ```

   El siguiente comando muestra los elementos que pertenecen a una categoría y subcategoría especificadas.

   ```
   aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
   ```

2. Estos son algunos ejemplos de búsqueda de tipos de cambios con consultas CLI:

   El siguiente comando busca en los resúmenes de las clasificaciones de CT las que contienen «S3" en el nombre del elemento y crea el resultado de la categoría, la subcategoría, el elemento, la operación y el identificador del tipo de cambio en forma de tabla.

   ```
   aws amscm list-change-type-classification-summaries --query
    "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
   [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
   ```

   ```
   +-------------------------------------------------------------+
   |              ListChangeTypeClassificationSummaries          |
   +----------+-------------------------+--+------+---------------+
   |Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
   +----------+-------------------------+--+------+---------------+
   ```

3. A continuación, puede utilizar el identificador del tipo de cambio para obtener el esquema CT y examinar los parámetros. El siguiente comando envía el esquema a un archivo JSON denominado Creates3Params.schema.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3Params.schema.json
```

   Para obtener información sobre el uso de consultas CLI, consulte Cómo filtrar la salida con la opción --query y la referencia del lenguaje de consulta, JMESPath Especificación.

4. Una vez que tengas el ID del tipo de cambio, te recomendamos que compruebes la versión del tipo de cambio para asegurarte de que es la última. Usa este comando para buscar la versión de un tipo de cambio específico:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

   Para `AutomationStatus` buscar el tipo de cambio específico, ejecute este comando:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

   Para `ExpectedExecutionDurationInMinutes` buscar el tipo de cambio específico, ejecuta este comando:

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
 --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Solución de problemas de errores de RFC en AMS

Muchos errores de RFC relacionados con el aprovisionamiento de AMS se pueden investigar a través de la documentación. CloudFormation Consulte Solución de problemas de AWS CloudFormation: Solución de errores

En las siguientes secciones se ofrecen sugerencias adicionales para la solución de problemas.

Errores de RFC de «administración» en AMS

Los tipos de cambio de categoría «Gestión» de AMS (CTs) permiten solicitar el acceso a los recursos, así como gestionar los recursos existentes. En esta sección se describen algunos problemas comunes.

Errores de acceso a RFC

- Asegúrese de que el nombre de usuario y el FQDN que especificó en el RFC son correctos y existen en el dominio. Para obtener ayuda para encontrar el FQDN, consulte Cómo encontrar el FQDN.
- Asegúrese de que el ID de pila que especificó para el acceso sea una pila EC2 relacionada. Las pilas como ELB y Amazon Simple Storage Service (S3) no son aptas para el acceso; en su lugar RFCs, utilice su función de acceso de solo lectura para acceder a estos recursos de pilas. Si necesitas ayuda para encontrar un ID de pila, consulta Cómo encontrar una pila IDs
- Asegúrate de que el ID de pila que has proporcionado es correcto y pertenece a la cuenta correspondiente.

Para obtener ayuda con otros errores de RFC de acceso, consulta Administración de acceso.

YouTube Vídeo: ¿Cómo puedo presentar correctamente una solicitud de cambio (RFC) para evitar rechazos y errores?

Errores en la programación del RFC (manual) por TC

La mayoría de los tipos de cambios son ExecutionMode =Automatizados, pero algunos son ExecutionMode =Manuales y eso afecta a la forma en que debe programarlos para evitar que se produzca un error en la RFC.

Programado RFCs con ExecutionMode =Manual, debe configurarse para que se ejecute al menos 24 horas en el futuro si utiliza la consola AMS para crear el RFC. Esta advertencia no se aplica a la API/CLI de AMS, pero aun así es importante programar el manual con al RFCs menos 8 horas de anticipación.

El objetivo de AMS es responder a una tomografía computarizada manual en un plazo de cuatro horas y se pondrá en contacto con ella lo antes posible, aunque la RFC podría tardar mucho más en ejecutarse realmente.

Se utiliza RFCs con actualización manual CTs

Las operaciones de AMS rechazan la gestión | Otras | Otras RFCs para actualizar las pilas cuando haya un tipo de cambio de actualización para el tipo de pila que se quiere actualizar.

RFC elimina los errores de pila

Fallos de eliminación de la pila mediante RFC: si utilizas el comando Management | Standard stacks | Stack | Delete CT, verás los eventos detallados de la pila con el nombre de la pila AMS en la CloudFormation consola. Puedes identificar tu pila comparándola con el nombre que tiene en la consola AMS. La CloudFormation consola proporciona más detalles sobre las causas de los errores.

Antes de eliminar una pila, debes tener en cuenta cómo se creó la pila. Si creó la pila con un AMS CT y no agregó ni editó los recursos de la pila, puede esperar eliminarla sin problemas. Sin embargo, es una buena idea eliminar los recursos añadidos manualmente de una pila antes de enviar una RFC para eliminarla. Por ejemplo, si crea una pila con la pila completa CT (HA de dos niveles), incluirá un grupo de seguridad:. SG1 Si, a continuación SG2, utiliza AMS para crear otro grupo de seguridad (-) y hace referencia al nuevo SG2 grupo SG1 creado como parte de la pila completa y, a continuación, utiliza la pila de eliminación CT para eliminar la pila, no SG1 se eliminará tal como se hace referencia a ella SG2.

Important

Eliminar pilas puede tener consecuencias no deseadas e imprevistas. Por este motivo, AMS prefiere *no* eliminar pilas o apilar recursos en nombre de los clientes. Tenga en cuenta que AMS solo eliminará los recursos en su nombre (mediante un tipo de cambio de gestión | Otros | Otros | Actualizar) que no sea posible eliminar mediante el tipo de cambio automatizado adecuado para eliminarlos. Consideraciones adicionales:

- Si los recursos están habilitados para la «protección contra la eliminación», AMS puede ayudarte a desbloquearla si envías un tipo de cambio de gestión | Otros | Otros | Actualizar y, una vez eliminada la protección de eliminación, puedes utilizar el CT automatizado para eliminar ese recurso.
- Si hay varios recursos en una pila y solo desea eliminar un subconjunto de los recursos de la pila, utilice el tipo de cambio de CloudFormation actualización (consulte Pila de CloudFormation ingesta: actualización). También puede enviar un tipo de cambio de administración | Otros | Otros | Actualizar y los ingenieros de AMS pueden ayudarle a crear el conjunto de cambios, si es necesario.

- Si hay problemas al utilizar la CloudFormation actualización CT debido a desviaciones, AMS puede ayudarle si envía una actualización de Management | Other | Other | Other para resolver la deriva (en la medida en que lo admita el CloudFormation servicio de AWS) y proporcionarle una ChangeSet que, a continuación, pueda validar y ejecutar mediante la CT, el Management/Custom Stack/Stack From CloudFormation Template/Approve conjunto de cambios y la actualización automatizados.

AMS mantiene las restricciones anteriores para garantizar que no se eliminen recursos de forma inesperada o imprevista.

Para obtener más información, consulte Solución de problemas de AWS CloudFormation: la eliminación de la pila falla.

Errores de DNS al actualizar el RFC

Es posible RFCs que se produzca un error al actualizar varias veces una zona alojada en el DNS, algunas veces sin motivo. Si se crean varias RFCs al mismo tiempo para actualizar las zonas alojadas en el DNS (privadas o públicas), algunas de ellas pueden RFCs fallar porque están intentando actualizar la misma pila al mismo tiempo. La administración de cambios de AMS rechaza o falla si RFCs no puede actualizar una pila porque otra RFC ya la está actualizando. AMS recomienda crear una RFC a la vez y esperar a que la RFC funcione correctamente antes de crear una nueva para la misma pila.

Errores de entidades de RFC IAM

AMS proporciona una serie de funciones y perfiles de IAM predeterminados en las cuentas de AMS que están diseñadas para satisfacer sus necesidades. Sin embargo, es posible que de vez en cuando necesite solicitar recursos de IAM adicionales.

El proceso de presentación de solicitudes RFCs de recursos de IAM personalizados sigue el flujo de trabajo estándar y manual RFCs, pero el proceso de aprobación también incluye una revisión de seguridad para garantizar que se han establecido los controles de seguridad adecuados. Por lo tanto, el proceso suele tardar más que otros manuales RFCs. Para reducir el tiempo de ciclo de estos RFCs, siga las siguientes pautas.

Para obtener información sobre lo que entendemos por una revisión de la IAM y cómo se ajusta a nuestras normas técnicas y al proceso de aceptación de riesgos, consulteComprenda las revisiones de seguridad de RFC.

Solicitudes comunes de recursos de IAM:

- Si está solicitando una política relativa a una aplicación importante compatible con la nube, por ejemplo CloudEndure, consulte la CloudEndure política de IAM aprobada previamente por la AMS: descomprima el archivo de ejemplo de WIGs Cloud Endure Landing Zone y abra el `customer_cloud_endure_policy.json`

  > **Note**
  >
  > Si desea una política más permisiva, hable con usted sobre sus necesidades y solicite, si es necesario, una revisión CloudArchitect/CSDM y aprobación de seguridad por parte de AMS antes de enviar una RFC para implementar la política.

- Si desea modificar un recurso implementado por AMS en su cuenta de forma predeterminada, le recomendamos que solicite una copia modificada de ese recurso en lugar de realizar cambios en el ya existente.
- Si solicita permisos para un usuario humano (en lugar de adjuntar los permisos al usuario), asocie los permisos a una función y, a continuación, conceda permiso al usuario para que asuma esa función. Para obtener más información sobre cómo hacerlo, consulte Acceso temporal a la consola AMS Advanced.
- Si necesita permisos excepcionales para una migración o un flujo de trabajo temporales, indique una fecha de finalización para dichos permisos en su solicitud.
- Si ya has discutido el tema de tu solicitud con tu equipo de seguridad, presenta a tu CSDM una prueba de su aprobación con el mayor detalle posible.

Si AMS rechaza un RFC de IAM, indicamos un motivo claro para rechazarlo. Por ejemplo, podríamos rechazar una solicitud de creación de una política de IAM y explicar qué aspectos de la política son inapropiados. En ese caso, puede realizar los cambios identificados y volver a enviar la solicitud. Si se requiere mayor claridad sobre el estado de una solicitud, envíe una solicitud de servicio o póngase en contacto con su CSDM.

La siguiente lista describe los riesgos típicos que AMS intenta mitigar al revisar su IAM. RFCs Si su RFC de IAM presenta alguno de estos riesgos, es posible que se rechace la RFC. En los casos en los que necesite una excepción, AMS solicitará la aprobación de su equipo de seguridad. Para solicitar una excepción de este tipo, coordínese con su CSDM.

> **Note**
>
> AMS puede, por cualquier motivo, rechazar cualquier cambio en los recursos de IAM de una cuenta. Si tiene dudas sobre el rechazo de un RFC, póngase en contacto con AMS Operations mediante una solicitud de servicio o póngase en contacto con su CSDM.

- Escalación de privilegios, como permisos que le permiten modificar sus propios permisos o modificar los permisos de otros recursos de la cuenta. Ejemplos:
  - El uso de `iam:PassRole` con otro rol más privilegiado.
  - Permiso para acceder a las políticas de attach/detach IAM por parte de un rol o un usuario.
  - La modificación de las políticas de IAM en la cuenta.
  - La capacidad de realizar llamadas a la API en el contexto de la infraestructura de administración.
- Permisos para modificar los recursos o las aplicaciones necesarios para proporcionarle los servicios de AMS. Ejemplos:
  - Modificación de la infraestructura de AMS, como los bastiones, el host de administración o la infraestructura de EPS.
  - Eliminación de las funciones o flujos de registro de AWS Lambda de administración de registros.
  - La eliminación o modificación de la aplicación de CloudTrail monitoreo predeterminada.
  - La modificación del Active Directory (AD) de los servicios de directorio.
  - Desactivación de las alarmas CloudWatch (CW).
  - La modificación de los principios, las políticas y los espacios de nombres implementados en la cuenta como parte de la landing zone.
- El despliegue de la infraestructura no se basa en las mejores prácticas, como los permisos que permiten crear una infraestructura en un estado que pone en peligro la seguridad de la información. Ejemplos:
  - La creación de depósitos de S3 públicos o no cifrados o el intercambio público de volúmenes de EBS.
  - El aprovisionamiento de direcciones IP públicas.
  - La modificación de los grupos de seguridad para permitir un acceso amplio.
- Permisos demasiado amplios que pueden afectar a las aplicaciones, como los permisos que pueden provocar la pérdida de datos, la pérdida de integridad, una configuración inadecuada o la interrupción del servicio de la infraestructura y las aplicaciones de la cuenta. Ejemplos:

  - Inhabilitar o redirigir el tráfico de red a través APIs de, por ejemplo, o. `ModifyNetworkInterfaceAttribute` `UpdateRouteTable`
  - La desactivación de la infraestructura gestionada mediante la separación de los volúmenes de los hosts gestionados.
- Los permisos para los servicios no forman parte de la descripción del servicio de AMS y AMS no los admite.

  Los servicios que no figuran en la descripción del servicio de AMS no se pueden utilizar en las cuentas de AMS. Para solicitar asistencia para una función o un servicio, póngase en contacto con su CSDM.
- Permisos que no cumplen con el objetivo establecido porque son demasiado generosos o demasiado conservadores o se aplican a los recursos incorrectos. Ejemplos:
  - Una solicitud de `s3:PutObject` permisos para un bucket de S3 que tiene un cifrado KMS obligatorio, sin `KMS:Encrypt` permisos para la clave correspondiente.
  - Permisos que pertenecen a recursos que no existen en la cuenta.
  - IAM RFCs donde la descripción de la RFC no parece coincidir con la solicitud.

Errores de RFC relacionados con el «despliegue»

Los tipos de cambio de categoría «Despliegue» de AMS (CTs) le permiten solicitar que se añadan a su cuenta varios recursos compatibles con AMS.

La mayoría de los AMS CTs que crean un recurso se basan CloudFormation en plantillas. Como cliente, tiene acceso de solo lectura a todos los servicios de AWS CloudFormation, incluidos los que puede identificar rápidamente la CloudFormation pila que representa su pila en función de la descripción de la pila mediante la CloudFormation consola. Es probable que la pila fallida se encuentre en un estado de DELETE_COMPLETE. Una vez que haya identificado la CloudFormation pila, los eventos le mostrarán el recurso específico que no se pudo crear y el motivo.

Uso de CloudFormation la documentación para solucionar problemas

La mayoría de los aprovisionamientos de AMS RFCs utilizan una CloudFormation plantilla y esa documentación puede resultar útil para solucionar problemas. Consulte la documentación de esa CloudFormation plantilla:

- Error al crear el balanceador de carga de aplicaciones: AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer)

- Crear grupo de Auto Scaling: AWS::AutoScaling::AutoScalingGroup (Auto Scaling Group)
- Crear caché de memcached: AWS::ElastiCache::CacheCluster (Clúster de caché)
- Crear caché de Redis: AWS::ElastiCache::CacheCluster (Clúster de caché)
- Crear zona alojada en DNS (utilizada con Crear DNS privado/público): AWS::Route53::HostedZone (Zona alojada R53)
- Crear conjunto de registros DNS (usado con Crear DNS privado/público): (Conjuntos de registros de recursos) AWS::Route53::RecordSet
- Crear EC2 pila: AWS::EC2::Instance (Elastic Compute Cloud)
- Crear un sistema de archivos elástico (EFS): AWS::EFS::FileSystem (Sistema de archivos elástico)
- Crear un balanceador de carga: AWS::ElasticLoadBalancing::LoadBalancer (Elastic Load Balancer)
- Crear RDS DB: AWS::RDS::DBInstance (base de datos relacional)
- Cree Amazon S3: AWS::S3::Bucket (servicio de almacenamiento simple)
- Crear cola: AWS::SQS::Queue (servicio de colas simple)

Errores de creación de RFC AMIs

Una Imagen de máquina de Amazon (AMI) es una plantilla que contiene una configuración de software (por ejemplo, un sistema operativo, un servidor de aplicaciones y aplicaciones). Desde una AMI, se lanza una instancia, que es una copia de la AMI que se ejecuta como un servidor virtual en la nube. AMIs son muy útiles y necesarios para crear EC2 instancias o grupos de Auto Scaling; sin embargo, debe cumplir algunos requisitos:

- La instancia que especifique `Ec2InstanceId` debe estar detenida para que la RFC se ejecute correctamente. No utilice instancias del grupo Auto Scaling (ASG) para este parámetro porque el ASG finalizará una instancia detenida.
- Para crear una Amazon Machine Image (AMI) de AMS, debe empezar con una instancia de AMS. Antes de poder usar la instancia para crear la AMI, debe prepararla asegurándose de que esté detenida y separada de su dominio. Para obtener más información, consulte Creación de una imagen de máquina Amazon estándar con Sysprep
- El nombre que especifique para la nueva AMI debe ser único en la cuenta o la RFC fallará. Cómo hacerlo se describe en AMI | Create y, para obtener más información, consulte Diseño de AMI de AWS.

> **Note**
>
> Para obtener información adicional sobre cómo preparar la creación de una AMI, consulte AMI | Create.

RFCs creación EC2s o errores ASGs

En el EC2 caso de errores de ASG con tiempos de espera, AMS recomienda que confirme si la AMI utilizada está personalizada. Si es así, consulte los pasos de creación de la AMI que se incluyen en esta guía (consulte AMI | Crear) para asegurarse de que la AMI se creó correctamente. Un error común al crear una AMI personalizada es no seguir los pasos de la guía para cambiar el nombre de Sysprep o invocarlo.

RFCs crear errores de RDS

Los errores del Amazon Relational Database Service (RDS) se pueden producir por muchos motivos diferentes, ya que puede utilizar muchos motores diferentes al crear el RDS y cada motor tiene sus propios requisitos y limitaciones. Antes de intentar crear una pila de AMS RDS, revise detenidamente los valores de los parámetros de AWS RDS (consulte Crear). DBInstance

Para obtener más información sobre Amazon RDS en general, incluidas las recomendaciones de tamaño, consulte la documentación de Amazon Relational Database Service.

RFCs errores de creación de Amazon S3

Un error común al crear un depósito de almacenamiento de S3 es no utilizar un nombre único para el depósito. Si ha enviado un depósito de S3 Create CT con el mismo nombre que el enviado anteriormente, se producirá un error porque ya existe un depósito de S3 con ese nombre BucketName. Esto se detallará en la CloudFormation consola, donde verá que el evento de pila indica que el nombre del bucket ya está en uso.

Errores de validación de RFC frente a errores de ejecución

Los errores de RFC y los mensajes relacionados difieren en los mensajes de salida de la página de detalles del RFC de la consola AMS para un RFC seleccionado:

- Los motivos de los errores de validación solo están disponibles en el campo de estado
- Los motivos de los errores de ejecución están disponibles en los campos de salida de la ejecución y de estado.

Mensajes de error de RFC

Si encuentra el siguiente error en los tipos de cambios de la lista (CTs), puede utilizar estas soluciones para encontrar el origen de los problemas y solucionarlos.

```
{"errorMessage":"An error has occurred during RFC execution. We are
investigating the issue.","errorType":"InternalError"}
```

Si necesita más ayuda después de consultar las siguientes opciones de solución de problemas, póngase en contacto con AMS a través de la correspondencia RFC o cree una solicitud de servicio. Consulte Correspondencia y adjuntos del RFC (consola) y Creación de una solicitud de servicio en AMS para obtener más información.

Errores de ingesta de carga de trabajo (WIGS)

> **Note**
>
> Las herramientas de validación para Windows y Linux se pueden descargar y ejecutar directamente en los servidores locales, así como en las EC2 instancias de AWS. Puede consultarlas en la Guía avanzada para desarrolladores de aplicaciones de AMS Migración de cargas de trabajo: validación previa a la ingesta de Linux y Migración de cargas de trabajo: validación previa a la ingesta de Windows.

- Asegúrese de que la instancia exista en la cuenta AMS de destino. EC2 Por ejemplo, si ha compartido su AMI de una cuenta que no es de AMS con una cuenta de AMS, tendrá que crear una EC2 instancia en su cuenta de AMS con la AMI compartida antes de poder enviar una RFC de Workload Ingest.
- Compruebe si los grupos de seguridad adjuntos a la instancia tienen permitido el tráfico de salida. El agente SSM debe poder conectarse a su punto final público.
- Comprueba si la instancia tiene los permisos adecuados para conectarse con el agente SSM. Estos permisos vienen con el`customer-mc-ec2-instance-profile`, puedes comprobarlo en la EC2 consola:

EC2 errores de parada de la pila de instancias

- Comprueba si la instancia ya está detenida o finalizada.
- Si la EC2 instancia está en línea y ves el `InternalError` error, envía una solicitud de servicio para que AMS la investigue.
- Tenga en cuenta que no puede usar el tipo de cambio Management | Advanced stack components | EC2 instance stack | Stop ct-3mvvt2zkyveqj para detener una instancia de grupo de Auto Scaling (ASG). Si necesitas detener una instancia de ASG, envía una solicitud de servicio.

EC2 errores de creación de la pila de instancias

El `InternalError` mensaje proviene de un motivo de estado CloudFormation CREATION_FAILED. Para obtener detalles sobre el error de la pila en los eventos de CloudWatch pila, sigue estos pasos:

- En la consola de administración de AWS, puede ver una lista de eventos de pila mientras se crea, actualiza o elimina la pila. Desde esta lista, encuentre un evento de error y, a continuación, vea la razón del estado de dicho evento.

  El motivo del estado puede contener un mensaje de error de AWS CloudFormation o de un servicio concreto que pueda ayudarle a entender el problema.
- Para obtener más información sobre la visualización de eventos de pila, consulte Visualización de datos y recursos de AWS CloudFormation Stack en la consola de administración de AWS.

EC2 errores de restauración del volumen de instancias

AMS crea un RFC interno de solución de problemas cuando se produce un error en la restauración del volumen de la EC2 instancia. Esto se debe a que la restauración del volumen de EC2 instancias es una parte importante de la recuperación ante desastres (DR) y AMS crea automáticamente este RFC interno de solución de problemas.

Cuando se crea el RFC interno de solución de problemas, aparece un banner con enlaces al RFC. Este RFC interno de solución de problemas le proporciona una mayor visibilidad de los errores del RFC y, en lugar de enviar un nuevo intento que RFCs provoque los mismos errores o tener que ponerse en contacto manualmente con AMS en caso de fallo, puede realizar un seguimiento de los cambios y saber que AMS está solucionando el error. Esto también reduce la métrica time-to-recovery (TTR) para su cambio, ya que los operadores de AMS trabajan de forma proactiva para solucionar el error de la RFC en lugar de esperar a que usted lo solicite.

¿Cómo obtener ayuda con una RFC

Puede ponerse en contacto con AMS para identificar la causa raíz del error. El horario de atención de AMS es las 24 horas del día, los 7 días de la semana, los 365 días del año.

AMS ofrece varias vías para solicitar ayuda o solicitar servicios.

- Para solicitar información o asesoramiento, o para acceder a un servicio de TI gestionado por AMS, o para solicitar un servicio adicional de AMS, utilice la consola de AMS y envíe una solicitud de servicio. Para obtener más información, consulte Creación de una solicitud de servicio. Para obtener información general sobre las solicitudes de servicio de AMS, consulte Administración de solicitudes de servicio.
- Para informar de un problema de rendimiento de los servicios de AWS o AMS que afecte a su entorno gestionado, utilice la consola AMS y envíe un informe de incidente. Para obtener más información, consulte Notificación de un incidente. Para obtener información general sobre la gestión de incidentes de AMS, consulte Respuesta a incidentes.
- Si tiene alguna pregunta específica sobre cómo usted o sus recursos o aplicaciones trabajan con AMS, o si desea agravar un incidente, envíe un correo electrónico a una o varias de las siguientes direcciones:
  1. En primer lugar, si no está satisfecho con la solicitud de servicio o la respuesta al informe de incidentes, envíe un correo electrónico a su CSDM: ams-csdm@amazon.com
  2. A continuación, si se requiere una escalación, puede enviar un correo electrónico al gerente de operaciones de AMS (pero es probable que su CSDM se encargue de ello): ams-opsmanager@amazon.com
  3. Para continuar, diríjase al director de AMS: ams-director@amazon.com
  4. Por último, siempre podrá ponerse en contacto con el vicepresidente de la AMS: ams-vp@amazon.com

Modo de cambio directo en AMS

Temas

- Cómo empezar con el modo Direct Change
- Seguridad y conformidad
- Gestión de cambios en el modo Direct Change
- Creación de pilas mediante el modo de cambio directo

- Casos de uso del modo de cambio directo

El modo Direct Change (DCM) de AWS Managed Services (AMS) amplía la administración avanzada de cambios de AMS al proporcionar AWS acceso nativo a las cuentas AMS Advanced Plus y Premium para aprovisionar y actualizar AWS los recursos. Con DCM, tiene la opción de utilizar la AWS API nativa (consola o CLI/SDK) o las solicitudes de cambio de AMS Advanced Change Management (RFCs) y, en cualquier caso, AMS admite plenamente los recursos y los cambios en ellos, incluidos la supervisión, los parches, las copias de seguridad y la gestión de la respuesta a incidentes. Los recursos aprovisionados a través de DCM se registran en el sistema de gestión del conocimiento del servicio AMS (SKMS), se unen al dominio de Active Directory administrado por AMS (cuando corresponde) y ejecutan los agentes de administración de AMS. Utilice las herramientas existentes (por ejemplo CloudFormation, el AWS SDK y el CDK) para desarrollar e implementar pilas administradas por AMS. CloudFormation

> **Note**
>
> El modo Direct Change no elimina la administración de cambios de AMS. RFCs RFCs Con DCM, tiene acceso completo a AMS.

Vea el vídeo de Akash para obtener más información (6:30)

Cómo empezar con el modo Direct Change

Comience por comprobar los requisitos previos y, a continuación, envíe una solicitud de cambio (RFC) en su cuenta de AMS Advanced que cumpla los requisitos.

1. Confirme que la cuenta que quiere usar con DCM cumpla los requisitos:
   - La cuenta es AMS Advanced Plus o Premium.
   - La cuenta no tiene activado Service Catalog. Actualmente, no admitimos la incorporación de cuentas a DCM y a Service Catalog al mismo tiempo. Si ya está incorporado a Service Catalog pero está interesado en DCM, hable de sus necesidades con su administrador de prestación de servicios en la nube (CSDM). Si decide cambiar de Service Catalog a DCM, fuera de Service Catalog, para ello, incluya la solicitud de cambio en la solicitud de cambio que aparece a continuación. Para obtener más información sobre el catálogo de servicios en AMS, consulte AMS y Service Catalog.

2. Envíe una solicitud de cambio (RFC) mediante el modo Administración | Cuenta gestionada | Cambio directo | Habilitar el tipo de cambio (ct-3rd4781c2nnhp). Para ver un ejemplo de tutorial, consulte Modo de cambio directo | Activar.

   Una vez procesado el CT, las funciones de IAM predefinidas `AWSManagedServicesUpdateRole` se aprovisionan en la cuenta especificada. `AWSManagedServicesCloudFormationAdminRole`
3. Asigne la función adecuada a los usuarios que requieren acceso a DCM mediante su proceso de federación interno.

> **Note**
>
> Puede especificar cualquier número de SAMLIdentity proveedores, AWS servicios y entidades de IAM (funciones, usuarios, etc.) para que asuman las funciones. Debe proporcionar al menos uno: `SAMLIdentityProviderARNsIAMEntityARNs`, o`AWSServicePrincipals`. Para obtener más información, consulte con el departamento de IAM de su empresa o con su arquitecto de nube (CA) de AMS.

Funciones y políticas de IAM del modo Direct Change

Cuando el modo Direct Change está habilitado en una cuenta, se implementan estas nuevas entidades de IAM:

`AWSManagedServicesCloudFormationAdminRole`: Esta función permite acceder a la CloudFormation consola, crear y actualizar CloudFormation pilas, ver los informes de desviaciones y crear y ejecutar. CloudFormation ChangeSets El acceso a este rol se administra a través de su proveedor de SAML.

Las políticas administradas que se implementan y se asocian a la función `AWSManagedServicesCloudFormationAdminRole` son:

- Cuenta de aplicación AMS Advanced multi-account landing zone (MALZ)
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2.
    - Esta política representa los permisos otorgados a. `AWSManagedServicesCloudFormationAdminRole` Tú y tus socios usáis esta política

para conceder acceso a un rol existente en la cuenta y permitir que ese rol lance y actualice CloudFormation pilas en la cuenta. Esto puede requerir actualizaciones adicionales de la política de control de servicios (SCP) de AMS para permitir que otras entidades de IAM lancen pilas. CloudFormation

- Cuenta AMS Advanced Single-Account Landing Zone (SALZ)
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2.
  - cdk-legacy-mode-s3 accesos [política en línea]
  - AWS ReadOnlyAccess política

`AWSManagedServicesUpdateRole`: Esta función otorga acceso restringido al AWS servicio APIs descendente. La función se implementa con políticas administradas que proporcionan operaciones de API mutantes y no mutantes, pero en general restringen las operaciones mutantes (por ejemploCreate/Delete/PUT) a ciertos servicios, como IAM, KMS, GuardDuty VPC, AMS, recursos y configuración de infraestructura, etc. El acceso a este rol se administra a través del proveedor de SAML.

Las políticas administradas que se implementan y se asocian a la función `AWSManagedServicesUpdateRole` son:

- Cuenta de aplicación AMS Advanced multicuenta para zonas de landing zone
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2Y RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolítica
- Cuenta AMS Advanced de una sola cuenta en la zona de landing zone
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2Y RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolítica 1
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolítica 2

Además, la `AWSManagedServicesUpdateRole` función de política administrada también tiene `ViewOnlyAccess` asociada la política AWS administrada.

Seguridad y conformidad

La seguridad y el cumplimiento son una responsabilidad compartida entre AMS Advanced y usted, como cliente nuestro. El modo AMS Advanced Direct Change no modifica esta responsabilidad compartida.

Seguridad en el modo Direct Change

AMS Advanced ofrece un valor adicional con una landing zone prescriptiva, un sistema de gestión de cambios y una gestión de acceso. Cuando se utiliza el modo Direct Change, este modelo de responsabilidad no cambia. Sin embargo, debe tener en cuenta los riesgos adicionales.

La función de «actualización» del modo Direct Change Mode (consulteFunciones y políticas de IAM del modo Direct Change) proporciona permisos elevados que permiten a la entidad con acceso a ella realizar cambios en los recursos de infraestructura de los servicios compatibles con AMS de su cuenta. Con el aumento de los permisos, existen diversos riesgos en función del recurso, el servicio y las acciones, especialmente en situaciones en las que se realiza un cambio incorrecto debido a un descuido, un error o una falta de cumplimiento del marco interno de procesos y control.

Según las normas técnicas de la AMS, se han identificado los siguientes riesgos y se formulan las siguientes recomendaciones. La información detallada sobre las normas técnicas de AMS está disponible en AWS Artifact. Para acceder AWS Artifact, póngase en contacto con su CSDM para obtener instrucciones o vaya a Primeros pasos con. AWS Artifact

AMS-STD-001: Etiquetado

Estándares	¿Se rompe	Riesgos	Recomendaciones
Todos los recursos propiedad de AMS deben tener el siguiente par clave-valor Todas las etiquetas propiedad de	Sí. Se interrumpe para CloudFormation la API EFS OpenSearch, CloudWatch Logs, SQS, SSM y Tagging, ya que estos servicios no admiten la	El etiquetado incorrecto de los recursos de AMS puede afectar negativamente a las operaciones de generación de informes, alertas y parches de sus	El acceso debe estar restringido para realizar cambios en los requisitos de etiquetado predeterminados de AMS para cualquier persona que

Estándares	¿Se rompe	Riesgos	Recomendaciones
AMS, distintas de las enumeradas anteriormente, deben tener prefijos iguales o iguales a mayúsculas y minúsculas. `AMS*` `MC*` upper/lower/mix	`aws:TagsKey` condición de restringir el etiquetado en el espacio de nombres AMS. CloudTrail El estándar que aparece a continuación en la tabla AMS-STD-003 establece que se puede cambiar AppId el entorno y, pero no los recursos que son propiedad de AMS. AppName No se puede lograr con los permisos de IAM.	recursos, por parte de AMS.	no sea un equipo de AMS.
No debes eliminar ninguna etiqueta de las pilas propiedad de AMS en función de tus solicitudes de cambio.	Sí. CloudFormation no admite la `aws:TagsKey` condición de restringir las etiquetas del espacio de nombres AMS.		

Estándares	¿Se rompe	Riesgos	Recomendaciones
No está permitido utilizar la convención de nomenclatura de etiquetas AMS en su infraestructura, tal y como se indica en la siguiente tabla AMS-STD-002.	Sí. Interrupciones para CloudFormation Amazon Elastic File System (EFS) OpenSearch, CloudWatch Logs, Amazon Simple Queue Service (SQS), Amazon EC2 Systems Manager (SSM) y Tagging API; estos servicios no `aws:TagsKey` admiten la condición de restringir el etiquetado en el espacio de nombres AMS. CloudTrail		

AMS-STD-002: Identity and Access Management (IAM) MexiAM)

Estándares	¿Se rompe	Riesgos	Recomendaciones
4.7 No se deben permitir acciones que eludan el proceso de administración de cambios (RFC), como iniciar o detener una instancia, crear buckets de S3 o instancias de RDS, etc. Las cuentas en modo desarroll	Sí. El objetivo de las acciones de autoservicio es permitir realizar acciones sin tener en cuenta el sistema RFC de AMS.	El modelo de acceso seguro es una faceta técnica fundamental de AMS, y un usuario de IAM para el acceso programático o mediante consola elude este control de acceso. El sistema de gestión de cambios de AMS no supervisa	El usuario de IAM debe tener un límite de tiempo y concederse los permisos en función del mínimo privilegio y. need-to-know

Estándares	¿Se rompe	Riesgos	Recomendaciones
ador y los servicios en modo aprovisionado de autoservicio (SSPS) están exentos siempre que las acciones se realicen dentro de los límites de la función asignada.		el acceso de los usuarios de IAM. CloudTrail Solo se inicia sesión en el acceso.	

AMS-STD-003: Seguridad de red

Estándares	¿Se rompe	Riesgos	Recomendaciones
S2. La IP elástica en EC2 las instancias solo debe usarse con un acuerdo formal de aceptación del riesgo o con un caso de uso válido por parte de los equipos internos.	Sí. Las acciones de autoservicio permiten asociar y desasociar direcciones IP elásticas (EIP).	Al agregar una IP elástica a una instancia, se expone a Internet. Esto aumenta el riesgo de divulgación de información y de actividad no autorizada.	Bloquee todo el tráfico innecesario que se dirija a esa instancia a través de grupos de seguridad y compruebe que sus grupos de seguridad estén asociados a la instancia para asegurarse de que solo permite el tráfico cuando sea necesario por motivos empresariales.
S14. Se pueden permitir el emparejamiento de VPC y las conexiones de punto final entre cuentas	Sí. No es posible mediante la política de IAM.	El tráfico que sale de su cuenta de AMS no se monitorea una vez que sale del límite de la cuenta.	Te recomendamos que realices el emparejamiento únicamente con las cuentas de AMS de tu propiedad. Si su caso

Estándares	¿Se rompe	Riesgos	Recomendaciones
que pertenecen al mismo cliente.			de uso lo requiere, utilice grupos de seguridad y tablas de enrutamiento para limitar los rangos, recursos y tipos de tráfico que pueden salir a través de la conexión correspon diente.
La base de AMS se AMIs puede compartir entre cuentas administradas y no administradas por AMS, siempre que podamos comprobar que pertenecen a la misma organización. AWS		AMIs puede contener datos confidenc iales y puede estar expuesto a cuentas no deseadas.	AMIs Compártel os únicamente con la cuenta que sea propiedad de tu organización o valida el caso de uso y la información de la cuenta antes de compartirlos con personas ajenas a la organización.

AMS-STD-007: Registro

Estándares	¿Se rompe	Riesgos	Recomendaciones
19. Cualquier registro se puede reenviar de una cuenta de AMS a otra cuenta de AMS del mismo cliente.	Sí. La política de IAM no permite verificar que las cuentas de los clientes pertenezcan a la misma organizac ión, ya que no es posible verificar que	Los registros pueden contener datos confidenciales y pueden estar expuestos a cuentas no deseadas.	Comparta los registros únicament e con las cuentas administradas por su AWS organización o valide el caso de uso y la información
20. Cualquier registro puede reenviars			

Estándares	¿Se rompe	Riesgos	Recomendaciones
e de AMS a una cuenta ajena a AMS únicamente si la cuenta ajena a AMS es propiedad del mismo cliente de AMS (confirmando que se encuentra bajo la misma AWS Organizations cuenta o haciendo coincidir el dominio de correo electrónico con el nombre de la empresa del cliente y la cuenta vinculada al PAGADOR) mediante herramientas internas.	las cuentas de los clientes pertenezcan a la misma organizac ión.		de la cuenta antes de compartirlos fuera de su organizac ión. Podemos verificarlo de varias maneras: consulte con su administrador de prestación de servicios en la nube (CSDM).

Trabaje con su equipo interno de autorización y autenticación para controlar en consecuencia los permisos de las funciones del modo Direct Change.

Cumplimiento en el modo Direct Change

El modo Direct Change es compatible con cargas de trabajo tanto de producción como de no producción. Es su responsabilidad garantizar el cumplimiento de cualquier norma de conformidad (por ejemplo, PHI, HIPAA o PCI) y asegurarse de que el uso del modo Direct Change cumpla con sus marcos y estándares de control interno.

Gestión de cambios en el modo Direct Change

La gestión de cambios es el proceso que AMS Advanced utiliza para implementar las solicitudes de cambio. Una solicitud de cambio (RFC) es una solicitud creada por usted o por AMS Advanced a través de la interfaz de AMS Advanced para realizar un cambio en su entorno gestionado e incluye

un identificador de cambio de tipo (CT) de AMS Advanced para una operación concreta. Para obtener más información, consulte Gestión de cambios.

> **Note**
>
> El modo Direct Change no elimina la administración de cambios de AMS RFCs, pero aún tiene acceso total a AMS RFCs con DCM.

El modo AMS Direct Change (DCM) amplía la gestión de cambios de AMS Advanced al proporcionar AWS acceso nativo a las cuentas AMS Advanced Plus y Premium para aprovisionar y actualizar AWS los recursos. Los usuarios a los que se les haya concedido el permiso del modo Direct Change a través de las funciones de IAM pueden utilizar el acceso a la AWS API nativa para aprovisionar y realizar cambios en los recursos de sus cuentas de AMS Advanced. Los usuarios pueden seguir RFCs utilizando la gestión de cambios avanzada de AMS con las mismas funciones de IAM. En ambos casos, AMS apoya plenamente los recursos y los cambios que se realicen en ellos, lo que incluye la supervisión, los parches, las copias de seguridad y la gestión de la respuesta a los incidentes. Los usuarios que no tengan la función adecuada en estas cuentas deben utilizar el proceso RFC de gestión avanzada de cambios de AMS para realizar cambios.

Casos de uso de la gestión de cambios

Por motivos de seguridad, algunos cambios en AMS Advanced solo se pueden realizar mediante el proceso de solicitud de cambio (RFC) de la administración de cambios. `AWSManagedServicesCloudFormationAdminRole`Se limita a las acciones realizadas mediante este procedimiento CloudFormation (CFN). Para obtener más información sobre cómo crear pilas mediante DCM, consulte Creación de pilas mediante el modo de cambio directo. `AWSManagedServicesUpdateRole`Está restringido a las siguientes acciones.

Para ver ejemplos de cada tipo de cambio, incluido el tipo de cambio Gestión | Cuenta gestionada | Modo de cambio directo | Habilitar (ct-3rd4781c2nnhp), consulte la sección «Información adicional» para ver el tipo de cambio correspondiente en la sección de AMS Advanced Change Type Reference Type Change Type Reference Type Change Tipos de Cambios por Clasificación.

Servicio	Acción
AWS Key Management Service (AWS KMS)	Actualización

Servicio	Acción
AWS Certificate Manager	Create
AWS Identity and Access Management (IAM)	Cualquiera
Site-to-Site VPN	Cualquiera
Programador de recursos AMS	
AWS Backup	Cree un plan de respaldo
Ingestión de carga de trabajo de AMS () WIGs	Cualquiera
Filtrado de salida AMS (gestionado por Palo Alto)	
Cambios en la cuenta de AMS Advanced MALZ	
Amazon GuardDuty	
Acceso avanzado a la pila a AMS	Cualquiera
Volumen de Amazon Elastic Block Store (EBS)	Eliminar
Cifrado predeterminado de Amazon Elastic Block Store (EBS)	Habilite el cifrado predeterminado
Amazon Elastic Compute Cloud (Amazon EC2)	Cambie el nombre de host
Imágenes de máquina de Amazon (AMI)	Eliminar, compartir
Grupo de EC2 seguridad de Amazon	Cualquiera
AMS Advanced SSPS	
AWS Microsoft AD gestionado	
Modo de desarrollador avanzado de AMS	
Amazon Simple Storage Service (Amazon S3)	Cree políticas de bucket de S3

Servicio	Acción
AWS Systems Manager	Create

Creación de pilas mediante el modo de cambio directo

Para que AMS pueda gestionar la pila`AWSManagedServicesCloudFormationAdminRole`, hay dos requisitos a la hora de lanzar pilas: CloudFormation

- La plantilla debe contener un`AmsStackTransform`.
- El nombre de la pila debe empezar por el prefijo `stack-` seguido de una cadena alfanumérica de 17 caracteres.

> **Note**
>
> Para utilizar correctamente el`AmsStackTransform`, debe reconocer que la plantilla de pila contiene la `CAPABILITY_AUTO_EXPAND` capacidad necesaria para que CloudFormation (CFN) cree o actualice la pila. Para ello, debes pasarla `CAPABILITY_AUTO_EXPAND` como parte de tu solicitud de creación de pila. CFN rechaza la solicitud si no se reconoce esta capacidad al incluirla en `AmsStackTransform` la plantilla. La consola CFN garantiza que superes esta capacidad si tienes la transformación en tu plantilla, pero es posible que no la utilices cuando interactúes con CFN a través de ella. APIs
> Debe utilizar esta función siempre que utilice las siguientes llamadas a la API de CFN:
>
> - CreateChangeSet
> - CreateStack
> - UpdateStack

Al crear o actualizar una pila con DCM, se realizan las mismas validaciones y ampliaciones de CFN Ingest y Stack Update CTs en la pila. Para obtener más información, consulte las pautas, mejores prácticas y limitaciones de la CloudFormation ingesta. La excepción a esto es que los grupos de seguridad predeterminados de AMS (SGs) no se adjuntarán a ninguna EC2 instancia independiente ni EC2 a ninguna instancia de los grupos de Auto Scaling (ASGs). Al crear la CloudFormation plantilla, con EC2 instancias independientes o bien ASGs, puede adjuntar la predeterminada. SGs

> **Note**
>
> Los roles de IAM ahora se pueden crear y administrar con. `AWSManagedServicesCloudFormationAdminRole`

De forma predeterminada, los AMS SGs tienen reglas de entrada y salida que permiten que las instancias se lancen correctamente y que las operaciones de AMS y usted puedan acceder a ellas más adelante mediante SSH o RDP. Si descubre que los grupos de seguridad predeterminados de AMS son demasiado permisivos, puede crear los suyos propios SGs con reglas más restrictivas y adjuntarlos a su instancia, siempre y cuando le permitan a usted y a las operaciones de AMS acceder a la instancia durante los incidentes.

Los grupos de seguridad predeterminados de AMS son los siguientes:

- SentinelDefaultSecurityGroupPrivateOnly: Se puede acceder a ellos en la plantilla CFN a través de este parámetro SSM `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: Se puede acceder a él en la plantilla CFN a través de este parámetro SSM `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

Transformación AMS

Añada una `Transform` declaración a su CloudFormation plantilla. Esto añade una CloudFormation macro que valida y registra la pila en AMS en el momento del lanzamiento.

Ejemplo de JSON

```
"Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  }
```

Ejemplo de YAML

```
Transform:
```

```
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

Agrega también la `Transform` declaración al actualizar la plantilla de una pila existente.

Ejemplo de JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
    "Transform": {
      "Name": "AmsStackTransform",
      "Parameters": {
        "StackId": {"Ref" : "AWS::StackId"}
     }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

Ejemplo de YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
```

```
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

Nombre de pila

El nombre de la pila debe empezar por el prefijo `stack-` seguido de una cadena alfanumérica de 17 caracteres. Esto es para mantener la compatibilidad con otros sistemas AMS que funcionan en la pila AMS. IDs

Los siguientes son ejemplos de formas de generar una pila compatible IDs:

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17  | %
 {[char]$_}) )
```

Casos de uso del modo de cambio directo

Los siguientes son casos de uso del modo de cambio directo:

Suministro y administración de recursos mediante CloudFormation

- Integre CloudFormation las herramientas y los procesos existentes.

Gestión y actualizaciones continuas de los recursos

- Pequeños cambios atómicos con bajo riesgo.
- Cambios que, de otro modo, se realizarían mediante una RFC manual o automática.
- Herramientas que requieren acceso a una AWS API nativa.
- La función de DCM se puede utilizar si se encuentra en la fase de migración. Los equipos de migración aprovechan los permisos del DCM para crear o modificar pilas.
- Las funciones de DCM se pueden utilizar en la CI/CD canalización para crear nuevas tareas AMIs, crear tareas de Amazon ECS, etc.

Modo AMS Advanced Developer

Temas

- Introducción al modo AMS Advanced Developer
- Seguridad y conformidad en el modo Desarrollador
- Gestión de cambios en modo Desarrollador
- Infraestructura de aprovisionamiento en modo AMS Developer
- Controles de Detective en el modo AMS Developer
- Registro, supervisión y gestión de eventos en el modo AMS Developer
- Gestión de incidentes en el modo AMS Developer
- Gestión de parches en el modo AMS Developer
- Gestión de la continuidad en el modo AMS Developer
- Gestión de seguridad y acceso en el modo AMS Developer

El modo Desarrollador de AWS Managed Services (AMS) utiliza permisos elevados en las cuentas AMS Advanced Plus y Premium para aprovisionar y actualizar los recursos de AWS fuera del proceso de administración de cambios de AMS Advanced. Para ello, el modo Desarrollador Avanzado de AMS aprovecha las llamadas a las API nativas de AWS dentro de la Nube Virtual Privada Avanzada (VPC) de AMS, lo que le permite diseñar e implementar infraestructuras y aplicaciones en su entorno gestionado.

Cuando se utiliza una cuenta que tiene activado el modo Desarrollador, se proporcionan la gestión de la continuidad, la gestión de parches y la gestión de cambios para los recursos aprovisionados mediante el proceso de gestión de cambios avanzada de AMS o mediante una Amazon Machine

Image (AMI) de AMS. Sin embargo, estas funciones de administración de AMS no se ofrecen para los recursos aprovisionados de forma nativa. AWS APIs

Usted es responsable de supervisar los recursos de infraestructura que se aprovisionan fuera del proceso avanzado de gestión de cambios de AMS. El modo desarrollador es compatible con cargas de trabajo de producción y de no producción. Con los permisos elevados, tiene una mayor responsabilidad a la hora de garantizar el cumplimiento de los controles internos.

> **Important**
>
> AMS Advanced solo puede gestionar los recursos que cree mediante el modo Desarrollador si se crean mediante los procesos de gestión de cambios de AMS Advanced.

El modo Desarrollador es uno de los modos AMS Advanced que puede emplear. Para obtener más información, consulte Descripción general de los modos.

Introducción al modo AMS Advanced Developer

Aprenda las distintas cuentas de AMS Advanced con el modo AMS Advanced Developer y cómo implementar correctamente el modo Developer.

Temas

- Antes de empezar con el modo AMS Developer
- Requisitos previos para el modo AMS Developer
- Cómo implementar el modo AMS Advanced Developer
- Permisos del modo AMS Advanced Developer

Antes de empezar con el modo AMS Developer

Antes de implementar el modo Desarrollador, hay algunas cosas que debe saber.

AMS Advanced no puede gestionar las pilas o los recursos existentes en una DevMode cuenta que se haya creado fuera del proceso de gestión de cambios de AMS Advanced mediante solicitudes de cambio (RFCs). Sin embargo, mientras la cuenta esté activa DevMode, AMS Advanced seguirá gestionando los recursos aprovisionados mediante el proceso de gestión de cambios de AMS Advanced con. RFCs

No puede empezar con una DevMode cuenta y convertirla posteriormente en una cuenta de aplicación gestionada por AMS Advanced.

Requisitos previos para el modo AMS Developer

Los siguientes son los requisitos previos para implementar el modo Desarrollador:

- Debe ser cliente de AMS Advanced y tener al menos una cuenta AMS Advanced Plus o Premium integrada.
- Cualquier cuenta que utilice debe ser una cuenta AMS Advanced Plus o Premium.
- Zona de destino multicuenta (MALZ): debe utilizar el rol `AWSManagedServicesDevelopmentRole` predefinido AWS Identity and Access Management (IAM). Solicita este rol. En la siguiente sección se describe cómo adquirir los permisos del modo Desarrollador.
- Zona de destino para una sola cuenta (SALZ): debes usar el rol `customer_developer_role` predefinido AWS Identity and Access Management (IAM). Solicita este rol. En la siguiente sección se describe cómo adquirir los permisos del modo Desarrollador.

Cómo implementar el modo AMS Advanced Developer

Para implementar el modo Desarrollador, solicite que a su cuenta de AMS Advanced que cumpla los requisitos se le asigne la función de IAM predefinida:

- MALZ: `AWSManagedServicesDevelopmentRole`
- SALZ: `customer_developer_role`

A continuación, asigne la función a los usuarios pertinentes de su red federada.

AMS Advanced le recomienda que se asegure de que el modo de desarrollador cumple con sus marcos y estándares de control interno, ya que el modo de desarrollador crea dos vectores de cambio: la gestión de cambios de AMS Advanced para los recursos gestionados por AMS Advanced y la federación de funciones gestionada por el cliente para los recursos que usted, como cliente nuestro, administra. Si bien los procesos de AMS Advanced siguen cumpliendo con nuestras declaraciones, es posible que sea necesario actualizar los procesos de los clientes y los marcos de control.

Para implementar el modo Desarrollador en tu cuenta de AMS Advanced

1. Confirme que la cuenta que quiere usar con el modo Desarrollador cumpla con los requisitos que se indican enRequisitos previos para el modo AMS Developer.
2. Envíe una solicitud de cambio (RFC) utilizando el tipo de cambio (CT) Gestión | Cuenta gestionada | Modo desarrollador | Activar (es necesario revisar). Para ver un ejemplo de cómo usar este CT, consulte Modo desarrollador | Habilitar (es necesario revisar).

   Una vez procesado el CT, la función de IAM predefinida (`AWSManagedServicesDevelopmentRole`para MALZ, **`customer_developer_role`** para SALZ) se aprovisiona en la cuenta solicitada.
3. Asigne la función adecuada a los usuarios que necesiten acceder al modo Desarrollador mediante su proceso de federación interno.

   AMS Advanced recomienda limitar el acceso para evitar el aprovisionamiento o los cambios en los recursos no deseados o no aprobados.

Permisos del modo AMS Advanced Developer

La función predefinida (`AWSManagedServicesDevelopmentRole`para MALZ o SALZ) otorga permiso `customer_developer_role` para crear recursos de infraestructura de aplicaciones dentro de la VPC avanzada de AMS, incluidas las funciones de IAM, al tiempo que restringe el acceso a los componentes de servicios compartidos que gestiona AMS Advanced (por ejemplo, hosts de administración, controladores de dominio, EPS de Trend Micro, bastiones y servicios de AWS no compatibles). El rol también restringe el acceso a los siguientes registros Servicios de AWS: Amazon GuardDuty AWS Organizations, AWS Directory Service APIs, y AMS Advanced.

Si bien el rol le permite crear roles de IAM adicionales, los mismos límites de permisos incluidos en el acceso en modo desarrollador se aplican a cualquier rol de IAM creado por el. `AWSManagedServicesDevelopmentRole`

Seguridad y conformidad en el modo Desarrollador

La seguridad y el cumplimiento son una responsabilidad compartida entre AMS Advanced y usted, como cliente nuestro. El modo de desarrollador avanzado de AMS le transfiere la responsabilidad compartida por los recursos aprovisionados fuera del proceso de gestión de cambios o aprovisionados mediante la gestión de cambios, pero actualizados con los permisos del modo de

desarrollador. Para obtener más información sobre la responsabilidad compartida, consulte AWS Managed Services.

Precauciones:

- DevMode le permite a usted y a su equipo autorizado eludir los deny-by-default principios fundamentales de la seguridad de AMS. Hay que sopesar las ventajas, el autoservicio y la reducción del tiempo de espera en el AMS y las desventajas: cualquiera puede realizar acciones inesperadas y destructivas sin el conocimiento de su equipo de seguridad. Se exponen los tipos de cambios automatizados para habilitar los modos Dev y Direct Change, y cualquier persona autorizada de su organización puede ejecutarlos CTs y habilitarlos.
- Usted es responsable de administrar los permisos de ejecución de CT desde su base de usuarios.
- AMS no administra los permisos de ejecución de CT

Recomendaciones:

- Proteja
  - Los clientes pueden impedir el acceso a este CT mediante permisos. Consulte las declaraciones de política sobre cómo restringir los permisos con las funciones de IAM
  - Impida el acceso a este CT implementando un proxy, como un sistema ITSM
  - Utilice políticas de control de servicios (SCPs) que eviten las políticas y los comportamientos según sea necesario, consulte la Biblioteca de Controles Preventivos y de Detectives de AMS
- Detectar
  - Supervise sus RFC para ver si se están ejecutando CTs (habilite el modo desarrollador ct-1opjmhuddw194 y el modo de cambio directo, habilite el ct-3rd4781c2nnhp) y responda en consecuencia
  - Revise y and/or audite sus cuentas para comprobar la presencia de los recursos de IAM e identificar las cuentas en las que se haya implementado el modo Desarrollador o el modo Direct Change
- Responda
  - Elimine las cuentas en el modo Desarrollador según sea necesario

Seguridad en el modo Desarrollador

AMS Advanced ofrece un valor adicional con una zona de aterrizaje obligatoria, un sistema de gestión de cambios y una gestión de acceso. Cuando se utiliza el modo Desarrollador, el valor de seguridad de AMS Advanced se mantiene utilizando la misma configuración de cuentas que las cuentas AMS Advanced estándar que establece la red básica reforzada de seguridad de AMS Advanced. La red está protegida por el límite de permisos establecido en el rol (`AWSManagedServicesDevelopmentRole`para MALZ, `customer_developer_role` para SALZ), lo que impide al usuario desglosar los parámetros de protección establecidos al configurar la cuenta.

Por ejemplo, los usuarios con ese rol pueden acceder a Amazon Route 53, pero la zona alojada interna de AMS Advanced está restringida. Los mismos límites de permisos se aplican a un rol de IAM creado por el`AWSManagedServicesDevelopmentRole`, lo `AWSManagedServicesDevelopmentRole` que impide que el usuario rompa las protecciones de parámetros establecidas cuando la cuenta se incorpora a AMS Advanced.

Cumplimiento en el modo Desarrollador

El modo desarrollador es compatible con cargas de trabajo tanto de producción como de no producción. Es su responsabilidad garantizar el cumplimiento de cualquier norma de conformidad (por ejemplo, PHI, HIPAA o PCI) y asegurarse de que el uso del modo de desarrollador cumpla con sus marcos y estándares de control interno.

Gestión de cambios en modo Desarrollador

La gestión de cambios es el proceso que utiliza el servicio AMS Advanced para implementar las solicitudes de cambio. Una solicitud de cambio (RFC) es una solicitud creada por usted o por AMS Advanced a través de la interfaz de AMS Advanced para realizar un cambio en su entorno gestionado e incluye un identificador de tipo de cambio (CT) para una operación concreta. Para obtener más información, consulte Modos de administración de cambios.

La gestión de cambios no se aplica en las cuentas de AMS Advanced, donde se conceden permisos en el modo Desarrollador. Los usuarios a los que se les haya concedido el permiso del modo Desarrollador con la función de IAM (`AWSManagedServicesDevelopmentRole`para MALZ, `customer_developer_role` para SALZ) pueden utilizar el acceso a la AWS API nativa para aprovisionar y realizar cambios en los recursos de sus cuentas de AMS Advanced. Los usuarios que no tengan la función adecuada en estas cuentas deben utilizar el proceso avanzado de gestión de cambios de AMS para realizar cambios.

> **Important**
>
> AMS Advanced solo puede gestionar los recursos que cree mediante el modo Desarrollador si se crean mediante los procesos de gestión de cambios de AMS Advanced. AMS Advanced rechaza las solicitudes de cambios enviadas a AMS Advanced para recursos creados fuera del proceso de gestión de cambios de AMS Advanced porque usted debe gestionarlas.

Restricciones de API de los servicios de aprovisionamiento de autoservicio

Todos los servicios autoaprovisionados de AMS Advanced son compatibles con el modo Desarrollador. El acceso a los servicios autoaprovisionados está sujeto a las limitaciones descritas en las respectivas secciones de la guía del usuario para cada uno de ellos. Si un servicio autoaprovisionado no está disponible con tu rol en el modo Desarrollador, puedes solicitar un rol actualizado mediante el tipo de cambio en el modo Desarrollador.

Los siguientes servicios no proporcionan acceso completo al servicio: APIs

Los servicios autoaprovisionados están restringidos en el modo de desarrollador

Servicio	Notas
Amazon API Gateway	Se permiten todas las APIs llamadas a Gateway, excepto. `SetWebACL`
Aplicación de escalado automático	Solo se pueden registrar o anular el registro de objetivos escalables y establecer o eliminar una política de escalado.
AWS CloudFormation	No se puede acceder ni modificar las CloudFormation pilas que tengan un nombre como prefijo. `mc-`
AWS CloudTrail	No se puede acceder ni modificar CloudTrai l los recursos que tienen un nombre con el prefijo. `ams-` and/or `mc-`
Amazon Cognito (grupos de usuarios)	No se pueden asociar los tokens de software.

Servicio	Notas
	No se pueden crear grupos de usuarios, trabajos de importación de usuarios, servidores de recursos ni proveedores de identidad.
AWS Directory Service	Los `WorkSpaces` servicios `Connect` y servicios solo requieren Directory Service las siguientes acciones. La política de límites de permisos del modo Desarrollador deniega todas las demás acciones de Directory Service: • `ds:AuthorizeApplication` • `ds:CreateAlias` • `ds:CreateIdentityPoolDirectory` • `ds:DeleteDirectory` • `ds:DescribeDirectories` • `ds:GetAuthorizedApplication Details` • `ds:ListAuthorizedApplications` • `ds:UnauthorizeApplication` En las cuentas de landing zone de una sola cuenta, la política de límites deniega explícita mente el acceso al directorio gestionado por AMS Advanced utilizado por AMS Advanced para mantener el acceso a las cuentas habilitad as para el modo dev.

Servicio	Notas
Amazon Elastic Compute Cloud	No puedo acceder a Amazon EC2 APIs que contenga la cadena: `DhcpOptio ns Gateway`,`Subnet`,`VPC`, y`VPN`. No puedo acceder ni modificar EC2 los recursos de Amazon que tengan una etiqueta con el prefijo`AMS`,, `mcManagementHostASG` , and/or `sentinel`.
Amazon EC2 (Informes)	Solo se concede el acceso de visualización (no se puede modificar). Nota: Amazon EC2 Reports se muda. El elemento de menú Informes se eliminará del menú de navegació n de la EC2 consola Amazon. Para ver tus informes EC2 de uso de Amazon después de eliminarlos, usa la consola AWS Billing y Cost Management.

Servicio	Notas
AWS Identity and Access Management (IAM)	No se pueden eliminar los límites de permisos existentes ni modificar las políticas de contraseñas de los usuarios de IAM. No puede crear ni modificar recursos de IAM a menos que utilice la función de IAM correcta (**`AWSManagedServicesDevelopmentRole`** para MALZ, **`customer_developer_role`** para SALZ). No se pueden modificar los recursos de IAM que tengan el prefijo:,,,. `ams` `mc` `customer_deny_policy` and/or `sentinel` Al crear un nuevo recurso de IAM (rol, usuario o grupo), se debe adjuntar el límite de permisos (MALZ:`AWSManagedServicesDevelopmentRolePermissionsBoundary` , SALZ:`ams-app-infra-permissions-boundary`).
AWS Key Management Service (AWS KMS)	No se pueden acceder ni modificar las claves de KMS administradas por AMS Advanced.
AWS Lambda	No se puede acceder ni modificar AWS Lambda las funciones que tienen el prefijo. `AMS`
CloudWatch Registros	No se puede acceder a las secuencias de CloudWatch registro con un nombre con el prefijo:`mc`,`aws`,`lambda`, and/or `AMS`.
Amazon Relational Database Service (Amazon RDS)	No se puede acceder ni modificar las bases de datos de Amazon Relational Database Service (Amazon RDS) DBs () que tengan un nombre con el prefijo:. `mc-`

Servicio	Notas
Grupos de recursos de AWS	Solo puede acceder a las acciones de la `Get` API `List` del grupo de `Search` recursos y al grupo de recursos.
Amazon Route 53	No se puede acceder ni modificar los recursos mantenidos por Route53 AMS Advanced.
Amazon S3	No se puede acceder a los buckets de Amazon S3 que tienen un nombre con el prefijo:`ams-*`, `amsms-a`, o. `mc-a`
AWS Security Token Service	La única API de servicio de token de seguridad permitida es. `DecodeAuthorizatio nMessage`
Amazon SNS	No puedo acceder a los temas de SNS que tengan un nombre con el prefijo:`AMS-`,`Energon-Topic` , o. `MMS-Topic`
AWS Systems Manager Administrador (SSM)	No se pueden modificar los parámetros del SSM que tienen el prefijo`ams`, `mc` o. `svc` No se puede usar la API `SendCommand` de SSM en EC2 instancias de Amazon que tengan una etiqueta con `ams` el prefijo o. `mc`
AWS Etiquetado	Solo tienes acceso a las acciones de la API de AWS etiquetado que tengan el prefijo. `Get`

Servicio	Notas
AWS Lake Formation	Se deniegan las siguientes acciones AWS Lake Formation de la API: • `lakeformation:DescribeResource` • `lakeformation:GetDataLakeSettings` • `lakeformation:DeregisterResource` • `lakeformation:RegisterResource` • `lakeformation:UpdateResource` • `lakeformation:PutDataLakeSettings`
Amazon Elastic Inference	Solo puedes llamar a la acción de la API de Elastic Inference. `elastic-inference:Connect` Este permiso está incluido en el `customer_sagemaker_admin_policy` que se adjunta a. `customer_sagemaker_admin_role` Esta acción le da acceso al acelerador de Elastic Inference.
AWS Shield	No tiene acceso a ninguno de estos servicios APIs ni a esta consola.
Amazon Simple Workflow Service	No hay acceso a ninguno de estos servicios APIs o consola.

Infraestructura de aprovisionamiento en modo AMS Developer

Los usuarios que no tengan la función de IAM en el modo DesarrolladorAWSManagedServicesDevelopmentRole, en las cuentas en las que el modo Desarrollador esté habilitado, deberán seguir el proceso de gestión de cambios de AMS Advanced, que utiliza AMS Advanced. AMIs Los usuarios con el rol correcto (MALZ:AWSManagedServicesDevelopmentRole, SALZ:customer_developer_role) pueden

usar el sistema de gestión de cambios AMS Advanced y AMS Advanced, AMIs pero no están obligados a hacerlo.

> **Note**
>
> Una AWS AMI que no se haya procesado mediante la ingesta de carga de trabajo de AMS Advanced o que no se haya creado en una cuenta de AMS Advanced no incluirá las configuraciones requeridas por AMS Advanced.

Controles de Detective en el modo AMS Developer

Esta sección se ha redactado porque contiene información confidencial relacionada con la seguridad de AMS. Esta información está disponible en la documentación de la consola AMS. Para acceder a AWS Artifact, puede ponerse en contacto con su CSDM para obtener instrucciones o ir a Introducción a AWS Artifact.

Registro, supervisión y gestión de eventos en el modo AMS Developer

El registro, la supervisión y la gestión de eventos no están disponibles para los recursos aprovisionados fuera del proceso avanzado de gestión de cambios de AMS, ni para los recursos aprovisionados mediante la gestión de cambios y luego modificados por una cuenta que utilice los permisos del modo Desarrollador.

Gestión de incidentes en el modo AMS Developer

Sin cambios en los tiempos de respuesta a los incidentes. La resolución de incidentes es lo mejor para los recursos aprovisionados fuera del proceso de gestión de cambios o para los recursos aprovisionados mediante la gestión de cambios y luego modificados por una cuenta que utiliza los permisos del modo de desarrollador.

> **Note**
>
> El acuerdo de nivel de servicio (SLA) de AMS no se aplica a los recursos creados o actualizados fuera del sistema de gestión de cambios de AMS (solicitudes de cambio o RFCs), incluido el modo desarrollador; por lo tanto, los recursos actualizados o creados en el modo desarrollador se degradan automáticamente a P3 y el soporte de AMS es lo mejor que se puede hacer.

Gestión de parches en el modo AMS Developer

La administración de parches no está disponible para los recursos aprovisionados fuera del proceso avanzado de gestión de cambios de AMS, ni para los recursos aprovisionados mediante la gestión de cambios y luego modificados por una cuenta que utilice los permisos del modo Desarrollador. Tiempos de aplicación de parches:

- En el caso de una actualización de seguridad crítica: en el plazo de 10 días laborables a partir de la publicación por parte del proveedor, en el caso de los recursos aprovisionados mediante la gestión de cambios y modificados posteriormente por una cuenta que utilice los permisos del modo Desarrollador.
- Para una actualización importante: en el plazo de 2 meses a partir de la publicación por parte del proveedor, para los recursos aprovisionados mediante la gestión de cambios y modificados posteriormente por una cuenta con permisos en el modo Desarrollador.

Gestión de la continuidad en el modo AMS Developer

La gestión de la continuidad no está disponible para los recursos aprovisionados fuera del proceso avanzado de gestión de cambios de AMS, ni para los recursos aprovisionados mediante la gestión de cambios y luego modificados por una cuenta que utilice los permisos del modo Desarrollador.

El tiempo de inicio de la recuperación del entorno puede tardar hasta 12 horas en el caso de los recursos aprovisionados fuera del proceso avanzado de gestión de cambios de AMS o en el caso de los recursos aprovisionados mediante la gestión de cambios y posteriormente modificados por una cuenta con permisos en el modo Desarrollador.

Gestión de seguridad y acceso en el modo AMS Developer

La protección antimalware recae en el caso de los recursos aprovisionados fuera del proceso avanzado de gestión de cambios de AMS o de los recursos aprovisionados mediante la gestión de cambios y posteriormente modificados por una cuenta que utilice los permisos del modo Desarrollador. El acceso a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) no aprovisionadas a través de AMS Advanced Change Management podría controlarse mediante pares de claves en lugar de proporcionar acceso federado.

Modo de aprovisionamiento de autoservicio en AMS

El modo Self-Service Provisioning (SSP) de AWS Managed Services (AMS) proporciona acceso total a las capacidades nativas de AWS servicio y API en las cuentas administradas por AMS. Puede acceder a los servicios mediante funciones estandarizadas y con un alcance reducido. AWS Identity and Access Management AMS proporciona solicitudes de servicio y gestión de incidentes. Las alertas, la supervisión, el registro, los parches, las copias de seguridad y la gestión de cambios son su responsabilidad. En muchos casos, los servicios de aprovisionamiento de autoservicio (SSPS) se autogestionan o no tienen servidor y no requieren la administración de determinadas tareas operativas, como la aplicación de parches. Puede utilizar estos servicios dentro de los límites del entorno definidos por las normas de protección de AMS, y cualquier cambio en la IAM (incluidas las funciones vinculadas a los servicios, las funciones de servicio, las funciones multicuentas o las actualizaciones de políticas) debe contar con la aprobación de AMS Operations para mantener la seguridad básica de la plataforma. Puede utilizar CloudFormation las plantillas para automatizar la implementación de estos servicios, pero esto no es compatible con todos los servicios del SSP.

> **Important**
>
> Utilice el modo SSP en sus cuentas de AWS Managed Services (AMS) para acceder a AWS los servicios y utilizarlos, con las restricciones indicadas.

Hay algunas Servicios de AWS que puede utilizar sin la administración de AMS, en su cuenta de AMS. En esta sección se describen los servicios del modo de aprovisionamiento de autoservicio (o SSPS, por sus siglas en inglés), cómo añadirlos a tu cuenta AMS y FAQs para cada uno de ellos.

Los servicios de aprovisionamiento de autoservicio se ofrecen tal cual y usted es responsable de administrarlos. AMS no proporciona alertas, supervisión, registro ni parches para los recursos asociados a esos servicios. AMS proporciona funciones de IAM que le permiten utilizar el servicio de su cuenta de AMS de forma segura. Los AMS SLAs no se aplican.

En el caso de los recursos que usted aprovisiona mediante el autoservicio, AMS proporciona servicios de gestión de incidentes, controles de detección y vigilancia, elaboración de informes, recursos específicos (administrador de prestación de servicios en la nube y arquitecto de nube), seguridad y acceso, y asistencia técnica en caso de solicitudes de servicio. Además, cuando proceda, usted asume la responsabilidad de gestionar la continuidad, los parches, la supervisión de la infraestructura y la gestión de los cambios de los recursos aprovisionados o configurados fuera del sistema de gestión de cambios de AMS.

Cómo empezar con el modo SSP en AMS

El aprovisionamiento de autoservicio es uno de los modos AMS para multi-account landing zone (MALZ) que puede emplear. Para obtener más información, consulte Descripción general de los modos.

Para ofrecer capacidades de aprovisionamiento de autoservicio, AMS ha creado funciones de IAM más exigentes con límites de permisos para limitar los cambios imprevistos derivados del acceso directo. Servicio de AWS Las funciones no impiden todos los cambios, por lo que debes cumplir con tus controles internos y tus políticas de conformidad, además de comprobar que todo lo que utilices cumpla con las Servicios de AWS certificaciones exigidas. Este es el modo de aprovisionamiento de autoservicio. Para obtener más información sobre los requisitos AWS de conformidad, consulte AWS Cumplimiento.

Para añadir un servicio de aprovisionamiento de autoservicio a su cuenta de aplicación multicuenta en la zona de landing zone, utilice Management | AWS service | Self-provisioned service | Add change type (CT), ya sea el CT que requiere revisión o el CT automatizado, según las instrucciones del servicio.

> **Note**
>
> Para solicitar que AMS proporcione un servicio de autoaprovisionamiento adicional, presente una solicitud de servicio.

Utilice AMS SSP para aprovisionar Amazon API Gateway en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon API Gateway directamente en su cuenta gestionada por AMS. Amazon API Gateway es un servicio totalmente gestionado que facilita a los desarrolladores la creación, publicación, mantenimiento, supervisión y protección APIs a cualquier escala. Con ellos, Consola de administración de AWS puede crear REST y WebSocket APIs que actúen como puerta de entrada para que las aplicaciones accedan a los datos, la lógica empresarial o la funcionalidad de sus servicios de back-end, como las cargas de trabajo que se ejecutan en Amazon Elastic Compute Cloud (Amazon EC2), el código que se ejecuta en él AWS Lambda, cualquier aplicación web o aplicaciones de comunicación en tiempo real.

API Gateway gestiona todas las tareas relacionadas con la aceptación y el procesamiento de hasta cientos de miles de llamadas simultáneas a la API, incluida la gestión del tráfico, la autorización y el control de acceso, la supervisión y la gestión de las versiones de la API. API Gateway no tiene tarifas mínimas ni costes de puesta en marcha. Solo paga por las llamadas a la API que recibe y la cantidad de datos transferidos y, con el modelo de precios por niveles de API Gateway, puede reducir sus costos a medida que aumenta el uso de la API. Para obtener más información, consulte Amazon API Gateway.

Preguntas frecuentes: API Gateway en AMS

P: ¿Cómo solicito acceso a Amazon API Gateway en mi cuenta de AMS?

Solicite acceso a API Gateway enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones de IAM a su cuenta: y. `customer_apigateway_author_role` `customer_apigateway_cloudwatch_role` Una vez aprovisionados en su cuenta, debe incorporar los roles a su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon API Gateway en mi cuenta de AMS?

- La configuración de API Gateway se limita a los recursos sin `AMS-` `MC-` prefijos para evitar cualquier modificación en la infraestructura de AMS.
- `CREATE`los privilegios para VPCLink están deshabilitados para evitar la creación no regulada de Elastic Load Balancers. VPCLinks Si es necesario, consulte Application Load Balancer | Create.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon API Gateway en mi cuenta de AMS?

Depende del tipo de API Gateway que desee implementar. Puede ser un servicio independiente, pero también puede solicitar acceso a los servicios existentes (por ejemplo, el balanceador de carga de red).

Usa AMS SSP para aprovisionar Alexa for Business en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Alexa for Business directamente en su cuenta gestionada por AMS. Alexa for Business es un servicio que permite a su organización y a sus empleados utilizar Alexa para realizar más tareas. Con Alexa for Business, puedes usar Alexa como tu asistente inteligente para ser más productivo en las salas de reuniones, en tu escritorio e incluso con los dispositivos Alexa que ya usas en casa o

cuando viajas. Los administradores de TI e instalaciones pueden usar Alexa for Business para medir y aumentar el uso de las salas de reuniones existentes en su lugar de trabajo.

Para obtener más información, consulta Alexa for Business.

Preguntas frecuentes sobre Alexa for Business en AWS Managed Services

P: ¿Cómo solicito acceso a Alexa for Business en mi cuenta de AMS?

Para solicitar acceso, envíe un formulario de administración | AWS servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_alexa_console_role` siguiente función de IAM a su cuenta:. También `customer_alexa_device_setup_user` se creó A para la herramienta de configuración de dispositivos proporcionada por Alexa for Business; esta herramienta de configuración de dispositivos se puede utilizar posteriormente para configurar sus dispositivos. Una vez aprovisionadas en tu cuenta, debes incorporar las funciones a tu solución de federación.

La puerta de enlace Alexa for Business le permite conectar Alexa for Business a sus terminales Cisco Webex y Poly Group Series para controlar las reuniones con la voz. El software de puerta de enlace se ejecuta en el hardware local y envía por proxy de forma segura las directivas de conferencia de Alexa for Business a su terminal Cisco. La puerta de enlace necesita dos pares de AWS credenciales para comunicarse con Alexa for Business. Ofrecemos dos usuarios de IAM de acceso limitado: `customer_alexa_gateway_installer_user` y `customer_alexa_gateway_execution_user` para las puertas de enlace de Alexa for Business, uno para instalar la puerta de enlace y otro para operar la puerta de enlace; se pueden solicitar enviando una RFC con el tipo de cambio Deployment | Advanced stack components | Identity and Access Management (IAM) | Crear entidad o política (es necesario revisar) el tipo de cambio (ct-3dpd8mdd9jn1r).

> **Note**
>
> Para generar informes de uso y enviarlos a Amazon S3, especifique el nombre del bucket de Amazon S3 en la RFC del servicio de autoaprovisionamiento.

P: ¿Cuáles son las restricciones para usar Alexa for Business en mi cuenta de AMS?

No hay restricciones. La funcionalidad completa de Alexa for Business está disponible con la función de servicio de autoaprovisionamiento de Alexa for Business.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Alexa for Business en mi cuenta de AMS?

- Si piensa utilizar una red Wi-Fi WPA2 empresarial para configurar sus dispositivos compartidos, especifique este tipo de seguridad de red en la herramienta de configuración del dispositivo, para lo cual AWS Private Certificate Authority es necesaria una.
- AMS solo crea claves secretas que comienzan con el espacio de nombres «A4B». Esto es restrictivo solo para este espacio de nombres.

P: ¿Qué funciones de Alexa for Business requieren por separado RFCs?

Para registrar un dispositivo Alexa Voice Service (AVS) en Alexa for Business, proporciona acceso al fabricante de dispositivos integrado de Alexa. Para ello, es necesario crear un rol de IAM en la consola de Alexa for Business que se pueda implementar mediante el tipo de cambio Management | Other | Other. Esto permite al fabricante de dispositivos AVS registrar y gestionar dispositivos con Alexa for Business en tu nombre.

Usa AMS SSP para aprovisionar Amazon AppStream 2.0 en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de Amazon AppStream 2.0 (AppStream 2.0) directamente en su cuenta gestionada por AMS. AppStream La versión 2.0 le permite trasladar sus aplicaciones de escritorio a ellas sin tener que volver a AWS escribirlas. Puede instalar sus aplicaciones en la AppStream versión 2.0, establecer configuraciones de inicio y poner sus aplicaciones a disposición de los usuarios. AppStream La versión 2.0 ofrece una amplia selección de opciones de máquinas virtuales para que pueda seleccionar el tipo de instancia que mejor se adapte a los requisitos de su aplicación y configurar los parámetros de escalado automático para que pueda satisfacer fácilmente las necesidades de sus usuarios finales. AppStream La versión 2.0 le permite lanzar aplicaciones en su propia red, lo que significa que las aplicaciones pueden interactuar con AWS los recursos existentes.

Amazon AppStream 2.0 le permite instalar, probar y actualizar sus aplicaciones de forma rápida y sencilla mediante el generador de imágenes. Se admite cualquier aplicación que se ejecute en Microsoft Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019 y no es necesario realizar ninguna modificación. Una vez finalizadas las pruebas, puede establecer las configuraciones de inicio de la aplicación, la configuración de usuario predeterminada y publicar la imagen para que los usuarios puedan acceder a ella.

Para obtener más información, consulte AppStream 2.0.

AppStream Preguntas frecuentes sobre la versión 2.0 en AWS Managed Services

P: ¿Cómo solicito el acceso a la AppStream versión 2.0 en mi cuenta de AMS?

Para solicitar el acceso a la AppStream versión 2.0, envíe una RFC junto con la dirección Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añada (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC asigna `customer_appstream_console_role` la siguiente función de IAM a su cuenta:.

A también `customer_appstream_stream_role` se implementa para transmitir aplicaciones que requieren que los usuarios se autentiquen con sus credenciales de inicio de sesión de Active Directory.

Una vez aprovisionadas en su cuenta, debe incorporar las funciones a su solución de federación.

P: ¿Cuáles son las restricciones para usar la AppStream versión 2.0 en mi cuenta de AMS?

- El equipo de soporte de AMS debe configurar la siguiente funcionalidad y requiere requisitos específicos RFCs. Las instrucciones sobre cómo solicitar funciones adicionales se encuentran en la sección 4.
  - Creación y transmisión desde puntos finales de VPC de interfaz.
  - Support para los puntos de enlace de Amazon S3 para la persistencia de carpetas de inicio y aplicaciones configurando la persistencia en una red privada.
  - Crear y elegir el rol de IAM que estará disponible en todas las instancias de streaming de la flota.
  - Unir flotas AppStream 2.0 y creadores de imágenes a los dominios de Microsoft Active Directory.
  - Creación de informes de uso personalizados AppStream 2.0.
  - Actualmente, no se admite la personalización de marca.

P: ¿Cuáles son los requisitos previos o las dependencias para usar la AppStream versión 2.0 en mi cuenta de AMS?

Al enviar el RFC a onboard AppStream 2.0, incluye el nombre del bucket de Amazon S3 que se utilizará en el informe de uso de AppStream 2.0. El nombre del bucket se añade al `customer-appstream-usagereports-policy` que se crea al incorporar la AppStream versión 2.0.

P: ¿Qué funcionalidad AppStream 2.0 requiere ser independiente? RFCs

- Para elegir un punto de enlace de VPC de interfaz para AppStream 2.0, envíe un RFC de tipo de cambio de administración | Otros | Otros | Actualice para crear un punto de enlace de VPC en su cuenta. Para ver los pasos para crear puntos de conexión personalizados para la AppStream versión 2.0, consulte Creación y transmisión desde puntos de conexión de VPC de la interfaz en AppStream la guía del usuario de la versión 2.0.
- La compatibilidad con los puntos de enlace de Amazon S3 para las carpetas principales y la persistencia de la configuración de aplicaciones en una red privada se puede configurar solicitando los puntos de enlace de la VPC de Amazon S3 con una RFC de administración | Otros | Otros | Crear tipo de cambio. La RFC debe incluir el bucket de Amazon S3 de destino que aloja el contenido de la carpeta de inicio o la configuración de la aplicación (buckets de Amazon S3, respectivamente). Esta RFC proporcionará a la AppStream versión 2.0 los permisos que necesita para acceder a los puntos de enlace de VPC de Amazon S3. Para ver los pasos para crear puntos de enlace personalizados para las transmisiones, consulte Uso de puntos de enlace de VPC de Amazon S3 para la persistencia de carpetas de inicio y configuración de aplicaciones en AppStream la guía del usuario de 2.0.
- Para crear y elegir un rol de IAM que esté disponible en todas las instancias de streaming de la flota, envíe un RFC de implementación | Advanced stack components | Identity and Access Management (IAM) | Crear entidad o política (es necesario revisar) tipo de cambio (ct-3dpd8mdd9jn1r) solicitando el rol de IAM con la política requerida. El nombre del rol de IAM siempre debe empezar con el prefijo: «customer_appstream».
- Las flotas y los creadores de imágenes de Amazon AppStream 2.0 se pueden unir a los dominios de Microsoft Active Directory enviando un RFC de tipo de cambio de Management | Other | Other | Update para la creación de la cuenta de servicio en Active Directory (AD). Los permisos mínimos necesarios para unirse a Microsoft Active Directory se definen en la documentación de la AppStream versión 2.0, en Concesión de permisos para crear y administrar objetos de equipo de Active Directory.
- Para crear informes de uso de la AppStream versión 2.0 personalizados, envíe una RFC de administración | Otros | Otros | Crear tipo de cambio solicitando lo siguiente:
  - «AppStreamUsageReports" Creación de una pila CFN
  - Se debe aprovisionar «customer_appstream_usagereports_role» en la cuenta
  - Además, proporciona los siguientes detalles:
    - Proporcione la expresión CRON para programar la ejecución de Crawler. De forma predeterminada, son las 23:00 UTC todos los días.
    - El ARN del bucket de Amazon S3 se utilizará en los resultados de las consultas de Athena. Este bucket debe tener el prefijo: `aws-athena-query-results`

- El ARN del bucket de Amazon S3 para los registros de informes de uso AppStream 2.0.

Una vez aprovisionado el rol, incorpore el rol a su solución de federación e inicie sesión y, a continuación, acceda a AWS GlueAWS Glue Athena para generar informes personalizados mediante el rol de informe de uso. Para obtener más información sobre el uso de los informes de uso de la AppStream versión 2.0, consulte Crear informes personalizados y analizar los datos de uso de la AppStream versión 2.0, en la documentación de la AppStream versión 2.0.

Utilice AMS SSP para aprovisionar Amazon Athena en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon Athena (Athena) directamente en su cuenta gestionada por AMS. Athena es un servicio de consultas interactivo que le ayuda a analizar datos en Amazon S3 mediante SQL estándar. Athena no requiere un servidor, por lo que no hay una infraestructura para administrar y solo pagará por las consultas que ejecute. Señala sus datos en Amazon S3, define el esquema y comienza a realizar consultas con SQL estándar. La mayoría de los resultados se obtienen en cuestión de segundos. Con Athena, no es necesario realizar tareas complejas extract-transform-load (ETL) para preparar los datos para el análisis. Esto hace que sea fácil para cualquier persona con conocimientos de SQL analizar rápidamente conjuntos de datos a gran escala. Para obtener más información, consulte Amazon Athena.

Preguntas frecuentes: Athena en AMS

P: ¿Cómo solicito acceso a Amazon Athena en mi cuenta de AMS?

Solicite acceso a Athena enviando un RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC asigna la `customer_athena_console_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Athena en mi cuenta de AMS?

No hay restricciones. Todas las funciones de Amazon Athena están disponibles en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon Athena en mi cuenta de AMS?

Athena depende en gran medida del AWS Glue servicio, ya que utiliza los datos catalog/metastore creados con él. AWS Glue Por lo tanto, AWS Glue los permisos se incluyen en el exitoso RFC de Athena.

El rol `customer_athena_console_role` tiene un requisito previo para un bucket de Amazon S3. Para crear un nuevo bucket, utilice el CT automatizado `ct-1a68ck03fn98r` (Implementación | Componentes de pila avanzados | Almacenamiento S3 | Creación). Cuando utilice este CT automatizado para crear un depósito de S3 para Athena, el nombre del depósito debe empezar por un prefijo. `athena-query-results-*`

Utilice AMS SSP para aprovisionar Amazon Bedrock en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de Amazon Bedrock directamente en su cuenta gestionada por AMS. Amazon Bedrock es un servicio totalmente gestionado que hace que los modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA AWS estén disponibles para su uso a través de una API unificada. Puede elegir entre una amplia gama de modelos fundacionales para encontrar el modelo que mejor se adapte a su caso de uso. Amazon Bedrock también ofrece un amplio conjunto de capacidades para desarrollar aplicaciones de IA generativa con seguridad, privacidad e IA responsable. Con Amazon Bedrock, puede experimentar y evaluar fácilmente los principales modelos fundacionales para sus casos de uso, personalizarlos de forma privada con sus datos mediante técnicas como el microajuste y la generación aumentada de recuperación (RAG) y crear agentes que ejecuten tareas con los sistemas y los orígenes de datos de su empresa.

Con la experiencia sin servidor de Amazon Bedrock, puede empezar rápidamente, personalizar de forma privada los modelos básicos con sus propios datos e integrarlos e implementarlos de forma fácil y segura en sus aplicaciones mediante las herramientas de AWS sin tener que gestionar ninguna infraestructura. Para obtener más información, consulte Amazon Bedrock.

Preguntas frecuentes: Amazon Bedrock en AMS

P: ¿Cómo solicito acceso a Amazon Bedrock en mi cuenta de AMS?

Para solicitar acceso a Amazon Bedrock, envíe una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (es necesario revisar) (ct-3qe6io8t6jtny). Este RFC asigna `customer_bedrock_console_role` la siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Bedrock en mi cuenta de AMS?

- Las bases de conocimiento de Amazon Bedrock no se admiten de forma predeterminada como parte de la función de SSPS debido a que dependen de Amazon OpenSearch Service Serverless, que actualmente no es compatible con AMS.
- Bedrock Studio no es compatible debido a que depende de servicios no compatibles, como Amazon. DataZone

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon Bedrock en mi cuenta de AMS?

- Las suscripciones de modelos de terceros que requieren AWS Marketplace permisos deben realizarse con el rol predeterminado (`AWSManagedServicesAdminRole`en MALZ y `Customer_ReadOnly_Role` SALZ). Esto se debe a que el rol predeterminado incluye AWS Marketplace los permisos.
- Si se utiliza el cifrado de datos, debe proporcionar la AWS KMS clave ARN cuando solicite la creación del rol de consola. Además, el bucket de Amazon S3 en uso debe incluir «bedrock» en su nombre.

Usa AMS SSP para aprovisionar Amazon CloudSearch en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a CloudSearch las capacidades de Amazon directamente en su cuenta gestionada por AMS. Amazon CloudSearch es un servicio gestionado en la AWS nube que utilizas de forma rentable para configurar, gestionar y escalar una solución de búsqueda para tu sitio web o aplicación. Amazon CloudSearch admite 34 idiomas y funciones de búsqueda populares, como el resaltado, la función de autocompletar y la búsqueda geoespacial. Para obtener más información, consulta Amazon CloudSearch.

> **Note**
>
> AWS ha cerrado el acceso de nuevos clientes a Amazon CloudSearch a partir del 25 de julio de 2024. Los clientes CloudSearch actuales de Amazon pueden seguir utilizando el servicio con normalidad. AWS sigue invirtiendo en mejoras de seguridad, disponibilidad y rendimiento para Amazon CloudSearch, pero no tenemos previsto introducir nuevas funciones.
> Para entender las diferencias entre Amazon CloudSearch y Amazon OpenSearch Service, y cómo puedes realizar la transición a OpenSearch Service, ponte en contacto con tu arquitecto de nube (CA) para que te asesore. Para obtener más información sobre la

transición al OpenSearch servicio, consulte Transición del servicio Amazon CloudSearch al OpenSearch servicio Amazon Service.

Preguntas frecuentes sobre Amazon CloudSearch en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon CloudSearch en mi cuenta de AMS?

Solicita acceso a Amazon CloudSearch enviando un RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones de IAM a su cuenta: y. `customer_csearch_admin_role` `customer_csearch_dev_role` Una vez aprovisionado en tu cuenta, debes incorporar el rol a tu solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon CloudSearch en mi cuenta de AMS?

Todas las funciones de Amazon CloudSearch están disponibles en tu cuenta AMS. Amazon admite actualmente todas las soluciones de bases de datos compatibles con AMS. CloudSearch Tenga en cuenta que, actualmente, DynamoDB es la única solución de base de datos AWS gestionada que no se puede indexar.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon CloudSearch en mi cuenta de AMS?

Amazon CloudSearch depende de que Amazon S3 colabore con los proveedores de identidad para analizar automáticamente los datos de entrada y determinar los campos de la tabla. El acceso a Amazon S3 no se proporciona con esta RFC y debe solicitarse por separado en una solicitud de servicio.

Utilice AMS SSP para aprovisionar Amazon CloudWatch Synthetics en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las funciones de Amazon Synthetics CloudWatch directamente en su cuenta gestionada por AMS. Puede usar Amazon CloudWatch Synthetics para crear «canarios» para monitorear sus puntos de conexión y. APIs

Los canarios son scripts configurables, escritos en Node.js o Python, que se ejecutan según una programación. Crean funciones de Lambda en la cuenta que usan Node.js o Python como marco. Los canaries funcionan a través de protocolos HTTP y HTTPS. Los canarios comprueban la disponibilidad y la latencia de los puntos finales y pueden almacenar datos sobre el tiempo de carga

y capturas de pantalla de la interfaz de usuario. Supervisan tu REST y el contenido de tu sitio web APIs URLs, y pueden comprobar si hay cambios no autorizados derivados de la suplantación de identidad, la inyección de código o la creación de scripts entre sitios.

Los canarios siguen las mismas rutas y realizan las mismas acciones que un cliente, lo que te permite verificar continuamente la experiencia de tus clientes incluso cuando no hay tráfico de clientes en tus aplicaciones. Mediante el uso de canaries, puede descubrir problemas antes de que sus clientes lo hagan. Para obtener más información, consulte Amazon CloudWatch: uso de la monitorización sintética.

Preguntas frecuentes CloudWatch sobre Amazon Synthetics en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon CloudWatch Synthetics en mi cuenta de AMS?

Solicite acceso a Amazon CloudWatch Synthetics enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC asigna la siguiente función de IAM a su cuenta: «customer_cw_synthetics_console_role» y «customer_cw_synthetics_canary_lambda_role». Una vez aprovisionada en su cuenta, debe incorporar la función «customer_cw_synthetics_console_role» a su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon CloudWatch Synthetics en mi cuenta de AMS?

No hay restricciones para el uso de Amazon CloudWatch Synthetics en su cuenta de AMS. Está prohibido crear roles para canarios fuera del rol de servicio proporcionado por AMS, «customer_cw_synthetics_canary_lambda_role».

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon CloudWatch Synthetics en mi cuenta de AMS?

Los canarios crean y utilizan un bucket Amazon CloudWatch Synthetics S3 predeterminado: cw-syn-results "*${accountnumber}*- -» *${default-region}*

Utilice AMS SSP para aprovisionar grupos de usuarios de Amazon Cognito en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de los grupos de usuarios de Amazon Cognito directamente en su cuenta gestionada por AMS. Los grupos de usuarios de Amazon Cognito proporcionan un directorio de usuarios seguro que se amplía a cientos de millones de usuarios. Al tratarse de un servicio totalmente gestionado, los

grupos de usuarios de Amazon Cognito se pueden configurar sin tener que preocuparse por el mantenimiento de la infraestructura de servidores. Este servicio le permite administrar un grupo de usuarios finales que puede utilizar para integrarlos con sus aplicaciones internas. Este servicio le ofrece una alternativa a una base de datos personalizada o a un directorio de usuarios finales para aplicaciones web o móviles. Al mismo tiempo, los grupos de usuarios de Amazon Cognito proporcionan el conjunto completo de funcionalidades de un servicio de directorio, como las políticas de contraseñas, la autenticación multifactor, la recuperación de contraseñas y el registro automático en los servicios. También permite a la aplicación federar el acceso en otros servicios públicos populares como OpenID, Facebook, Amazon o Google.

Amazon Cognito se divide en dos productos principales. Grupos de usuarios de Amazon Cognito y Amazon Cognito Identity Provider. Esta sección se centra en los grupos de usuarios de Amazon Cognito, que proporcionan acceso a otros AWS servicios, como Amazon S3 o DynamoDB. El servicio le permite utilizar grupos de usuarios de Amazon Cognito o un proveedor de identidad externo para proporcionar acceso a AWS los servicios. También proporciona acceso a los AWS servicios mediante el acceso de invitados anónimos. Debido a la poderosa naturaleza de los grupos de usuarios de Amazon Cognito, se administraría manualmente como un case-by-case servicio manual de operaciones, a fin de evitar posibles violaciones de seguridad en la cuenta. Para obtener más información, consulte Grupos de usuarios de Amazon Cognito.

Preguntas frecuentes sobre los grupos de usuarios de Amazon Cognito en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a los grupos de usuarios de Amazon Cognito en mi cuenta de AMS?

La implementación de los grupos de usuarios de Amazon Cognito en AMS es un proceso de dos pasos:

1. Envíe un tipo de cambio de Management | Other | Other | Create (ct-1e1xtak34nx76) y solicite la creación de los grupos de usuarios de Amazon Cognito en su cuenta de AMS. Incluya la siguiente información:
   - AWS Región.
   - Nombre del grupo de usuarios de Cognito.
   - Si deseas utilizar el Amazon Simple Email Service (Amazon SES) para enviar mensajes y notificaciones en lugar del servicio de correo interno predeterminado de Cognito, el cliente debe proporcionar una dirección de correo electrónico ya validada para el Servicio Amazon SES en

la cuenta. Esta dirección se utilizará para los campos «De» y «RESPONDER A» del mensaje. También deben indicar la región en la que se activó Amazon SES (us-east-1, eu-west-1 o us-west-2).

- Si deseas utilizar los mensajes SMS como contraseñas de un solo uso y para la verificación, el cliente debe indicarlo.

2. Solicite el acceso de los usuarios enviando un mensaje de administración | AWS servicio | Servicio autoaprovisionado | Añadir tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones de IAM a su cuenta: y. `customer_cognito_admin_role` `customer_cognito_importjob_role` Una vez aprovisionado en tu cuenta, debes incorporar el rol a tu solución de federación. Estas funciones le permiten gestionar los grupos de usuarios de Amazon Cognito, gestionar los usuarios y grupos del grupo, crear trabajos de importación para los usuarios, modificar los mensajes de notificación y suscripción, asociar aplicaciones al grupo de usuarios, autogestionar la adición de servicios de federación al grupo y eliminar los grupos ya creados.

P: ¿Cuáles son las restricciones para usar los grupos de usuarios de Amazon Cognito en mi cuenta de AMS?

No podrá crear los grupos de usuarios de Amazon Cognito. Esa acción requiere la creación de funciones de IAM para aprovechar los servicios que utiliza Amazon Cognito, como Amazon SES y Amazon Simple Notification Service (Amazon SNS).

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar los grupos de usuarios de Amazon Cognito en mi cuenta de AMS?

Si desea utilizar Amazon SES para enviar mensajes y notificaciones por correo electrónico a sus grupos de usuarios, estos ya deben activar el servicio Amazon SES en la cuenta y validar la dirección de correo electrónico que debe utilizarse en los campos «DE» y «RESPONDER» de los correos electrónicos enviados. Para obtener más información sobre la validación de direcciones de correo electrónico con Amazon SES, consulte Verificación de direcciones de correo electrónico en Amazon SES.

Utilice AMS SSP para aprovisionar Amazon Comprehend en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de Amazon Comprehend directamente en su cuenta gestionada por AMS. Amazon Comprehend es

un servicio de procesamiento del lenguaje natural (PNL) que utiliza el aprendizaje automático para encontrar información y relaciones en el texto, sin necesidad de tener experiencia en aprendizaje automático. Amazon Comprehend utiliza el aprendizaje automático para ayudarlo a descubrir la información y las relaciones en sus datos no estructurados. El servicio identifica el idioma del texto; extrae frases clave, lugares, personas, marcas o eventos; comprende qué tan positivo o negativo es el texto; analiza el texto mediante la tokenización y partes del discurso; y organiza automáticamente una colección de archivos de texto por tema. También puede utilizar las capacidades de AutoML de Amazon Comprehend para crear un conjunto personalizado de entidades o modelos de clasificación de texto que se adapten exclusivamente a las necesidades de su organización. Para obtener más información, consulte Amazon Comprehend.

Preguntas frecuentes sobre Amazon Comprehend in AWS Managed Services

P: ¿Cómo solicito acceso a Amazon Comprehend en mi cuenta de AMS?

Las funciones de acceso a datos y a la consola de Amazon Comprehend se pueden solicitar mediante el envío de dos servicios AMS: RFCs

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_comprehend_console_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Comprehend en mi cuenta de AMS?

La funcionalidad de creación de un nuevo rol de IAM a través de la consola Amazon Comprehend está restringida. De lo contrario, todas las funciones de Amazon Comprehend están disponibles en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon Comprehend en mi cuenta de AMS?

Amazon S3 y AWS Key Management Service (AWS KMS) son necesarios para poder utilizar Amazon Comprehend si los buckets de Amazon S3 están cifrados con claves. AWS KMS

Utilice AMS SSP para aprovisionar Amazon Connect en su cuenta de AMS

> **Note**
>
> Tras pensarlo detenidamente, hemos decidido dejar de dar soporte a Amazon Connect Voice ID a partir del 20 de mayo de 2026. El Voice ID de Amazon Connect dejará de

aceptar nuevos clientes a partir del 20 de mayo de 2025. Como cliente actual con una cuenta registrada en el servicio antes del 20 de mayo de 2025, puedes seguir utilizando las funciones de Voice ID de Amazon Connect. Después del 20 de mayo de 2026, ya no podrás usar Amazon Connect Voice ID.

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon Connect directamente en su cuenta gestionada por AMS. Amazon Connect es un centro de contacto omnicanal en la nube que ayuda a las empresas a ofrecer un servicio de atención al cliente superior a un coste menor. Amazon Connect ofrece una experiencia fluida a través de voz y chat para clientes y agentes. Esto incluye un conjunto de herramientas para el enrutamiento basado en habilidades, potentes análisis históricos y en tiempo real y herramientas de administración easy-to-use intuitivas, todo ello con pay-as-you-go precios.

Puede crear una o más instancias de las instancias del centro de contacto virtual en las cuentas de zona de aterrizaje multicuenta o de zona de aterrizaje de una sola cuenta de AMS. Puede utilizar los proveedores de identidad SAML 2.0 existentes para el acceso de los agentes o utilizar el soporte nativo de Amazon Connect para la gestión del ciclo de vida de los usuarios.

Además, puedes solicitar los números de free/direct teléfono de pago de cada instancia de Amazon Connect desde la consola Amazon Connect. Puede crear flujos de contactos enriquecidos para lograr la experiencia de cliente y la ruta deseadas mediante una interfaz easy-to-use gráfica de usuario. Los flujos de contacto pueden aprovechar AWS Lambda las funciones para integrarse con las API y los almacenes de datos locales. También puede habilitar la transmisión de datos mediante Kinesis Streams y Firehose.

Las grabaciones de llamadas, las transcripciones de los chats y los informes se almacenan en un bucket de Amazon S3 cifrado con una AWS KMS clave. Los registros del flujo de contactos se pueden guardar en grupos de CloudWatch registros.

Para obtener más información, consulte Amazon Connect.

Preguntas frecuentes sobre Amazon Connect en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon Connect en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona las `customer_connect_console_role` `customer_connect_user_role`

siguientes funciones de IAM a su cuenta: y. Una vez aprovisionado en tu cuenta, debes incorporar el rol a tu solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Connect en mi cuenta de AMS?

No hay restricciones. Todas las funciones de Amazon Connect están disponibles en su cuenta AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon Connect en mi cuenta de AMS?

- Debe crear una AWS KMS clave y un bucket de Amazon S3 con el AMS estándar RFCs; el bucket de Amazon S3 es necesario para almacenar las grabaciones de llamadas y las transcripciones de los chats.
- Si desea realizar la integración con Active Directory (AD), necesitará un conector AD para la integración entre las instancias de Amazon Connect alojadas en AMS y sus servicios de directorio locales. AD Connector se puede configurar en su cuenta solicitando una RFC de «Administración | Otros | Otros».
- Puedes habilitar los siguientes servicios opcionales de autoaprovisionamiento en función de tus requisitos de flujo de contactos.
  - AWS Lambda: Puede utilizar las funciones de Lambda para ampliar los flujos de contactos y aprovechar los almacenes de datos locales existentes o. APIs Puede usar el servicio de autoaprovisionamiento de Lambda para crear las funciones de Lambda.
  - Amazon Kinesis Data Streams: puede crear transmisiones de datos para permitir la transmisión de datos a aplicaciones externas. Puede transmitir los registros de rastreo de contactos o los eventos de los agentes.
  - Amazon Kinesis Data Firehose: puede crear Data Firehose para transmitir registros de rastreo de contactos de gran volumen a aplicaciones externas.
  - Amazon Lex: puede aprovechar los chatbots de Amazon Lex para crear flujos de contacto inteligentes y aprovechar los servicios de Amazon Alexa para ofrecer una experiencia de cliente enriquecida y una automatización.
- P: ¿Cómo solicito añadir una lista de países para las llamadas entrantes o salientes?

  Para añadir una lista de países para las llamadas entrantes o salientes, envía una solicitud de servicio a AMS.

Utilice AMS SSP para aprovisionar Amazon Data Firehose en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon Data Firehose directamente en su cuenta gestionada por AMS. Firehose es la forma más sencilla de cargar datos de streaming de forma fiable en lagos de datos, almacenes de datos y herramientas de análisis. Puede capturar, transformar y cargar datos de streaming en Amazon S3, Amazon Redshift, Amazon OpenSearch Service y Splunk, lo que permite realizar análisis casi en tiempo real con las herramientas y paneles de inteligencia empresarial existentes que ya utiliza en la actualidad. Se trata de un servicio totalmente gestionado que se escala automáticamente para adaptarse al rendimiento de sus datos y no requiere una administración continua. También puede agrupar, comprimir, transformar y cifrar los datos antes de cargarlos, lo que minimiza la cantidad de almacenamiento utilizada en el destino y aumenta la seguridad. Para obtener más información, consulte ¿Qué es Amazon Data Firehose?

Preguntas frecuentes sobre Firehose in AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Amazon Data Firehose en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_kinesis_firehose_user_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Firehose en mi cuenta de AMS?

No hay restricciones. Todas las funciones de Amazon Data Firehose están disponibles en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Firehose en mi cuenta de AMS?

Se deben solicitar nuevas funciones de IAM vinculadas al servicio para cada transmisión de entrega. También puede reutilizar un único rol vinculado a un servicio para todas las transmisiones actualizando la política de roles con los permisos de recursos necesarios (incluidos los cubos de S3, las claves de KMS, las funciones de Lambda y las transmisiones de Kinesis).

Tras enviar el RFC para añadir Firehose, un ingeniero de operaciones de AMS se pondrá en contacto con usted mediante una solicitud de servicio para obtener ARNs los recursos que desee conectar con Data Firehose (por ejemplo AWS KMS, S3, Lambda y Kinesis Streams).

Utilice AMS SSP para aprovisionar Amazon DevOps Guru en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon DevOps Guru directamente en su cuenta gestionada por AMS. Amazon DevOps Guru es un servicio de operaciones totalmente gestionado que facilita a los desarrolladores y operadores la mejora del rendimiento y la disponibilidad de sus aplicaciones. DevOpsGuru le permite librarse de las tareas administrativas asociadas a la identificación de problemas operativos para poder implementar rápidamente recomendaciones para mejorar su aplicación. DevOpsGuru crea información reactiva que puede utilizar ahora para mejorar su aplicación. También crea información proactiva para ayudarlo a evitar problemas operativos que puedan afectar a su aplicación en el futuro. DevOpsGuru aplica el aprendizaje automático para analizar los datos operativos y las métricas y eventos de las aplicaciones a fin de identificar comportamientos que se desvían de los patrones operativos normales. Se le notifica cuando DevOps Guru detecta un problema o riesgo operativo. Para cada número, DevOps Guru presenta recomendaciones inteligentes para abordar los problemas operativos actuales y futuros previstos.

Para obtener más información, consulta Qué es Amazon DevOps Guru.

Preguntas frecuentes sobre Amazon DevOps Guru en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon DevOps Guru en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC asigna la `customer_devopsguru_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon DevOps Guru en mi cuenta de AMS?

No hay restricciones. Todas las funciones de Amazon DevOps Guru están disponibles en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon DevOps Guru en mi cuenta de AMS?

No hay requisitos previos. DevOpsGuru aprovecha los siguientes AWS servicios: Amazon CloudWatch Logs, RDS Insights AWS X-Ray y AWS Lambda. AWS CloudTrail

Utilice AMS SSP para aprovisionar Amazon DocumentDB (compatible con MongoDB) en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de Amazon DocumentDB (con compatibilidad con MongoDB) directamente en su cuenta gestionada por AMS. Amazon DocumentDB (compatible con MongoDB) es un servicio de base de datos de documentos rápido, escalable, de alta disponibilidad y totalmente gestionado que admite cargas de trabajo de MongoDB. Amazon DocumentDB le ofrece el rendimiento, la escalabilidad y la disponibilidad que necesita para operar cargas de trabajo de MongoDB de misión crítica a escala. Amazon DocumentDB implementa la API MongoDB 3.6 de código abierto Apache 2.0 emulando las respuestas que un cliente de MongoDB espera de un servidor MongoDB, lo que le permite usar sus controladores y herramientas de MongoDB existentes con Amazon DocumentDB. En Amazon DocumentDB, el almacenamiento y el procesamiento están desacoplados, lo que permite que cada uno se escale de forma independiente, y puede aumentar la capacidad de lectura a millones de solicitudes por segundo al agregar hasta 15 réplicas de lectura de baja latencia, independientemente del tamaño de los datos. Amazon DocumentDB está diseñada para ofrecer una disponibilidad del 99,99% y replica seis copias de los datos en tres zonas de AWS disponibilidad (). AZs Puede utilizar AWS Database Migration Service (DMS) de forma gratuita (durante seis meses) para migrar sus bases de datos locales o de Amazon Elastic Compute Cloud (Amazon) EC2 MongoDB a Amazon DocumentDB prácticamente sin tiempo de inactividad. Para obtener más información, consulte Amazon DocumentDB (compatible con MongoDB).

Preguntas frecuentes sobre Amazon DocumentDB en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon DocumentDB en mi cuenta de AMS?

Las funciones de acceso a datos y a la consola de Amazon DocumentDB se pueden solicitar mediante el envío de dos AMS RFCs, acceso a la consola y acceso a los datos:

Solicite acceso a Amazon DocumentDB enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC asigna la `customer_documentdb_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon DocumentDB en mi cuenta de AMS?

Amazon DocumentDB requiere permisos específicos de Amazon RDS. Dado que AMS administra Amazon RDS en su totalidad, la función de IAM para Amazon DocumentDB incluye algunas restricciones a las acciones en Amazon RDS. Se aplican las siguientes restricciones:

- Se ha restringido el acceso a `DeleteDBInstance` y se ha restringido. `DeleteDBCluster` APIs Para utilizar esas eliminaciones APIs, envíe una RFC con el tipo de cambio Management | Advanced stack components | Identity and Access Management (IAM) | Actualizar entidad o política (es necesario revisar) (ct-27tuth19k52b4).
- No puede añadir ni eliminar etiquetas de las instancias de Amazon RDS.
- No puede hacer pública su instancia de Amazon DocumentDB.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon DocumentDB en mi cuenta de AMS?

Amazon S3 y AWS KMS son necesarios para utilizar Amazon DocumentDB si los buckets de Amazon S3 están cifrados con claves. AWS KMS

Utilice AMS SSP para aprovisionar Amazon DynamoDB en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las capacidades de Amazon DynamoDB (DynamoDB) directamente en su cuenta gestionada por AMS. Amazon DynamoDB es una base de datos de documentos y valores clave que ofrece un rendimiento de milisegundos de un solo dígito a cualquier escala. Se trata de una base de datos multirregional y multiactiva totalmente gestionada con funciones integradas de seguridad, copias de seguridad y restauración y almacenamiento en caché en memoria para aplicaciones a escala de Internet. Para obtener más información, consulte Amazon DynamoDB.

Amazon DynamoDB Accelerator (DAX) es un servicio de almacenamiento en caché de escritura indirecta (write-through), diseñado para simplificar el proceso de agregar una caché a las tablas de DynamoDB. DAX está pensado para aplicaciones que requieren lecturas de alto rendimiento.

Preguntas frecuentes sobre DynamoDB en AWS Managed Services

P: ¿Cómo solicito acceso a DynamoDB y DAX en mi cuenta de AMS?

Solicite acceso a DynamoDB y DAX enviando una RFC con el tipo de cambio Management AWS | service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones y políticas de IAM a su cuenta:

- Nombre del rol de DynamoDB: `customer_dynamodb_role`

  Nombre de la función de servicio de DAX: `customer_dax_service_role`
- Nombre de la política de DynamoDB: `customer_dynamodb_policy`

  Política de servicio de DAX: `customer_dax_service_policy`

Una vez aprovisionada en su cuenta, debe incorporarla a su `customer_dynamodb_role` solución de federación.

P: ¿Cuáles son las restricciones para usar DynamoDB en mi cuenta de AMS?

Se admiten todas las funciones de DynamoDB, incluido DynamoDB Accelerator (DAX).

Al crear alarmas para una tabla determinada, el nombre de la alarma debe ir precedido de «cliente*»; por ejemplo,. `customer-employee-table-high-put-latency`

Al crear un tema de Amazon SNS para DynamoDB, debe tener el nombre:. `dynamodb`

Para eliminar el tema de Amazon SNS creado por DynamoDB, envíe una RFC de tipo de cambio de Management | Other | Other | Update.

P: ¿Cuáles son los requisitos previos o las dependencias para usar DynamoDB en mi cuenta de AMS?

No hay requisitos previos ni dependencias para usar DynamoDB en su cuenta de AMS.

Utilice AMS SSP para aprovisionar Amazon Elastic Container Registry en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las funciones de Amazon Elastic Container Registry (Amazon ECR) directamente en su cuenta gestionada por AMS. Amazon Elastic Container Registry es un registro de contenedores de Docker totalmente administrado que facilita a los desarrolladores el almacenamiento, la administración y la implementación de imágenes de contenedores de Docker. Amazon ECR está integrado con Amazon Elastic Container Service (Amazon ECS), lo que simplifica el flujo de trabajo desde el desarrollo hasta la producción. Amazon

ECR elimina la necesidad de operar sus propios repositorios de contenedores o preocuparse por escalar la infraestructura subyacente. Amazon ECS aloja sus imágenes en una arquitectura escalable y de alta disponibilidad, lo que le permite implementar contenedores para sus aplicaciones de forma fiable. La integración con AWS Identity and Access Management (IAM) proporciona un control a nivel de recursos de cada repositorio. Con Amazon ECR, no hay comisiones ni compromisos por adelantado. Solo paga por la cantidad de datos que almacena en sus repositorios y por los datos transferidos a Internet.

Para obtener más información, consulte Amazon Elastic Container Registry.

Preguntas frecuentes sobre Amazon Elastic Container Registry en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon ECR en mi cuenta de AMS?

Solicite acceso a Amazon ECR enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones de IAM a su cuenta:, y con las políticas de IAM asociadas, y, respectivamente. `customer_ecr_console_role` `customer_ecr_poweruser_instance_profile` `customer_ecr_console_policy` `customer_ecr_poweruser_instance_profile_policy` Una vez aprovisionado en su cuenta, debe incorporar el rol a su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon ECR en mi cuenta de AMS?

Existen restricciones en cuanto a los espacios de nombres de AMS para el uso de Amazon ECR en su cuenta de AMS. Las imágenes de los contenedores no pueden llevar el prefijo «AMS-» o «Sentinel-».

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon ECR en mi cuenta de AMS?

No hay requisitos previos ni dependencias para utilizar Amazon ECR en su cuenta de AMS.

Utilice AMS SSP para aprovisionar EC2 Image Builder en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las funciones de EC2 Image Builder directamente en su cuenta gestionada por AMS. EC2 Image Builder es un AWS servicio totalmente gestionado que facilita la automatización de la creación, la administración y el despliegue

de imágenes de servidor personalizadas, seguras y up-to-date «doradas» que vienen preinstaladas y preconfiguradas con software y ajustes para cumplir con estándares de TI específicos.

Puede usar la Consola de administración de AWS AWS CLI o APIs crear imágenes personalizadas en su AWS cuenta. Cuando utilice el Consola de administración de AWS, el asistente Amazon EC2 Image Builder le guiará paso a paso para:

- Proporcione los artefactos iniciales
- Cómo agregar y eliminar software.
- Personalización de los ajustes y los scripts
- Ejecución de las pruebas seleccionadas
- Distribuya imágenes a AWS las regiones

Las imágenes que cree se crean en su cuenta y se pueden configurar para los parches del sistema operativo de forma continua. Para obtener más información, consulte EC2 Image Builder.

EC2 Preguntas frecuentes sobre Image Builder en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a EC2 Image Builder en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Mediante este RFC, se aprovisionará la siguiente función de IAM en su cuenta:. `customer_ec2_imagebuilder_role` Una vez aprovisionado en su cuenta, debe incorporar el rol a su solución de federación.

P: ¿Cuáles son las restricciones de EC2 Image Builder?

AMS no admite el uso de los valores predeterminados del servicio para la configuración de la infraestructura. Puede crear una nueva configuración de infraestructura o utilizar una existente.

Actualmente, AMS no admite la creación de recetas de contenedores.

P: ¿Cuáles son los requisitos previos o las dependencias para activar EC2 Image Builder?

- EC2 Función vinculada a un servicio de Image Builder: no es necesario crear manualmente una función vinculada a un servicio. Cuando crea su primer recurso de Image Builder en la Consola

de administración de AWS AWS CLI o la AWS API, Image Builder crea automáticamente el rol vinculado al servicio.

- Las instancias utilizadas para crear imágenes y ejecutar pruebas con Image Builder deben tener acceso al servicio Systems Manager. El agente SSM se instalará en la imagen de origen si aún no está presente y se eliminará antes de crear la imagen.
- AWS IAM: la función de IAM que asocie al perfil de la instancia debe tener permisos para ejecutar los componentes de compilación y prueba incluidos en la imagen. Las siguientes políticas de rol de IAM deben estar asociadas al rol de IAM asociado a los perfiles de instancia: y. `EC2InstanceProfileForImageBuilder` `AmazonSSMManagedInstanceCore` El nombre del rol de IAM debe contener la palabra clave. `*imagebuilder*`
- Si configura el registro, el perfil de instancia especificado en la configuración de la infraestructura debe tener permisos `s3:PutObject` para el bucket de destino (`arn:aws:s3:::`*`{bucket-name}`*`/*`). Por ejemplo:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- Cree un tema de SNS con el nombre «imagebuilder» para recibir cualquier alerta y notificación de Image Builder EC2 .

Utilice AMS SSP para aprovisionar Amazon ECS AWS Fargate en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a Amazon ECS en AWS Fargate las funciones directamente de su cuenta gestionada por AMS. AWS Fargate es una

tecnología que puede utilizar con Amazon ECS para ejecutar contenedores (consulte Contenedores en AWS) sin tener que gestionar servidores o clústeres de EC2 instancias de Amazon. Con AWS Fargate ello, ya no tendrá que aprovisionar, configurar ni escalar clústeres de máquinas virtuales para ejecutar contenedores. De esta manera, se elimina la necesidad de elegir tipos de servidores, decidir cuándo escalar los clústeres u optimizar conjuntos de clústeres.

Para obtener más información, consulte Amazon ECS en AWS Fargate.

Preguntas frecuentes sobre Amazon ECS en Fargate en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon ECS en Fargate desde mi cuenta de AMS?

Solicite acceso a Amazon ECS en Fargate enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones de IAM a su cuenta: `customer_ecs_fargate_console_role` (si no se proporciona ninguna función de IAM existente a la que asociar la política de ECS),,, y. `customer_ecs_fargate_events_service_role` `customer_ecs_task_execution_service_role` `customer_ecs_codedeploy_service_role` `AWSServiceRoleForApplicationAutoScaling_ECSService` Una vez aprovisionadas en su cuenta, debe incorporar las funciones a su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon ECS en Fargate en mi cuenta de AMS?

- La supervisión y el registro de las tareas de Amazon ECS se consideran de su responsabilidad, ya que las actividades a nivel de contenedor se llevan a cabo por encima del hipervisor y Amazon ECS en Fargate limita las capacidades de registro. Como usuario de Amazon ECS en Fargate, le recomendamos que tome las medidas necesarias para habilitar el registro en sus tareas de Amazon ECS. Para obtener más información, consulte Habilitar el controlador de registro awslogs para sus contenedores.
- La seguridad y la protección contra el malware a nivel de contenedor también se consideran de su responsabilidad. Amazon ECS en Fargate no incluye Trend Micro ni componentes de seguridad de red preconfigurados.
- Este servicio está disponible tanto para cuentas AMS de zona de aterrizaje multicuenta como de zona de aterrizaje de cuenta única.
- Amazon ECS Service Discovery está restringido de forma predeterminada en la función de autoaprovisionamiento, ya que se requieren permisos elevados para crear zonas alojadas privadas de Route 53. Para habilitar Service Discovery en un servicio, envíe un tipo de cambio

de administración | Otros | Otros | Actualización. Para proporcionar la información necesaria para habilitar Service Discovery para su servicio Amazon ECS, consulte el manual de Service Discovery.

- Actualmente, AMS no administra ni restringe las imágenes utilizadas para implementarlas en los contenedores de Amazon ECS Fargate. Podrá implementar imágenes desde Amazon ECR, Docker Hub o cualquier otro repositorio de imágenes privado. Por lo tanto, recomendamos que no se desplieguen imágenes públicas o no seguras, ya que podrían provocar actividades maliciosas en la cuenta.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon ECS en Fargate en mi cuenta de AMS?

- Las siguientes son dependencias de Amazon ECS en Fargate; sin embargo, no se requiere ninguna acción adicional para habilitar estos servicios con su función de autoaprovisionamiento:
  - CloudWatch registros
  - CloudWatch eventos
  - CloudWatch alarmas
  - CodeDeploy
  - App Mesh
  - Cloud Map
  - Route 53
- Según su caso de uso, Amazon ECS utiliza los siguientes recursos y que puede necesitar antes de utilizar Amazon ECS en Fargate en su cuenta:
  - Grupo de seguridad que se utilizará con el servicio Amazon ECS. Puede usar Deployment | Advanced stack components | Security Group | Create (auto) (ct-3pc215bnwb6p7) o, si su grupo de seguridad requiere reglas especiales, Deployment | Advanced stack components | Security Group | Create (es necesario revisar) (ct-1oxx2g2d7hc90). Nota: El grupo de seguridad que seleccione con Amazon ECS debe crearse específicamente para Amazon ECS donde reside el servicio o el clúster de Amazon ECS. Puede obtener más información en la sección Grupos de seguridad en Configuración con Amazon ECS y Seguridad en Amazon Elastic Container Service.
  - Equilibrador de carga de aplicaciones (ALB), balanceador de carga de red (NLB) y balanceador de carga clásico (ELB) para equilibrar la carga entre tareas.
  - Grupos objetivo para. ALBs

- Recursos de malla de aplicaciones (por ejemplo, enrutadores virtuales, servicios virtuales, nodos virtuales) para integrarlos con su clúster de Amazon ECS.
- Actualmente, AMS no puede mitigar automáticamente el riesgo asociado a los permisos de los grupos de seguridad compatibles cuando se crean fuera de los tipos de cambios estándar de AMS. Le recomendamos que solicite un grupo de seguridad específico para usarlo con su clúster de Fargate a fin de limitar la posibilidad de usar un grupo de seguridad no designado para su uso con Amazon ECS.

Utilice AMS SSP para aprovisionar Amazon EKS AWS Fargate en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las AWS Fargate funciones de Amazon EKS directamente en su cuenta gestionada por AMS. AWS Fargate es una tecnología que proporciona una capacidad informática a pedido y del tamaño adecuado para los contenedores (para entender los contenedores, consulte ¿Qué son los contenedores?). Con AWS Fargate ello, ya no tendrá que aprovisionar, configurar ni escalar grupos de máquinas virtuales para ejecutar contenedores. De esta manera, se elimina la necesidad de elegir tipos de servidores, decidir cuándo escalar los grupos de nodos u optimizar conjuntos de clústeres.

Amazon Elastic Kubernetes Service (Amazon EKS) integra AWS Fargate Kubernetes mediante controladores que se crean AWS con el modelo extensible y ascendente que proporciona Kubernetes. Estos controladores se ejecutan como parte del plano de control de Kubernetes administrado por Amazon EKS y son responsables de programar los pods nativos de Kubernetes en Fargate. Los controladores de Fargate incluyen un nuevo programador que se ejecuta junto con el programador predeterminado de Kubernetes, además de varios controladores de admisión de mutación y validación. Cuando inicia un pod que cumple los criterios para ejecutarse en Fargate, los controladores de Fargate que se ejecutan en el clúster reconocen, actualizan y programan el pod en Fargate.

Para obtener más información, consulte Amazon EKS AWS Fargate ya disponible para todos y la Guía de mejores prácticas de seguridad de Amazon EKS (incluye «recomendaciones» como «Revisar y revocar el acceso anónimo innecesario» y más).

> **Tip**
>
> AMS tiene un tipo de cambio, Deployment | Advanced stack components | Identity and Access Managment (IAM) | Create OpenID Connect provider (ct-30ecvfi3tq4k3), que puede

utilizar con Amazon EKS. Para ver un ejemplo, consulte Identity and Access Management (IAM) | Create OpenID Connect Provider.

Preguntas frecuentes sobre Amazon EKS AWS Fargate en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon EKS en Fargate desde mi cuenta de AMS?

Solicite el acceso enviando un formulario de administración | AWS servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC asigna la siguiente función de IAM a su cuenta.

- `customer_eks_fargate_console_role`.

  Una vez aprovisionado en tu cuenta, debes incorporar el rol en tu solución de federación.
- Estas funciones de servicio permiten a Amazon EKS on Fargate llamar a otros AWS servicios en su nombre:
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

P: ¿Cuáles son las restricciones para usar Amazon EKS en Fargate en mi cuenta de AMS?

- AMS no admite la creación de EC2 grupos de nodos gestionados o autogestionados. Si necesita utilizar EC2 nodos de trabajo, póngase en contacto con su administrador de entrega de servicios en la nube (CSDM) o Cloud Architect (CA) de AMS.
- AMS no incluye Trend Micro ni componentes de seguridad de red preconfigurados para las imágenes de contenedores. Se espera que gestione sus propios servicios de digitalización de imágenes para detectar imágenes de contenedores malintencionadas antes de su despliegue.
- El EKSCTL no es compatible debido a CloudFormation las interdependencias.
- Durante la creación del clúster, tiene permisos para deshabilitar el registro del plano de control del clúster. Para obtener más información, consulte Registro del plano de control de Amazon EKS. Le recomendamos que habilite todos los registros importantes de API, autenticación y auditoría al crear el clúster.
- Durante la creación del clúster, el acceso al punto final del clúster para los clústeres de Amazon EKS se establece de forma predeterminada en público; para obtener más información, consulte Control de acceso al punto final del clúster de Amazon EKS. Recomendamos que los puntos de

enlace de Amazon EKS se configuren como privados. Si se requieren puntos de enlace para el acceso público, se recomienda configurarlos como públicos solo para rangos de CIDR específicos.

- AMS no tiene un método para forzar ni restringir las imágenes utilizadas para desplegarlas en contenedores de Amazon EKS Fargate. Puede implementar imágenes desde Amazon ECR, Docker Hub o cualquier otro repositorio de imágenes privado. Por lo tanto, existe el riesgo de implementar una imagen pública que pueda realizar actividades maliciosas en la cuenta.
- AMS no admite la implementación de clústeres de EKS mediante el kit de desarrollo en la nube (CDK) o mediante CloudFormation Ingest.
- Debe crear el grupo de seguridad necesario mediante ct-3pc215bnwb6p7 Deployment | Componentes de pila avanzados | Grupo de seguridad | Crear y hacer referencia a él en el archivo de manifiesto para crear el ingreso. Esto se debe a que el rol no está autorizado a crear grupos de seguridad. `customer-eks-alb-ingress-controller-role`

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon EKS en Fargate en mi cuenta de AMS?

Para poder utilizar el servicio, se deben configurar las siguientes dependencias:

- Para autenticarse con el servicio, aws-iam-authenticator deben estar instalados tanto KUBECTL como yo; para obtener más información, consulte Administrar la autenticación de clústeres.
- Kubernetes se basa en un concepto denominado «cuentas de servicio». Para utilizar la funcionalidad de cuentas de servicio dentro de un clúster de kubernetes en EKS, se necesita un RFC de administración | Otros | Otros | Actualización con las siguientes entradas:
  - [Obligatorio] Nombre del clúster de Amazon EKS
  - [Obligatorio] Espacio de nombres del clúster Amazon EKS donde se implementará la cuenta de servicio (SA).
  - [Obligatorio] Nombre de Amazon EKS Cluster SA.
  - [Obligatorio] Nombre de la política de IAM y permissions/document datos a asociar.
  - [Obligatorio] Se solicita el nombre del rol de IAM.
  - [Opcional] URL del proveedor de OpenID Connect. Para obtener más información, consulte
    - Habilitar las funciones de IAM para las cuentas de servicio de su clúster
    - Presentamos funciones de IAM detalladas para las cuentas de servicio
- Recomendamos que las reglas de Config se configuren y supervisen para
  - Puntos finales de clústeres públicos

- El registro de API está deshabilitado

Es su responsabilidad supervisar y corregir estas reglas de Config.

Si desea implementar un controlador de entrada de ALB, envíe un RFC de administración | Otros | Otras actualizaciones para asignar la función de IAM necesaria para utilizarla con el módulo de controlador de entrada de ALB. Se requieren las siguientes entradas para crear los recursos de IAM que se asociarán al controlador de ingreso de ALB (inclúyalos en su RFC):

- [Obligatorio] Nombre del clúster de Amazon EKS
- [Opcional] URL del proveedor de OpenID Connect
- [Opcional] Espacio de nombres de Amazon EKS Cluster donde se implementará el servicio de controlador de ingreso del balanceador de carga de aplicaciones (ALB). [predeterminado: kube-system]
- [Opcional] Nombre de la cuenta de servicio (SA) de Amazon EKS Cluster. [predeterminado: aws-load-balancer-controller]

Si desea habilitar el cifrado de los secretos de los sobres en su clúster (lo cual recomendamos), proporcione la clave de KMS que IDs piensa usar en el campo de descripción de la RFC para agregar el servicio (Management | service | Self-provisioned AWS service | Add (ct-1w8z66n899dct). Para obtener más información sobre el cifrado de sobres, consulte Amazon EKS añade el cifrado de sobres para los secretos con AWS KMS.

Utilice AMS SSP para aprovisionar Amazon EMR en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de Amazon EMR directamente en su cuenta gestionada por AMS. Amazon EMR es la plataforma de macrodatos en la nube líder del sector para procesar grandes cantidades de datos mediante herramientas de código abierto como Apache Spark, Apache Hive, Apache, Apache Flink HBase, Apache Hudi y Presto. Con Amazon EMR, puede ejecutar análisis a escala de petabytes a menos de la mitad del costo de las soluciones locales tradicionales y más de 3 veces más rápido que el Apache Spark estándar. En el caso de los trabajos de corta duración, puede activar y desactivar los clústeres y pagar por segundo por las instancias utilizadas. Para cargas de trabajo de larga duración, puede crear clústeres de alta disponibilidad que se escalen automáticamente para satisfacer la demanda.

Puede crear una o más instancias de los clústeres de Amazon EMR en las cuentas de zona de aterrizaje multicuenta o de zona de aterrizaje de una sola cuenta de AMS para admitir clústeres

de Amazon EMR tanto transitorios como persistentes. También puede habilitar la autenticación Kerberos para autenticar a los usuarios desde un dominio de Active Directory local.

Puede aprovechar varios almacenes de datos con los clústeres de Amazon EMR para admitir bibliotecas y herramientas de Hadoop para casos de uso específicos. Los clústeres de Amazon EMR se pueden crear mediante instancias puntuales OnDemand o bien configurar el escalado automático para gestionar la capacidad y reducir el coste.

Los archivos de registro del clúster se pueden archivar en un bucket de Amazon S3 para registrarlos y depurarlos. También puede acceder a las interfaces web alojadas en el clúster de Amazon EMR para cumplir con los requisitos de administración de Hadoop o las experiencias de cuaderno para los clientes.

Para obtener más información, consulte Amazon EMR.

Preguntas frecuentes sobre Amazon EMR en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon EMR en mi cuenta de AMS?

Solicite el acceso enviando un formulario de administración | AWS servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona las siguientes funciones de IAM a su cuenta:

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

Una vez aprovisionado en su cuenta, debe incorporar el customer_emr_console_role a su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon EMR en mi cuenta de AMS?

Al crear Amazon EMR en un EC2 clúster desde la consola de AWS, le recomendamos que utilice la opción Create Cluster — Advanced. Los clústeres de Amazon EMR se deben crear añadiendo la etiqueta con la clave "for-use-with-amazon-emr-managed-policies" con el valor «true». Seleccione las siguientes configuraciones en las opciones de seguridad:

- Seleccione funciones personalizadas para su clúster:
  - Función de EMR: customer_emr_cluster_service_role

  - EC2 Perfil de instancia: customer_emr_cluster_instance_profile
  - Función de Auto Scaling: customer_emr_cluster_autoscaling_role
- EC2 Grupos de seguridad:
  - Maestro: ams-emr-master-security -group
  - Núcleo y tarea: ams-emr-worker-security -grupo
  - Acceso al servicio: -group ams-emr-serviceaccess-security

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon EMR en mi cuenta de AMS?

AMS crea grupos de seguridad predeterminados para los nodos maestro, de trabajo y de servicios de Amazon EMR.

Las plantillas de lanzamiento y los grupos de seguridad que se van a utilizar con los clústeres de Amazon EMR deben tener la clave de etiqueta "for-use-with-amazon-emr-managed-policies" con el valor «true».

El perfil de instancia de clúster de Amazon EMR predeterminado permite el acceso a los recursos, como los buckets s3 y las tablas de dynamodb, cuyos nombres contienen «emr». Puede solicitar políticas de IAM adicionales para utilizar cualquier recurso adicional que se utilice con Amazon EMR. Los siguientes ARN de recursos se pueden utilizar con los trabajos de Amazon EMR que utilizan customer_emr_cluster_instance_profile:

- arn:aws:dynamodb: *:*:table/*emr*
- arn:aws:kinesis: *:*:stream/*emr*
- arn:aws:sns: *:*: *emr*arn:aws:sqs: *:*: *emr*
- arn:aws:sqs: *:*: *emr*
- arn:aws:sqs: *:*:AWS- -* ElasticMapReduce
- arn:aws:sdb: *:*:dominio: *emr*
- arn:aws:s3: ::*emr*

Si se requiere la autenticación kerberos para el clúster de Amazon EMR:

- Proporcione el nombre de dominio que se utilizará para cada clúster de Amazon EMR kerberizado y las direcciones IP de Active Directory locales.

- Requisitos de infraestructura:

  Zona de destino multicuenta (MALZ): envíe una RFC para crear una nueva cuenta de aplicación gestionada o una nueva VPC en una cuenta de aplicación existente.

  Zona de aterrizaje de cuenta única (SALZ): envíe una RFC para crear una nueva subred en su VPC.
- Configure la confianza entrante para el dominio del clúster en el Active Directory local.
- Envíe una RFC para configurar las zonas DNS del dominio en el AD administrado.
- Configuración del dominio:

  MALZ: Envíe un RFC de administración | Otros | Otros | Actualice (ct-0xdawir96cy7k) para actualizar el conjunto de opciones de DHCP de la VPC para utilizar el nombre de dominio como sufijo del nombre de dominio.

  SALZ: Envíe un RFC de administración | Otros | Otros | Actualice (ct-0xdawir96cy7k) para generar una nueva AMI de Amazon EMR que utilice el dominio específico para el sufijo del nombre de dominio.

Para implementar Amazon EMR studio, el rol `customer_emr_cluster_service_role` requiere un depósito de Amazon Simple Storage Service como requisito previo. Para crear el depósito, utilice el CT automatizado `ct-1a68ck03fn98r` (Implementación | Componentes de pila avanzados | Almacenamiento S3 | Creación). Cuando utilice este CT automatizado para crear un bucket de Amazon S3 para Amazon EMR, el nombre del bucket debe empezar por el prefijo. `customer-emr-*` Además, debe crear el bucket en la misma AWS región que el clúster de Amazon EMR.

Usa AMS SSP para aprovisionar Amazon EventBridge en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a EventBridge las capacidades de Amazon directamente en su cuenta gestionada por AMS. Amazon EventBridge es un servicio de bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones Software-as-a-Service (SaaS) y AWS servicios, y dirige esos datos a objetivos como. AWS Lambda Puede configurar reglas de direccionamiento para determinar dónde enviar los datos para crear arquitecturas de aplicaciones que reaccionen en tiempo real a todos los orígenes de

datos. EventBridge le permite crear arquitecturas basadas en eventos, que están ligeramente acopladas y distribuidas.

Para obtener más información, consulta Amazon EventBridge.

EventBridge en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a EventBridge mi cuenta de AMS?

Solicite acceso EventBridge enviando una RFC junto con Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) tipo de cambio. Este RFC proporciona las siguientes funciones de IAM a su cuenta: y. `customer_eventbridge_role` `customer_eventbridge_scheduler_execution_role` Una vez aprovisionado en tu cuenta, debes incorporar el rol a tu solución de federación.

La función de ejecución `customer_eventbridge_scheduler_execution_role` es una función de IAM que EventBridge Scheduler asume para interactuar con otras personas Servicios de AWS en su nombre. Las políticas de permisos asociadas a esta función otorgan a EventBridge Scheduler acceso para invocar objetivos.

> **Note**
>
> De forma predeterminada, EventBridge Scheduler utiliza claves AWS propias EventBridge para cifrar los datos. Para usar una clave administrada por el cliente EventBridge para cifrar los datos, envíe la RFC mediante Management | AWS service | Self-provisioned service | Agregue (es necesario revisar) el tipo de cambio (ct-3qe6io8t6jtny) para el aprovisionamiento del servicio.

P: EventBridge ¿Cuáles son las restricciones de uso de mi cuenta de AMS?

Debe enviar el AMS RFCs y crear los siguientes recursos: funciones de servicio para activar el trabajo por lotes CodeBuild CodePipeline, cola de SQS y comandos SSM.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarlos en mi cuenta de AMS? EventBridge

Debe solicitar un rol de EventBridge servicio con una RFC mediante el tipo de cambio Deployment | Advanced stack components | Identity and Access Management (IAM) | Crear entidad o política (es necesario revisar) (ct-3dpd8mdd9jn1r) antes de utilizarlo para activar EventBridge otros recursos

AWS , como Lambda, Amazon SNS, Amazon SQS o Amazon Logs. AWS Batch CloudWatch Especifique los servicios que se van a invocar al solicitar el rol de servicio. Para obtener más información sobre los permisos necesarios para invocar destinos, consulte Uso de políticas basadas en recursos para. EventBridge

EventBridge está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o una persona. Servicio de AWS EventBridge CloudTrail debe estar habilitado y autorizado a almacenar los archivos de registro en los depósitos de S3. Nota: Todas las cuentas de AMS están CloudTrail habilitadas, por lo que no es necesario realizar ninguna acción.

P: El rol customer_eventbridge_scheduler_execution_role tiene como requisito previo la existencia de una clave (opcional si se usa para el cifrado). AWS Key Management Service ¿ AWS KMS CMKs Cómo puedo adoptar el cifrado de datos en reposo o en tránsito?

De forma predeterminada, EventBridge Scheduler cifra los metadatos de los eventos y los datos de los mensajes que almacena con una AWS clave propia (cifrado en reposo). EventBridge El programador también cifra los datos que pasan entre EventBridge Scheduler y otros servicios mediante Transport Layer Security (TLS) (cifrado en tránsito).

Si su caso de uso específico requiere que controle y audite las claves de cifrado que protegen sus datos en EventBridge Scheduler, puede utilizar una clave gestionada por el cliente.

Debes solicitar una RFC mediante el tipo de cambio Management | Servicio de AWS | Self-provisioned service | Add (es necesario revisar) antes de utilizar Amazon EventBridge para incorporar el permiso. AWS KMS

Utilice AMS SSP para aprovisionar Amazon Forecast en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las funciones de Amazon Forecast (Forecast) directamente en su cuenta gestionada por AMS. Amazon Forecast es un servicio totalmente gestionado que utiliza el aprendizaje automático para ofrecer previsiones muy precisas.

> **Note**
>
> AWS ha cerrado el acceso de nuevos clientes a Amazon Forecast a partir del 29 de julio de 2024. Los clientes actuales de Amazon Forecast pueden seguir utilizando el servicio con normalidad. AWS sigue invirtiendo en mejoras de seguridad, disponibilidad y rendimiento para Amazon Forecast, pero AWS no tiene previsto introducir nuevas funciones.

Si quieres utilizar Amazon Forecast, ponte en contacto con tu CSDM para que te dé más información sobre cómo hacer la transición de tu uso de Amazon Forecast a Amazon SageMaker Canvas.

Basado en la misma tecnología utilizada en Amazon.com, Forecast utiliza el aprendizaje automático para combinar datos de series temporales con variables adicionales para generar pronósticos. Forecast no requiere experiencia en aprendizaje automático para empezar. Solo tienes que proporcionar datos históricos, además de cualquier dato adicional que consideres que pueda afectar a tus previsiones. Por ejemplo, la demanda de un color concreto de una camisa puede cambiar con las estaciones y la ubicación de la tienda. Esta relación compleja es difícil de determinar por sí sola, pero el aprendizaje automático es ideal para reconocerla. Una vez que proporcione sus datos, Forecast los examinará automáticamente, identificará lo que es significativo y generará un modelo de pronóstico capaz de realizar predicciones que son hasta un 50% más precisas que si se analizaran únicamente los datos de series temporales.

Para obtener más información, consulta Amazon Forecast.

Preguntas frecuentes sobre Amazon Forecast en AWS Managed Services

P: ¿Cómo solicito acceso a Forecast en mi cuenta de AMS?

Solicita el acceso AWS Firewall Manager enviando una RFC junto con Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añade (ct-1w8z66n899dct) el tipo de cambio. Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_forecast_admin_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Forecast en mi cuenta de AMS?

El acceso predeterminado a los buckets de S3 solo te permite acceder a los buckets con el patrón de denominación «customer-forecast-*». Si tienes tu propia convención de nomenclatura para los depósitos de datos, consulta con tu Cloud Architect (CA) el nombre de los depósitos y la configuración de acceso relacionada. Por ejemplo:

- Puede definir su función específica de servicio Amazon Forecast con nombres como 'AmazonForecast- ExecutionRole -*' y un acceso adecuado al bucket de S3 asociado. Consulte la función de servicio (AmazonForecast-ExecutionRole-Adminy la política de IAM) customer_forecast_default_s3_access_policy en la consola de IAM.

- Es posible que tengas que asociar el acceso a los buckets de S3 relacionados a la función de federación de IAM. Consulte la política de IAM, customer_forecast_default_s3_access_policy, en la consola de IAM.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Forecast en mi cuenta de AMS?

- Se deben crear los buckets de Amazon S3 adecuados antes de usar Forecast. Especialmente, el acceso predeterminado a los buckets de S3 es mediante el patrón de nomenclatura «customer-forecast-*»
- Si desea utilizar patrones de nomenclatura en los buckets de S3 distintos de «customer-forecast-*», debe crear un nuevo rol de servicio con permisos de acceso de S3 en los buckets:
  1. Se creará un nuevo rol de servicio con el nombre '- - {suffix}'. AmazonForecast ExecutionRole
  2. Se creará una nueva política de IAM similar a customer_forecast_default_s3_access_policy y que se asociará al nuevo rol de servicio y al rol de administrador de la federación relacionado (por ejemplo, 'customer_forecast_admin_role')

P: ¿Cómo puedo mejorar la seguridad de los datos al utilizar Amazon Forecast?

- Para el cifrado de datos en reposo, puede utilizar AWS KMS para aprovisionar una CMK administrada por el cliente para proteger el almacenamiento de datos en el servicio Amazon S3:
  - Habilite el cifrado predeterminado en el depósito con la clave de aprovisionamiento y configure una política de depósito para aceptar el cifrado de AWS KMS datos al colocar los datos.
  - Habilite el rol de servicio Amazon Forecast 'AmazonForecast- ExecutionRole -*' y el rol de administrador de la federación (por ejemplo,' customer_forecast_admin_role ') como usuario clave. AWS KMS
- Para el cifrado de datos en tránsito, puede configurar el protocolo HTTPS, que es necesario para transferir objetos en la política de bucket de Amazon S3.
- Para restringir aún más el control de acceso, habilite una política de bucket para el acceso aprobado para el rol de servicio Amazon Forecast 'AmazonForecast- ExecutionRole -*' y el rol de administrador (por ejemplo,' customer_forecast_admin_role ').

P: ¿Cuáles son las prácticas recomendadas al utilizar Amazon Forecast?

- Debe conocer bien sus prácticas de clasificación de datos y planificar las necesidades de seguridad de los datos relacionadas al utilizar buckets de S3 con Amazon Forecast.

- Para la configuración de los buckets de Amazon S3, le recomendamos encarecidamente que habilite la aplicación de HTTPS en su política de buckets de S3.
- Debe tener en cuenta que el rol de administrador 'customer_forecast_admin_role' admite el acceso permisivo (objetos S3Get/Delete/Put) en los buckets de Amazon S3 con el nombre 'customer-forecast-*'. NOTA: Si necesita un control de acceso detallado para varios equipos, siga estas prácticas:
  - Defina su identidad de IAM de acceso basada en equipos (rol/usuario) con el acceso con privilegios mínimos a los buckets de Amazon S3 relacionados.
  - Cree y conceda el acceso adecuado a las identidades de team/project AWS KMS CMKs IAM correspondientes. (acceso de usuario y 'AmazonForecast- ExecutionRole - {equipo/proyecto}'.
  - Configure el cifrado predeterminado del bucket S3 con el creado. AWS KMS CMKs
  - Aplica los tráficos de la API de S3 con el protocolo HTTPS en la política de cubos de S3.
  - Imponga la configuración de los buckets de S3 para permitir el acceso autorizado a las identidades de IAM relacionadas (acceso de usuario) y «AmazonForecast- ExecutionRole - {equipo/proyecto}» a los buckets.
- Si desea utilizar el «customer_forecast_admin_role» con fines generales, tenga en cuenta los puntos enumerados anteriormente para proteger los buckets de S3.

P: ¿Dónde está la información de conformidad sobre Amazon Forecast?

Consulte el Programa de conformidad de AWS los servicios.

Usa AMS SSP para aprovisionar Amazon FSx en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a FSx las capacidades de Amazon directamente en su cuenta gestionada por AMS. Amazon FSx proporciona sistemas de archivos de terceros totalmente gestionados. Amazon le FSx proporciona la compatibilidad nativa de sistemas de archivos de terceros con conjuntos de funciones para cargas de trabajo como el almacenamiento basado en Windows, la informática de alto rendimiento (HPC), el aprendizaje automático y la automatización del diseño electrónico (EDA). Amazon FSx automatiza las tareas de administración que consumen mucho tiempo, como el aprovisionamiento de hardware, la configuración del software, la aplicación de parches y las copias de seguridad. Amazon FSx integra los sistemas de archivos con los AWS servicios nativos de la nube, lo que los hace aún más útiles para un conjunto más amplio de cargas de trabajo.

Amazon le FSx ofrece dos sistemas de archivos entre los que elegir: Amazon FSx for Windows File Server para aplicaciones basadas en Windows y Amazon for Lustre para cargas de trabajo con un FSx uso intensivo de cómputo. Para obtener más información, consulta Amazon FSx.

Preguntas frecuentes sobre Amazon FSx en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon FSx en mi cuenta de AMS?

Solicita el acceso a Amazon FSx enviando un RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC asigna la siguiente función de IAM a su cuenta:. `customer_fsx_admin_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon FSx en mi cuenta de AMS?

No hay restricciones. Está disponible la funcionalidad completa del servicio.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon FSx en mi cuenta de AMS?

No hay requisitos previos. Sin embargo, para configuraciones avanzadas como Multi-AZ, debe instalar y administrar los servicios de replicación de DFS y de espacios de nombres de DFS. Para obtener más información, consulte Implementación de sistemas de archivos Multi-AZ.

P: ¿Cómo puedo integrar mi sistema de FSx archivos de Amazon con mi AD gestionado por múltiples cuentas en una zona de landing zone?

Al crear un sistema de FSx archivos de Amazon, puede especificar su AD gestionado por MALZ como «Microsoft Active Directory AWS gestionado» para la autenticación de Windows. Para obtener más información, consulte Uso de Amazon FSx con AWS Directory Service Microsoft Active Directory

También debe compartir primero el AD administrado con la cuenta de la aplicación. Para ello, envíe una RFC con el tipo de cambio Management | Directory Service | Directory | Share directory (ct-369odosk0pd9w).

P: ¿Qué usuarios pertenecen al grupo de FSx administradores delegados de AWS?

Solo administradores de servidores de archivos de TI. Este grupo tiene privilegios de acceso total a todos los recursos compartidos de archivos.

P: ¿Debo usar el recurso compartido de archivos predeterminado, el recurso compartido, que se crea cuando se aprovisiona el FSx sistema?

No, no recomendamos utilizar el recurso compartido de archivos predeterminado, el recurso compartido, tal como está aprovisionado. Otorga acceso total a todos, lo que infringe el principio del privilegio mínimo. En su lugar, cree recursos compartidos de archivos más pequeños y personalizados que se adapten a las necesidades de su empresa.

P: ¿Cómo puedo crear recursos compartidos de archivos personalizados para organizaciones específicas de mi empresa?

Consulte Recursos compartidos de archivos para obtener instrucciones sobre cómo crear recursos compartidos de archivos personalizados. Restrinja el acceso a cada recurso compartido de archivos utilizando el principio del privilegio mínimo.

Usa AMS SSP para aprovisionar Amazon FSx para OpenZFS en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de Amazon FSx for OpenZFS directamente en su cuenta gestionada por AMS. FSx for OpenZFS es un servicio de almacenamiento de archivos totalmente gestionado que facilita el traslado de los datos que residen en ZFS u otros servidores de archivos basados en Linux a AWS sin cambiar el código de la aplicación ni la forma de gestionar los datos. Ofrece un almacenamiento de archivos altamente confiable, escalable, eficiente y rico en funciones basado en el sistema de archivos OpenZFS de código abierto, que proporciona las características y capacidades familiares de los sistemas de archivos OpenZFS con la agilidad, escalabilidad y simplicidad de un AWS servicio totalmente administrado. Para los desarrolladores que crean aplicaciones nativas de la nube, ofrece un almacenamiento simple y de alto rendimiento con amplias capacidades para trabajar con datos.

FSx para los sistemas de archivos OpenZFS, se puede acceder ampliamente desde instancias y contenedores de cómputo de Linux, Windows y macOS que utilizan el protocolo NFS estándar del sector (v3, v4.0, v4.1, v4.2). Con procesadores AWS Graviton y las últimas tecnologías de AWS disco y redes (incluidas las redes de datagramas AWS escalables y confiables y el sistema AWS Nitro), OpenZFS ofrece hasta 1 millón de IOPS con latencias FSx de cientos de microsegundos. Con una compatibilidad total con las funciones de OpenZFS, como las point-in-time instantáneas instantáneas y la clonación de datos, FSx OpenZFS le facilita la sustitución de los servidores de archivos locales por un AWS almacenamiento que proporciona las funciones conocidas del sistema de archivos y elimina la necesidad de realizar largas calificaciones y cambiar o rediseñar las aplicaciones o herramientas existentes. Además, al combinar la potencia de las capacidades de administración de datos de OpenZFS con el alto rendimiento y la rentabilidad de las últimas

tecnologías de AWS, FSx OpenZFS le permite crear y ejecutar aplicaciones de alto rendimiento con uso intensivo de datos.

Al tratarse de un servicio totalmente gestionado, FSx OpenZFS facilita el lanzamiento, la ejecución y el escalado de sistemas de archivos totalmente gestionados AWS que sustituyen a los servidores de archivos que se ejecutan en las instalaciones y, al mismo tiempo, ayudan a mejorar la agilidad y reducir los costes. Con FSx OpenZFS, ya no tendrá que preocuparse por configurar y aprovisionar servidores de archivos y volúmenes de almacenamiento, replicar datos, instalar y aplicar parches al software del servidor de archivos, detectar y corregir los fallos de hardware y realizar copias de seguridad manualmente. También proporciona una rica integración con otros AWS servicios, como AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS) CloudWatch, Amazon y AWS CloudTrail.

Amazon le FSx ofrece dos sistemas de archivos entre los que elegir: Amazon FSx for Windows File Server para aplicaciones basadas en Windows y Amazon for Lustre para cargas de trabajo con un FSx uso intensivo de cómputo. Para obtener más información, consulta Amazon FSx.

Preguntas frecuentes FSx sobre Amazon for OpenZFS en AWS Managed Services

P: ¿Cómo solicito el acceso FSx para usar OpenZFS en mi cuenta de AMS?

Solicite acceso a Amazon FSx OpenZFS enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC asigna la `customer_fsx_ontap_admin_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso FSx de OpenZFS en mi cuenta de AMS?

Para reemplazar el grupo de seguridad en las interfaces de red FSx elásticas de Amazon (ENIs), debe enviar Management | Other | Other | Update, RFCs ya que los grupos de seguridad son un perímetro crítico para el entorno AMS. Esa es la única restricción.

P: ¿Cuáles son los requisitos previos o las dependencias FSx para usar OpenZFS en mi cuenta de AMS?

No hay requisitos previos. Sin embargo, debe haberlo Usa AMS SSP para aprovisionar Amazon FSx en tu cuenta de AMS instalado.

Usa AMS SSP para aprovisionar Amazon FSx para NetApp ONTAP en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon FSx for NetApp ONTAP directamente en su cuenta gestionada por AMS. Amazon FSx for NetApp ONTAP es un servicio totalmente gestionado que proporciona un almacenamiento de archivos altamente fiable, escalable, eficiente y rico en funciones basado en NetApp el popular sistema de archivos ONTAP. Ofrece las funciones, el rendimiento, las capacidades y los sistemas APIs de NetApp archivos que ya conocemos con la agilidad, escalabilidad y sencillez de un sistema totalmente gestionado. Servicio de AWS

Amazon FSx for NetApp ONTAP proporciona un almacenamiento de archivos compartido rápido, flexible y rico en funciones al que se puede acceder fácilmente desde instancias informáticas de Linux, Windows y macOS que se ejecutan en las instalaciones AWS o en ellas. FSx for ONTAP ofrece almacenamiento SSD de alto rendimiento con latencias inferiores a un milisegundo y agiliza y facilita la gestión de los datos, ya que permite capturar, clonar y replicar los archivos con solo pulsar un botón. Además, organiza automáticamente sus datos en niveles de almacenamiento flexibles y de menor coste, lo que elimina la necesidad de aprovisionar o gestionar la capacidad y le permite alcanzar los niveles de rendimiento de los SSD para su carga de trabajo sin tener que pagar solo por el almacenamiento en SSD de una pequeña fracción de sus datos. Proporciona un almacenamiento duradero y de alta disponibilidad con copias de seguridad totalmente gestionadas y es compatible con la recuperación ante desastres en todas las regiones. Además, es compatible con las populares aplicaciones antivirus y de seguridad de datos que facilitan aún más la protección y la protección de los datos. Para los clientes que utilizan NetApp ONTAP de forma local, ONTAP es la solución ideal FSx para migrar, realizar copias de seguridad o agrupar sus aplicaciones basadas en archivos de forma local a otras AWS sin necesidad de cambiar el código de la aplicación ni la forma de gestionar los datos.

Como servicio totalmente gestionado, Amazon FSx for NetApp ONTAP facilita el lanzamiento y el escalado de un almacenamiento de archivos compartido fiable, eficaz y seguro en la nube. Con Amazon FSx for NetApp ONTAP, ya no tendrá que preocuparse por configurar y aprovisionar servidores de archivos y volúmenes de almacenamiento, replicar datos, instalar y parchar el software del servidor de archivos, detectar y corregir los fallos de hardware, gestionar la conmutación por error y la conmutación por error y realizar copias de seguridad manualmente. También proporciona una rica integración con otros Servicios de AWS AWS Identity and Access Management, como Amazon WorkSpaces y AWS CloudTrail. AWS Key Management Service

Amazon le FSx ofrece dos sistemas de archivos entre los que elegir: Amazon FSx for Windows File Server para aplicaciones basadas en Windows y Amazon for Lustre para cargas de trabajo con un FSx uso intensivo de cómputo. Para obtener más información, consulta Amazon FSx.

Preguntas frecuentes sobre Amazon FSx for NetApp ONTAP en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon FSx for NetApp ONTAP en mi cuenta de AMS?

Solicita el acceso a Amazon FSx para NetApp ONTAP enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC asigna `customer_fsx_ontap_admin_role` la siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon FSx for NetApp ONTAP en mi cuenta de AMS?

Para reemplazar el grupo de seguridad en Amazon FSx por las interfaces de red elásticas de NetApp ONTAP (ENIs), debe enviar Management | Other | Other | Update, RFCs ya que los grupos de seguridad son un perímetro fundamental para el entorno AMS. Esa es la única restricción.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon FSx for NetApp ONTAP en mi cuenta de AMS?

No hay requisitos previos. Sin embargo, debe haberlo Usa AMS SSP para aprovisionar Amazon FSx en tu cuenta de AMS instalado.

Utilice AMS SSP para aprovisionar Amazon Inspector Classic en su cuenta de AMS

> **Note**
>
> Aviso de fin de soporte: el 20 de mayo de 2026, AWS finalizará el soporte para Amazon Inspector Classic. Después del 20 de mayo de 2026, ya no podrá acceder a la consola de Amazon Inspector Classic ni a los recursos de Amazon Inspector Classic. Amazon Inspector Classic ya no estará disponible para las cuentas nuevas ni para las cuentas que no hayan completado una evaluación en los últimos seis meses. Para todas las demás cuentas, el acceso seguirá siendo válido hasta el 20 de mayo de 2026, tras lo cual ya no podrá acceder a la consola Amazon Inspector Classic ni a los recursos de Amazon Inspector Classic. Para obtener más información, consulte el fin del soporte de Amazon Inspector Classic.

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon Inspector Classic directamente en su cuenta gestionada por AMS. Amazon Inspector Classic es un servicio de evaluación de seguridad automatizado que ayuda a mejorar la seguridad y la conformidad de las aplicaciones implementadas en ellas AWS. Amazon Inspector Classic evalúa automáticamente la exposición, las vulnerabilidades y las desviaciones de las aplicaciones con respecto a las mejores prácticas. Tras realizar una evaluación, Amazon Inspector Classic elabora una lista detallada de los hallazgos de seguridad priorizados por nivel de gravedad. Estos resultados se pueden revisar directamente o como parte de informes de evaluación detallados, que están disponibles a través de la consola o API de Amazon Inspector Classic. Para obtener más información, consulte Amazon Inspector Classic.

Preguntas frecuentes sobre Amazon Inspector en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon Inspector Classic en mi cuenta de AMS?

Solicite acceso a Amazon Inspector Classic enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC asigna la función de IAM a su cuenta. `customer_inspector_admin_role` La función incluye la política AWS gestionada AmazonInspectorFullAccess . Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Inspector Classic en mi cuenta de AMS?

No hay restricciones. Todas las funciones de Amazon Inspector Classic están disponibles en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon Inspector Classic en mi cuenta de AMS?

No hay requisitos previos ni dependencias para utilizar Amazon Inspector Classic en su cuenta de AMS.

Usa el nuevo Amazon Inspector en AMS

Ahora puedes usar el nuevo Amazon Inspector en tu cuenta de AMS.

Para Amazon Inspector Classic, los `customer-inspector-admin-role-ssm-inspector-agent-policy` caracteres y `AmazonInspectorFullAccess` eran obligatorios. Sin embargo, se ha actualizado la función de SSP`customer-inspector-admin-role`, que ahora incluye una función adicional`policyAmazonInspector2FullAccess`. Esta nueva política permite permisos de API para la nueva versión de Amazon Inspector.

Utilice AMS SSP para aprovisionar Amazon Kendra en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon Kendra directamente en su cuenta gestionada por AMS. Amazon Kendra es un servicio de búsqueda inteligente que utiliza el procesamiento del lenguaje natural y algoritmos avanzados de aprendizaje automático para devolver respuestas específicas a las preguntas de búsqueda a partir de sus datos. A diferencia de la búsqueda tradicional basada en palabras clave, Amazon Kendra utiliza sus capacidades de comprensión semántica y contextual para determinar si un documento es relevante para una consulta de búsqueda. Amazon Kendra devuelve respuestas específicas a las preguntas, por lo que su experiencia es similar a la de interactuar con un experto humano. Amazon Kendra es altamente escalable, capaz de cumplir con las exigencias de rendimiento, está estrechamente integrado con otros AWS servicios, como Amazon S3 y Amazon Lex, y ofrece seguridad de nivel empresarial. Para obtener más información, consulte Amazon Kendra;.

Preguntas frecuentes sobre Amazon Kendra en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon Kendra en mi cuenta de AMS?

Para solicitar acceso a Amazon Inspector Classic, envíe una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny). Este RFC asigna la función de IAM a su cuenta. `customer_kendra_console_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Kendra en mi cuenta de AMS?

No hay restricciones. Todas las funciones de Amazon Kendra están disponibles en tu cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon Kendra en mi cuenta de AMS?

No hay requisitos previos ni dependencias para empezar a utilizar Amazon Kendra. Sin embargo, según su caso de uso específico, es posible que necesite acceder a otros servicios. AWS

Utilice AMS SSP para aprovisionar Amazon Kinesis Data Streams en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las capacidades de Amazon Kinesis Data Streams (KDS) directamente en su cuenta gestionada por AMS. Amazon Kinesis Data

Streams es un servicio de streaming de datos en tiempo real duradero y altamente escalable. KDS puede capturar de forma continua gigabytes de datos por segundo de cientos de miles de fuentes, como secuencias de clics en sitios web, transmisiones de eventos de bases de datos, transacciones financieras, feeds de redes sociales, registros de TI y eventos de seguimiento de ubicación. Los datos recopilados están disponibles en milisegundos para permitir casos de uso de análisis en tiempo real, como paneles de control en tiempo real, detección de anomalías en tiempo real, precios dinámicos y más. Para obtener más información, consulte Amazon Kinesis Data Streams.

Preguntas frecuentes sobre Kinesis Data Streams en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Amazon Kinesis Data Streams en mi cuenta de AMS?

Solicite acceso a Amazon Kinesis Data Streams enviando una RFC a Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct). Este RFC asigna `customer_kinesis_data_streaming_user_role` la siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Kinesis Data Streams en mi cuenta de AMS?

No hay restricciones. La funcionalidad completa de Amazon Kinesis Data Streams está disponible en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon Kinesis Data Streams en mi cuenta de AMS?

No hay requisitos previos ni dependencias para utilizar Amazon Kinesis Data Streams en su cuenta de AMS.

Utilice AMS SSP para aprovisionar Amazon Kinesis Video Streams en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las capacidades de Amazon Kinesis Video Streams (KVS) directamente en su cuenta gestionada por AMS. Amazon Kinesis Video Streams le ayuda a transmitir vídeo de forma segura desde los dispositivos conectados AWS para fines de análisis, aprendizaje automático (ML), reproducción y otros tipos de procesamiento. Kinesis Video Streams aprovisiona automáticamente y escala de forma elástica toda la infraestructura necesaria para ingerir datos de vídeo en streaming desde millones de dispositivos. También

almacena, cifra e indexa de forma duradera los datos de vídeo de sus transmisiones y le permite acceder a los datos a través de ellos. easy-to-use APIs Kinesis Video Streams le permite reproducir vídeos para verlos en directo y bajo demanda, y crear rápidamente aplicaciones que aprovechen la visión artificial y el análisis de vídeo mediante la integración con Amazon Rekognition Video y bibliotecas para marcos de aprendizaje automático MxNet como TensorFlow Apache y OpenCV. Para obtener más información, consulte Amazon Kinesis Video Streams.

Preguntas frecuentes sobre Amazon Kinesis Video Streams en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Amazon Kinesis Video Streams en mi cuenta de AMS?

Solicite acceso a Amazon Kinesis Video Streams enviando una RFC a Management AWS | service | Self-provisioned service | Add change type (ct-1w8z66n899dct). Este RFC asigna `customer_kinesis_video_streaming_user_role` la siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Kinesis Video Streams en mi cuenta de AMS?

No hay restricciones. La funcionalidad completa de Amazon Kinesis Video Streams está disponible en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon Kinesis Video Streams en mi cuenta de AMS?

No hay requisitos previos ni dependencias para utilizar Amazon Kinesis Video Streams en su cuenta de AMS.

Utilice AMS SSP para aprovisionar Amazon Lex en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon Lex directamente en su cuenta gestionada por AMS. Amazon Lex es un servicio para crear interfaces de conversación en cualquier aplicación mediante voz y texto. Amazon Lex ofrece las funcionalidades avanzadas de aprendizaje profundo del reconocimiento automático de voz (ASR) para convertir la voz en texto y la comprensión del lenguaje natural (NLU) para reconocer la intención del texto, lo que le permite crear aplicaciones con experiencias de usuario muy atractivas e interacciones conversacionales realistas. Con Amazon Lex, las mismas tecnologías de aprendizaje

profundo que impulsan Amazon Alexa ahora están disponibles para cualquier desarrollador, lo que le permite crear de forma rápida y sencilla bots conversacionales o chatbots sofisticados en lenguaje natural. Para obtener más información, consulte Amazon Lex.

Preguntas frecuentes sobre Amazon Lex en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Amazon Lex en mi cuenta de AMS?

Para solicitar acceso, envíe un mensaje de administración | AWS servicio | Servicio autoaprovisionado | Añada un tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_lex_author_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Lex en mi cuenta de AMS?

La integración de Amazon Lex con Lambda se limita a las funciones de Lambda sin el prefijo «AMS-», a fin de evitar cualquier modificación en la infraestructura de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon Lex en mi cuenta de AMS?

No hay requisitos previos ni dependencias para utilizar Amazon Lex en su cuenta de AMS.

Usa AMS SSP para aprovisionar Amazon MQ en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de Amazon MQ directamente en su cuenta gestionada por AMS. Amazon MQ es un servicio de intermediación de mensajes gestionado para Apache ActiveMQ que le ayuda a configurar y operar agentes de mensajería en la nube. Los intermediarios de mensajes permiten que diferentes sistemas de software, que suelen utilizar diferentes lenguajes de programación y en diferentes plataformas, se comuniquen e intercambien información. Amazon MQ reduce la carga operativa al gestionar el aprovisionamiento, la configuración y el mantenimiento de ActiveMQ, un popular agente de mensajes de código abierto. La conexión de sus aplicaciones actuales a Amazon MQ utiliza estándares APIs y protocolos del sector para la mensajería, incluidos JMS, NMS, AMQP, STOMP, MQTT y. WebSocket El uso de estándares significa que, en la mayoría de los casos, no es necesario volver a escribir ningún código de mensajería al migrar a. AWS Para obtener más información, consulta ¿Qué es Amazon MQ?

Preguntas frecuentes sobre Amazon MQ en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Amazon MQ en mi cuenta de AMS?

El uso de Amazon MQ en tu cuenta de AMS es un proceso de dos pasos:

1. Aprovisione el Amazon MQ Broker. Para ello, envíe una plantilla de CFN, con el agente de Amazon MQ incluido, a través de una RFC con el tipo de cambio Implementación | Ingestión | Pila CloudFormation desde plantilla | Creación de cambio (ct-36cn2avfrrj9v), o envíe una RFC al tipo de cambio Management | Other | Other | Other | Create change type (ct-1e1xtak34nx76) solicitando que Amazon MQ Broker se aprovisione en su cuenta.
2. Accede a la consola Amazon MQ. Una vez aprovisionado el Amazon MQ Broker, obtenga acceso a la consola de Amazon MQ enviando una RFC con Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct). Este RFC asigna `customer_mq_console_role` la siguiente función de IAM a su cuenta:.

Una vez aprovisionado el rol en su cuenta, debe incorporarlo a su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon MQ en mi cuenta de AMS?

Todas las funciones de Amazon MQ están disponibles en su cuenta de AMS; sin embargo, el aprovisionamiento de Amazon MQ Broker no está disponible a través de la política debido a la necesidad de un permiso elevado. Consulte más arriba para obtener detalles sobre cómo aprovisionar el agente Amazon MQ en sus cuentas.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon MQ en mi cuenta de AMS?

No hay requisitos previos ni dependencias para usar Amazon MQ en tu cuenta de AMS.

Utilice AMS SSP para aprovisionar Amazon Managed Service para Apache Flink en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de Amazon Managed Service for Apache Flink directamente en su cuenta gestionada de AMS. El servicio gestionado para Apache Flink es la forma más sencilla de analizar los datos de streaming, obtener información útil y responder a las necesidades de su empresa y de sus clientes en tiempo

real. Amazon Managed Service for Apache Flink reduce la complejidad de crear, administrar e integrar aplicaciones de streaming con otros AWS servicios. Los usuarios de SQL pueden consultar fácilmente los datos de streaming o crear aplicaciones de streaming completas mediante plantillas y un editor SQL interactivo. Los desarrolladores de Java pueden crear rápidamente aplicaciones de streaming sofisticadas mediante AWS integraciones y bibliotecas Java de código abierto para transformar y analizar los datos en tiempo real. Amazon Managed Service para Apache Flink se encarga de todo lo necesario para ejecutar sus aplicaciones en tiempo real de forma continua y escala automáticamente para adaptarse al volumen y el rendimiento de los datos entrantes. Con Amazon Managed Service para Apache Flink, solo pagas por los recursos que consumen tus aplicaciones de streaming. No hay una tarifa mínima ni un costo de configuración. Para obtener más información, consulte Amazon Managed Service para Apache Flink.

Preguntas frecuentes sobre Managed Service for Apache Flink en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Amazon Managed Service for Apache Flink en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_kinesis_analytics_application_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Managed Service for Apache Flink en mi cuenta de AMS?

- Las configuraciones se limitan a los recursos sin los prefijos «AMS-» o «MC-» para evitar cualquier modificación en la infraestructura de AMS.
- Se ha eliminado de la política el permiso para eliminar o crear nuevos Kinesis Data Streams o Firehose. Tenemos otra política que lo permite.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon Kinesis Data Streams en mi cuenta de AMS?

Existen algunas dependencias:

- Amazon Managed Service for Apache Flink requiere que se creen Kinesis Data Streams o Firehose antes de configurar una aplicación con Managed Service for Apache Flink.

- Los permisos de la política basada en los recursos deben indicar una fuente de datos de entrada concreta.

Utilice AMS SSP para aprovisionar Amazon Managed Streaming for Apache Kafka Kafka en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las funciones de Amazon Managed Streaming for Apache Kafka (Amazon MSK) directamente en su cuenta gestionada por AMS. Amazon Managed Streaming for Apache Kafka es un servicio de AWS transmisión de datos totalmente gestionado que le permite crear y ejecutar aplicaciones que utilizan Apache Kafka para procesar datos de streaming sin necesidad de convertirse en un experto en el manejo de clústeres de Apache Kafka. Amazon MSK administra por usted el aprovisionamiento, la configuración y el mantenimiento de los clústeres y ZooKeeper nodos de Apache Kafka. Amazon MSK también muestra las principales métricas de rendimiento de Apache Kafka en la AWS consola.

Amazon MSK proporciona varios niveles de seguridad para sus clústeres de Apache Kafka, incluidos el aislamiento de la red de VPC, la AWS IAM para la autorización de la API en el plano de control, el cifrado en reposo, el cifrado TLS en tránsito, la autenticación con certificados basada en TLS y la autenticación protegida por. SASL/SCRAM AWS Secrets Manager Para obtener más información, consulte Amazon MSK.

Preguntas frecuentes sobre Amazon MSK en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Amazon MSK en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC establece las siguientes políticas y funciones de IAM para su cuenta:

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

Una vez aprovisionado en su cuenta, debe incorporar el rol a su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon MSK?

Para que Amazon MSK entregue los registros de los corredores a los destinos que configure, asegúrese de que la `AmazonMSKFullAccess` política esté asociada a su función de IAM. Por lo tanto, los permisos de acceso total ya están en vigor.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon MSK?

Antes de crear el clúster de MSK, debe tener una VPC y subredes dentro de esa VPC. De forma predeterminada, AMS cubre esta cuestión como parte de la creación predeterminada de una VPC de AMS.

Para obtener más información sobre las limitaciones de Amazon MSK, consulta Amazon MSK Limits.

Utiliza AMS SSP para aprovisionar Amazon Managed Service para Prometheus en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon Managed Service for Prometheus (AMP) directamente en su cuenta gestionada de AMS. Amazon Managed Service para Prometheus es un servicio de supervisión de métricas de contenedores sin servidor compatible con Prometheus que facilita la supervisión de los entornos de contenedores a escala. Con Amazon Managed Service para Prometheus, puede utilizar el mismo modelo de datos y lenguaje de consulta de Prometheus de código abierto que utiliza actualmente para supervisar el rendimiento de sus cargas de trabajo en contenedores y, además, disfrutar de una escalabilidad, disponibilidad y seguridad mejoradas sin tener que administrar la infraestructura subyacente.

Amazon Managed Service for Prometheus escala automáticamente la ingesta, el almacenamiento y la consulta de las métricas operativas a medida que las cargas de trabajo aumentan o disminuyen. Se integra con los servicios de AWS seguridad para permitir un acceso rápido y seguro a los datos. Para obtener más información, consulta ¿Qué es Amazon Managed Service para Prometheus?

Preguntas frecuentes sobre Amazon Managed Service for Prometheus en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Amazon Managed Service for Prometheus en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de gestión | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer-prometheus-console-role` siguiente función de IAM a su cuenta:. Una vez

aprovisionado en su cuenta, debe incorporar el `customer-prometheus-console-role` rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Managed Service for Prometheus en mi cuenta de AMS?

Se admiten todas las funciones.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon Managed Service for Prometheus en mi cuenta de AMS?

No hay requisitos previos ni dependencias para empezar a utilizar Amazon Managed Service para Prometheus. Sin embargo, según su caso de uso específico, es posible que necesite acceder a otros servicios. AWS

Utilice AMS SSP para aprovisionar Amazon Personalize en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las funciones de Amazon Personalize directamente en su cuenta gestionada por AMS. Amazon Personalize es un servicio de aprendizaje automático que facilita a los desarrolladores la creación de recomendaciones individualizadas para los clientes que utilizan sus aplicaciones.

El aprendizaje automático se utiliza cada vez más para mejorar la participación de los clientes al ofrecer recomendaciones personalizadas de productos y contenido, resultados de búsqueda personalizados y promociones de marketing específicas. Sin embargo, desarrollar las capacidades de aprendizaje automático necesarias para producir estos sofisticados sistemas de recomendación ha estado fuera del alcance de la mayoría de las organizaciones hoy en día debido a la complejidad. Amazon Personalize permite a los desarrolladores sin experiencia previa en aprendizaje automático incorporar fácilmente capacidades de personalización sofisticadas a sus aplicaciones, mediante una tecnología de aprendizaje automático perfeccionada tras años de uso en Amazon.com.

Con Amazon Personalize, proporciona un flujo de actividad de su aplicación (clics, visitas a la página, registros, compras, etc.), así como un inventario de los artículos que desea recomendar, como artículos, productos, vídeos o música. También puede optar por proporcionar a Amazon Personalize información demográfica adicional de sus usuarios, como la edad o la ubicación geográfica. Amazon Personalize procesará y examinará los datos, identificará lo que es significativo, seleccionará los algoritmos correctos y entrenará y optimizará un modelo de personalización personalizado para sus datos. Todos los datos analizados por Amazon Personalize se mantienen privados y seguros, y solo se utilizan para tus recomendaciones personalizadas. Puede empezar a ofrecer recomendaciones

personalizadas mediante una simple llamada a la API. Solo pagas por lo que usas y no hay tarifas mínimas ni compromisos por adelantado.

Para obtener más información, consulta Amazon Personalize.

Preguntas frecuentes sobre Amazon Personalize in AWS Managed Services

P: ¿Cómo solicito acceso a Amazon Personalize en mi cuenta de AMS?

Para solicitar el acceso, envíe un tipo de cambio de Administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) y especifique qué bucket de S3 contiene los datos que utilizará Personalize para generar las recomendaciones. AWS Este RFC `customer_personalize_console_role` `customer_personalize_service_role` proporciona las siguientes funciones de IAM a su cuenta: y.

- Una vez que `customer_personalize_console_role` esté aprovisionado en su cuenta, debe incorporar el rol a su solución de federación. También puede asociarlo `customer_personalize_console_policy` a otro rol existente que no sea`Customer_ReadOnly_Role`.
- Una vez que `customer_personalize_service_role` se haya proporcionado a su cuenta, podrá hacer referencia a su ARN al crear un nuevo grupo de conjuntos de datos.

En este momento, AMS Operations también implementará este rol de servicio en su cuenta:`aws_code_pipeline_service_role_policy`.

P: ¿Cuáles son las restricciones para usar Amazon Personalize en mi cuenta de AMS?

La configuración de Amazon Personalize se limita a los recursos sin los prefijos «ams-» o «mc-», para evitar cualquier modificación en la infraestructura de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon Personalize en mi cuenta de AMS?

- Si el depósito de S3 en el que se almacenan los datos está cifrado, se debe proporcionar el ID de clave de KMS para que podamos permitir que la función utilizada por Amazon Personalize descifre el depósito.

  Amazon Personalize no admite la clave S3 de KMS predeterminada. Si es necesario utilizar KMS, cree una clave personalizada y añada la siguiente política abriendo una RFC con el tipo de cambio KMS Key | Create (es necesario revisar):

JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "Service": "personalize.amazonaws.com"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

- Se debe crear un bucket de S3 con la siguiente política de bucket. Para ello, envíe una RFC con el tipo de cambio S3 Storage | Create Policy. Esta política permite a Amazon Personalize acceder a los datos; ese depósito contendrá los datos que utilizará Amazon Personalize.

  JSON

```
{
"Version":"2012-10-17",
"Id": "PersonalizeS3BucketAccessPolicy",
"Statement": [
{
"Sid": "PersonalizeS3BucketAccessPolicy",
"Effect": "Allow",
"Principal": {
"Service": "personalize.amazonaws.com"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::bucket-name",
"arn:aws:s3:::bucket-name/*"
]
}
```

```
]
}
```

Usa AMS SSP para aprovisionar Amazon QuickSight en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a QuickSight las funciones de su cuenta gestionada por AMS. QuickSight es un servicio de inteligencia empresarial rápido y basado en la nube que ofrece información a todos los miembros de su organización. Al tratarse de un servicio totalmente gestionado, QuickSight le permite crear y publicar fácilmente paneles interactivos que incluyen información sobre el aprendizaje automático (ML). Para obtener más información, consulta Amazon QuickSight.

QuickSight en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a QuickSight mi cuenta de AMS?

Solicite el acceso enviando un mensaje de administración | AWS servicio | Servicio autoaprovisionado | Agregue un tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_quicksight_console_admin_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso QuickSight en mi cuenta de AMS?

- AWS QuickSight No podrá acceder a la configuración de recursos activada debido a que depende de la política de IAM. Sin embargo, el equipo de AMS habilita cada recurso para ti en respuesta a tu solicitud de habilitar el servicio.
- Este modelo no admite el acceso a los recursos para usuarios y grupos individuales porque esta función permite a los usuarios modificar los permisos de IAM, lo que podría comprometer la infraestructura de AMS.
- No se admite la posibilidad de invitar a identidades de IAM desde dentro QuickSight debido al riesgo que implica alterar los objetos de IAM.
- QuickSight El servicio ofrece dos ediciones: Enterprise y Standard. Ambos ofrecen una opción de inicio de sesión único (SSO) que es compatible con AMS. Sin embargo, la edición Enterprise tiene la opción de integrarse QuickSight con Active Directory (AD). QuickSight on AMS no admite la integración con AD debido a incompatibilidades entre la estructura de cuentas de AMS y los requisitos de QuickSight confianza.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla QuickSight en mi cuenta de AMS?

- Cuando AMS reciba este RFC para añadirlo QuickSight, se le enviará una solicitud de servicio con información adicional; envíele lo siguiente:
  - QuickSight nombre de la cuenta (por ejemplo, *CustomerName*-quicksight
  - QuickSight Edición (Standard versus Enterprise)
  - La AWS región en la que se habilita el QuickSight servicio (de forma predeterminada es su AWS región de AMS).
  - Una dirección de correo electrónico de notificación para la QuickSight cuenta.
  - (Opcional) El depósito de S3 donde se encuentran los archivos de datos que se van a analizar.
  - La VPC y la subred IDs que se conectan QuickSight admiten una función para agregar una conexión de VPC, lo que permite la conectividad privada entre los recursos de la cuenta QuickSight y los recursos dentro de ella.

Un operador de AMS realiza el proceso de registro en tu nombre y configura dos funcionalidades: QuickSight

- Detección automática de fuentes de datos.
- Conexiones de VPC.

> **Note**
>
> Estas acciones deben ser realizadas por un operador de AMS porque se requieren permisos elevados de IAM y VPC durante el proceso de inicio de sesión.

Utilice AMS SSP para aprovisionar Amazon Rekognition en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon Rekognition directamente en su cuenta gestionada por AMS. Amazon Rekognition facilita la adición de análisis de imágenes y vídeo a sus aplicaciones mediante una tecnología de aprendizaje profundo comprobada y altamente escalable que no requiere conocimientos de aprendizaje automático para su uso. Con Amazon Rekognition, puede identificar objetos, personas, texto,

escenas y actividades en imágenes y vídeos, así como detectar cualquier contenido inapropiado. Amazon Rekognition también ofrece funciones de búsqueda y análisis faciales de alta precisión que puede utilizar para detectar, analizar y comparar rostros en una amplia variedad de casos de uso relacionados con la verificación de usuarios, el conteo de personas y la seguridad pública.

Con las etiquetas personalizadas Amazon Rekognition, puede identificar objetos y escenas en imágenes que se adapten específicamente a las necesidades de su empresa. Por ejemplo, puede crear un modelo para clasificar piezas específicas de la máquina en su línea de ensamblaje o para detectar plantas insalubres. Amazon Rekognition Custom Labels se ocupa del trabajo pesado de desarrollo de modelos por usted, por lo que no es necesario tener experiencia en aprendizaje automático. Solo tiene que proporcionar imágenes de los objetos o escenas que desee identificar y el servicio se encargará del resto.

Para obtener más información, consulte Amazon Rekognition.

Preguntas frecuentes sobre Amazon Rekognition en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Amazon Rekognition en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_rekognition_console_role & customer_rekognition_service_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Rekognition en mi cuenta de AMS?

La funcionalidad completa de Amazon Rekognition está disponible con la función de servicio autoaprovisionada de Amazon Rekognition.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon Rekognition en mi cuenta de AMS?

Si utiliza Kinesis Video Streams que proporciona la transmisión de vídeo de origen para un procesador de transmisión de Amazon Rekognition Video o una transmisión de datos como destino para escribir datos en Kinesis Data Streams, proporcione a AMS un al crear el RFC. `kinesisStreamName`

Utilice AMS SSP para aprovisionar Amazon SageMaker AI en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon SageMaker AI directamente en su cuenta gestionada por AMS. SageMaker La IA proporciona a todos los desarrolladores y científicos de datos la capacidad de crear, entrenar e implementar modelos de aprendizaje automático rápidamente. Amazon SageMaker AI es un servicio totalmente gestionado que cubre todo el flujo de trabajo de aprendizaje automático para etiquetar y preparar los datos, elegir un algoritmo, entrenar el modelo, ajustarlo y optimizarlo para su implementación, hacer predicciones y tomar medidas. Sus modelos se ponen en producción más rápido, con mucho menos esfuerzo y menor coste. Para obtener más información, consulta Amazon SageMaker AI.

SageMaker Preguntas frecuentes sobre la IA en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito el acceso a la SageMaker IA en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (ct-1w8z66n899dct) el tipo de cambio. Este RFC proporciona las siguientes funciones de IAM a su cuenta: y una función de servicio. `customer_sagemaker_admin_role` `AmazonSageMaker-ExecutionRole-Admin` Una vez que se haya aprovisionado la SageMaker IA en su cuenta, debe incorporar la `customer_sagemaker_admin_role` función a su solución de federación. No puedes acceder directamente al rol de servicio; el servicio de SageMaker IA lo usa mientras realiza diversas acciones, tal como se describe aquí: Transferir roles.

P: ¿Cuáles son las restricciones para usar la SageMaker IA en mi cuenta de AMS?

- La función Amazon SageMaker AI IAM de AMS no admite los siguientes casos de uso:
  - SageMaker AI Studio no es compatible en este momento.
  - SageMaker No se admite AI Ground Truth para gestionar el personal privado, ya que esta función requiere un acceso demasiado permisivo a los recursos de Amazon Cognito. Si es necesario gestionar un personal privado, puede solicitar un rol de IAM personalizado con permisos combinados de SageMaker IA y Amazon Cognito. De lo contrario, recomendamos utilizar personal público (respaldado por Amazon Mechanical Turk) o proveedores de AWS Marketplace servicios para el etiquetado de los datos.

- Creación de puntos de enlace de VPC para admitir las llamadas de API a los servicios de SageMaker IA (aws.sagemaker). {region} .notebook, com.amazonaws. {region} .sagemaker.api y com.amazonaws. {region} .sagemaker.runtime) no es compatible, ya que los permisos no se pueden limitar únicamente a los servicios relacionados con la IA. SageMaker Para respaldar este caso de uso, envíe un RFC de administración | Otros | Otros para crear puntos de enlace de VPC relacionados.
- SageMaker No se admite el escalado automático de terminales de SageMaker IA, ya que la IA requiere `DeleteAlarm` permisos en cualquier recurso («*»). Para admitir el escalado automático de un punto final, envíe una RFC de administración | Otros | Otros para configurar el escalado automático de un punto final de SageMaker IA.

P: ¿Cuáles son los requisitos previos o las dependencias para usar la SageMaker IA en mi cuenta de AMS?

- Los siguientes casos de uso requieren una configuración especial antes de su uso:
  - Si se va a utilizar un depósito de S3 para almacenar datos y artefactos de modelos, debe solicitar un depósito de S3 con el nombre de las palabras clave necesarias (» SageMaker «, «Sagemaker», «sagemaker» o «aws-glue») con un mensaje de Deployment | Advanced stack components | S3 storage | Create RFC.
  - Si se va a utilizar Elastic File Store (EFS), el almacenamiento de EFS debe configurarse en la misma subred y estar permitido por los grupos de seguridad.
  - Si otros recursos requieren acceso directo a los servicios de SageMaker IA (cuadernos, API, tiempo de ejecución, etc.), la configuración debe solicitarla:
    - Enviar una RFC para crear un grupo de seguridad para el punto final (Implementación | Componentes de pila avanzados | Grupo de seguridad | Crear (auto)).
    - Envío de una administración | Otra | Otra | Cree una RFC para configurar los puntos finales de VPC relacionados.

P: ¿Cuáles son las convenciones de nomenclatura admitidas para los recursos a los que se **`customer_sagemaker_admin_role`** puede acceder directamente? (Las siguientes son para actualizar y eliminar permisos; si necesita otras convenciones de nomenclatura compatibles para sus recursos, póngase en contacto con un arquitecto de nube de AMS para que lo asesore).

- Recurso: `AmazonSageMaker-ExecutionRole-*` Función pasajera

    - Permisos: la función de servicio autoaprovisionada de SageMaker IA respalda el uso de la función de servicio de SageMaker IA (`AmazonSageMaker-ExecutionRole-*`) con AWS Glue AWS RoboMaker, y. AWS Step Functions
- Recurso: Secrets on AWS Secrets Manager
    - Permisos: describir, crear, obtener y actualizar los secretos con un `AmazonSageMaker-*` prefijo.
    - Permisos: Describa y obtenga los secretos cuando la etiqueta `SageMaker` de recurso esté configurada en. `true`
- Recurso: Repositorios en AWS CodeCommit
    - Permisos: crear/eliminar repositorios con un prefijo. `AmazonSageMaker-*`
    - Permisos: Git Pull/Push en repositorios con los siguientes prefijos, `*sagemaker**SageMaker*`, y. `*Sagemaker*`
- Recurso: Repositorios de Amazon ECR (Amazon Elastic Container Registry)
    - Permisos: Permisos: establezca, elimine las políticas de repositorio y cargue imágenes de contenedores cuando se utilice la siguiente convención de nomenclatura de recursos. `*sagemaker*`
- Recurso: buckets de Amazon S3
    - Permisos: obtener, colocar, eliminar un objeto y anular la carga multiparte de objetos de S3 cuando los recursos tengan los siguientes prefijos:`*SageMaker*`, y. `*Sagemaker* *sagemaker* aws-glue`
    - Permisos: obtiene los objetos de S3 cuando la `SageMaker` etiqueta está establecida en. `true`
- Recurso: Amazon CloudWatch Log Group
    - Permisos: crear un grupo de registros o transmitir, colocar un evento de registro, enumerar, actualizar, crear, eliminar la entrega de registros con el siguiente prefijo:`/aws/sagemaker/*`.
- Recurso: Amazon CloudWatch Metric
    - Permisos: coloque los datos de las métricas cuando se usen los siguientes prefijos: `AWS/SageMaker` `AWS/SageMaker/aws/SageMaker`,`aws/SageMaker/`,, `aws/sagemakeraws/sagemaker/`, y`/aws/sagemaker/.`.
- Recurso: Amazon CloudWatch Dashboard
    - Permisos: Create/Delete paneles de control cuando se utilizan los siguientes prefijos:. `customer_*`
- Recurso: tema Amazon SNS (Simple Notification Service)

- Permisos: Subscribe/Create tema en el que se utilizan los siguientes prefijos: `*sagemaker**SageMaker*`, y. `*Sagemaker*`

P: ¿Cuál es la diferencia entre **`AmazonSageMakerFullAccess`** y? **`customer_sagemaker_admin_role`**

`customer_sagemaker_admin_role`Con el `customer_sagemaker_admin_policy` proporciona casi los mismos permisos que, AmazonSageMakerFullAccess excepto:

- Permiso para conectarse con AWS RoboMaker Amazon Cognito y AWS Glue sus recursos.
- SageMaker Escalado automático de puntos finales de IA. Debe enviar una RFC junto con el tipo de cambio Management | Advanced stack components | Identity and Access Management (IAM) | Actualizar entidad o política (es necesario revisar) el tipo de cambio (ct-27tuth19k52b4) para aumentar los permisos de escalado automático de forma temporal o permanente, ya que el escalado automático requiere un acceso permisivo al servicio. CloudWatch

P: ¿Cómo puedo adoptar una clave gestionada por el cliente en el cifrado de datos en reposo? AWS KMS

Debe asegurarse de que la política de claves se haya configurado correctamente en las claves administradas por el cliente para que los usuarios o roles de IAM relacionados puedan utilizarlas. Para obtener más información, consulte el documento sobre la política AWS KMS clave.

Utilice AMS SSP para aprovisionar Amazon Simple Email Service en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las funciones de Amazon Simple Email Service (Amazon SES) directamente en su cuenta gestionada por AMS. Amazon Simple Email Service es un servicio de envío de correo electrónico basado en la nube diseñado para ayudar a los profesionales del marketing digital y a los desarrolladores de aplicaciones a enviar correos electrónicos de marketing, notificaciones y transacciones.

Puede utilizar la interfaz SMTP o una de ellas AWS SDKs para integrar Amazon SES directamente en sus aplicaciones existentes. También puede integrar las capacidades de envío de correo electrónico de Amazon SES en el software que ya utiliza, como los sistemas de venta de entradas y los clientes de correo electrónico.

Para obtener más información, consulta Amazon Simple Email Service.

Preguntas frecuentes sobre Amazon SES en AWS Managed Services

P: ¿Cómo solicito acceso a Amazon SES en mi cuenta de AMS?

Solicite acceso a Amazon SES enviando una RFC con el servicio Management | AWS | Self-provisioned service | Add (ct-1w8z66n899dct) tipo de cambio. Este RFC asigna la siguiente función de IAM a su cuenta:. `customer_ses_admin_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon SES en mi cuenta de AMS?

- Debe configurar una política de bucket de S3 para permitir que Amazon SES publique eventos en el bucket.
- Debe usar una clave CMK predeterminada (AWS SES) o configurar una clave CMK para permitir que Amazon SES cifre los correos electrónicos y envíe eventos a otros recursos de servicio, como Amazon S3, Amazon SNS, Lambda y Firehose, que pertenezcan a la cuenta.

P: ¿Cuáles son las restricciones para usar Amazon SES en mi cuenta de AMS?

Debe recaudar fondos RFCs para crear los siguientes recursos:

- Un usuario de SMTP y un rol de servicio de IAM con PutEvents permiso para una transmisión de Kinesis Firehose.
- Debe crear nuevos AWS recursos, como un bucket de S3, una transmisión de Firehose o un tema de SNS, mediante los tipos de cambio de AMS para que las reglas y los destinos de los conjuntos de configuración de Amazon SES funcionen con esos recursos.
- Credenciales SMTP. Para solicitar nuevas credenciales SMTP, utilice el tipo de cambio (Administración | Otros | Otros | Crear). AMS crea las credenciales y las añade a Secrets Manager por usted.

Utilice AMS SSP para aprovisionar Amazon Simple Workflow Service en su cuenta de AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las funciones de Amazon Simple Workflow Service (Amazon SWF) directamente en su cuenta gestionada por AMS. Amazon Simple Workflow Service ayuda a los desarrolladores a crear, ejecutar y escalar trabajos en

segundo plano que tienen pasos paralelos o secuenciales. Puede pensar en Amazon SWF como un rastreador de estado y coordinador de tareas totalmente gestionado en la nube. Si los pasos de la aplicación tardan más de 500 milisegundos en completarse, necesita realizar un seguimiento del estado del procesamiento o necesita recuperarse o volver a intentarlo si se produce un error en una tarea, Amazon SWF puede ayudarle. Para obtener más información, consulte Amazon Simple Workflow Service.

Preguntas frecuentes sobre Amazon SWF en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo puedo solicitar acceso a Amazon SWF en mi cuenta de AMS?

Para solicitar el acceso, envíe un mensaje de administración | AWS servicio | Servicio de aprovisionamiento automático | Añada un tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_swf_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon SWF en mi cuenta de AMS?

Los `InvokeFunction` permisos de Lambda se han incluido en este servicio; sin embargo, el AMS `customer_deny_policy` que se añade a todas las funciones de cliente de AMS deniega explícitamente el acceso a las funciones de Lambda de AMS y a los recursos propiedad de AMS. Para etiquetar o quitar la etiqueta de los recursos de Amazon SWF, envíe un formulario Management | Other | Other Change Type.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar Amazon SWF en mi cuenta de AMS?

Amazon SWF depende del AWS Lambda servicio, por lo que se han proporcionado permisos para invocar Lambda como parte de esta función y no se requieren permisos adicionales para invocar Lambda desde Amazon SWF. De lo contrario, no hay requisitos previos para utilizar Amazon SWF.

Utilice AMS SSP para aprovisionar Amazon Textract en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Amazon Textract directamente en su cuenta gestionada por AMS. Amazon Textract es un servicio de aprendizaje automático totalmente gestionado que extrae automáticamente el texto impreso, la escritura a mano y otros datos de los documentos escaneados, lo que va más allá del

simple reconocimiento óptico de caracteres (OCR) para identificar, comprender y extraer datos de formularios y tablas. Para obtener más información, consulte Amazon Textract.

Preguntas frecuentes sobre Amazon Textract en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito que Amazon Textract se configure en mi cuenta de AMS?

Para solicitar acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona las siguientes funciones de IAM a su cuenta:, y. `customer_textract_console_role` `customer_textract_human_review_execution_role` `customer_ec2_textract_instance_profile` Una vez aprovisionado en su cuenta, debe incorporar el rol a su solución de `customer_textract_console_role` federación.

P: ¿Cuáles son las restricciones para usar Amazon Textract en mi cuenta de AMS?

No hay restricciones para el uso de Amazon Textract en tu cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon Textract en mi cuenta de AMS?

Para solicitar la creación de un bucket de S3, envíe un RFC Deployment | Advanced stack components |S3 storage | Create (ct-1a68ck03fn98r).

Utilice AMS SSP para aprovisionar Amazon Transcribe en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de Amazon Transcribe directamente en su cuenta gestionada por AMS. Amazon Transcribe es un servicio de reconocimiento de voz automático totalmente gestionado y con formación continua que genera automáticamente transcripciones de texto con fecha y hora a partir de archivos de audio. Amazon Transcribe permite a los desarrolladores añadir speech-to-text funciones a sus aplicaciones con facilidad. Los datos de audio son prácticamente imposibles de buscar y analizar para las computadoras. Por lo tanto, la voz grabada debe convertirse en texto antes de poder utilizarla en aplicaciones. Históricamente, los clientes tenían que trabajar con proveedores de transcripciones, lo que les obligaba a firmar contratos costosos y les resultaba difícil integrarlos en sus equipos tecnológicos para llevar a cabo esta tarea. Muchos de estos proveedores utilizan tecnologías anticuadas que no se adaptan bien a los diferentes escenarios, como el audio de baja fidelidad de

los teléfonos, que es común en los centros de atención al cliente, lo que se traduce en una precisión deficiente.

Amazon Transcribe utiliza un proceso de aprendizaje profundo denominado reconocimiento automático de voz (ASR) para convertir la voz en texto de forma rápida y precisa. Amazon Transcribe se puede utilizar para transcribir las llamadas del servicio de atención al cliente, automatizar los subtítulos y los subtítulos opcionales y generar metadatos para los activos multimedia a fin de crear un archivo con capacidad de búsqueda completa. Puede usar Amazon Transcribe Medical para añadir speech-to-text capacidades médicas a las aplicaciones de documentación clínica. Para obtener más información, consulte Amazon Transcribe.

Preguntas frecuentes sobre Amazon Transcribe en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito que Amazon Transcribe se configure en mi cuenta de AMS?

Solicite acceso enviando un formulario de administración | AWS servicio | Servicio autoaprovisionado | Agregue (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_transcribe_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Amazon Transcribe en mi cuenta de AMS?

Debe usar «customer-transcribe*» como prefijo para sus buckets cuando trabaje con Transcribe, a menos que RA especifique lo contrario.

No puedes crear un rol de IAM en Amazon Transcribe.

No puede usar un bucket de S3 administrado por un servicio para generar datos en el SSPS predeterminado (si es necesario, póngase en contacto con la CA de su cuenta).

Debe enviar Risk Acceptance si quiere utilizar claves de KMS administradas por el cliente que no estén incluidas en el espacio de nombres AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Amazon Transcribe en mi cuenta de AMS?

S3 debe tener acceso a los buckets con el nombre «customer-transcribe*». Se requiere KMS para poder utilizar Amazon Transcribe si los buckets de S3 están cifrados con claves de KMS. Si no es necesario cifrar un bucket, se puede eliminar la opción «KMStranscribePermitir».

Usa AMS SSP para aprovisionar Amazon WorkSpaces en tu cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a WorkSpaces las funciones de su cuenta gestionada por AMS. WorkSpaces le permite aprovisionar escritorios virtuales de Microsoft Windows o Amazon Linux basados en la nube para sus usuarios, conocidos como WorkSpaces. WorkSpaces elimina la necesidad de adquirir e implementar hardware o instalar software complejo. Puede agregar o eliminar rápidamente a los usuarios en función de las necesidades. Los usuarios acceden a ellos WorkSpaces mediante una aplicación cliente desde un dispositivo compatible o, en el caso de Windows WorkSpaces, desde un navegador web, e inician sesión con sus credenciales de Active Directory (AD) locales existentes.

Para obtener más información, consulta Amazon WorkSpaces.

WorkSpaces en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a WorkSpaces mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_workspaces_console_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso WorkSpaces en mi cuenta de AMS?

La funcionalidad completa de Workspaces está disponible con la función de servicio de WorkSpaces autoaprovisionamiento de Amazon.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla en mi cuenta de AMS? WorkSpaces

- WorkSpaces están limitados por AWS región; por lo tanto, el AD Connector debe configurarse en la misma AWS región en la que se alojan las WorkSpaces instancias.

  Los clientes pueden conectarse WorkSpaces al AD del cliente mediante uno de los dos métodos siguientes:

  1. Uso del conector AD para la autenticación mediante proxy en el servicio de Active Directory local (preferido):

Configura Active Directory (AD) Connector en tu cuenta AMS antes de integrar la WorkSpaces instancia con el servicio de directorio local. El AD Connector actúa como un proxy para que los usuarios de AD existentes (de su dominio) se conecten WorkSpaces mediante las credenciales de AD locales existentes. Se prefiere esta opción porque WorkSpaces se unen directamente al dominio local del cliente, que actúa como bosque de recursos y de usuarios, lo que proporciona un mayor control por parte del cliente.

Para obtener más información, consulte Prácticas recomendadas para implementar Amazon WorkSpaces (escenario 1).

2. Uso de AD Connector con AWS Microsoft AD, una VPC de Shared Services y una confianza unidireccional con el entorno local:

   También puedes autenticar a los usuarios con tu directorio local estableciendo primero una confianza de salida unidireccional entre el AD administrado por AMS y el AD local. WorkSpaces se unirá a AD administrado por AMS mediante un AD Connector. WorkSpaces Luego, los permisos de acceso se delegarán a las WorkSpaces instancias a través del AD administrado por AMS, sin necesidad de establecer una confianza bidireccional con el entorno local. En este escenario, el bosque de usuarios estará en el AD del cliente y el bosque de recursos estará en el AD administrado por AMS (los cambios en el AD administrado por AMS se pueden solicitar mediante RFC). Tenga en cuenta que la conectividad entre la WorkSpaces VPC y la VPC de MALZ Shared Services que ejecuta AD gestionado por AMS se establece mediante Transit Gateway.

   Para obtener más información, consulte Prácticas recomendadas para implementar Amazon WorkSpaces (escenario 6).

> **Note**
>
> El AD Connector se puede configurar enviando una RFC de administración | Otros | Otros | Crear tipo de cambio con los detalles de configuración de AD necesarios; para obtener más información, consulte Crear un conector AD. Si se utiliza el método 2 para crear un bosque de recursos en un AD administrado por AMS, envíe otro RFC de administración | Otros | Otros | Cree un tipo de cambio en la cuenta de servicios compartidos de AMS ejecutando el AD administrado por AMS.

Utilice AMS SSP para proporcionar servicios de código AMS en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades de los servicios de código de AMS directamente en su cuenta gestionada por AMS. Los servicios de código de AMS son un paquete patentado de los servicios de administración de código de AWS, tal como se detalla a continuación. Puede optar por implementar todos los servicios de AMS con los servicios de código de AMS o puede implementarlos en AMS de forma individual.

Los servicios de AMS Code incluyen los siguientes servicios:

- AWS CodeCommit: un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git. Permite que los equipos puedan colaborar en el código en un ecosistema seguro y altamente escalable. CodeCommit elimina la necesidad de operar su propio sistema de control de código fuente o preocuparse por escalar su infraestructura. Puede usar CodeCommit para almacenar de forma segura cualquier cosa, desde código fuente a binarios, y funciona perfectamente con sus herramientas Git existentes. Para obtener más información, consulte AWS CodeCommit

  Para implementarlo en su cuenta de AMS de forma independiente de los servicios de AMS Code, consulteUtilice AMS SSP para aprovisionar AWS CodeCommit en su cuenta AMS.
- AWS CodeBuild: Un servicio de integración continua totalmente gestionado que compila el código fuente, ejecuta pruebas y produce paquetes de software listos para su implementación. Con CodeBuild esto, no necesita aprovisionar, administrar ni escalar sus propios servidores de compilación. CodeBuild escala de forma continua y procesa varias compilaciones simultáneamente, para que sus compilaciones no se queden esperando en una cola. Puede comenzar con rapidez usando entornos de compilación preempaquetados, o crear sus propios entornos de compilación personalizados que utilicen sus propias herramientas de compilación. Con CodeBuild, se le cobra por minuto por los recursos informáticos que utilice. Para obtener más información, consulte AWS CodeBuild

  Para implementarlo en su cuenta de AMS independientemente de los servicios de AMS Code, consulteUtilice AMS SSP para aprovisionar AWS CodeBuild en su cuenta AMS.
- AWS CodeDeploy: un servicio de implementación totalmente gestionado que automatiza las implementaciones de software en una variedad de servicios informáticos, como Amazon EC2 y sus servidores locales. AWS CodeDeploy le ayuda a lanzar nuevas funciones rápidamente, le ayuda a evitar el tiempo de inactividad durante la implementación de las aplicaciones y gestiona

la complejidad de la actualización de las aplicaciones. Se puede utilizar AWS CodeDeploy para automatizar las implementaciones de software, lo que elimina la necesidad de realizar operaciones manuales propensas a errores. El servicio se amplía para adaptarse a sus necesidades de implementación. Para obtener más información, consulte AWS CodeDeploy

Para implementarlo en su cuenta de AMS independientemente de los servicios de AMS Code, consulteUtilice AMS SSP para aprovisionar AWS CodeDeploy en su cuenta AMS.

- AWS CodePipeline: un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para actualizar las aplicaciones y la infraestructura de forma rápida y fiable. CodePipeline automatiza las fases de creación, prueba e implementación del proceso de lanzamiento cada vez que se produce un cambio de código, en función del modelo de lanzamiento que defina. Le permite entregar características y actualizaciones de forma rápida y de confianza. Puedes integrarlo fácilmente AWS CodePipeline con servicios de terceros, como GitHub tu propio complemento personalizado. Con AWS CodePipeline, solo pagas por lo que usas. No es necesario pagar cuotas iniciales ni asumir compromisos a largo plazo. Para obtener más información, consulte AWS CodePipeline

  Para implementar esto en su cuenta de AMS independientemente de los servicios de AMS Code, consulteUtilice AMS SSP para aprovisionar AWS CodePipeline en su cuenta AMS.

Preguntas frecuentes sobre los servicios de código AMS en AWS Managed Services

P: ¿Cómo solicito acceso a los servicios de AMS Code en mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_code_suite_console_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación. En este momento`customer_codebuild_service_role`, `customer_codedeploy_service_role` AMS Operations también desplegará las funciones de `aws_code_pipeline_service_role` servicio en su cuenta CodeDeploy y CodeBuild los CodePipeline servicios. Si se necesitan permisos de IAM adicionales para ello, envíe una solicitud de servicio de AMS. `customer_codebuild_service_role`

> **Note**
>
> También puede añadir estos servicios por separado; para obtener más información, consulte Utilice AMS SSP para aprovisionar AWS CodeBuild en su cuenta AMSUtilice AMS SSP para

aprovisionar AWS CodeDeploy en su cuenta AMS, yUtilice AMS SSP para aprovisionar AWS CodePipeline en su cuenta AMS, respectivamente.

P: ¿Cuáles son las restricciones para usar los servicios de AMS Code en mi cuenta AMS?

- AWS CodeCommit: La función de activación CodeCommit está desactivada debido a los derechos asociados para crear temas de SNS. La autenticación directa CodeCommit está restringida; los usuarios deben autenticarse con Credential Helper. Algunos comandos de KMS también están restringidos: kms: cifrar, kms: descifrar,, y. kms: ReEncrypt kms: GenereteDataKey kms: GenerateDataKeyWithoutPlaintext kms: DescribeKey
- CodeBuild: Para el acceso de administrador de la AWS CodeBuild consola, los permisos están limitados a nivel de recursos; por ejemplo, CloudWatch las acciones están limitadas a recursos específicos y el `iam:PassRole` permiso está controlado.
- CodeDeploy: Actualmente solo CodeDeploy admite despliegues en Amazon EC2 /On-Premimises. No se admiten implementaciones directas en ECS y CodeDeploy Lambda.
- CodePipeline: las CodePipeline funciones, las etapas y los proveedores se limitan a lo siguiente:
  - Etapa de implementación: Amazon S3 y AWS CodeDeploy
  - Etapa de origen: Amazon S3 AWS CodeCommit, Bit Bucket y GitHub
  - Fase de construcción: AWS CodeBuild y Jenkins
  - Etapa de aprobación: Amazon SNS
  - Etapa de prueba: Jenkins AWS CodeBuild, BlazeMeter pruebas de interfaz de usuario de Ghost Inspector, StormRunner carga de Micro Focus, monitoreo de la API de Runscope
  - Invoke Stage: Step Functions y Lambda

> **Note**
>
> AMS Operations lo implementa `customer_code_pipeline_lambda_policy` en su cuenta; debe estar asociado a la función de ejecución de Lambda para la etapa de invocación de Lambda. Proporcione el nombre del service/execution rol de Lambda con el que desea que se añada esta política. Si no hay una service/execution función Lambda personalizada, AMS crea una nueva función denominada`customer_code_pipeline_lambda_execution_role`, que es una copia de `customer_lambda_basic_execution_role` junto con. `customer_code_pipeline_lambda_policy`

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar los servicios de AMS Code en mi cuenta de AMS?

- CodeCommit: Si los depósitos de S3 están cifrados con AWS KMS claves, es obligatorio utilizarlos AWS KMS con S3. AWS CodeCommit
- CodeBuild: Si se requieren permisos de IAM adicionales para la función de AWS CodeBuild servicio definida, solicítelos mediante una solicitud de servicio de AMS.
- CodeDeploy: Ninguno.
- CodePipeline: Ninguno. AWS los servicios compatibles—AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy—deben lanzarse antes o junto con el lanzamiento de CodePipeline. Sin embargo, esto lo hace un ingeniero de AMS.

Utilice AMS SSP para aprovisionar AWS Amplify en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Amplify las funciones de su cuenta gestionada por AMS. AWS Amplify Se trata de una solución completa que permite a los desarrolladores frontend, web y móvil crear, conectar y alojar fácilmente aplicaciones completas. Amplify ofrece flexibilidad para aprovechar la variedad de AWS servicios a medida que evolucionan sus casos de uso. Amplify ofrece productos para crear aplicaciones completas para iOS, Android, Flutter, Web y React Native. Para obtener más información, consulte AWS Amplify.

AWS Amplify en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo AWS Amplify solicito que se configure mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_amplify_console_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

Además, debe proporcionar una certificación de aceptación del riesgo, ya que AWS Amplify tiene permisos que modifican la infraestructura. Para ello, trabaje con su administrador de prestación de servicios en la nube (CSDM).

P: ¿Cuáles son las restricciones de uso AWS Amplify en mi cuenta de AMS?

Debes usarlo `'amplify*'` como prefijo para tus cubos cuando trabajes con Amplify, a menos que RA y especifiquen lo contrario.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarlos en mi cuenta de AMS? AWS Amplify

No hay requisitos previos para el uso de AWS Amplify en su cuenta de AMS.

Solo entornos Malz: el rol incorporado predeterminado para Amplify es «customer_amplify_console_role». Para usar un rol personalizado, primero implemente las entidades de IAM. A continuación, cree una RFC adicional para añadir su función personalizada a la lista de cuentas de aplicaciones permitidas por la Política de control de servicios.

Utilice AMS SSP para aprovisionar AWS AppSync

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS AppSync las funciones de su cuenta gestionada por AMS. AWS AppSync simplifica el desarrollo de aplicaciones al permitirle crear una API flexible para acceder, manipular y combinar de forma segura los datos de una o más fuentes de datos. AWS AppSync es un servicio gestionado que utiliza GraphQL para facilitar que las aplicaciones obtengan exactamente los datos que necesitan.

Con AWS AppSync, puede crear aplicaciones escalables, incluidas las que requieren actualizaciones en tiempo real, en una variedad de fuentes de datos, como almacenes de datos NoSQL, bases de datos relacionales APIs, HTTP y sus fuentes de datos personalizadas con. AWS Lambda En el caso de las aplicaciones móviles y web, AWS AppSync también ofrece acceso local a los datos cuando los dispositivos se desconectan y sincronización de datos con resolución de conflictos personalizable cuando vuelven a estar en línea. Para obtener más información, consulte AWS AppSync.

AWS AppSync en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito el acceso AWS AppSync a mi cuenta AMS?

Solicite el acceso enviando un mensaje de administración | AWS servicio | Servicio autoaprovisionado | Agregue un tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones de IAM a su cuenta: y. `customer_appsync_service_role` `customer_appsync_author_role` Una vez aprovisionadas en su cuenta, debe incorporarlas a su solución `customer_appsync_author_role` de federación.

P: ¿Cuáles son las restricciones para su uso? AWS AppSync

- Al crear una fuente de datos, AppSync el cliente debe especificar el rol de servicio creado anteriormente, no se permite la creación de un nuevo rol y, por lo tanto, devolverá un acceso denegado
- AppSync Los roles se configuran para restringir los permisos a los recursos que contienen los prefijos «AMS-» o «MC-» a fin de evitar cualquier modificación en la infraestructura de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para su uso? AWS AppSync

El servicio permite utilizar varios otros servicios como fuente de datos. Los permisos básicos para usarlos como tales están incluidos en la función de servicio (`customer_appsync_service_role`), pero debe seleccionar manualmente la función de servicio al utilizar el servicio.

Utilice AMS SSP para aprovisionar AWS App Mesh en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS App Mesh las funciones de su cuenta gestionada por AMS. AWS App Mesh proporciona redes a nivel de aplicación para facilitar que sus servicios se comuniquen entre sí a través de varios tipos de infraestructuras informáticas. App Mesh estandariza la forma en que se comunican sus servicios, lo que le brinda end-to-end visibilidad y garantiza una alta disponibilidad para sus aplicaciones.

AWS App Mesh facilita la ejecución de los servicios al proporcionar una visibilidad uniforme y controles de tráfico de red para los servicios integrados en varios tipos de infraestructuras informáticas. App Mesh elimina la necesidad de actualizar el código de la aplicación para cambiar la forma en que se recopilan los datos de supervisión o se enruta el tráfico entre los servicios. App Mesh configura cada servicio para exportar los datos de supervisión e implementa una lógica de control de comunicaciones coherente en toda la aplicación. Esto permite identificar rápidamente la ubicación exacta de los errores y redirigir automáticamente el tráfico de la red cuando se producen fallos o cuando es necesario implementar cambios en el código. Para obtener más información, consulte AWS App Mesh.

AWS App Mesh en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito el acceso AWS App Mesh a mi cuenta AMS?

Solicite el acceso enviando un mensaje de administración | AWS servicio | Servicio autoaprovisionado | Agregue un tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona

la siguiente función de IAM a su cuenta:. `customer_app_mesh_console_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso del? AWS App Mesh

Todas las funciones AWS App Mesh de están disponibles en su cuenta AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para su uso? AWS App Mesh

No hay requisitos previos ni dependencias que debas usar AWS App Mesh en tu cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Audit Manager en su cuenta AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las funciones de Audit Manager directamente en su cuenta gestionada por AMS. Audit Manager le ayuda a auditar continuamente su AWS uso para simplificar la evaluación del riesgo y el cumplimiento de las normativas y los estándares del sector. Audit Manager automatiza la recopilación de evidencias para facilitar la evaluación de si sus políticas, procedimientos y actividades funcionan de manera eficaz. Cuando llega el momento de realizar una auditoría, Audit Manager le ayuda a gestionar las revisiones de sus controles por parte de las partes interesadas y le ayuda a crear informes listos para la auditoría con un esfuerzo manual significativamente menor. Para obtener más información, consulte Audit Manager.

AWS Audit Manager en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS Audit Manager mi cuenta de AMS?

Puede solicitar el acceso mediante el envío de los AWS servicios RFC Management | AWS service | Self-provisioned service | Add (es necesario revisar) (ct-3qe6io8t6jtny). Este RFC establece `customer-audit-manager-admin-Role` la siguiente función de IAM en su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso? AWS Audit Manager

No hay restricciones de uso AWS Audit Manager en tu cuenta de AMS. AWS Audit Manager Se proporciona una funcionalidad completa para.

P: ¿Cuáles son los requisitos previos o las dependencias para su uso? AWS Audit Manager

1. Debe proporcionar a AMS el depósito s3 en el que desea reports/assessments residir.

2. Si desea cifrar con el servicio, debe proporcionar a AMS el ARN CMK de KMS para que lo utilice.
3. Si desea enviar una notificación de SNS a un tema, debe proporcionar el nombre del tema o ARN.
4. (Opcional) Hay un requisito previo adicional si quiere habilitar Organizations como parte de su zona de aterrizaje multicuenta en Audit Manager y desea una cuenta de administrador delegado: en el campo de descripción de RFC (Management | AWS service | Compatible Service| Add), mencione que desea utilizar la cuenta de administrador delegado como parte de la configuración de Audit Manager y proporcione la siguiente información:
   - KMS CMK ARN (utilizado inicialmente para configurar Audit Manager)
   - ID de cuenta de administrador delegado para que Audit Manager lo utilice como parte de esta zona de aterrizaje multicuenta (puede ser una cuenta de aplicación MALZ)

Utilice AMS SSP para aprovisionar AWS Batch en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Batch las funciones de su cuenta gestionada por AMS. AWS Batch permite a los desarrolladores, científicos e ingenieros ejecutar cientos de miles de trabajos de computación por lotes de manera fácil y eficiente. AWS AWS Batch aprovisiona de forma dinámica la cantidad y el tipo óptimos de recursos informáticos (como instancias optimizadas para la CPU o la memoria) en función del volumen y los requisitos de recursos específicos de los trabajos por lotes enviados. De este AWS Batch modo, no es necesario instalar ni administrar el software de computación por lotes ni los clústeres de servidores que utiliza para ejecutar sus trabajos, lo que le permite centrarse en analizar los resultados y resolver los problemas. Para obtener más información, consulte AWS Batch.

AWS Batch en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS Batch mi cuenta de AMS?

1. Para solicitar acceso a AWS Batch, envíe el RFC Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC establece las siguientes funciones y políticas de IAM en su cuenta:

Funciones de IAM:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`

- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

Políticas:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. Una vez aprovisionado en su cuenta, debe incorporar el rol a su `customer_batch_console_role` solución de federación.

P: ¿Cuáles son las restricciones de uso? AWS Batch

Al crear el entorno de cómputo, debes etiquetar EC2 las instancias como «customer_batch» o «customer-batch». Si las instancias no están etiquetadas, las instancias no se finalizarán por lotes cuando se complete el trabajo.

P: ¿Cuáles son los requisitos previos o las dependencias para su uso? AWS Batch

No hay requisitos previos ni dependencias que debas usar AWS Batch en tu cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Certificate Manager en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades AWS Certificate Manager (ACM) directamente en su cuenta gestionada por AMS. AWS Certificate Manager es un servicio que le permite aprovisionar, administrar e implementar certificados de Layer/Transport Secure Sockets Layer Security (SSL/TLS) públicos y privados para usarlos con los servicios y los recursos internos conectados. AWS SSL/TLS los certificados se utilizan para proteger las comunicaciones de red y establecer la identidad de los sitios web a través de Internet, así como de los recursos de las redes privadas. AWS Certificate Manager elimina el lento proceso manual de compra, carga y renovación SSL/TLS de certificados.

Con AWS Certificate Manager, puede solicitar un certificado, implementarlo en AWS recursos integrados en ACM, como Elastic Load Balancers, CloudFront distribuciones de Amazon y API APIs

Gateway, y dejar AWS Certificate Manager que se encargue de las renovaciones de certificados. También le permite crear certificados privados para sus recursos internos y gestionar el ciclo de vida de los certificados de forma centralizada. Los certificados públicos y privados proporcionados AWS Certificate Manager para su uso con los servicios integrados de ACM son gratuitos. Solo paga por los AWS recursos que cree para ejecutar la aplicación. Con AWS Private Certificate Authority, paga mensualmente por el funcionamiento de los certificados privados que emita Autoridad de certificación privada de AWS y por los certificados privados que emita. Para obtener más información, consulte AWS Certificate Manager - AWS Documentación.

Preguntas frecuentes sobre ACM en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS Certificate Manager mi cuenta de AMS?

Solicite el acceso enviando un mensaje de administración | AWS servicio | Servicio autoaprovisionado | Agregue un tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_acm_create_role` Puede usar este rol para crear y administrar certificados ACM. Una vez que se haya aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

Los certificados de ACM se pueden crear mediante los siguientes tipos de cambios, incluso si no ha agregado la función de `customer_acm_create_role` IAM:

- ACM | Crear certificado público
- ACM | Crear certificado privado
- Certificado ACM con adicional | Crear SANs

P: ¿Cuáles son las restricciones de uso del? AWS Certificate Manager

Debe enviar una solicitud de cambio (RFC) a AMS para eliminar o modificar los certificados existentes, ya que estas acciones requieren pleno acceso de administrador (utilice el tipo de cambio Administración | Otros | Otros | Actualización (ct-0xdawir96cy7k). Tenga en cuenta que la política de IAM no puede excluir derechos en función de los nombres de las etiquetas (mc*, ams*, etc.). Los certificados no conllevan ningún coste, por lo que eliminar los certificados no utilizados no es urgente.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Certificate Manager?

Nombre de DNS público existente y acceso para crear registros CNAME de DNS, pero no es necesario que estén alojados en la cuenta gestionada.

Utilice AMS SSP para aprovisionar AWS Private Certificate Authority en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Private Certificate Authority las funciones de su cuenta gestionada por AMS. Los certificados privados se utilizan para identificar y proteger la comunicación entre los recursos conectados en redes privadas, como servidores, dispositivos y aplicaciones móviles y de IoT. Autoridad de certificación privada de AWS es un servicio de CA privado gestionado que le ayuda a gestionar de forma fácil y segura el ciclo de vida de sus certificados privados. Autoridad de certificación privada de AWS le proporciona un servicio de CA privada de alta disponibilidad sin la inversión inicial ni los costos de mantenimiento continuos que implica operar su propia CA privada. Autoridad de certificación privada de AWS extiende las capacidades de administración de certificados de ACM a los certificados privados, lo que le permite crear y administrar certificados públicos y privados de forma centralizada. Puede crear e implementar fácilmente certificados privados para sus AWS recursos mediante la consola de AWS administración o la API de ACM. Para EC2 instancias, contenedores, dispositivos de IoT y recursos locales, puede crear y rastrear certificados privados fácilmente y usar su propio código de automatización del lado del cliente para implementarlos. También tiene la flexibilidad de crear certificados privados y administrarlos usted mismo para las aplicaciones que requieren una vida útil personalizada de los certificados, algoritmos clave o nombres de recursos. Para obtener más información, consulte. Autoridad de certificación privada de AWS

Autoridad de certificación privada de AWS en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito el acceso Autoridad de certificación privada de AWS a mi cuenta AMS?

Solicite el acceso mediante el envío del AWS RFC (Administración | AWS servicio | Servicio compatible). Mediante este RFC, se aprovisionará la siguiente función de IAM en su cuenta:. `customer_acm_pca_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso del? Autoridad de certificación privada de AWS

Actualmente, AWS Resource Access Manager (AWS RAM) no se puede usar para compartir Autoridad de certificación privada de AWS cuentas múltiples.

P: ¿Cuáles son los requisitos previos o las dependencias para su uso? Autoridad de certificación privada de AWS

1. Si planea crear una CRL, necesitará un bucket de S3 para guardarla. Autoridad de certificación privada de AWS deposita automáticamente la CRL en el bucket de Amazon S3 que designe y la actualiza periódicamente. Es un requisito previo que el bucket de S3 tenga la siguiente política de bucket antes de poder configurar una CRL. Para continuar con esta solicitud, cree un RFC con ct-0fpjlxa808sh2 (Administración | Componentes de pila avanzados | Almacenamiento en S3 | Política de actualizaciones) de la siguiente manera:

- Proporcione el nombre o el ARN del bucket de S3.
- Copia la siguiente política en el RFC y sustitúyela por el `bucket-name` nombre del bucket de S3 que desees.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"acm-pca.amazonaws.com"
         },
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::bucket-name/*",
            "arn:aws:s3:::bucket-name"
         ]
      }
   ]
}
```

2. Si el depósito de S3 anterior está cifrado, el director del servicio, acm-pca.amazonaws.com, necesitará permisos para descifrarlo. Para continuar con esta solicitud, cree un RFC con ct-3ovo7px2vsa6n (Administración | Componentes de pila avanzados | Clave KMS | Actualización) de la siguiente manera:

- Proporcione el ARN clave de KMS en el que se debe actualizar la política.
- Copie la siguiente política en el RFC y sustitúyala por el `bucket-name` nombre del bucket de S3 que desee.

```
{
   "Sid":"Allow ACM-PCA use of the key",
   "Effect":"Allow",
   "Principal":{
      "Service":"acm-pca.amazonaws.com"
   },
   "Action":[
      "kms:GenerateDataKey",
      "kms:Decrypt"
   ],
   "Resource":"*",
   "Condition":{
      "StringLike":{
         "kms:EncryptionContext:aws:s3:arn":[
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
            "arn:aws:s3:::bucket_name/audit-report/*",
            "arn:aws:s3:::bucket_name/crl/*"
         ]
      }
   }
}
```

3. Autoridad de certificación privada de AWS CRLs no admiten la configuración de S3 «Bloquear el acceso público a los depósitos y objetos concedidos mediante nuevas listas de control de acceso (ACLs)». Debe deshabilitar esta configuración con la cuenta y el bucket de S3 para poder escribir, CRLs como se menciona en Cómo crear y almacenar de forma segura su CRL para ACM Private CA. Si desea deshabilitarla, cree una nueva RFC con ct-0xdawir96cy7k (Administración | Otros | Otros | Actualizar) y adjunte una Aceptación de riesgo. Autoridad de certificación privada de AWS Si tiene alguna duda sobre la aceptación del riesgo, póngase en contacto con su arquitecto de nube.

Utilice AMS SSP para aprovisionar AWS CloudEndure en su cuenta AMS

> **Note**
>
> Tras el exitoso lanzamiento de AWS Application Migration Service, el servicio de CloudEndure migración ha llegado al final de su vida útil en todas AWS las regiones. Recomendamos a los clientes que lo utilicen AWS Application Migration Service para realizar migraciones a las GovCloud regiones y a las regiones comerciales. Para obtener más información, consulte ¿Qué es? AWS Application Migration Service .
> Si quieres utilizarlos AWS Application Migration Service, ponte en contacto con tu CA para que te guíen.

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a AWS CloudEndure las funciones directamente en su cuenta gestionada por AMS. AWS CloudEndure la migración simplifica, agiliza y automatiza las migraciones a gran escala desde infraestructuras físicas, virtuales y basadas en la nube a otras. AWS CloudEndure La recuperación ante desastres (DR) protege contra el tiempo de inactividad y la pérdida de datos a causa de cualquier amenaza, incluidos el ransomware y la corrupción de los servidores.

AWS CloudEndure en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a CloudEndure mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona el `customer_cloud_endure_user` siguiente usuario de IAM a su cuenta:. Una vez aprovisionadas en tu cuenta, la clave de acceso y la clave secreta del usuario se comparten en AWS Secrets Manager.

Estas políticas también se proporcionan a la cuenta: `customer_cloud_endure_policy` y. `customer_cloud_endure_deny_policy`

Además, debe proporcionar una aceptación del riesgo, ya que la solución de CloudEndure recuperación ante desastres para la integración de aplicaciones tiene permisos que modifican la infraestructura. Para ello, trabaje con su administrador de prestación de servicios en la nube (CSDM).

P: ¿Cuáles son las restricciones de uso CloudEndure en mi cuenta de AMS?

Las instancias de replicación y conversión duraderas en la nube solo se pueden lanzar en la subred que usted indique.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarlas CloudEndure en mi cuenta de AMS? Comparta lo siguiente a través de la correspondencia bidireccional RFC:

- Detalles de la subred de VPC para las instancias de replicación y conversión que se van a lanzar.
- La clave KMS Amazon Resource Name (ARN) si los volúmenes de EBS están cifrados.

Utilice AMS SSP para aprovisionar AWS CloudHSM en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS CloudHSM las funciones de su cuenta gestionada por AMS. AWS CloudHSM le ayuda a cumplir los requisitos corporativos, contractuales y normativos en materia de seguridad de los datos mediante el uso de instancias dedicadas del módulo de seguridad de hardware (HSM) en la nube. AWS AWS y los socios de AWS Marketplace ofrecen una variedad de soluciones para proteger los datos confidenciales dentro de la AWS plataforma, pero para algunas aplicaciones y datos sujetos a mandatos contractuales o reglamentarios para la administración de claves criptográficas, puede ser necesaria una protección adicional. AWS CloudHSM complementa las soluciones de protección de datos existentes y le permite proteger sus claves de cifrado, ya HSMs que están diseñadas y validadas según los estándares gubernamentales para una gestión segura de las claves. AWS CloudHSM le permite generar, almacenar y gestionar de forma segura las claves criptográficas que se utilizan para el cifrado de datos de forma que solo usted pueda acceder a ellas. Para obtener más información, consulte AWS CloudHSM.

AWS CloudHSM en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS CloudHSM mi cuenta de AMS?

La utilización de su cuenta de AMS es un proceso de dos pasos:

1. Solicita un AWS CloudHSM clúster. Para ello, envíe una RFC con el tipo de cambio Management | Other | Other | Create (ct-1e1xtak34nx76). Incluya los siguientes detalles:
   - AWS Región.
   - El ARN de VPC ID/ARN. Provide a VPC ID/VPC que se encuentra en la misma cuenta que el RFC que ha enviado.

- Especifique al menos dos zonas de disponibilidad para el clúster.
- ID de EC2 instancia de Amazon que se conectará al clúster de HSM.

2. Acceda a la AWS CloudHSM consola. Para ello, envíe una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_cloudhsm_console_role`

Una vez aprovisionado el rol en su cuenta, debe incorporarlo a su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS CloudHSM en mi cuenta de AMS?

El acceso a la AWS CloudHSM consola no permite crear, finalizar o restaurar el clúster. Para ello, envíe un tipo de cambio de Administración | Otros | Otros | Crear tipo de cambio (ct-1e1xtak34nx76).

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla en mi cuenta de AMS? AWS CloudHSM

Debe permitir el tráfico TCP mediante el puerto 2225 a través de una EC2 instancia de Amazon cliente dentro de una VPC, o usar Direct Connect VPN para los servidores locales que desean acceder al clúster de HSM. AWS CloudHSM depende de Amazon EC2 para los grupos de seguridad y las interfaces de red. Para la supervisión o auditoría de los registros, HSM se basa en CloudTrail (las operaciones de la AWS API) y en CloudWatch los registros para toda la actividad de los dispositivos HSM locales.

P: ¿Quién aplicará las actualizaciones al AWS CloudHSM cliente y a las bibliotecas de software relacionadas?

Usted es responsable de aplicar las actualizaciones de la biblioteca y del cliente. Querrá supervisar la página del historial de versiones de CloudHSM para ver las versiones y, a continuación, aplicar las actualizaciones mediante la actualización del cliente de CloudHSM.

> **Note**
>
> El servicio siempre aplica automáticamente los parches de software para el dispositivo HSM. AWS CloudHSM

Utilice AMS SSP para aprovisionar AWS CodeBuild en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS CodeBuild las funciones de su cuenta gestionada por AMS. AWS CodeBuild es un servicio de integración continua totalmente gestionado que compila el código fuente, ejecuta pruebas y produce paquetes de software listos para su implementación. Con CodeBuild esto, no necesita aprovisionar, administrar ni escalar sus propios servidores de compilación. CodeBuild escala de forma continua y procesa varias compilaciones simultáneamente, para que sus compilaciones no se queden esperando en una cola. Puede comenzar con rapidez usando entornos de compilación preempaquetados, o crear sus propios entornos de compilación personalizados que utilicen sus propias herramientas de compilación. Con CodeBuild, se le cobra por minuto por los recursos informáticos que utilice. Para obtener más información, consulte AWS CodeBuild.

> **Note**
>
> Para incorporarlo CodeCommit CodeBuild CodeDeploy, y CodePipeline con una sola RFC, envíe el tipo de cambio Administración | AWS servicio | Servicio autoaprovisionado | Añadir (es necesario revisar) (ct-3qe6io8t6jtny) y solicite los tres servicios:, y. CodeBuild CodeDeploy CodePipeline A continuación, las tres funciones,, y se aprovisionan en su cuenta. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Tras el aprovisionamiento en su cuenta, debe incorporar el rol a su solución de federación.

CodeBuild en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS CodeBuild mi cuenta de AMS?

La utilización de AWS CodeBuild la cuenta AMS es un proceso de dos pasos:

1. Aprovisione el proceso de compilación `CodeBuild Service Role` para que se coordine con los buckets de AWS S3, Amazon CloudWatch y los grupos de registros
2. Solicita acceso a la consola CodeBuild

Puedes solicitar que ambas se configuren en tu cuenta de AMS enviando una RFC al tipo de gestión | AWS servicio | Servicio autoaprovisionado | Añadir cambio (ct-1w8z66n899dct). Una vez aprovisionado en tu cuenta, debes incorporar el rol a tu solución de federación.

P: ¿Cuáles son las restricciones de uso AWS CodeBuild en mi cuenta de AMS?

Para el acceso de administrador de la AWS CodeBuild consola, los permisos están limitados a nivel de recursos; por ejemplo, CloudWatch las acciones están limitadas a recursos específicos y el `iam:PassRole` permiso está controlado.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarlos CodeBuild en mi cuenta de AMS?

Si se requieren permisos de IAM adicionales para el rol de AWS CodeBuild servicio definido, solicítelos mediante una solicitud de servicio de AMS.

Utilice AMS SSP para aprovisionar AWS CodeCommit en su cuenta AMS

> **Note**
>
> AWS ha cerrado el acceso de nuevos clientes a AWS CodeCommit partir del 25 de julio de 2024. AWS CodeCommit los clientes actuales pueden seguir utilizando el servicio con normalidad. AWS sigue invirtiendo en mejoras de seguridad, disponibilidad y rendimiento AWS CodeCommit, pero no tenemos previsto introducir nuevas funciones.
> Para migrar los repositorios de CodeCommit Git de AWS a otros proveedores de Git, póngase en contacto con su arquitecto de nube (CA) para obtener orientación. Para obtener más información sobre la migración de sus repositorios de Git, consulte Cómo migrar su CodeCommit repositorio de AWS a otro proveedor de Git.

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a AWS CodeCommit las funciones directamente en su cuenta gestionada por AMS. AWS CodeCommit es un servicio de control de código fuente totalmente gestionado que aloja repositorios seguros basados en Git. Ayuda a los equipos a colaborar en el código en un ecosistema seguro y altamente escalable. CodeCommit elimina la necesidad de operar su propio sistema de control de código fuente o preocuparse por escalar su infraestructura. Puedes usarlo CodeCommit para almacenar de forma segura cualquier cosa, desde código fuente hasta binarios, y funciona a la perfección con tus herramientas de Git existentes. Para obtener más información, consulte AWS CodeCommit.

> **Note**
>
> Para incorporarlo CodeCommit CodeBuild CodeDeploy, y CodePipeline con un único RFC, envía el tipo de cambio Gestión | AWS Servicio | Servicio autoaprovisionado | Añadir (es necesario revisar) (ct-3qe6io8t6jtny) y solicita los tres servicios:, y. CodeBuild CodeDeploy CodePipeline A continuación, las tres funciones,, y se aprovisionan en su cuenta. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Tras el aprovisionamiento en su cuenta, debe incorporar el rol a su solución de federación.

CodeCommit en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a CodeCommit mi cuenta de AMS?

AWS CodeCommit Las funciones de acceso a la consola y a los datos se pueden solicitar mediante el envío de dos AWS servicios RFCs: el acceso a la consola y el acceso a los datos:

- Solicite el acceso AWS CodeCommit enviando una RFC con el tipo de cambio Administración | AWS servicio | Servicio autoaprovisionado | Agregue (ct-1w8z66n899dct). Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_codecommit_console_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

  El acceso a los datos (como las listas de formación y de entidades) requiere información independiente CTs para cada fuente de datos, especificando la fuente de datos de S3 (obligatoria), el segmento de salida (obligatorio) y el KMS (opcional). No hay limitaciones a la creación de puestos de AWS CodeCommit trabajo siempre que se hayan asignado funciones de acceso a todas las fuentes de datos. Para solicitar el acceso a los datos, envíe una RFC a Management | Other | Other | Create (ct-1e1xtak34nx76).

P: ¿Cuáles son las restricciones de uso en mi cuenta de AMS? AWS CodeCommit

La función de activación CodeCommit está desactivada debido a los derechos asociados para crear temas de SNS. La autenticación directa CodeCommit está restringida; los usuarios deben autenticarse con Credential Helper. Algunos comandos de KMS también están restringidos:`kms:Encrypt`,, `kms:Decrypt`, `kms:ReEncrypt`, `kms:GenereteDataKey` y. `kms:GenerateDataKeyWithoutPlaintext` `kms:DescribeKey`

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarlos AWS CodeCommit en mi cuenta de AMS?

Si los buckets de S3 están cifrados con claves KMS, es necesario usarlos con S3 y KMS. AWS CodeCommit

Utilice AMS SSP para aprovisionar AWS CodeDeploy en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS CodeDeploy las funciones de su cuenta gestionada por AMS. AWS CodeDeploy es un servicio de implementación totalmente gestionado que automatiza las implementaciones de software en una variedad de servicios informáticos, como Amazon EC2, AWS Fargate AWS Lambda, y sus servidores locales. AWS CodeDeploy le ayuda a lanzar nuevas funciones rápidamente, le ayuda a evitar el tiempo de inactividad durante la implementación de las aplicaciones y gestiona la complejidad de la actualización de las aplicaciones. Se puede utilizar AWS CodeDeploy para automatizar las implementaciones de software, lo que elimina la necesidad de realizar operaciones manuales propensas a errores. El servicio se amplía para adaptarse a sus necesidades de implementación. Para obtener más información, consulte AWS CodeDeploy.

> **Note**
>
> Para incorporarlo CodeCommit CodeBuild CodeDeploy, y CodePipeline con un único RFC, envíe el tipo de cambio Administración | AWS servicio | Servicio de autoaprovisionamiento | Añadir (es necesario revisar) (ct-3qe6io8t6jtny) y solicite los tres servicios:, y. CodeBuild CodeDeploy CodePipeline A continuación, las tres funciones,, y se aprovisionan en su cuenta. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Tras el aprovisionamiento en su cuenta, debe incorporar el rol a su solución de federación.

CodeDeploy en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a CodeDeploy mi cuenta de AMS?

Solicite acceso CodeDeploy enviando una RFC junto con Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) tipo de cambio. Este RFC proporciona las siguientes funciones de IAM a su cuenta: y. `customer_codedeploy_console_role` `customer_codedeploy_service_role` Una vez aprovisionado en tu cuenta, debes incorporar el `customer_codedeploy_console_role` rol a tu solución de federación.

P: ¿Cuáles son las restricciones de uso CodeDeploy en mi cuenta de AMS?

Actualmente, solo admitimos Compute Platform como Amazon EC2 /On-Premies. Blue/Green No se admiten las implementaciones.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarlos CodeDeploy en mi cuenta de AMS?

No hay requisitos previos ni dependencias para su uso CodeDeploy en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS CodePipeline en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS CodePipeline las funciones de su cuenta gestionada por AMS. AWS CodePipeline es un servicio de entrega continua totalmente gestionado que le ayuda a automatizar sus procesos de lanzamiento para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. CodePipeline automatiza las fases de creación, prueba e implementación del proceso de lanzamiento cada vez que se produce un cambio de código, en función del modelo de lanzamiento que defina. Le permite entregar características y actualizaciones de forma rápida y de confianza. Puedes integrarlo fácilmente AWS CodePipeline con servicios de terceros, como GitHub tu propio complemento personalizado. Con AWS CodePipeline, solo pagas por lo que usas. No es necesario pagar cuotas iniciales ni asumir compromisos a largo plazo. Para obtener más información, consulte AWS CodePipeline.

> **Note**
>
> Para incorporarlo CodeCommit CodeBuild CodeDeploy, y CodePipeline con un único RFC, envíe el tipo de cambio Administración | AWS servicio | Servicio autoaprovisionado | Añadir (es necesario revisar) (ct-3qe6io8t6jtny) y solicite los tres servicios:, y. CodeBuild CodeDeploy CodePipeline A continuación, las tres funciones,, y se aprovisionan en su cuenta. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Tras el aprovisionamiento en su cuenta, debe incorporar el rol a su solución de federación. CodePipeline in AMS no admite «Amazon CloudWatch Events» para Source Stage porque necesita permisos elevados para crear la función y la política de servicio, lo que evita el modelo de privilegios mínimos y el proceso de gestión de cambios de AMS.

CodePipeline en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a CodePipeline mi cuenta de AMS?

Solicita el acceso CodePipeline enviando una solicitud de servicio para `customer_code_pipeline_console_role` la cuenta correspondiente. Una vez aprovisionado en tu cuenta, debes incorporar el rol a tu solución de federación.

En este momento, AMS Operations también implementará esta función de servicio en su cuenta:`aws_code_pipeline_service_role_policy`.

P: ¿Cuáles son las restricciones de uso CodePipeline en mi cuenta de AMS?

Sí. CodePipeline las características, las etapas y los proveedores se limitan a lo siguiente:

1. Etapa de implementación: limitada a Amazon S3 y AWS CodeDeploy
2. Fase de origen: limitada a Amazon S3 AWS CodeCommit, BitBucket, y GitHub
3. Etapa de compilación: limitada a AWS CodeBuild y Jenkins
4. Etapa de aprobación: limitada a Amazon SNS
5. Etapa de prueba: limitada a las AWS CodeBuild pruebas de interfaz de usuario de Jenkins BlazeMeter, Ghost Inspector, Micro Focus StormRunner Load y Runscope API Monitoring
6. Invoke Stage: limitado a Step Functions y Lambda

> **Note**
>
> AMS Operations se implementará `customer_code_pipeline_lambda_policy` en su cuenta; debe estar asociada a la función de ejecución de Lambda para la etapa de invocación de Lambda. Proporcione el nombre de la service/execution función de Lambda con el que desea que se añada esta política. Si no hay un service/execution rol Lambda personalizado, AMS creará un nuevo rol denominado`customer_code_pipeline_lambda_execution_role`, del que será una copia `customer_lambda_basic_execution_role` junto con. `customer_code_pipeline_lambda_policy`

P: ¿Cuáles son los requisitos previos o las dependencias para usarlo CodePipeline en mi cuenta de AMS?

AWS los servicios AWS CodeCommit compatibles AWS CodeDeploy deben lanzarse antes o junto con el lanzamiento de. AWS CodeBuild CodePipeline

Utilice AMS SSP para aprovisionar AWS Compute Optimizer en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Compute Optimizer las funciones de su cuenta gestionada por AMS. AWS Compute Optimizer recomienda recursos AWS informáticos óptimos para sus cargas de trabajo a fin de reducir los costes y mejorar el rendimiento mediante el uso del aprendizaje automático para analizar las métricas de utilización históricas. El aprovisionamiento excesivo de recursos informáticos (Amazon EC2 y ASGs) puede generar costes de infraestructura innecesarios, y el aprovisionamiento insuficiente de recursos informáticos puede provocar un rendimiento deficiente de las aplicaciones. Compute Optimizer le ayuda a elegir los tipos de EC2 instancias de Amazon óptimos, incluidas las que forman parte de un grupo de Amazon EC2 Auto Scaling, en función de sus datos de utilización. Para obtener más información, consulte AWS Compute Optimizer.

Preguntas frecuentes sobre Compute Optimizer en AWS Managed Services

P: ¿Cómo solicito acceso a Compute Optimizer en mi cuenta de AMS?

Para solicitar acceso, envíe un formulario de administración | AWS servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_compute_optimizer_readonly_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Compute Optimizer en mi cuenta de AMS?

No hay restricciones. La funcionalidad completa de AWS Compute Optimizer está disponible en su cuenta AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Compute Optimizer en mi cuenta de AMS?

- Debes enviar un RFC (Administración | Otros | Otros | Actualización) que autorice a AMS Ops a habilitar el servicio en la cuenta. Durante la implementación, se crea un rol vinculado al servicio (SLR) para permitir la recopilación de métricas y la generación de informes. La SLR lleva la etiqueta "» AWSServiceRoleForComputeOptimizer. Para obtener más información, consulte Uso de funciones vinculadas a servicios para AWS Compute Optimizer

- CloudWatch las métricas deben estar habilitadas para las siguientes métricas:
  - Utilización de la CPU: el porcentaje de unidades de EC2 cómputo de Amazon asignadas que se utilizan en la instancia. Esta métrica identifica la potencia de procesamiento necesaria para ejecutar una aplicación en una instancia seleccionada.
  - Utilización de memoria: cantidad de memoria que se ha utilizado de alguna manera durante el período de muestra. Esta métrica identifica la memoria necesaria para ejecutar una aplicación en una instancia seleccionada. El uso de la memoria se analiza solo para los recursos que tienen el CloudWatch agente unificado instalado en ellos. Para obtener más información, consulte Habilitar el uso de la memoria con el CloudWatch agente (pág. 10).
  - Entrada de red: la cantidad de bytes que la instancia recibe en todas las interfaces de red. Esta métrica identifica el volumen del tráfico de red entrante en una sola instancia.
  - Salida de red: la cantidad de bytes que la instancia envía a todas las interfaces de red. Esta métrica identifica el volumen del tráfico de red saliente desde una sola instancia.
  - Disco local input/output (E/S): el número de input/output operaciones del disco local. Esta métrica identifica el rendimiento del volumen raíz de una instancia

Utilice AMS SSP para aprovisionar AWS DataSync en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS DataSync las funciones de su cuenta gestionada por AMS. AWS DataSync mueve grandes cantidades de datos en línea entre el almacenamiento local y Amazon S3, Amazon Elastic File System (Amazon Elastic File System) o Amazon FSx. Las tareas manuales relacionadas con las transferencias de datos pueden ralentizar las migraciones y sobrecargar las operaciones de TI. DataSync elimina o gestiona automáticamente muchas de estas tareas, como la creación de scripts para los trabajos de copia, la programación y el monitoreo de las transferencias, la validación de los datos y la optimización del uso de la red. El agente de DataSync software se conecta al almacenamiento del sistema de archivos de red (NFS) y del bloque de mensajes del servidor (SMB) para que no tenga que modificar las aplicaciones. DataSync puede transferir cientos de terabytes y millones de archivos a velocidades hasta 10 veces más rápidas que las herramientas de código abierto, a través de Internet o mediante enlaces. AWS Direct Connect Puede utilizarlos DataSync para migrar conjuntos de datos o archivos activos AWS, transferir datos a la nube para analizarlos y procesarlos oportunamente, o replicarlos AWS para garantizar la continuidad empresarial.

Para obtener más información, consulte AWS DataSync.

DataSync en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a DataSync mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_datasync_console_role` siguiente función de IAM a su cuenta:.

Una vez aprovisionados en su cuenta, debe incorporar los roles en su solución de federación.

El grupo de CloudWatch registros que se debe usar para transmitir los registros de tareas es «/aws/datasync».

P: ¿Cuáles son las restricciones de uso en mi cuenta de AMS? DataSync

Todas las funciones de AWS DataSync están disponibles en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla DataSync en mi cuenta de AMS?

- Se requiere Amazon S3 ARNs (nombres de recursos de Amazon) para todos los buckets de S3 asociados a DataSync las tareas que se realizarán con el rol `customer_datasync_service_role` de DataSync servicio.
- Los puntos de enlace de VPC y los grupos de seguridad para los DataSync agentes deben solicitarse con una RFC con el tipo de cambio Management | Other | Other | Create (ct-1e1xtak34nx76) antes de utilizar los puntos de enlace de VPC.
- AWS DataSync los agentes se ejecutan en AMS como un dispositivo. El servicio parchea y actualiza el AWS DataSync agente; para obtener más información, consulte las AWS DataSync preguntas frecuentes.
- Para lanzar un AWS DataSync agente, envíe una RFC con el tipo de cambio Management | Other | Other | Create (ct-1e1xtak34nx76) y solicite la implementación del agente. Proporcione el ID de AWS DataSync Amazon EC2 AMI, el tipo de instancia, la subred y el grupo de seguridad y haga referencia a un EC2 par de claves de Amazon existente o solicite la creación de uno nuevo.

> **Note**
>
> AMS aprovisiona al AWS DataSync agente manualmente en nombre del cliente y no requiere el proceso de ingestión de WIGS en la Amazon AWS DataSync AMI EC2 .

Utilice AMS SSP para aprovisionar AWS Device Farm en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Device Farm las funciones de su cuenta gestionada por AMS. AWS Device Farm es un servicio de pruebas de aplicaciones que le permite mejorar la calidad de sus aplicaciones web y móviles probándolas en una amplia gama de navegadores de escritorio y dispositivos móviles reales, sin tener que aprovisionar ni gestionar ninguna infraestructura de pruebas. El servicio le permite ejecutar sus pruebas simultáneamente en varios navegadores de escritorio o dispositivos reales para acelerar la ejecución de su conjunto de pruebas, y genera vídeos y registros para ayudarle a identificar rápidamente los problemas con su aplicación.

Para obtener más información, consulte AWS Device Farm.

AWS Device Farm en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a AWS Device Farm mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_devicefarm_role` siguiente función de IAM a su cuenta:.

Una vez aprovisionados en su cuenta, debe incorporar los roles en su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Device Farm en mi cuenta de AMS?

Se proporciona acceso completo al AWS Device Farm servicio, con la excepción del uso del espacio de nombres AMS en la etiqueta «Nombre».

P: ¿Cuáles son los requisitos previos o las dependencias para usarlo AWS Device Farm en mi cuenta de AMS?

Ninguna.

Utilice AMS SSP para aprovisionar AWS Elastic Disaster Recovery en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Elastic Disaster Recovery las funciones de su cuenta gestionada por AMS. AWS Elastic Disaster Recovery minimiza el tiempo de inactividad y la pérdida de datos con una recuperación rápida y fiable de las aplicaciones locales y basadas en la nube mediante un almacenamiento

asequible, un cálculo y una recuperación mínimos. point-in-time Puede aumentar la resiliencia de la TI al AWS Elastic Disaster Recovery replicar aplicaciones locales o basadas en la nube que se ejecutan en sistemas operativos compatibles. Úselo Consola de administración de AWS para configurar los ajustes de replicación e inicio, supervisar la replicación de datos y lanzar instancias para realizar simulacros o recuperaciones.

Para obtener más información, consulte AWS Elastic Disaster Recovery.

AWS Elastic Disaster Recovery en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a AWS Elastic Disaster Recovery mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_drs_console_role` siguiente función de IAM a su cuenta:.

Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Elastic Disaster Recovery en mi cuenta de AMS?

No hay restricciones de uso AWS Elastic Disaster Recovery en tu cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS Elastic Disaster Recovery en mi cuenta de AMS?

- Una vez que tenga acceso a la función de consola, debe inicializar el servicio Elastic Disaster Recovery para crear las funciones de IAM necesarias en la cuenta.
  - Debe enviar el tipo de cambio Gestión | Aplicaciones | Perfil de instancia de IAM | Crear (es necesario revisar) el tipo de cambio ct-0ixp4ch2tiu04 RFC para crear un clon del perfil de instancia y adjuntar la política. `customer-mc-ec2-instance-profile` `AWSElasticDisasterRecoveryEc2InstancePolicy` Debe especificar a qué máquinas desea adjuntar la nueva política.
  - Si la instancia no utiliza el perfil de instancia predeterminado, AMS puede realizar la conexión `AWSElasticDisasterRecoveryEc2InstancePolicy` mediante automatización.
- Debes usar una clave de KMS propiedad del cliente para la recuperación entre cuentas. La clave KMS de la cuenta de origen debe actualizarse siguiendo la política para permitir el acceso a la cuenta de destino. Para obtener más información, consulte Compartir la clave de cifrado de EBS con la cuenta de destino.

- La política de claves de KMS debe actualizarse `customer_drs_console_role` para permitir ver la política si no desea cambiar de rol de visualización.
- Para la recuperación ante desastres entre cuentas y regiones, AMS debe configurar la cuenta de origen y la de destino como cuentas de confianza e implementar las funciones de recuperación ante fallos y de asignación de tamaño mediante ellas AWS . CloudFormation

Utilice AMS SSP para aprovisionar AWS Elemental MediaConvert en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Elemental MediaConvert las funciones de su cuenta gestionada por AMS. AWS Elemental MediaConvert es un servicio de transcodificación de vídeo basado en archivos con funciones aptas para la radiodifusión. Le permite crear contenido video-on-demand (VOD) para su emisión y distribución multipantalla a gran escala. El servicio combina capacidades avanzadas de vídeo y audio con una sencilla interfaz de servicios web y pay-as-you-go precios. Con AWS Elemental MediaConvertél, puede centrarse en ofrecer experiencias multimedia atractivas sin tener que preocuparse por la complejidad de crear y operar su propia infraestructura de procesamiento de vídeo.

Para obtener más información, consulte AWS Elemental MediaConvert.

MediaConvert en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a MediaConvert mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_mediaconvert_author_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

Se proporcionará una segunda función`customer_MediaConvert_Default_Role`, que se utilizará para leer el bucket de S3 de origen y escribir el resultado MediaConvert en el bucket de S3 de destino, y también para invocar la pasarela de API en caso de que necesite gestionar los derechos digitales (DRM).

P: ¿Cuáles son las restricciones de uso MediaConvert en mi cuenta de AMS?

No hay restricciones de uso MediaConvert en AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla MediaConvert en mi cuenta de AMS?

No hay requisitos previos ni dependencias para su uso MediaConvert en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Elemental MediaLive en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Elemental MediaLive las funciones de su cuenta gestionada por AMS. AWS Elemental MediaLive es un servicio de procesamiento de vídeo en directo con calidad de emisión. Le permite crear transmisiones de vídeo de alta calidad para distribuirlas en televisores y dispositivos multipantalla conectados a Internet, como tabletas TVs, teléfonos inteligentes y decodificadores conectados. El servicio funciona codificando las transmisiones de vídeo en directo en tiempo real, cogiendo una fuente de vídeo en directo de mayor tamaño y comprimiéndola en versiones más pequeñas para distribuirlas a los espectadores. Con él AWS Elemental MediaLive, puedes configurar fácilmente transmisiones tanto para eventos en directo como para canales que funcionan las 24 horas del día, los 7 días de la semana, con funciones de transmisión avanzadas, alta disponibilidad y precios. pay-as-you-go AWS Elemental MediaLive le permite centrarse en crear experiencias de vídeo en directo atractivas para sus espectadores sin la complejidad de crear y operar una infraestructura de procesamiento de vídeo adecuada para la radiodifusión.

Para obtener más información, consulte AWS Elemental MediaLive.

MediaLive en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a MediaLive mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_medialive_author_role` siguiente función de IAM a su cuenta:.

Como parte de esta RFC, se implementa una segunda función en su cuenta; esta `customer_medialive_service_role` función se puede asignar a sus canales y entradas de Media Live para interactuar con otros servicios MediaStore, como Amazon S3 y CloudWatch Logs.

Una vez aprovisionados los roles en su cuenta, debe incorporarlos a su solución de federación.

P: ¿Cuáles son las restricciones de uso MediaLive en mi cuenta de AMS?

No hay restricciones de uso MediaLive en AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla MediaLive en mi cuenta de AMS?

No hay requisitos previos ni dependencias para su uso MediaLive en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Elemental MediaPackage en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Elemental MediaPackage las funciones de su cuenta gestionada por AMS. AWS Elemental MediaPackage prepara y protege de forma fiable el vídeo para su distribución a través de Internet. A partir de una sola entrada de vídeo, AWS Elemental MediaPackage crea secuencias de vídeo formateadas para reproducirse en teléfonos móviles TVs, ordenadores, tabletas y consolas de videojuegos conectados. Facilita la implementación de funciones de vídeo populares para los espectadores (volver a empezar, pausar, retroceder, etc.), como las que se encuentran habitualmente en las pantallas. DVRs AWS Elemental MediaPackage también puede proteger su contenido mediante la gestión de derechos digitales (DRM). AWS Elemental MediaPackage se amplía automáticamente en función de la carga, por lo que tus espectadores siempre disfrutarán de una experiencia fantástica sin que tengas que predecir con precisión y de antemano la capacidad que necesitarás.

Para obtener más información, consulte AWS Elemental MediaPackage.

MediaPackage en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a AWS Elemental MediaPackage mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_mediapackage_author_role` siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

Se proporcionará una segunda función`customer_mediapackage_service_role`, que podrá asignar a sus canales y entradas de Media Live para interactuar con otros servicios, como S3 y Secrets Manager.

P: ¿Cuáles son las restricciones de uso MediaPackage en mi cuenta de AMS?

No hay restricciones de uso MediaPackage en AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla MediaPackage en mi cuenta de AMS?

No hay requisitos previos ni dependencias para su uso MediaPackage en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Elemental MediaStore en su cuenta AMS

> **Note**
>
> Tras una cuidadosa consideración, AWS ha tomado la decisión de suspenderlo MediaStore, con efecto a partir del 13 de noviembre de 2025. Si es un cliente activo de MediaStore, podrá utilizarlo con normalidad MediaStore hasta el 13 de noviembre de 2025, fecha en la que finalizará el soporte del servicio. Después de esta fecha, ya no podrá utilizar MediaStore ninguna de las funciones que ofrece este servicio.

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a AWS Elemental MediaStore las funciones directamente en su cuenta gestionada por AMS. AWS Elemental MediaStore es un servicio de AWS almacenamiento optimizado para contenido multimedia. Le ofrece el rendimiento, la consistencia y la baja latencia necesarios para ofrecer contenido de vídeo en streaming en directo. AWS Elemental MediaStore actúa como almacén de origen en tu flujo de trabajo de vídeo. Sus capacidades de alto rendimiento satisfacen las necesidades de las cargas de trabajo de distribución de contenido multimedia más exigentes, combinadas con un almacenamiento rentable y a largo plazo. Para obtener más información, consulte AWS Elemental MediaStore.

MediaStore en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a MediaStore mi cuenta de AMS?

Solicite acceso MediaStore enviando una RFC junto con Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) tipo de cambio. Este RFC asigna la siguiente función de IAM a su cuenta:. `customer_mediastore_author_role` Como parte de este RFC, se implementa un segundo rol en su cuenta; `MediaStoreAccessLogs` rol, que el MediaStore servicio utiliza para registrar la actividad CloudWatch, si decide habilitar esa función. Una vez aprovisionados en tu cuenta, debes incorporar los roles a tu solución de federación.

En este momento, AMS Operations también implementará este rol de servicio en su cuenta:`aws_code_pipeline_service_role_policy`.

P: ¿Cuáles son las restricciones de uso MediaStore en mi cuenta de AMS?

No hay restricciones de uso MediaStore en AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla MediaStore en mi cuenta de AMS?

No hay requisitos previos ni dependencias para su uso MediaStore en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Elemental MediaTailor en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Elemental MediaTailor las funciones de su cuenta gestionada por AMS. AWS Elemental MediaTailor permite a los proveedores de vídeo insertar publicidad segmentada de forma individual en sus transmisiones de vídeo sin sacrificar el nivel de emisión. quality-of-service De este AWS Elemental MediaTailor modo, los espectadores de tus vídeos en directo o bajo demanda reciben cada uno una transmisión en la que se combina tu contenido con anuncios personalizados para ellos. Sin embargo, a diferencia de otras soluciones de anuncios personalizados, toda la transmisión (vídeo y anuncios) se reproduce con una calidad de vídeo de calidad de emisión para mejorar la experiencia de los espectadores. AWS Elemental MediaTailor AWS Elemental MediaTailor ofrece informes automatizados basados en métricas de publicación de anuncios tanto del lado del cliente como del servidor, para medir con precisión las impresiones publicitarias y el comportamiento de los espectadores. Puedes monetizar fácilmente eventos inesperados de visualización de alta demanda sin costes iniciales. AWS Elemental MediaTailor También mejora las tasas de publicación de anuncios, lo que te permite ganar más dinero con cada vídeo, y funciona con una variedad más amplia de redes de distribución de contenido, servidores de decisiones publicitarias y dispositivos cliente.

Para obtener más información, consulte AWS Elemental MediaTailor.

MediaTailor en Preguntas frecuentes sobre AWS Managed Services

P: ¿Cómo solicito acceso a MediaTailor mi cuenta de AMS?

Solicite acceso MediaTailor enviando una RFC junto con Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) tipo de cambio. Este RFC asigna la siguiente función

de IAM a su cuenta:. `customer-mediatailor-role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso MediaTailor en mi cuenta de AMS?

No hay restricciones de uso MediaTailor en AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla MediaTailor en mi cuenta de AMS?

No hay requisitos previos ni dependencias para su uso MediaTailor en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Global Accelerator en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Global Accelerator directamente en su cuenta gestionada por AMS. Global Accelerator es un servicio de capa de red en el que puede crear aceleradores para mejorar la disponibilidad y el rendimiento de las aplicaciones de Internet utilizadas por un público global. Para obtener más información, consulte Global Accelerator.

Preguntas frecuentes sobre Global Accelerator en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito que Global Accelerator se configure en mi cuenta AMS?

Solicite el acceso mediante el envío del RFC sobre los AWS servicios (administración | AWS servicio | servicio autoaprovisionado). Mediante este RFC, se aprovisionarán las siguientes funciones de IAM en su cuenta:. `customer_global_accelerator_console_role` Una vez aprovisionado en su cuenta, debe incorporar el rol de consola en su solución de federación.

P: ¿Cuáles son las restricciones para usar Global Accelerator en mi cuenta de AMS?

Global Accelerator es un servicio global que admite puntos de conexión en varias AWS regiones, que se muestran en la AWS tabla de regiones.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Global Accelerator en mi cuenta de AMS?

Cuando configuras tu acelerador con Global Accelerator, asocias las direcciones IP estáticas a los puntos finales regionales de una o más regiones. AWS En el caso de los aceleradores estándar, los puntos finales son los balanceadores de carga de red, los balanceadores de carga de aplicaciones, las instancias de EC2 Amazon o las direcciones IP elásticas. En el caso de los aceleradores de enrutamiento personalizados, los puntos finales son subredes de nube privada virtual (VPC) con una o más instancias. EC2

Utilice AMS SSP para aprovisionar AWS Glue en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Glue las funciones de su cuenta gestionada por AMS. AWS Glue es un servicio de extracción, transformación y carga (ETL) totalmente gestionado que le ayuda a preparar y cargar sus datos para su análisis. Puede crear y ejecutar un trabajo de ETL con unos pocos clics en Consola de administración de AWS. Señala AWS Glue los datos almacenados en AWS, AWS Glue descubre sus datos y almacena los metadatos asociados (por ejemplo, la definición de la tabla y el esquema) en el AWS Glue Data Catalog. Una vez catalogados, sus datos se pueden buscar y consultar inmediatamente y están disponibles para realizar acciones de ETL. Para obtener más información, consulte AWS Glue.

AWS Glue en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo AWS Glue solicito que se configure mi cuenta AMS?

Solicite acceso AWS Glue enviando una RFC a Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones de IAM a su cuenta:

- `customer_glue_console_role`
- `customer_glue_service_role`

Las funciones anteriores incluyen las siguientes políticas adjuntas:

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

Una vez aprovisionadas las funciones en su cuenta, debe incorporarlas a su solución de federación.

Para acceder a los rastreadores, los trabajos y los puntos finales de desarrollo (funciones necesarias para casos de uso específicos), envíe una RFC con Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (ct-3dpd8mdd9jn1r).

P: ¿Cuáles son las restricciones de uso en mi cuenta de AMS? AWS Glue

No hay restricciones. La funcionalidad completa de AWS Glue está disponible en su cuenta AMS. Para un entorno interactivo en el que pueda crear y probar scripts ETL, utilice Notebooks on AWS Glue Studio. AWS Glue Las sesiones interactivas y las libretas de trabajo son funciones sin servidor AWS Glue que puede utilizar AWS Glue y que utilizan la función de AWS Glue servicio.

AWS Glue antes de la versión 2.0: las AWS Glue libretas son un recurso no gestionado que lanza EC2 instancias de Amazon en una cuenta. Se recomienda lanzar tus propias EC2 instancias de Amazon e instalar el software necesario para respaldar el entorno y el desarrollo de un portátil. Para obtener más información, consulte el tutorial: Configurar un portátil Apache Zeppelin local para probar y depurar scripts de ETL y utilizar puntos de enlace de desarrollo para desarrollar scripts.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla en mi cuenta de AMS? AWS Glue

AWS Glue depende de Amazon S3 y CloudWatch CloudWatch Logs. Las dependencias transitivas varían en función de las fuentes de datos y es posible que interactúen con otras funciones del AWS Glue servicio (por ejemplo: Amazon Redshift, Amazon RDS o Athena).

Utilice AMS SSP para aprovisionar AWS Lake Formation en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Lake Formation las funciones de su cuenta gestionada por AMS. AWS Lake Formation es un servicio que facilita la configuración de un lago de datos seguro en cuestión de días. Un lago de datos es un repositorio centralizado, seleccionado y seguro que almacena todos los datos, tanto en su forma original como preparado para su análisis. Un lago de datos le permite desglosar los silos de datos y combinar diferentes tipos de análisis para obtener información y guiarlo a tomar mejores decisiones empresariales.

Crear un lago de datos con Lake Formation es tan simple como definir orígenes de datos y qué acceso a los datos y qué políticas de seguridad desea aplicar. Lake Formation le ayuda a recopilar y catalogar datos de bases de datos y almacenamiento de objetos, mover los datos a su nuevo lago de datos de Amazon S3, limpiar y clasificar sus datos mediante algoritmos de machine learning y asegurar el acceso a su información confidencial. Los usuarios pueden acceder a un catálogo de datos centralizado (para obtener más información, consulte las AWS Glue preguntas frecuentes)

en el que se describen los conjuntos de datos disponibles y su uso adecuado. Luego, sus usuarios aprovechan estos conjuntos de datos con los servicios de análisis y aprendizaje automático que elijan, como Amazon Redshift, Amazon Athena y (en versión beta) Amazon EMR para Apache Spark. Lake Formation se basa en las capacidades disponibles en AWS Glue.

Para obtener más información, consulte AWS Lake Formation.

Preguntas frecuentes sobre Lake Formation en AWS Managed Services

P: ¿Cómo solicito acceso a AWS Lake Formation mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona la `customer_lakeformation_data_analyst_role` siguiente función de IAM a su cuenta:. Una vez aprovisionados en su cuenta, debe incorporar los roles en su solución de federación.

Además, las dos funciones siguientes son opcionales:

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

En cuanto a los permisos de administrador, puede optar por incorporar el rol `customer_lakeformation_admin_role` como parte del mismo tipo de cambio de SSPS (ct-3qe6io8t6jtny).

Si desea crear planos en la AWS Lake Formation consola, debe enviar un RFC de administración | Otros | Otros (ct-1e1xtak34nx76) para implementarlos. `customer_lakeformation_workflow_role` En la RFC, debe proporcionar el nombre del bucket de S3 si el bucket es una fuente cuando se creen los blueprints. El bucket S3 se aplica si el tipo de blueprint es AWS CloudTrail Classic Load Balancer Logs o Application Load Balancer Logs.

P: ¿Cuáles son las restricciones de uso AWS Lake Formation en mi cuenta de AMS?

Todas las funciones de Lake Formation están disponibles en AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS Lake Formation en mi cuenta de AMS?

Lake Formation se integra con el AWS Glue servicio, por lo que AWS Glue los usuarios solo pueden acceder a las bases de datos y tablas en las que tienen permisos de Lake Formation. Además, los

usuarios de AWS Athena y Amazon Redshift solo pueden consultar AWS Glue las bases de datos y tablas en las que tengan permisos de Lake Formation.

Utilice AMS SSP para aprovisionar AWS Lambda en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Lambda las funciones de su cuenta gestionada por AMS. AWS Lambda le permite ejecutar código sin aprovisionar ni administrar servidores. Solo paga por el tiempo de cómputo que consuma; no hay ningún cargo cuando el código no se está ejecutando. Con Lambda, puede ejecutar código para prácticamente cualquier tipo de aplicación o servicio de back-end, todo sin necesidad de administración. Cargue su código y Lambda se ocupará de todo lo necesario para ejecutar y escalar su código con alta disponibilidad. Puede configurar el código para que se active automáticamente desde otros AWS servicios o llamarlo directamente desde cualquier aplicación web o móvil. Para obtener más información, consulte AWS Lambda.

Preguntas frecuentes sobre Lambda en AWS Managed Services

P: ¿Cómo solicito acceso a AWS Lambda mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (es necesario revisar) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona las `customer_lambda_admin_role` `customer_lambda_basic_execution_role` siguientes funciones de IAM a su cuenta: y. Una vez aprovisionados en su cuenta, debe incorporar los roles a su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Lambda en mi cuenta de AMS?

- Una función Lambda está diseñada para que las fuentes de eventos la invoquen. Para obtener una lista de los servicios que se pueden usar como fuente de eventos de Lambda, consulte Uso AWS Lambda con otros servicios. Actualmente, no todos estos servicios están disponibles en las cuentas de AMS. Si necesita un servicio que no está disponible, póngase en contacto con su CSDM de AMS para solicitar una excepción.
- De forma predeterminada, AMS le proporciona una función de iniciación Lambda básica que contiene los `AWSXrayWriteOnlyAccess` permisos `AWSLambdaBasicExecutionRole` y; para obtener más información, consulte Función de AWS Lambda iniciación. Si necesita permisos adicionales, como la capacidad de aprovisionar funciones Lambda en su VPC de AMS, envíe una RFC con el tipo de cambio Management | AWS service | Self-provisioning service | Add (es necesario revisar) (ct-3qe6io8t6jtny).

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarlos en mi cuenta de AMS? AWS Lambda

No hay requisitos previos ni dependencias con los que empezar AWS Lambda; sin embargo, según tu caso de uso específico, es posible que necesites acceso a otros AWS servicios para crear fuentes de eventos o permisos adicionales para que tu función pueda realizar diversas acciones. Si necesita permisos adicionales, envíe una RFC a Management | AWS service | Self-provisioned service | Add (es necesario revisar) el tipo de cambio (ct-3qe6io8t6jtny).

P: ¿Qué debo hacer para ejecutar una función Lambda en alguna de mis cuentas?

Para implementar una función Lambda en una cuenta principal, siga las siguientes pautas:

- Asegúrese de que SSPS for AWS Lambda esté incorporado.
- No hay restricciones específicas que prohíban este despliegue en virtud de las responsabilidades de AMS, siempre y cuando sus recursos de AMS estén protegidos y cumplan con las normas.
- Si desea que AMS cree la función Lambda, primero debe usar la función SSPS que se proporciona. AWS Lambda Luego, si aún necesita la ayuda de AMS para implementar o respaldar la función, póngase en contacto con su CA e inicie el proceso fuera de alcance (OOS).

Utilice AMS SSP para aprovisionar AWS License Manager en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS License Manager las funciones de su cuenta gestionada por AMS. AWS License Manager se integra con AWS servicios para simplificar la administración de licencias en varias AWS cuentas, catálogos de TI y locales, a través de una sola cuenta. AWS AWS License Manager permite a los administradores crear reglas de licencia personalizadas que emulan los términos de sus acuerdos de licencia y, a continuación, EC2 hace cumplir estas reglas cuando se lanza una instancia de Amazon. Las normas AWS License Manager permiten limitar el incumplimiento de la licencia impidiendo físicamente el lanzamiento de la instancia o notificando la infracción a los administradores. Para obtener más información, consulte AWS License Manager.

Preguntas frecuentes sobre License Manager en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo AWS License Manager solicito que se configure mi cuenta AMS?

Solicita el acceso AWS License Manager enviando una RFC junto con Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añade (ct-1w8z66n899dct) el tipo de cambio. Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_license_manager_role` Una vez que el rol de IAM de License Manager esté aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS License Manager en mi cuenta de AMS?

Puedes asociar AWS License Manager reglas a las AMIs tuyas (filtradas en «De mi propiedad»). Si decide aplicar una asociación de límites a una AMI (por ejemplo, solo puede admitir 100 vCPU de esta AMI) y agota el límite, los lanzamientos futuros con esa AMI se bloquearán y mostrará un error que indica «No hay licencias disponibles». Este es el comportamiento previsto de este servicio (no permitir el agotamiento de las licencias). En caso de que agote el límite pero necesite volver a lanzar la AMI, debe modificar la regla configurada en AWS License Manager.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS License Manager en mi cuenta de AMS?

No hay requisitos previos ni dependencias para su uso AWS License Manager en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Migration Hub en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Migration Hub las funciones de su cuenta gestionada por AMS. AWS Migration Hub proporciona una ubicación única donde puede realizar un seguimiento del progreso de las migraciones de aplicaciones en soluciones múltiples AWS y asociadas. El uso de Migration Hub le permite elegir las herramientas de migración AWS y asociarse que mejor se adapten a sus necesidades, a la vez que proporciona visibilidad del estado de las migraciones en toda su cartera de aplicaciones. Migration Hub también proporciona métricas clave y el progreso de las aplicaciones individuales, independientemente de las herramientas que se utilicen para migrarlas. Esto le permite obtener rápidamente actualizaciones sobre el progreso de todas sus migraciones, identificar y solucionar fácilmente cualquier problema y reducir el tiempo y el esfuerzo generales dedicados a sus proyectos de migración. Para obtener más información, consulte AWS Migration Hub.

Preguntas frecuentes sobre Migration Hub en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Migration Hub en mi cuenta de AMS?

Solicite acceso a Migration Hub enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC asigna la siguiente función de IAM a su cuenta:. `customer_migrationhub_author_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de Migration Hub?

Ninguna.

P: ¿Cuáles son los requisitos previos para habilitar Migration Hub?

No hay requisitos previos para empezar a usar Migration Hub en su cuenta de AMS. Sin embargo, es posible que se requieran permisos externos a Migration Hub durante la administración del servicio, como permisos de escritura en Amazon S3 para cargar información del servidor.

Utilice AMS SSP para aprovisionar AWS Outposts en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Outposts las funciones de su cuenta gestionada por AMS. AWS Outposts es un servicio totalmente gestionado que extiende la AWS infraestructura APIs, AWS los servicios y las herramientas a prácticamente cualquier centro de datos, espacio compartido o instalación local para ofrecer una experiencia híbrida uniforme. AWS Outposts es ideal para cargas de trabajo que requieren un acceso de baja latencia a los sistemas locales, al procesamiento de datos local o al almacenamiento local de datos. Para obtener más información, consulte AWS Outposts.

AWS Outposts en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo AWS Outposts solicito que se configure mi cuenta de AMS?

Solicita el acceso AWS Outposts enviando una RFC junto con Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añade (ct-1w8z66n899dct) el tipo de cambio. Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_outposts_role` Una vez que el rol esté aprovisionado en su cuenta, debe incorporarlo a su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Outposts en mi cuenta de AMS?

No hay restricciones de uso AWS Outposts en tu cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS Outposts en mi cuenta de AMS?

No hay requisitos previos ni dependencias para su uso AWS Outposts en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Resilience Hub en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Resilience Hub las funciones de su cuenta gestionada por AMS. AWS Resilience Hub le ayuda a preparar y proteger sus AWS aplicaciones de forma proactiva contra las interrupciones. El Resilience Hub ofrece una evaluación y validación de la resiliencia que se integran en su ciclo de vida de desarrollo de software para descubrir las debilidades de la resiliencia. Resilience Hub le ayuda a estimar si sus aplicaciones pueden cumplir o no los objetivos de tiempo de recuperación (RTO) y objetivo de punto de recuperación (RPO), y ayuda a resolver los problemas antes de que pasen a la fase de producción. Después de implementar una AWS aplicación en producción, puede usar Resilience Hub para seguir realizando un seguimiento del estado de resiliencia de la aplicación. Si se produce una interrupción, Resilience Hub envía una notificación al operador para iniciar el proceso de recuperación asociado.

AWS Resilience Hub en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS Resilience Hub mi cuenta de AMS?

Solicite acceso a Resilience Hub enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones y políticas de IAM a su cuenta:

IAM roles

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

Políticas

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

Una vez aprovisionado el rol en su cuenta, debe incorporarlo a su solución de `customer_resiliencehub_console_role` federación.

P: ¿Cuáles son las restricciones de uso AWS Resilience Hub en mi cuenta de AMS?

No hay restricciones. La funcionalidad completa de Resilience Hub está disponible en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS Resilience Hub en mi cuenta de AMS?

No hay requisitos previos ni dependencias para usar Resilience Hub en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Secrets Manager en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Secrets Manager las funciones de su cuenta gestionada por AMS. AWS Secrets Manager le ayuda a proteger los secretos necesarios para acceder a sus aplicaciones, servicios y recursos de TI. El servicio le permite rotar, gestionar y recuperar fácilmente las credenciales de las bases de datos, las claves de API y otros datos secretos a lo largo de su ciclo de vida. Los usuarios y las aplicaciones recuperan los secretos con una llamada al Secrets Manager APIs, lo que elimina la necesidad de codificar la información confidencial en texto plano. Secrets Manager ofrece una rotación de secretos con una integración incorporada para Amazon RDS, Amazon Redshift y Amazon DocumentDB. Además, el servicio se puede extender a otros tipos de secretos, incluidas las claves y OAuth los tokens de API. Para obtener más información, consulte AWS Secrets Manager.

> **Note**
>
> De forma predeterminada, los operadores de AMS pueden acceder a AWS Secrets Manager los secretos cifrados mediante la AWS KMS clave predeterminada de la cuenta (CMK). Si quiere que AMS Operations no pueda acceder a sus secretos, utilice una CMK personalizada, con una política de claves AWS Key Management Service (AWS KMS) que defina los permisos adecuados para los datos almacenados en el secreto.

Preguntas frecuentes sobre Secrets Manager in AWS Managed Services

P: ¿Cómo solicito acceso a AWS Secrets Manager mi cuenta de AMS?

Solicite acceso a Secrets Manager enviando un RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny). Este

RFC proporciona `customer_secrets_manager_console_role` las `customer-rotate-secrets-lambda-role` siguientes funciones de IAM a su cuenta: y. `customer_secrets_manager_console_role`Se usa como función de administrador para aprovisionar y administrar los secretos, y `customer-rotate-secrets-lambda-role` se usa como función de ejecución de Lambda para las funciones de Lambda que rotan los secretos. Una vez aprovisionado en su cuenta, debe incorporar el `customer_secrets_manager_console_role` rol a su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Secrets Manager en mi cuenta de AMS?

La funcionalidad completa de AWS Secrets Manager está disponible en tu cuenta de AMS, junto con la función de rotación automática de los secretos. Sin embargo, tenga en cuenta que no se admite la configuración de la rotación mediante la opción «Crear una nueva función de Lambda para realizar la rotación», ya que se requieren permisos elevados para crear CloudFormation la pila (creación de roles de IAM y funciones de Lambda), lo que evita el proceso de administración de cambios. AMS Advanced solo admite la opción «Utilizar una función de Lambda existente para realizar la rotación», en la que se gestionan las funciones de Lambda para rotar los secretos mediante la AWS función de administrador de Lambda SSPS. AMS Advanced no crea ni administra Lambda para ocultar los secretos.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS Secrets Manager en mi cuenta de AMS?

Los siguientes espacios de nombres están reservados para su uso por parte de AMS y no están disponibles como parte del acceso directo a: AWS Secrets Manager

- arn:aws:secretsmanager: *:*:secret:ams-shared/*
- arn:aws:secretsmanager: *:*:secreto: compartido con clientes /*
- arn:aws:administrador de secretos: *:*:secreto: ams/*

Compartir claves mediante Secrets Manager (AMS SSPS)

Si se comparten secretos con AMS en el texto simple de una RFC, una solicitud de servicio o un informe de incidente, se produce un incidente de divulgación de información, por lo que AMS elimina esa información del caso y solicita que se regeneren las claves.

Puede usar AWS Secrets Manager(Secrets Manager) en este espacio de nombres,. `customer-shared`

Preguntas frecuentes sobre cómo compartir claves mediante Secrets Manager

P: ¿Qué tipo de secretos se deben compartir con Secrets Manager?

Algunos ejemplos son las claves previamente compartidas para la creación de una VPN y las claves confidenciales, como las claves de autenticación (IAM, SSH), las claves de licencia y las contraseñas.

P: ¿Cómo puedo compartir las claves con AMS mediante Secrets Manager?

1. Inicie sesión en la consola AWS de administración con su acceso federado y el rol correspondiente:

   para SALZ, el `Customer_ReadOnly_Role`

   para MALZ,. `AWSManagedServicesChangeManagementRole`
2. Ve a la AWS Secrets Manager consola y haz clic en Guardar un secreto nuevo.
3. Seleccione Other type of secrets (Otro tipo de secretos).
4. Introduzca el valor secreto como texto sin formato y utilice el cifrado KMS predeterminado. Haga clic en Next (Siguiente).
5. Introduzca el nombre y la descripción del secreto; el nombre siempre empieza por customer-shared/. Por ejemplo, customer-shared/mykey2022. Haga clic en Next (Siguiente).
6. Deje la rotación automática desactivada y haga clic en Siguiente.
7. Revisa y haz clic en Guardar para guardar el secreto.
8. Respóndenos con el nombre secreto mediante la solicitud de servicio, el RFC o el informe de incidente para que podamos identificar y recuperar el secreto.

P: ¿Qué permisos se requieren para compartir las claves con Secrets Manager?

SALZ: Busque la política de IAM `customer_secrets_manager_shared_policy` gestionada y compruebe que el documento de política es el mismo que se adjunta en los pasos de creación que se indican a continuación. Confirme que la política esté asociada a las siguientes funciones de IAM:. `Customer_ReadOnly_Role`

MALZ: Valide que el`AMSSecretsManagerSharedPolicy`, esté asociado al `AWSManagedServicesChangeManagementRole` rol que le permite realizar la `GetSecretValue` acción en el `ams-shared` espacio de nombres.

Ejemplo:

```
{
 "Action": "secretsmanager:*",
 "Resource": [
 "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
 "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
 ],
 "Effect": "Allow",
 "Sid": "AllowAccessToSharedNameSpaces"
 }
```

> **Note**
>
> Los permisos necesarios se otorgan cuando se agrega un servicio aprovisionado de AWS Secrets Manager autoservicio.

Utilice AMS SSP para aprovisionar AWS Security Hub CSPM en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Security Hub CSPM las funciones de su cuenta gestionada por AMS. AWS Security Hub CSPM le proporciona una visión completa del estado de su seguridad interna y de su cumplimiento de los estándares AWS y las mejores prácticas del sector de la seguridad. Security Hub centraliza y prioriza los hallazgos de seguridad y cumplimiento de todas AWS las cuentas, servicios y socios externos compatibles para ayudarlo a analizar sus tendencias de seguridad e identificar los problemas de seguridad más prioritarios. Para obtener más información, consulte AWS Security Hub CSPM.

Preguntas frecuentes sobre Security Hub en AWS Managed Services

P: ¿Cómo solicito acceso a AWS Security Hub CSPM mi cuenta de AMS?

Solicite acceso a Security Hub enviando una RFC con el servicio Management | AWS | Self-provisioned service | Add (ct-1w8z66n899dct) tipo de cambio. Este RFC asigna la siguiente función de IAM a su cuenta:. `customer_securityhub_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar Security Hub en mi cuenta de AMS?

La funcionalidad de archivado se ha considerado un posible riesgo operativo y de seguridad, y se ha restringido como parte de la función de seguridad del servicio de autoaprovisionamiento.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla en mi cuenta de AMS? AWS Security Hub CSPM

No hay requisitos previos ni dependencias para su uso AWS Security Hub CSPM en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Service Catalog AppRegistry en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AppRegistry las funciones de su cuenta gestionada por AMS. AppRegistry permite realizar acciones de búsqueda, generación de informes y administración de aplicaciones desde una ubicación central. Los desarrolladores rara vez crean aplicaciones en una sola AWS cuenta. Por lo general, separan los recursos de las aplicaciones por fases del ciclo de vida, como el desarrollo, las pruebas y la producción. AppRegistry le permite agrupar y ver todas sus colecciones de recursos en las AWS cuentas que defina.

Con AppRegistry él, puede almacenar sus AWS aplicaciones, la colección de recursos que están asociados a sus aplicaciones y los grupos de atributos de las aplicaciones. Para obtener más información, consulte Qué es AppRegistry.

Preguntas frecuentes: AWS Service Catalog AppRegistry en AMS

P: ¿Cómo solicito acceso a AWS Service Catalog AppRegistry mi cuenta de AMS?

Solicita el acceso AppRegistry enviando un RFC junto con Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añade (es necesario revisarlo) (ct-3qe6io8t6jtny) el tipo de cambio. Este RFC proporciona `customer-appregistry-console-role` la siguiente función de IAM a su cuenta:. Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Service Catalog AppRegistry en mi cuenta de AMS?

Se proporciona acceso completo al AppRegistry servicio, con la excepción del uso del espacio de nombres AMS en la `'Name'` etiqueta.

P: ¿Cuáles son los requisitos previos o las dependencias para usarlo AWS Service Catalog AppRegistry en mi cuenta de AMS?

No hay requisitos previos ni dependencias para su uso AppRegistry en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Shield Advanced en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Shield Advanced las funciones de su cuenta gestionada por AMS. AWS Shield Advanced es un servicio gestionado de protección contra la denegación de servicio distribuido que protege las aplicaciones que se ejecutan en ellas. DDo AWS Shield Advanced proporciona una detección permanente y mitigaciones automáticas en línea que minimizan el tiempo de inactividad y la latencia de las aplicaciones, por lo que no es necesario contratar a AWS Support para beneficiarse de la protección S. DDo Hay dos niveles AWS Shield : Estándar y Avanzado; AMS ofrece Shield Advanced. Para obtener más información, consulte Shield Advanced.

Todos AWS los clientes se benefician de las protecciones automáticas de AWS Shield Standard, sin cargo adicional. AWS Shield Standard se defiende contra los ataques de nivel DDo S de red y transporte más comunes y frecuentes que tienen como objetivo su sitio web o sus aplicaciones. Cuando lo utiliza AWS Shield Standard con Amazon CloudFront y Amazon Route 53, recibe una protección de disponibilidad integral contra todos los ataques conocidos a la infraestructura (capas 3 y 4).

Para obtener niveles más altos de protección contra los ataques dirigidos a sus aplicaciones que se ejecutan en los recursos de Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB) CloudFront AWS Global Accelerator, Amazon y Amazon Route 53, puede suscribirse a AWS Shield Advanced.

Además de las protecciones incluidas en las capas de red y transporte AWS Shield Standard, AWS Shield Advanced ofrece detección y mitigación adicionales contra los ataques tipo DDo S grandes y sofisticados, visibilidad prácticamente en tiempo real de los ataques e integración con AWS WAF un firewall de aplicaciones web. AWS Shield Advanced también le ofrece acceso ininterrumpido al equipo de AWS Shield respuesta (SRT) y protección contra los picos relacionados con DDo S en sus cargos de Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (Elastic Load Balancing) CloudFront AWS Global Accelerator, Amazon y Amazon Route 53.

Preguntas frecuentes sobre Shield Advanced en AWS Managed Services

P: ¿Cómo solicito acceso a Shield Advanced en mi cuenta de AMS?

Solicite acceso a Shield Advanced enviando una RFC con el tipo de cambio Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones de IAM a su cuenta: y. `customer_shield_role` `aws_drt_shield_role` Una vez aprovisionados en su cuenta, debe incorporar los roles a su solución de federación.

Una vez implementados los roles en su cuenta, puede usarlos `customer_shield_role` para confirmar su suscripción AWS Shield Advanced en su cuenta.

> **Note**
>
> Tenga en cuenta que el uso de conlleva una cuota mensual y un compromiso de AWS Shield Advanced un año. Además, su uso AWS Shield Advanced en AMS autoriza a AMS a recurrir a la AWS Shield (SRT), que puede realizar cambios en las reglas del firewall de aplicaciones web durante un aumento de los incidentes de denegación de servicio distribuida.AWS WAF DDo Estos cambios se realizarán en coordinación con AMS.

P: ¿Cuáles son las restricciones para usar Shield Advanced en mi cuenta de AMS?

Aunque no es una restricción, debes entender que al usar Shield Advanced se implementa`aws_drt_shield_role`, lo que permite a AWS Shield los equipos (SRT) realizar cambios de emergencia en AWS WAF las reglas de las cuentas de AMS durante una escalada DDo de incidentes de tipo S. AMS recomienda esta opción para solucionar los ataques DDo S lo más rápidamente posible, y se produciría tras una escalada de AMS a la SRT.

P: ¿Cuáles son los requisitos previos o las dependencias para usar Shield Advanced en mi cuenta de AMS?

No hay requisitos previos ni dependencias para usar Shield Advanced en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Snowball Edge en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de Snowball Edge directamente en su cuenta gestionada por AMS. Snowball Edge es una solución de transporte de datos a escala de petabytes que utiliza dispositivos diseñados para ser seguros y transferir grandes cantidades de datos a la nube y desde ella. AWS Snowball Edge aborda los desafíos comunes de las transferencias de datos a gran escala, incluidos los altos costes de red, los largos tiempos de transferencia y los problemas de seguridad. Puede utilizar Snowball Edge para migrar datos de análisis, datos genómicos, bibliotecas de vídeo, repositorios de imágenes, copias

de seguridad y archivar parte de los proyectos de cierre de centros de datos, sustitución de cintas o migración de aplicaciones. La transferencia de datos con Snowball Edge es sencilla, rápida y segura, y puede costar tan solo una quinta parte del coste de la transferencia de datos a través de Internet de alta velocidad.

Con Snowball Edge, no necesita escribir ningún código ni comprar ningún hardware para transferir los datos. Comience por usar la consola AWS de administración para crear un trabajo de importación para Snowball y se le enviará automáticamente un dispositivo Snowball. Cuando llegue, conecte el dispositivo a la red local, descargue y ejecute el Cliente Snowball («Cliente») para establecer una conexión y, a continuación, utilice el Cliente para seleccionar los directorios de archivos que desee transferir al dispositivo. A continuación, el cliente cifra y transfiere los archivos al dispositivo a alta velocidad. Cuando se complete la transferencia y el dispositivo esté listo para su devolución, la etiqueta de envío de tinta electrónica se actualizará automáticamente y podrás realizar un seguimiento del estado del trabajo con Amazon Simple Notification Service (Amazon SNS), mensajes de texto o directamente en la consola. Para obtener más información, consulte AWS Snowball Edge.

Preguntas frecuentes sobre Snowball Edge en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS Snowball Edge mi cuenta de AMS?

La implementación de Snowball Edge en AMS es un proceso de dos pasos:

1. Envíe un tipo de cambio de administración | Otros | Cree (ct-1e1xtak34nx76) y solicite un rol de servicio para Snowball Edge para su cuenta de AMS.
2. Solicite el acceso de los usuarios enviando un mensaje de administración | AWS servicio | Servicio autoaprovisionado | Añadir tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona las siguientes funciones de IAM a su cuenta:, y. `customer_snowball_console_role` `customer_snowball_export_role` `customer_snowball_import_role` Una vez aprovisionado en tu cuenta, debes incorporar el rol a tu solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Snowball Edge en mi cuenta de AMS?

Todas las AWS Snowball Edge funciones están disponibles en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS Snowball Edge en mi cuenta AMS?

Debe tener la cuenta de rol de servicio indicada anteriormente.

Utilice AMS SSP para aprovisionar AWS Step Functions en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Step Functions las funciones de su cuenta gestionada por AMS. AWS Step Functions es un servicio web que le permite coordinar los componentes de las aplicaciones distribuidas y los microservicios mediante flujos de trabajo visuales. La creación de aplicaciones a partir de componentes individuales cada uno de los cuales realiza una función o tarea discreta le permite escalar y modificar las aplicaciones rápidamente. Step Functions proporciona una manera fiable de coordinar los componentes y procesar las funciones de su aplicación. Step Functions ofrece una consola gráfica para visualizar los componentes de su aplicación en una serie de pasos. Activa y rastrea automáticamente cada paso, y lo vuelve a intentar cuando hay errores, para que la aplicación se ejecute siempre en orden y según lo esperado. Step Functions registra el estado de cada paso, de manera que, cuando algo sale mal, puede diagnosticar y depurar los problemas con rapidez. Para obtener más información, consulte AWS Step Functions.

Preguntas frecuentes sobre Step Functions en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS Step Functions mi cuenta de AMS?

Solicita el acceso AWS Step Functions enviando un RFC a la Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añadir tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_step_functions_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Step Functions en mi cuenta de AMS?

Todas las AWS Step Functions funciones están disponibles en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS Step Functions en mi cuenta AMS?

En tiempo de ejecución, el rol utilizado por Step Functions debe tener acceso a los servicios utilizados por la función step. Por ejemplo, una función escalonada podría depender de las funciones Lambda. Es probable que alguien que cree una función escalonada cree funciones Lambda al mismo tiempo y también tenga que solicitar acceso a ese servicio.

Utilice AMS SSP para aprovisionar el almacén de AWS Systems Manager parámetros en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones del almacén de AWS Systems Manager parámetros directamente en su cuenta gestionada por AMS. AWS Systems Manager Parameter Store proporciona un almacenamiento jerárquico y seguro para la gestión de los datos de configuración y la gestión de secretos. Puede almacenar datos como contraseñas, cadenas de base de datos y códigos de licencia como valores de parámetros. Puede almacenar valores como texto sin formato o como datos cifrados. A continuación, puede hacer referencia a los valores utilizando el nombre exclusivo especificado al crear el parámetro. Parameter Store, altamente escalable, disponible y duradero, está respaldado por la AWS nube. Para obtener más información, consulte AWS Systems Manager Parameter Store.

> **Note**
>
> Si desea un almacén de secretos dedicado con administración del ciclo de vida, utilícelo Utilice AMS SSP para aprovisionar AWS Secrets Manager en su cuenta AMS en lugar de Parameter Store. Secrets Manager le ayuda a cumplir sus requisitos de seguridad y conformidad al permitirle rotar los secretos automáticamente. Secrets Manager ofrece una integración integrada para MySQL, PostgreSQL y Amazon Aurora en Amazon RDS, que se puede ampliar a otros tipos de secretos mediante la personalización de las funciones de Lambda.

AWS Systems Manager Preguntas frecuentes sobre el almacenamiento de parámetros en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso al almacén de parámetros de Systems Manager en mi cuenta AMS?

Para solicitar acceso al almacén de AWS Systems Manager parámetros, envíe una RFC a Management | AWS service | Self-provisioning service | Add change type (ct-1w8z66n899dct). Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_systemsmanager_parameterstore_console_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones para usar AWS Systems Manager Parameter Store en mi cuenta de AMS?

Debe utilizar claves AWS administradas; el acceso está restringido a la creación de claves KMS personalizadas. Sin embargo, si se necesita una clave personalizada, envíe una RFC para crear una clave gestionada por el cliente (CMK) utilizando la clave Deployment | Advanced Stack Components | KMS | Create change type (ct-1d84keiri1jhg) con esta función de IAM como valor para los parámetros y. `customer_systemsmanager_parameterstore_console_role` `IAMPrincipalsRequiringDecryptPermissions` `IAMPrincipalsRequiringEncryptPermissionsPrincipal` Una vez creada la clave KMS, puede crear una cadena segura con ella.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizar el almacén de AWS Systems Manager parámetros en mi cuenta de AMS?

No hay requisitos previos; sin embargo, el almacén de parámetros de SSM depende de KMS para crear una cadena segura que permita cifrar y descifrar los valores almacenados en el almacén de parámetros.

Utilice AMS SSP para aprovisionar la AWS Systems Manager automatización en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las funciones de AWS Systems Manager automatización directamente en su cuenta gestionada por AMS. AWS Systems Manager La automatización simplifica las tareas comunes de mantenimiento e implementación de las instancias y otros AWS recursos de Amazon Elastic Compute Cloud mediante manuales de ejecución, acciones y cuotas de servicio. Le permite crear, ejecutar y supervisar automatizaciones a escala. Una automatización de Systems Manager es un tipo de documento de Systems Manager que define las acciones que Systems Manager realiza en las instancias gestionadas. Un manual que se usa para realizar tareas comunes de mantenimiento e implementación, como ejecutar comandos o scripts de automatización en las instancias administradas. Systems Manager incluye funciones que le ayudan a dirigirse a grandes grupos de instancias mediante etiquetas de Amazon Elastic Compute Cloud y controles de velocidad que le ayudan a implementar cambios de acuerdo con los límites que defina. Los manuales de ejecución se escriben con JavaScript Object Notation (JSON) o YAML. Sin embargo, con el Generador de documentos en la consola de Automatización de Systems Manager, puede crear un manual de procedimientos sin tener que utilizar YAML o JSON nativo. Como alternativa, puede utilizar los manuales proporcionados por Systems Manager con pasos predefinidos que se adapten a sus

necesidades. Para obtener más información, consulte Trabajar con manuales de ejecución en la documentación. AWS Systems Manager

> **Note**
>
> Aunque Systems Manager Automation admite 20 tipos de acciones que se pueden usar en el runbook, hay un número limitado de acciones que puede usar al crear el runbook para usarlas en su cuenta de AMS Advanced. Del mismo modo, se puede utilizar un número limitado de manuales proporcionados por Systems Manager directamente o desde su propio manual. Para obtener más información, consulte las restricciones en las siguientes preguntas frecuentes.

AWS Systems Manager Preguntas frecuentes sobre la automatización en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a Systems Manager Automation en mi cuenta de AMS?

Para solicitar acceso a AWS Systems Manager Automation, envíe una RFC a la sección Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añadir tipo de cambio (ct-1w8z66n899dct). Este RFC asigna la siguiente función de IAM a su cuenta:. `customer_systemsmanager_automation_console_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las limitaciones para usar la AWS Systems Manager automatización en mi cuenta de AMS?

Debe crear su manual de ejecución, con un conjunto limitado de acciones compatibles con Systems Manager para la automatización, solo para ejecutar and/or scripts de comandos en las instancias administradas. Las acciones que tiene a su disposición, junto con las restricciones, se describen a continuación.

AWS Systems Manager Limitaciones de automatización

Acción	Descripción	Limitación
leyes: assertAwsResource Propiedad —	Afirmar el estado AWS de un recurso o un estado de evento	Solo EC2 instancias

Acción	Descripción	Limitación
aws:aws:branch —	Ejecute los pasos de automatización condicional	Sin limitación
AWS: CreateTags —	Crear etiquetas para los recursos AWS	Solo a los manuales de automatización de SSM que usted cree
AWS: Ejecute Automation —	Ejecute otra automatización	Solo el manual de automatiz ación que hayas creado
AWS:ExecuteScript —	Ejecute un script	El único script que no realiza ninguna llamada a la API a ningún servicio
aws:pause —	Pausar una automatización	Sin limitación
AWS: RunCommand —	Ejecuta un comando en una instancia gestionada	Utilice únicamente el documento proporcionado por System Manager (AWS RunShellScript y AWS) RunPowerShellScript
aws:sleep —	Retrasar una automatización	Sin limitación
leyes: waitForAws ResourceP roperty —	Espera una propiedad AWS de recurso	Solo EC2 instancias

También puede optar por ejecutar el comando o el script directamente con el runbook proporcionado por Systems Manager (AWS) RunShellScript y AWS, RunPowerShellScript mediante la función «Ejecutar comando» desde la consola de Systems Manager. También puede agrupar estos manuales de ejecución dentro de su propio manual de ejecución, ya sea para realizar validaciones previas o para cualquier lógica de and/or automatización compleja.

La función se rige por el principio de privilegios mínimos y solo proporciona los permisos necesarios para crear, ejecutar y recuperar los detalles de ejecución de los manuales de ejecución destinados a ejecutar and/or scripts de comandos en las instancias gestionadas. No permite utilizar ninguna otra

función que ofrezca el AWS Systems Manager servicio. Si bien la función le permite crear manuales de automatización, la ejecución de los manuales no puede estar orientada a los recursos propiedad de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para usar la AWS Systems Manager automatización en mi cuenta de AMS?

No hay requisitos previos; sin embargo, debe asegurarse de cumplir con los controles internos de and/or cumplimiento de los procesos al crear los manuales de instrucciones. También recomendamos probar minuciosamente los manuales de ejecución antes de ejecutarlos con los recursos de producción.

P: ¿Se puede asociar la política de **`customer_systemsmanager_automation_policy`** Systems Manager a otras funciones de IAM?

No, a diferencia de otros servicios habilitados para el autoaprovisionamiento, esta política solo se puede asignar a la función predeterminada aprovisionada. `customer_systemsmanager_automation_console_role`

A diferencia de las políticas de otras funciones de SSPS, esta política de SSM SSPS no se puede compartir con otras funciones de IAM personalizadas, ya que este servicio de AMS solo sirve para ejecutar comandos o scripts de automatización en las instancias gestionadas. Si se permitiera asociar estos permisos a otras funciones de IAM personalizadas, posiblemente con permisos en otros servicios, el ámbito de las acciones permitidas podría extenderse a los servicios gestionados y, potencialmente, reducir la seguridad de su cuenta.

Para evaluar cualquier solicitud de cambio (RFCs) con respecto a nuestros estándares técnicos de AMS, trabaje con su arquitecto de nube o gerente de prestación de servicios correspondiente (consulte las revisiones de seguridad de la RFC).

> **Note**
>
> AWS Systems Manager le permite usar manuales que se comparten con su cuenta. Te recomendamos que actúes con cautela y compruebes con la diligencia debida cuando utilices manuales compartidos y que te asegures de revisar el contenido para entender cómo command/scripts funcionan antes de ejecutar los manuales. Para obtener más información, consulte las prácticas recomendadas para los documentos SSM compartidos.

Utilice AMS SSP para aprovisionar AWS Transfer Family en su cuenta AMS

Utilice el modo AMS Self-Service Provisioning (SSP) para acceder a las capacidades (Transfer AWS Transfer Family Family) directamente en su cuenta gestionada por AMS. AWS Transfer Family es un AWS servicio totalmente gestionado que le permite transferir archivos a través del Protocolo seguro de transferencia de archivos (SFTP) dentro y fuera del almacenamiento de Amazon Simple Storage Service (Amazon S3). SFTP también se conoce como protocolo de transferencia de archivos Secure Shell (SSH). SFTP se usa en los flujos de intercambio de datos en diversos sectores, como los servicios financieros, la sanidad y el comercio minorista, entre otros.

Con AWS SFTP, puede acceder a un servidor SFTP AWS sin necesidad de ejecutar ninguna infraestructura de servidor. Puede usar este servicio para migrar sus flujos de trabajo basados en SFTP y, al AWS mismo tiempo, mantener los clientes y las configuraciones de sus usuarios finales tal como están. Primero debe asociar su nombre de host al punto final del servidor SFTP y, a continuación, agregar los usuarios y proporcionarles el nivel de acceso adecuado. Una vez hecho esto, las solicitudes de transferencia de los usuarios se atienden directamente desde el punto final del servidor AWS SFTP. Para obtener más información AWS Transfer for SFTP, consulte también Crear un servidor compatible con SFTP.

AWS Transfer for SFTP en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS Transfer for SFTP mi cuenta de AMS?

Solicita el acceso AWS Transfer for SFTP enviando un RFC a la Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añadir tipo de cambio (ct-1w8z66n899dct). Mediante este RFC, se aprovisionan en su cuenta las siguientes funciones de IAM y una política:

- `customer_transfer_author_role`. Esta función está diseñada para que pueda administrar el servicio SFTP a través de la consola.
- `customer_transfer_sftp_server_logging_role`. Esta función está diseñada para estar asociada al servidor SFTP. Permite al servidor SFTP acceder a los registros. CloudWatch
- `customer_transfer_sftp_user_role`. Esta función está diseñada para asignarse a los usuarios de SFTP. Permite a los usuarios de SFTP interactuar con el bucket de S3.
- `policy customer_transfer_scope_down_policy`. Esta política es una política de ámbito reducido que se puede aplicar al usuario de SFTP para limitar su acceso al bucket de S3 a sus carpetas de inicio.

- `customer_transfer_sftp_efs_user_role`. Esta función está diseñada para asignarse a los usuarios de SFTP. Permite a los usuarios de SFTP interactuar con el sistema de archivos EFS.

Una vez aprovisionados en su cuenta, debe incorporar los roles a su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Transfer for SFTP en mi cuenta de AMS?

AWS La transferencia para la configuración de SFTP se limita a los recursos sin los prefijos «AMS-» o «MC-» para evitar cualquier modificación en la infraestructura de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS Transfer for SFTP en mi cuenta de AMS?

- Debe tener un bucket de Amazon S3 con un nombre que contenga la palabra clave «transfer» antes de crear el AWS Transfer for SFTP servidor y los usuarios.
- Para utilizar un «proveedor de identificación del cliente», debe implementar la API Gateway, la función Lambda y su repositorio de usuarios (AD, Secrets Manager, etc.). Para obtener más información, consulte Habilitar la autenticación por contraseña para AWS Transfer for SFTP usar proveedores de identidad AWS Secrets Manager y trabajar con ellos.

Utilice AMS SSP para aprovisionar AWS Transit Gateway en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Transit Gateway las funciones de su cuenta gestionada por AMS. AWS Transit Gateway es un servicio que le permite conectar su Amazon Virtual Private Cloud (VPCs) y sus redes locales a una única puerta de enlace. A medida que aumenta la cantidad de cargas de trabajo en las que se ejecutan AWS, debe poder escalar sus redes entre varias cuentas y Amazon VPCs para mantenerse al día con el crecimiento. Hoy en día, puedes conectar pares de Amazon VPCs mediante el peering. Sin embargo, gestionar la point-to-point conectividad en muchos Amazon VPCs, sin la capacidad de gestionar de forma centralizada las políticas de conectividad, puede resultar engorroso y costoso desde el punto de vista operativo. Para la conectividad local, debe conectar su AWS VPN a cada Amazon VPC individual. La creación de esta solución puede llevar mucho tiempo y ser difícil de administrar cuando el número de ellas VPCs asciende a cientos. Para obtener más información, consulte AWS Transit Gateway.

AWS Transit Gateway en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS Transit Gateway mi cuenta de AMS?

Solicita el acceso AWS Transit Gateway enviando un RFC a la Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añadir tipo de cambio (ct-1w8z66n899dct). Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_tgw_console_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Transit Gateway en mi cuenta de AMS?

Todas las funciones de AWS Transit Gateway están disponibles en tu cuenta de zona de aterrizaje de cuenta única de AMS, a excepción de las modificaciones de la tabla de rutas para las rutas de Transit Gateway. Solicite cambios en la tabla de rutas enviando un tipo de cambio de Administración | Otros | Otros | Crear (ct-1e1xtak34nx76).

> **Note**
>
> Este servicio solo se admite en las zonas de aterrizaje de una sola cuenta (SALZ), no en las zonas de aterrizaje de varias cuentas (MALZ).

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarlo en mi cuenta AMS? AWS Transit Gateway

No hay requisitos previos ni dependencias para su uso AWS Transit Gateway en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS WAF un firewall de aplicaciones web en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS WAF las funciones de su cuenta gestionada por AMS. AWS WAF es un firewall de aplicaciones web (AWS WAF) que ayuda a proteger sus aplicaciones web de los ataques web más comunes que podrían afectar a la disponibilidad de las aplicaciones, comprometer la seguridad o consumir recursos excesivos. AWS WAF le permite controlar qué tráfico debe permitir o bloquear en sus aplicaciones web mediante la definición de reglas de seguridad web personalizables. Puede utilizarlas AWS WAF para crear reglas personalizadas que bloqueen los patrones de ataque más

comunes, como la inyección de SQL o la creación de scripts entre sitios, y reglas diseñadas para su aplicación específica.

Para obtener más información, consulte AWS WAF Web Application Firewall.

AMS no admite la supervisión (CloudWatch alarmas, eventos o alertas MMS) durante AWS WAF. Por su naturaleza AWS WAF, debe crear reglas personalizadas para sus aplicaciones; AMS no puede cuantificar ni crear alarmas por usted sin el contexto de su aplicación. Para obtener más información, consulte AWS WAF Web Application Firewall.

AWS WAF en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo AWS WAF solicito que se configure mi cuenta de AMS?

Solicite acceso AWS WAF enviando una RFC a Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct). Este RFC asigna la siguiente función de IAM a su cuenta:. `customer_waf_role` Una vez aprovisionado el rol de AWS WAF IAM en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso? AWS WAF

Una vez que se hayan aprovisionado los permisos, dispondrá de todas las funciones de AWS WAF.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarlos? AWS WAF

No hay requisitos previos ni dependencias que debas usar AWS WAF en tu cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS Well-Architected Tool en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Well-Architected Tool las funciones de su cuenta gestionada por AMS. AWS Well-Architected Tool Esto le ayuda a revisar el estado de sus cargas de trabajo y a compararlas con las mejores prácticas arquitectónicas más recientes AWS . La herramienta se basa en el AWS Well-Architected Framework, desarrollado para ayudar a los arquitectos de la nube a crear una infraestructura de aplicaciones segura, de alto rendimiento, resiliente y eficiente. Este marco proporciona un enfoque coherente para evaluar las arquitecturas, se ha utilizado en decenas de miles de revisiones de cargas de trabajo realizadas por el equipo de arquitectura de AWS soluciones y proporciona orientación para ayudar a implementar diseños que se adapten a las necesidades de

las aplicaciones a lo largo del tiempo. Para obtener más información, consulte AWS Well-Architected Tool.

AWS WA Tool en Preguntas frecuentes sobre AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS Well-Architected Tool mi cuenta de AMS?

Solicite acceso AWS Well-Architected Tool enviando una RFC a Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct). Este RFC asigna la siguiente función de IAM a su cuenta:. `customer_well_architected_tool_console_admin_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

P: ¿Cuáles son las restricciones de uso AWS Well-Architected Tool en mi cuenta de AMS?

Todas las AWS Well-Architected Tool funciones están disponibles en su cuenta de AMS.

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla AWS Well-Architected Tool en mi cuenta AMS?

No hay requisitos previos ni dependencias para su uso AWS Well-Architected Tool en su cuenta de AMS.

Utilice AMS SSP para aprovisionar AWS X-Ray en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a las capacidades (AWS X-Ray X-Ray) directamente en su cuenta gestionada por AMS. AWS X-Ray ayuda a los desarrolladores a analizar y depurar las aplicaciones distribuidas y de producción, como las creadas con una arquitectura de microservicios. Con X-Ray, puede comprender el rendimiento de su aplicación y sus servicios subyacentes para identificar y solucionar la causa raíz de los problemas y errores de rendimiento. X-Ray proporciona una end-to-end vista de las solicitudes a medida que se desplazan por la aplicación y muestra un mapa de los componentes subyacentes de la aplicación. Puede usar X-Ray para analizar aplicaciones tanto en desarrollo como en producción, desde aplicaciones simples de tres niveles hasta aplicaciones de microservicios complejas que constan de miles de servicios. Para obtener más información, consulte AWS X-Ray.

Preguntas frecuentes sobre X-Ray in AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito acceso a AWS X-Ray mi cuenta de AMS?

Para solicitar el acceso, envíe un formulario de administración | AWS Servicio | Servicio autoaprovisionado | Añada (ct-1w8z66n899dct) el tipo de cambio. Este RFC proporciona la siguiente función de IAM a su cuenta:. `customer_xray_console_role` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación. Además, debe tener la capacidad de `customer_xray_daemon_write_instance_profile` enviar los datos de sus EC2 instancias de Amazon a X-Ray. Este perfil de instancia se crea cuando recibe el`customer_xray_console_role`.

Puede enviar una solicitud de servicio a AMS Operations para asignarla `customer_xray_daemon_write_policy` al perfil de instancia existente, o puede usar el perfil de instancia que se crea cuando AMS Operations habilita X-Ray para usted.

P: ¿Cuáles son las restricciones de uso AWS X-Ray en mi cuenta de AMS?

Todas las funciones de AWS X-Ray están disponibles en su cuenta AMS, excepto el cifrado con la clave AWS KMS (clave KMS). AWS X-Ray cifra todos los datos de rastreo de forma predeterminada. De forma predeterminada, X-Ray cifra las trazas y los datos relacionados en reposo. Si necesita cifrar los datos en reposo con una clave, puede elegir entre una clave de KMS administrada (aws/xray) o una clave de KMS AWS administrada por el cliente. En el caso de la clave gestionada por el cliente de KMS para el cifrado de X-Ray, envíe un tipo de cambio Management | Other | Other | Create (ct-1e1xtak34nx76).

P: ¿Cuáles son los requisitos previos o las dependencias para utilizarla en mi cuenta de AMS? AWS X-Ray

AWS X-Ray depende de Amazon S3 y CloudWatch Logs CloudWatch, que ya están implementados en las cuentas de AMS. Las dependencias transitivas varían en función de las fuentes de datos y otros AWS servicios con los AWS X-Ray que las funciones puedan estar interactuando (por ejemplo, Amazon Redshift, Amazon RDS o Athena).

Utilice AMS SSP para aprovisionar la VM Import/Export en su cuenta de AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder a la máquina virtual Import/Exportcapabilities directamente en su cuenta gestionada por AMS. Import/Export La máquina virtual le permite importar fácilmente imágenes de máquinas virtuales de su entorno existente a las EC2 instancias de Amazon y exportarlas de nuevo a su entorno local. Esta oferta le permite aprovechar sus inversiones actuales en las máquinas virtuales que ha creado para cumplir con sus requisitos de seguridad de TI, gestión de la configuración y conformidad al incorporar esas

máquinas virtuales a Amazon EC2 como ready-to-use instancias. También puede exportar las instancias importadas a su infraestructura de virtualización local, lo que le permite implementar cargas de trabajo en toda su infraestructura de TI. Para obtener más información, consulte Import/Export de máquinas virtuales.

Preguntas frecuentes sobre máquinas virtuales Import/Export en AWS Managed Services

Preguntas y respuestas frecuentes:

P: ¿Cómo solicito el acceso a la máquina virtual Import/Export en mi cuenta de AMS?

Para solicitar el acceso a la máquina virtual Import/Export , envíe una RFC junto con Administración | AWS Servicio | Servicio de autoaprovisionamiento | Añadir tipo de cambio (ct-1w8z66n899dct). Este RFC establece la siguiente política de IAM para su cuenta:. `customer_vmimport_policy` Una vez aprovisionado en su cuenta, debe incorporar el rol en su solución de federación.

Se requiere un rol adicional, el rol de Import/Export servicio de máquina virtual, para que el servicio pueda realizar acciones en su cuenta.

P: ¿Cuáles son las restricciones para usar VM Import/Export en mi cuenta de AMS?

- La funcionalidad para importar imágenes de máquinas y volúmenes de datos personalizados está disponible en AMS VM Import/Export. Sin embargo, se han reducido los permisos de S3 para limitar las acciones a los depósitos que coincidan con el nombre y así limitar `customer-vmimport-*` el acceso a la información de la cuenta.
- La importación de imágenes y instantáneas se admite en AMS VM Import/Export. Sin embargo, las funciones de importación y exportación de instancias no están disponibles debido a medidas de seguridad.
- Además, se ha desactivado la funcionalidad de exportación para mitigar el riesgo de exportar datos confidenciales y restringidos.

P: ¿Cuáles son los requisitos previos o las dependencias para usar VM Import/Export en mi cuenta de AMS?

- Debe proporcionar una imagen de disco compatible para importarla al entorno. AWS Para obtener más información, consulte Import/Export Requisitos de máquinas virtuales.
- Import/Export No se puede acceder a la máquina virtual a través de la AWS consola. Debe acceder a este servicio a través de AWS CLI Herramientas de AWS para PowerShell,, o AWS

SDKs. O bien, puede solicitar un perfil de instancia enviando el tipo de cambio ct-117rmp64d5mvb: Deployment | Advanced stack components | Identity and Access Management (IAM) | Create instance profile. EC2 Este perfil de instancia permite a las herramientas ejecutar comandos desde una instancia.

Modo gestionado por el cliente

El modo gestionado por el cliente de AWS Managed Services (AMS) proporciona un modelo de gobierno que es flexible y se puede adaptar a sus requisitos. Esto puede considerarse una opción alternativa para los servicios y aplicaciones que AMS no puede gestionar por usted. AMS no opera la infraestructura alojada en las cuentas creadas con este modo. Sin embargo, puede aprovechar la administración centralizada de múltiples cuentas en este modo. En este modo, se pueden aprovechar las siguientes funciones de la zona de destino multicuenta:

- Despliegue automatizado de cuentas
- Conectividad a través de Transit Gateway en la cuenta de red
- Biblioteca de reglas AMS Config
- Guarde copias de los registros en la cuenta de registro
- Agregación de las alertas de Guard Duty gestionadas por el cliente a la cuenta de seguridad
- Facturación unificada
- Habilitación de políticas de control de servicios personalizadas.

Por ejemplo: si desea ejecutar cargas de trabajo en Ubuntu Pro, que no es un sistema operativo gestionado por AMS, puede utilizar una cuenta gestionada por el cliente para alojarlo. También puede consolidar las cargas de trabajo a través de cuentas administradas por el cliente, para aprovechar el descuento por volumen en los Instances/Sharing planes reservados que se ofrece al compartir en una organización de AWS.

Cómo empezar con el modo Customer Managed

El modo gestionado por el cliente de AMS está disponible a través de una cuenta especial de aplicación multicuenta para zonas de landing zone.

Para obtener más información, incluida la forma de crear una cuenta de aplicación gestionada por el cliente, consulte Cuentas de aplicaciones gestionadas por el cliente.

Catálogo de servicios de AMS y AWS

El catálogo de servicios de AWS Managed Services (AMS) permite a las organizaciones crear y administrar catálogos de servicios de tecnología de la información (TI) de AWS y permite a los administradores de TI crear, administrar y distribuir catálogos de productos aprobados a los usuarios finales de sus cuentas, quienes pueden acceder a los productos que necesitan en un portal de servicios personalizado. Los administradores pueden controlar qué usuarios tienen acceso a cada producto para garantizar el cumplimiento de las políticas empresariales de la organización. Los administradores también pueden configurar funciones para que los usuarios finales solo necesiten acceso de IAM a Service Catalog para implementar los recursos aprobados. Service Catalog permite que su organización se beneficie de una mayor agilidad y una reducción de costos, ya que los usuarios finales pueden encontrar y lanzar solo los productos que necesitan de un catálogo que usted controla.

Service Catalog le ofrece una alternativa al proceso de solicitud de cambio (RFC) de AMS para aprovisionar y actualizar los recursos de sus cuentas gestionadas por AMS. AMS gestiona todas las tareas de operaciones de infraestructura necesarias para ejecutar AWS a escala para todos los recursos de infraestructura aprovisionados a través de Service Catalog, incluidos la seguridad, el cumplimiento, el aprovisionamiento, la disponibilidad, los parches, la supervisión, las alertas, los informes, la respuesta a incidentes y la optimización de costes. El uso de Service Catalog en su cuenta gestionada por AMS le proporciona un mecanismo para gestionar de forma centralizada los servicios de TI que se implementan habitualmente y le ayuda a lograr una gobernanza coherente, al tiempo que permite a los usuarios implementar rápidamente solo los servicios de TI aprobados que necesitan en sus entornos gestionados.

Introducción a Service Catalog

Para empezar a utilizar Service Catalog en AMS, envíe una solicitud de servicio a través de la consola de AMS para solicitar acceso al Service Catalog. Tras enviar la solicitud, se desplegarán tres funciones de IAM en sus cuentas junto con una pila gestionada por AMS que contiene la CloudFormation macro que invoca la AMS `Transform` (descrita anteriormente) para que podamos registrar los productos en nuestros sistemas y realizar operaciones en la infraestructura aprovisionada a través de Service Catalog. Las tres funciones de IAM implementadas incluyen una función para que los administradores de TI administren los productos como administradores de Service Catalog; una función para los propietarios de aplicaciones y los usuarios finales para configurar, lanzar y administrar los productos; y una función que se utilizará como restricción de lanzamiento, que define los permisos que utilizará Service Catalog al lanzar o actualizar el producto.

Service Catalog en AMS antes de empezar

¿Service Catalog reemplaza el proceso de solicitud de cambio (RFC) de AMS existente?

En las cuentas en las que Service Catalog esté activado, actuará como el sistema de gestión de cambios en el que podrá aprovisionar y actualizar los servicios de TI de su cuenta de AMS a través de su catálogo de productos predefinido; AMS proporcionará un portfolio/product catálogo predeterminado y sus administradores de TI podrán crear y configurar el suyo propio. Service Catalog solo reconocerá las pilas aprovisionadas a través de Service Catalog. Del mismo modo, los servicios aprovisionados a través de Service Catalog no se podrán modificar mediante el proceso de RFC de AMS, ya que la modificación fuera del Catálogo de Servicios desviará la pila de la configuración del producto aprobada.

¿Puedo ver las pilas aprovisionadas a través del catálogo de servicios en la consola AMS?

Sí. Puede ver todas las pilas aprovisionadas a través del catálogo de servicios en la consola AMS. Las pilas aprovisionadas a través del catálogo de servicios se identifican fácilmente mediante el identificador de pila «SC-». Aunque las pilas se pueden ver en la consola de AMS, no podrá actualizarlas mediante el proceso de RFC de AMS. El acceso al sistema de gestión de cambios AMS (RFCs) está limitado únicamente a la solicitud de acceso, la organización de parches y la creación de copias de seguridad. RFCs

Si aprovisiono o and/or actualizo una pila a través de Service Catalog, ¿habrá el RFC correspondiente en la consola AMS?

El único RFC que se mostrará en la consola de AMS es un RFC para registrar la pila en AMS cuando se aprovisione inicialmente una pila. Este RFC se archiva automáticamente mediante el proceso de validación de AMS que se activa cuando se lanza una pila a través de Service Catalog. El resto del aprovisionamiento y los cambios se rastrean directamente en Service Catalog y se pueden ver en la consola de Service Catalog. Además, puede utilizar la función Plan de producto aprovisionado de Service Catalog para ver la lista de cambios que se realizarán en los recursos antes de aprovisionar o actualizar el producto.

¿Debo hacer algo específico para aprovisionar los productos en mi cuenta gestionada por AMS?

Sí. Todos los productos de Service Catalog aprovisionados en las cuentas de AMS deben contener esta línea de JSON en la plantilla CFN que define ese producto:

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

Este fragmento de CloudFormation código activa las validaciones de AMS necesarias para poder aprovisionar el recurso en su cuenta gestionada por AMS. Es su responsabilidad incluir esta línea de código como parte de la definición del producto. Si no se incluye, se producirá un error en el aprovisionamiento y aparecerá el siguiente mensaje de error: «No se pudo crear el producto». AMS administra esta cuenta. Todos los productos de las cuentas de AMS deben tener el `Transform` código AMS en la plantilla».

¿Existe alguna funcionalidad de Service Catalog que no esté disponible y and/or limitada para los clientes de AMS en el momento del lanzamiento?

Sí, las siguientes funciones de SC no estaban disponibles para los clientes de AMS en el momento del lanzamiento inicial:

- Creación de cuentas mediante Service Catalog
- Posibilidad de lanzar todos los servicios de AWS a través de Service Catalog en una cuenta administrada por AMS. La disponibilidad de los servicios de AWS se limita a los servicios compatibles con AMS (gestionados y autoaprovisionados). Para obtener más información sobre los servicios compatibles con AMS, consulte la descripción del servicio AMS.
- Los conectores del administrador de servicios de TI (ITSM) de Service Catalog no se comunicarán con los informes de incidentes y las solicitudes de servicio de AMS.
- Capacidad para aprovechar los inicios rápidos y las arquitecturas de referencia de Service Catalog sin necesidad de realizar modificaciones. Recuerde que los productos de Service Catalog para cuentas AMS deben contener esta línea de código JSON:

  ```
  "Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
  {"Ref":"AWS::StackId"}}}
  ```

  en la plantilla CNF. Tenga en cuenta que esta línea no forma parte de una CloudFormation plantilla típica de AWS y debe añadirse de forma explícita.
- AMS no admite actualmente Terraform para el aprovisionamiento de productos de Service Catalog.
- AMS no admite los conjuntos de pilas CFN de AWS.
- No puede crear funciones de IAM personalizadas.
- Las acciones de servicio se limitan a:
  - AWS- RebootRdsInstance
  - Instancia de reinicio de AWS EC2
  - Instancia AWS-Start EC2

- AWS- StartRdsInstance
- Instancia AWS-Stop EC2
- AWS- StopRdsInstance
- AWS- CreateImage
- AWS- CreateRdsSnapshot
- AWS- CreateSnapshot

> **Note**
>
> Al crear acciones de servicio, puede configurar la función de ejecución para que sea la función de permisos del usuario final, la función de lanzamiento o la función de IAM personalizada que elija. La función de ejecución seleccionada debe tener permisos suficientes para realizar la acción de servicio y tener una TrustPolicy que permita que Service Catalog la asuma; de lo contrario, esa acción de servicio fallará en el momento de la ejecución. Recomendamos utilizar la AWSManagedServicesServiceCatalogLaunchRole, que tiene los permisos y la política de confianza correctos para utilizarla como acción de servicio.

¿Para qué tendré que seguir utilizando el sistema RFC de AMS?

Cuando esté disponible para el público general (GA), necesitará seguir utilizando el RFC para ejecutar las siguientes acciones:

- Configuración de Patch Orchestrator
- Configuración de políticas de respaldo
- Solicitar acceso a la instancia
- Crear y asignar grupos de seguridad que no cumplan las directrices de AMS.
- Realizar la ingesta de carga de trabajo (WIGS)
- Creación de roles de IAM

¿Puedo usar la CLI de Service Catalog para acceder a Service Catalog en mi cuenta gestionada por AMS?

Sí, Service Catalog APIs está disponible y activado a través de la CLI. Están disponibles acciones que van desde la administración de los artefactos de Service Catalog hasta el aprovisionamiento y la terminación de dichos artefactos. Para obtener más información, consulte los recursos de AWS Service Catalog o descargue la CLI o el SDK más recientes de AWS.

¿Quién crea, administra y distribuye los catálogos de productos aprobados de los clientes?

El administrador del catálogo del cliente, el administrador de and/or TI o el recurso asignado, es responsable de la administración de los catálogos de Service Catalog y los productos aprobados.

¿Puedo usar AMS? AMIs

Los AMS AMIs vendidos después de marzo de 2020 se pueden implementar a través de AWS Service Catalog.

¿Cómo puedo migrar a AMS mediante Service Catalog?

Para migrar su carga de trabajo a AMS mediante Service Catalog, comience por seguir el proceso Workload Ingest (WIGs) para crear una AMI en AMS. Utiliza la AMI producida por WIGS para crear un producto en Service Catalog. Cómo hacerlo se detalla en AWS Service Catalog: Getting Started.

Incorporación de AMS Multi-Account Landing Zone (MALZ)

Arquitectura de red MALZ

Acerca de la arquitectura de red de landing zone multicuenta

Antes de iniciar el proceso de incorporación a la zona de aterrizaje multicuenta (MALZ) de AWS Managed Services (AMS), es importante que comprenda la arquitectura básica, o zona de aterrizaje, que AMS crea en su nombre, así como sus componentes y funciones.

La zona de aterrizaje multicuenta AMS es una arquitectura de varias cuentas, preconfigurada con la infraestructura necesaria para facilitar la autenticación, la seguridad, la creación de redes y el registro.

> **Note**
>
> Para obtener estimaciones de los costos, consulte los componentes básicos del entorno AMS multi-account landing zone.

Temas

- Región del servicio
- Unidades organizativas
- Políticas de control de servicios y AWS Organization

El siguiente diagrama describe en detalle la estructura de las cuentas y cómo se segrega la infraestructura en cada una de las cuentas:

Región del servicio

Todos los recursos de una zona de aterrizaje multicuenta de AMS se implementan en la única región de AWS que elija, debido a la limitación actual entre regiones con Active Directory y Transit Gateway.

Unidades organizativas

Una típica zona de aterrizaje multicuenta de AMS consta de cuatro unidades organizativas de nivel superior ()OUs:

- La unidad organizativa (OU) principal (utilizada para agrupar cuentas y administrarlas como una sola unidad)
- La unidad organizativa de la aplicación
- La unidad organizativa gestionada por el cliente
- La OU acelerada

La zona de aterrizaje multicuenta administrada por AMS también le permite crear una cuenta personalizada OUs para agrupar y organizar las cuentas de AWS y asociarlas SCPs con la personalización; para ver ejemplos de cómo hacerlo, consulte Cuenta de administración | Crear cuenta de administración | Crear una cuenta de administración personalizada OUs y de administración | Crear SCP personalizada (es necesario revisar), respectivamente. AMS ofrece cuatro cuentas existentes que OUs permiten solicitar cuentas nuevas: Accelerate, aplicaciones > administradas, aplicaciones > desarrollo OUs y administradas por el cliente.

- Acelere la OU:

  Se trata de una unidad organizativa de nivel superior en la zona de aterrizaje multicuenta (MALZ) de AMS. AMS aprovisiona las cuentas de esta OU con un RFC (Deployment | Managed landing zone | Management account | Create Accelerate Accelerate, ID de tipo de cambio: ct-2p93tyd5angmi). En estas cuentas de aplicaciones aceleradas, puede beneficiarse de servicios operativos acelerados, como la supervisión y las alertas, la gestión de incidentes, la gestión de la seguridad y la gestión de las copias de seguridad. Para obtener más información, consulte las cuentas de AMS Accelerate.

- aplicaciones > OU gestionada:

  En esta subunidad organizativa de la OU de la aplicación, AMS administra en su totalidad las cuentas, incluidas todas las tareas operativas. Las tareas operativas incluyen la gestión de las solicitudes de servicio, la gestión de incidentes, la gestión de la seguridad, la gestión de la continuidad, la gestión de los parches, la optimización de costes, la supervisión y la gestión de eventos. Estas tareas se llevan a cabo para la gestión de su infraestructura. Se OUs pueden crear varios elementos secundarios según sea necesario, hasta que OUs se alcance un límite máximo

de anidados para las organizaciones de AWS. Para obtener más información, consulte Quotas for AWS Organizations.

- aplicaciones > OU de desarrollo:

  Según esta sub-OU de la OU de la aplicación en una zona de aterrizaje gestionada por AMS, las cuentas son cuentas en modo desarrollador que le proporcionan permisos elevados para aprovisionar y actualizar los recursos de AWS fuera del proceso de gestión de cambios de AMS. Esta unidad organizativa también permite la creación de nuevas unidades organizativas secundarias, según sea necesario.

- OU gestionada por el cliente:

  Se trata de una unidad organizativa de nivel superior en la zona de aterrizaje multicuenta de AMS. AMS aprovisiona las cuentas incluidas en esta OU con una RFC. En estas cuentas, las operaciones de las cargas de trabajo y los recursos de AWS son su responsabilidad. Esta unidad organizativa también apoya la creación de nuevas unidades organizativas secundarias, según sea necesario.

Como práctica recomendada, recomendamos agrupar las cuentas incluidas en estas OUs subdivisiones y las solicitadas de forma OUs personalizada en función de sus funcionalidades y políticas.

Políticas de control de servicios y AWS Organization

AWS proporciona políticas de control de servicios (SCPs) para la administración de permisos en una organización de AWS. SCPs se utilizan para definir barreras adicionales sobre qué acciones pueden realizar los usuarios y cuáles. OUs De forma predeterminada, AMS proporciona un conjunto de cuentas integradas SCPs en la administración que proporcionan protección en diferentes niveles de unidad organizativa predeterminados. Para conocer las restricciones de SCP, póngase en contacto con su CSDM.

También puede crear personalizadas SCPs y adjuntarlas a otras específicas. OUs Se pueden solicitar desde su cuenta de administración mediante el tipo de cambio ct-33ste5yc7hprs. A continuación, AMS revisa la personalización solicitada antes de aplicarla al objetivo. SCPs OUs Para ver ejemplos, consulte Cuenta de administración | Crear una cuenta de administración OUs y personalizada | Crear un SCP personalizado (es necesario revisar).

Elegir un solo MALZ o varios MALZs

La siguiente tabla proporciona algunas consideraciones de alto nivel a la hora de decidir entre una sola zona de aterrizaje multicuenta (MALZ) o varias zonas de aterrizaje multicuenta (por ejemplo, dos zonas de aterrizaje multicuenta: Prod y no Prod). En general, la elección depende de las necesidades individuales, los requisitos legales y las prácticas operativas.

Una sola zona de aterrizaje multicuenta frente a varias zonas de aterrizaje multicuenta

Entidad	Zona de aterrizaje AMS única	Varias (dos o más) zonas de aterrizaje
Costo de la base	Más baja, optimizada a un precio aproximado de 3000$ al mes.	Más alto, un costo adicional de aproximadamente 3000 dólares por entorno.
Facturación	Factura única, debido a una sola cuenta de facturación/administración.	Factura separada para cada landing zone multicuenta. Actualmente, la organización de AWS no admite cuentas de administración múltiple con una sola factura.
Portabilidad de las instancias reservadas existentes () RIs	Baja. Actualmente, AWS no RIs se puede convertir en varias cuentas de facturación. Reutilizarías la existente RIs para una zona de aterrizaje multicuenta.	Inferior. Reutilizarías y distribuirías RIs en todas las zonas de landing zone con múltiples cuentas.
Descuentos por estratificación de productos	Alta. Consulta los descuentos por volumen.	Bajo. Consulte Descuentos por volumen.
Gastos generales de configuración inicial (según project/m	Bajo. Integraciones de Active Directory , redes e inicio de sesión único (SSO) una sola vez.	Alta. Realizaría integraciones de Active Directory, integración de red e integraciones de SSO para cada landing zone. Esto podría provocar posibles retrasos en cualquier proyecto de migración.

Entidad	Zona de aterrizaje AMS única	Varias (dos o más) zonas de aterrizaje
igration los plazos)		
Configura bilidad de los servicios comunes	Esfuerzos bajos. Usted configura common/shared servicios como DNS, respaldo, monitoreo, registro, etc.	Grandes esfuerzos. Se requiere una planificación adicional para determina r dónde se ubicarán la infraestructura o los servicios comunes. El tráfico que atraviese varias pasarelas de tránsito (TGWs) en cada landing zone podría suponer un coste adicional.
Escalabilidad	Medio. AMS tiene un límite práctico actual de 150 cuentas por zona de aterrizaje multicuenta. Varios equipos o proveedores que ejecuten aplicacio nes en la misma cuenta podrían tener acceso a las pilas que pertenecen a diferentes equipos. Esta limitación se puede mitigar controlando el acceso a las pilas específicas de cada aplicació n en la ServiceNow capa (integrando la aplicación AMS ServiceNow Connector y utilizando etiquetas). Pregunte a los directores de servicios técnicos (TDMs) o a los arquitectos de la nube (CAs) de AMS cómo implementarlo.	Alta. Posibilidad de aprovechar varias zonas de aterrizaje multicuenta para distribuir las cuentas y, al mismo tiempo, lograr un nivel de segregación de cuentas o aplicaciones. Administr ar un gran número de cuentas puede provocar gastos generales operativos o de costes.
Riesgo operativo	(Depende) Bajo. Integración operativa y preparación una sola vez. Menos posibilidades de que el proceso se desvíe.	(Depende) Bajo. Múltiples actividades operativas y de integración. La deriva en varias zonas de aterrizaje durante el período podría conllevar riesgos operativos.

Entidad	Zona de aterrizaje AMS única	Varias (dos o más) zonas de aterrizaje
Varias regiones de AWS	Región única de AWS. La zona de landing de cuentas múltiples de AMS está restringida a una sola región de AWS. Para abarcar varias regiones de AWS, utilice varias zonas de landing con varias cuentas.	Varias regiones de AWS. Con varias zonas de destino con varias cuentas, puede implementar cada MALZ en una región e interconectarlas mediante el peering de Transit Gateway (TGW).
Migración o portabilidad de cuentas	Sí. Es posible mover cuentas de una OU a otra dentro de la misma organización de AWS.	No. AMS no admite la migración de una cuenta entre zonas de destino, es decir, entre AWS Organizations. Las cargas de trabajo pueden llegar a todas las zonas de aterrizaje con Transit Gateway (TGW) o intercone xión de VPC.
Administr ación de cambios	Medio. Realizar cambios destructi vos en componentes comunes como TGW, Active Directory (AD) o salientes (egress) puede afectar a todas las cargas de trabajo de una landing zone con varias cuentas. Sin embargo, los cambios en los componentes administr ados por AMS se prueban intername nte y se incluyen en actualizaciones sucesivas.	Bajo. Realizar cambios destructivos en componentes comunes como TGW, AD o Outbound (egress) solo puede afectar a las cargas de trabajo de esa landing zone específica con varias cuentas.
Controles de acceso y datos	(Depende) Bajo control si desea conectarse a diferentes redes ADs y locales para cargas de trabajo propias o ajenas a Prod. La federación de SAML, los dominios TGW y los grupos de seguridad (SGs) también pueden ayudar a implementar los controles necesarios.	(Depende) Alto control si desea conectarse a diferentes redes ADs y locales para cargas de trabajo propias y ajenas a Prod. Utilice zonas de aterrizaje separadas para cumplir con los estrictos requisitos de cumplimie nto.

Entidad	Zona de aterrizaje AMS única	Varias (dos o más) zonas de aterrizaje
Cumplimiento y seguridad	(Depende) Bajo si hay requisitos de cumplimiento estrictos para separar por completo las cargas de trabajo materiales de las no materiales. Se han establecido controles preventivos y de detección estándares por la AMS.	(Depende) Una zona de aterrizaje con múltiples cuentas podría ayudar a lograr estrictos requisitos de cumplimiento al segregar por completo las cargas de trabajo materiales de las no materiales. Se han establecido controles preventivos y de detección estándar por parte de la AMS.

Recomendación: Sin un cumplimiento estricto o una necesidad multirregional, empezar con una sola landing zone multicuenta de AMS lograría un buen equilibrio entre el costo, la seguridad, la excelencia operativa y la complejidad de la migración. Siempre puedes configurar una landing zone adicional si te encuentras con alguna restricción empresarial o de cuenta.

Zona de aterrizaje multicuenta única frente a zona de aterrizaje multicuenta FAQs

Algunas preguntas frecuentes a la hora de elegir configurar una sola zona de aterrizaje multicuenta o varias zonas de aterrizaje multicuenta:

P1: ¿Puedo empezar con una sola zona de aterrizaje multicuenta y pasar a una zona de aterrizaje multicuenta si se encuentra algún límite de cuenta o restricciones empresariales?

R: Sí. Puedes elegir configurar otra landing zone multicuenta en cualquier momento:

- Será necesario configurar una nueva cuenta de pagador de facturación (actualmente, AWS no admite cuentas de múltiples pagadores en una sola organización de AWS).
- La creación de la base de una zona de aterrizaje multicuenta tarda hasta 2 semanas una vez que se complete el cuestionario sobre la zona de aterrizaje multicuenta.
- Cada landing zone con varias cuentas supone una adición de unos 3000 USD al mes de coste de funcionamiento.
- Será necesaria la integración de N/W, AD, DNS y SSO para establecer el nuevo MALZ.
- Será necesario configurar cualquier instancia reservada (RIs) y planes de ahorro de costes para la nueva landing zone multicuenta (no RIs son transferibles).

- La zona de aterrizaje multicuenta de AMS no admite la migración de una cuenta entre cuentas de zona de aterrizaje con varias cuentas; por ejemplo, entre organizaciones de AWS. Sin embargo, es posible mover aplicaciones de una cuenta a otra mediante métodos de migración estándar.

Q2: ¿Cuál es el enfoque de AMS respecto a la underlying/shared infraestructura y la cuantificación del riesgo updates/changes para los clientes con respecto a MALZ? Proporcione detalles sobre las garantías incluidas en el proceso. ¿Cómo se dan cuenta los clientes de que MALZ no updates/changes afectará a los clientes? ¿Hay alguna medida que el cliente deba tomar para evitar interrupciones?

R: AMS sigue una metodología de cambio estricta que utiliza herramientas internas que nos permiten definir, revisar, programar y ejecutar cambios en los entornos de los clientes.

El proceso de publicación de las actualizaciones exige la revisión del código, las pruebas de integración, el despliegue en entornos gamma y beta y un tiempo adicional de preparación y pruebas en los entornos beta y gamma antes de lanzarlas a los entornos de los clientes. Todas las versiones incluyen procedimientos de reversión y son supervisadas de cerca por el equipo de versiones y el equipo que creó y solicitó el cambio. El alcance de las versiones se limita a las pilas propiedad de AMS y aprovisionadas por esta. De media, ejecutamos al menos una versión por semana.

Además:

- Se aplican los SLA de AMS. Según la descripción del servicio AMS, cualquier incidente que surja después de una actividad de mantenimiento de infraestructura compartida se regirá por el SLA correspondiente en materia de resolución o créditos.
- Los clientes no requieren medidas preventivas especiales para evitar la interrupción de la infraestructura común. Los clientes tienen permisos de solo lectura en las cuentas de AWS Org o Core OU, por lo que no pueden realizar cambios destructivos en el entorno principal de MALZ. Todas las solicitudes de los clientes a la infraestructura principal requieren la revisión y aprobación de AMS.
- Los clientes pueden probar ciertos cambios a nivel de la organización, por ejemplo, SCPs/Roles a nivel de cuentas individuales que no son de producción, antes de propagar los cambios a nivel de la OU de la aplicación. Está previsto en la hoja de ruta de AMS permitir el uso de varias aplicaciones OUs (segundo trimestre de 2020), lo que reduciría aún más el riesgo de realizar algunos de los cambios a nivel de la organización. El equipo de MALZ ya ha lanzado una unidad organizativa independiente para las cuentas del «modo de creación», a fin de garantizar una clara separación entre la propiedad de los clientes y unos controles separados.

- La mayoría de estos cambios permiten a AMS gestionar la carga de trabajo de manera eficaz y eficiente y no afectan necesariamente a la carga de trabajo de los clientes. Cuando AMS cree que un cambio en la infraestructura compartida puede repercutir en la carga de trabajo de los clientes, opta por adaptarse al calendario de cambios de los clientes.

Recomendación de alto nivel: comience con varias zonas de destino con varias cuentas si:

- Si le ayuda a lograr algún cumplimiento específico.
- Si necesita usar Multi-Region.
- Si tiene diferentes entornos locales ADs y redes para cargas de trabajo y para cargas de trabajo Prod/Material ajenas a ellas. Prod/Non-Material workloads, to clearly segregate b/w

Cuentas multicuenta de Landing Zone

Temas

- Cuenta de administración
- Cuenta de red
- Cuenta de Shared Services
- Cuenta de Log Archive
- Cuenta de seguridad
- Tipos de cuentas de aplicaciones
- Cuenta AMS Tools (migración de cargas de trabajo)

Cuenta de administración

La cuenta de administración es su cuenta de AWS inicial cuando comienza a incorporarse a AMS. Utiliza AWS Organizations como cuenta de administración (también conocida como cuenta de pagador que paga los cargos de todas las cuentas de los miembros), lo que permite a la cuenta crear y administrar financieramente cuentas de miembros. Contiene el marco de AWS landing zone (ALZ), los conjuntos de conjuntos de configuraciones de cuentas, las políticas de control de servicios de AWS Organization (SCPs), etc.

Para obtener más información sobre el uso de una cuenta de administración, consulte Prácticas recomendadas para la cuenta de administración.

El siguiente diagrama proporciona una descripción general de alto nivel de los recursos contenidos en la cuenta de administración.

Recursos de la cuenta de administración

Además de los servicios estándar anteriores, no se crean recursos de AWS adicionales en la cuenta de administración durante la incorporación. Se requieren los siguientes datos durante la incorporación a AMS:

- ID de cuenta de administración: ID de cuenta de AWS que usted creó inicialmente.
- Correos electrónicos de las cuentas principales: indique los correos electrónicos que se van a asociar a cada una de las cuentas principales: cuenta de redes, servicios compartidos, registro y cuenta de seguridad.
- Región de servicio: indique la región de AWS en la que se desplegarán todos los recursos de su AMS landing zone.

Cuenta de red

La cuenta de red sirve como centro central para el enrutamiento de la red entre las cuentas de landing zone multicuenta de AMS, la red local y el tráfico de salida a Internet. Además, esta cuenta contiene bastiones DMZ públicos que son el punto de entrada para que los ingenieros de AMS accedan a los hosts del entorno AMS. Para obtener más información, consulte el siguiente diagrama de alto nivel de la cuenta de red que aparece a continuación.

Arquitectura de cuentas de red

El siguiente diagrama muestra el entorno de zona de landing de cuentas múltiples de AMS, que muestra los flujos de tráfico de red entre cuentas, y es un ejemplo de una configuración de alta disponibilidad.

AMS configura automáticamente todos los aspectos de la red en función de nuestras plantillas estándar y de las opciones que haya seleccionado durante la incorporación. Se aplica un diseño de red de AWS estándar a su cuenta de AWS y se crea una VPC para usted y se conecta a AMS

mediante VPN o Direct Connect. Para obtener más información sobre Direct Connect, consulte AWS Direct Connect. VPCs Los estándares incluyen la DMZ, los servicios compartidos y una subred de aplicaciones. Durante el proceso de incorporación, es VPCs posible que se soliciten y creen más en función de sus necesidades (por ejemplo, divisiones de clientes o socios). Tras la incorporación, se le proporciona un diagrama de red: un documento de entorno que explica cómo se ha configurado la red.

> **Note**
>
> Para obtener información sobre los límites y restricciones de servicio predeterminados para todos los servicios activos, consulte la documentación sobre los límites de servicio de AWS.

El diseño de nuestra red se basa en el «Principio de Privilegio Mínimo» de Amazon. Para lograrlo, enrutamos todo el tráfico, de entrada y salida, a través de una zona desmilitarizada, excepto el tráfico que proviene de una red confiable. La única red de confianza es la que se configura entre el entorno local y la VPC mediante el uso de una and/or VPN y AWS Direct Connect (DX). El acceso se concede mediante el uso de instancias bastión, lo que impide el acceso directo a cualquier recurso de producción. Todas sus aplicaciones y recursos residen en subredes privadas a las que se puede acceder mediante balanceadores de carga públicos. El tráfico de salida público fluye a través de las puertas de enlace NAT de la VPC de salida (en la cuenta de red) hacia la puerta de enlace de Internet y, después, hacia Internet. Como alternativa, el tráfico puede fluir a través de su VPN o Direct Connect a su entorno local.

Conectividad de red privada al entorno AMS Multi-Account Landing Zone

AWS ofrece conectividad privada mediante conectividad de red privada virtual (VPN) o líneas dedicadas con AWS Direct Connect. La conectividad privada en su entorno de múltiples cuentas se configura mediante uno de los métodos que se describen a continuación:

- Conectividad perimetral centralizada mediante Transit Gateway
- Conexión de la and/or VPN Direct Connect (DX) a las nubes privadas virtuales de cuentas (VPCs)

Conectividad perimetral centralizada mediante una pasarela de tránsito

AWS Transit Gateway es un servicio que le permite conectar sus redes locales VPCs y las suyas a una única puerta de enlace. La pasarela de tránsito (TGW) se puede utilizar para consolidar su conectividad perimetral existente y enrutarla a través de un único ingress/egress punto. La pasarela

de tránsito se crea en la cuenta de red de su entorno de cuentas múltiples de AMS. Para obtener más información sobre Transit Gateway, consulte AWS Transit Gateway.

La puerta de enlace AWS Direct Connect (DX) se utiliza para conectar su conexión DX a través de una interfaz virtual de tránsito a la puerta de enlace de tránsito VPCs o VPNs que está conectada a la puerta de enlace de tránsito. Asocie una puerta de enlace de Direct Connect con la puerta de enlace de tránsito. A continuación, cree una interfaz virtual de tránsito para su conexión de AWS Direct Connect a la puerta de enlace Direct Connect. Para obtener información sobre las interfaces virtuales DX, consulte Interfaces virtuales AWS Direct Connect.

Esta configuración ofrece los siguientes beneficios. Puede hacer lo siguiente:

- Administre una única conexión para varias VPCs o VPNs que estén en la misma región de AWS.
- Anuncie prefijos de las instalaciones locales a AWS y de AWS a las instalaciones locales.

> **Note**
>
> Para obtener información sobre el uso de una DX con los servicios de AWS, consulte la sección Classic del kit de herramientas de resiliencia. Para obtener más información, consulte las asociaciones de Transit Gateway.

Para aumentar la resiliencia de su conectividad, le recomendamos que conecte al menos dos interfaces virtuales de tránsito desde diferentes ubicaciones de AWS Direct Connect a la puerta de enlace Direct Connect. Para obtener más información, consulte la recomendación de resiliencia de AWS Direct Connect.

Conexión de DX o VPN a la cuenta VPCs

Con esta opción, los entornos VPCs de landing zone con múltiples cuentas de AMS se conectan directamente a Direct Connect o VPN. El tráfico fluye directamente desde Direct Connect o VPN sin atravesar la puerta de enlace de tránsito. VPCs

Recursos de la cuenta de red

Como se muestra en el diagrama de la cuenta de red, los siguientes componentes se crean en la cuenta y requieren su entrada.

La cuenta de red contiene dos VPCs: la VPC de salida y la VPC DMZ, también conocida como VPC perimetral.

Administrador de redes de AWS

AWS Network Manager es un servicio que le permite visualizar sus redes de pasarelas de tránsito (TGW) sin coste adicional para AMS. Proporciona una supervisión de red centralizada tanto en los recursos de AWS como en las redes locales, una vista global única de su red privada en un diagrama de topología y en un mapa geográfico, y métricas de uso, como el estado de in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down conexión de los bytes. Para obtener información, consulte AWS Network Manager.

Utilice uno de los siguientes roles para acceder a este recurso:

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

VPC de salida

La VPC de salida se utiliza principalmente para el tráfico de salida a Internet y se compone public/private de subredes en un máximo de tres zonas de disponibilidad (). AZs Las puertas de enlace de traducción de direcciones de red (NAT) se aprovisionan en las subredes públicas y los adjuntos de VPC de las pasarelas de tránsito (TGW) se crean en las subredes privadas. El tráfico de Internet de salida o saliente de todas las redes ingresa a través de la subred privada a través de TGW, donde luego se enruta a una NAT a través de tablas de enrutamiento de VPC.

En el caso de las VPCs que contienen aplicaciones orientadas al público en una subred pública, el tráfico que se origina en Internet está contenido en esa VPC. El tráfico de retorno no se enruta a la TGW ni a la VPC de salida, sino que se redirige a través de la puerta de enlace de Internet (IGW) de la VPC.

> **Note**
>
> Rango CIDR de VPC de red: al crear una VPC, debe especificar un rango de direcciones IPv4 para la VPC en forma de bloque de enrutamiento entre dominios sin clase (CIDR); por ejemplo, 10.0.16.0/24. Se trata del bloque de CIDR principal de la VPC.

El equipo de landing zone multicuenta de AMS recomienda el rango de 24 (con más direcciones IP) para proporcionar algo de amortiguación en caso de que se desplieguen otros recursos/dispositivos en el futuro.

Firewall de salida gestionado de Palo Alto

AMS ofrece una solución de firewall de salida gestionada de Palo Alto, que permite filtrar el tráfico saliente con destino a Internet para todas las redes del entorno de zonas de aterrizaje con múltiples cuentas (excepto los servicios de acceso público). Esta solución combina la tecnología de firewall líder del sector (Palo Alto VM-300) con las capacidades de administración de infraestructura de AMS para implementar, monitorear, administrar, escalar y restaurar la infraestructura en entornos operativos compatibles. Los terceros, incluida Palo Alto Networks, no tienen acceso a los firewalls; los gestionan únicamente los ingenieros de AMS.

Control de tráfico

La solución de firewall de salida gestionado gestiona una lista de dominios permitidos compuesta por los dominios necesarios por AMS para servicios como copias de seguridad y parches, así como los dominios definidos por usted. Cuando el tráfico de Internet saliente se enruta al firewall, se abre una sesión, se evalúa el tráfico y, si coincide con un dominio permitido, se reenvía al destino.

Arquitectura

La solución de firewall de salida gestionado sigue un modelo de alta disponibilidad, en el que se implementan de dos a tres firewalls en función del número de zonas de disponibilidad (). AZs La solución utiliza parte del espacio IP de la VPC de salida predeterminada, pero también proporciona una extensión de VPC (/24) para los recursos adicionales necesarios para administrar los firewalls.

Flujo de red

En un nivel alto, el enrutamiento del tráfico de salida público sigue siendo el mismo, excepto en lo que respecta a la forma en que se enruta el tráfico a Internet desde la VPC de salida:

1. El tráfico de salida destinado a Internet se envía a la Transit Gateway (TGW) a través de la tabla de enrutamiento de VPC
2. TGW enruta el tráfico a la VPC de salida a través de la tabla de enrutamiento de TGW

3. La VPC enruta el tráfico a Internet a través de las tablas de enrutamiento de subredes privadas
    a. En el entorno predeterminado de la zona de destino multicuenta, el tráfico de Internet se envía directamente a una puerta de enlace de traducción de direcciones de red (NAT). La solución de firewall administrado reconfigura las tablas de enrutamiento de las subredes privadas para que, en su lugar, dirijan la ruta predeterminada (0.0.0.0/0) a una interfaz de firewall.

Los propios firewalls contienen tres interfaces:

1. Interfaz de confianza: interfaz privada para recibir el tráfico que se va a procesar.
2. Interfaz no confiable: interfaz pública para enviar tráfico a Internet. Como los firewalls realizan la NAT, los servidores externos aceptan solicitudes de estas direcciones IP públicas.
3. Interfaz de administración: interfaz privada para la API del firewall, las actualizaciones, la consola, etc.

Durante todo el enrutamiento, el tráfico se mantiene dentro de la misma zona de disponibilidad (AZ) para reducir el tráfico entre zonas de disponibilidad. El tráfico solo AZs se cruza cuando se produce una conmutación por error.

Modificación de la lista de permitidos

Tras la incorporación, se crea una lista de puntos permitidos predeterminada, que contiene los puntos de conexión públicos necesarios para AMS`ams-allowlist`, así como los puntos de conexión públicos para aplicar parches a los hosts de Windows y Linux. Una vez en funcionamiento, puede crear RFC en la consola AMS, en la categoría Administración | Firewall gestionado | Outbound (Palo Alto) para crear o eliminar listas de permitidos o modificar los dominios. Tenga en cuenta que `ams-allowlist` no se puede modificar. Los RFC se gestionan con total automatización (no son manuales).

Política de seguridad personalizada

Las políticas de seguridad determinan si se debe bloquear o permitir una sesión en función de los atributos del tráfico, como la zona de seguridad de origen y destino, la dirección IP de origen y destino y el servicio. Se admiten políticas de seguridad personalizadas y totalmente automatizadas RFCs. CTs Puede encontrar información sobre cómo crear o eliminar una política de seguridad en la categoría Gestión | Firewall gestionado | Saliente (Palo Alto), y el código para editar una política de seguridad existente en la categoría Implementación | Firewall gestionado | Saliente (Palo Alto). Podrá crear nuevas políticas de seguridad, modificarlas o eliminarlas.

> **Note**
>
> La política de seguridad predeterminada `ams-allowlist` no se puede modificar

CloudWatch Paneles de salida de PA

Se pueden encontrar dos paneles CloudWatch para proporcionar una vista agregada de Palo Alto (PA). El panel de control AMS-MF-PA-Egress-Config-Dashboard proporciona una descripción general de la configuración de PA, enlaces a listas de permitidos y una lista de todas las políticas de seguridad, incluidos sus atributos. El panel de control AMS-MF-PA-Egress-Dashboard se puede personalizar para filtrar los registros de tráfico. Por ejemplo, para crear un panel de control para una política de seguridad, puede crear un RFC con un filtro como el siguiente:

```
fields @timestamp, @message
| filter @logStream like /pa-traffic-logs/
| filter @message like /<Security Policy Name>/
| parse @message
 "*,*,*,
```

Escalado

AMS supervisa el firewall para determinar los límites de rendimiento y escalado. Cuando los límites de rendimiento superan los umbrales mínimos mínimos (CPU/red), AMS recibe una alerta. Un umbral inferior indica que los recursos se están acercando a la saturación, por lo que AMS evaluará las métricas a lo largo del tiempo y se pondrá en contacto con ellos para sugerir soluciones de escalabilidad.

Copia de seguridad y restauración

Las copias de seguridad se crean durante el lanzamiento inicial, después de cualquier cambio de configuración y en intervalos regulares. Las copias de seguridad del lanzamiento inicial se crean para cada host, pero las copias de seguridad modificadas y a intervalos regulares se realizan en todos los hosts del firewall cuando se invoca el flujo de trabajo de copia de seguridad. Los ingenieros de AMS pueden crear copias de seguridad adicionales fuera de esas ventanas o proporcionar los detalles de las copias de seguridad si así lo solicitan.

Los ingenieros de AMS pueden restaurar las copias de seguridad de la configuración si es necesario. Si es necesaria una restauración, se realizará en todos los hosts para mantener sincronizada la configuración entre los hosts.

La restauración también se puede realizar cuando un host requiere el reciclaje completo de una instancia. La restauración automática de la última copia de seguridad se produce cuando se aprovisiona una nueva EC2 instancia. En general, los hosts no se reciclan con regularidad y se reservan para errores graves o cambios de AMI necesarios. El reciclaje del host se inicia manualmente y se le notifica antes de que se produzca un reciclaje.

Además de las copias de seguridad de la configuración del firewall, las reglas específicas de la lista de permitidos se guardan por separado. Cuando se modifican las reglas de la lista de permitidos definidas, se crea automáticamente una copia de seguridad. Si es necesario, un ingeniero de AMS puede restaurar la copia de seguridad de la lista de personas permitidas.

Actualizaciones

La solución de firewall gestionado AMS requiere varias actualizaciones a lo largo del tiempo para añadir mejoras al sistema, funciones adicionales o actualizaciones al sistema operativo (SO) o al software del firewall.

La mayoría de los cambios no afectarán al entorno de ejecución, como la actualización de la infraestructura de automatización, pero otros cambios, como la rotación de las instancias del firewall

o la actualización del sistema operativo, pueden provocar interrupciones. Cuando se evalúe una posible interrupción del servicio debido a las actualizaciones, AMS se pondrá en contacto con usted para adaptarse a los plazos de mantenimiento.

Acceso del operador

Los operadores de AMS utilizan sus ActiveDirectory credenciales para iniciar sesión en el dispositivo de Palo Alto y realizar operaciones (por ejemplo, aplicar parches, responder a un evento, etc.). La solución conserva los registros estándar de autenticación y cambios de configuración de los operadores de AMS para realizar un seguimiento de las acciones realizadas en los hosts de Palo Alto.

Registros predeterminados

De forma predeterminada, los registros generados por el firewall residen en el almacenamiento local de cada firewall. Con el tiempo, los registros locales se eliminarán en función del uso del almacenamiento. La solución AMS permite el envío en tiempo real de los troncos de las máquinas a CloudWatch los troncos; para obtener más información, consulteCloudWatch Integración de registros.

Los ingenieros de AMS aún tienen la capacidad de consultar y exportar los registros directamente desde las máquinas si es necesario. Además, los registros se pueden enviar a un Panorama propiedad del cliente; para obtener más información, consulte. Integración de Panorama

Los registros recopilados por la solución son los siguientes:

Códigos de estado RFC

Tipo de registro	Descripción
Tráfico	Muestra una entrada para el inicio y el final de cada sesión. Cada entrada incluye la fecha y la hora, las zonas de origen y destino, las direcciones y los puertos, el nombre de la aplicación, el nombre de la regla de seguridad aplicada al flujo, la acción de la regla (permitir, denegar o eliminar), la interfaz de entrada y salida, el número de bytes y el motivo del final de la sesión. La columna Tipo indica si la entrada es para el inicio o el final de la sesión, o si la sesión se denegó o canceló. Una «exclusión» indica que la regla de seguridad que bloqueó el tráfico especificó «cualquier»

Tipo de registro	Descripción
	aplicación, mientras que una «denegación» indica que la regla identificó una aplicación específica. Si se interrumpe el tráfico antes de identificar la aplicación, por ejemplo, cuando una regla elimina todo el tráfico de un servicio específico, la aplicación se muestra como «no aplicable».
Amenaza	Muestra una entrada para cada alarma de seguridad generada por el firewall. Cada entrada incluye la fecha y la hora, el nombre o la URL de la amenaza, las zonas de origen y destino, las direcciones y los puertos, el nombre de la aplicación y la acción de alarma (permitir o bloquear) y su gravedad. La columna Tipo indica el tipo de amenaza, como «virus» o «spyware» ; la columna Nombre es la descripción de la amenaza o la URL; y la columna Categoría es la categoría de amenaza (por ejemplo, «keylogger») o la categoría de URL.
Filtrado de URL	Muestra los registros de los filtros de URL, que controlan el acceso a los sitios web y si los usuarios pueden enviar credenciales a los sitios web.
Configuración	Muestra una entrada para cada cambio de configuración. Cada entrada incluye la fecha y la hora, el nombre de usuario del administrador, la dirección IP desde la que se realizó el cambio, el tipo de cliente (interfaz web o CLI), el tipo de comando ejecutado, si el comando se ejecutó correctamente o no, la ruta de configuración y los valores antes y después del cambio.
Sistema	Muestra una entrada para cada evento del sistema. Cada entrada incluye la fecha y la hora, la gravedad del evento y una descripción del evento.
alarmas	El registro de alarmas registra información detallada sobre las alarmas generadas por el sistema. La información de este registro también se incluye en Alarmas. Consulte «Definir la configuración de las alarmas».

Tipo de registro	Descripción
Autenticación	Muestra información sobre los eventos de autenticación que se producen cuando los usuarios finales intentan acceder a los recursos de la red cuyo acceso está controlado por las reglas de la política de autentica ción. Los usuarios pueden utilizar esta información para soluciona r problemas de acceso y ajustar la política de autenticación de los usuarios según sea necesario. Junto con los objetos de correlación, los usuarios también pueden usar los registros de autenticación para identificar actividades sospechosas en la red del usuario, como los ataques de fuerza bruta. De forma opcional, los usuarios pueden configurar las reglas de autenticación para registrar los tiempos de espera de la autenticación. Estos tiempos de espera se refieren al período de tiempo en el que un usuario necesita autenticarse para un recurso solo una vez, pero puede acceder a él repetidamente. Ver información sobre los tiempos de espera ayuda a los usuarios a decidir si deben ajustarlos y cómo hacerlo.
Unificado	Muestra las últimas entradas de registro de tráfico, amenazas, filtrado de URL, WildFire envíos y filtrado de datos en una sola vista. La vista de registro colectiva permite a los usuarios investigar y filtrar estos diferente s tipos de registros juntos (en lugar de buscar en cada conjunto de registros por separado). O bien, los usuarios pueden elegir qué tipos de registro mostrar: hacen clic en la flecha situada a la izquierda del campo de filtro y seleccionan tráfico, amenaza, URL, datos o and/or incendios forestales para mostrar solo los tipos de registro seleccionados.

Gestión de eventos

AMS monitorea continuamente la capacidad, el estado y la disponibilidad del firewall. Las métricas generadas por el firewall, así como las métricas AWS/AMS generadas, se utilizan para crear alarmas que reciben los ingenieros de operaciones de AMS, quienes investigarán y resolverán el problema. Las alarmas actuales cubren los siguientes casos:

Alarmas de eventos:

- Utilización de la CPU del Firewall Dataplane
  - Utilización de la CPU: CPU del plano de datos (tráfico de procesamiento)
- La utilización de paquetes del plano de datos del firewall es superior al 80%
  - Utilización de paquetes: plano de datos (tráfico de procesamiento)
- Utilización de las sesiones del plano de datos del firewall
- Sesión de Firewall Dataplane activa
- Utilización agregada de la CPU del firewall
  - Utilización de la CPU en todos CPUs
- Conmutación por error por parte de AZ
  - Se activa cuando se produce una conmutación por error en una zona de disponibilidad
- Host de Syslog en mal estado
  - El host de Syslog no pasa la comprobación de estado

Alarmas de administración:

- Alarma de fallo del monitor Health Check
  - Cuando el flujo de trabajo de comprobación de estado falla inesperadamente
  - Esto se aplica al flujo de trabajo en sí, no si se produce un error en la comprobación del estado del firewall
- Alarma de error al rotar la contraseña
  - Cuando la rotación de la contraseña falla
  - La contraseña de usuario de la API o del servicio se rota cada 90 días

Métricas

Todas las métricas se capturan y almacenan CloudWatch en la cuenta de red. Se pueden ver accediendo desde la consola a la cuenta de red y navegando hasta la CloudWatch consola. Las métricas individuales se pueden ver en la pestaña de métricas o en un panel de control único para ver las métricas seleccionadas y las métricas agregadas. Para ello, vaya a la pestaña Panel de control y seleccione AMS-MF-PA-Egress-Dashboard.

Métricas personalizadas:

- Comprobación de estado

- Espacio de nombres: AMS/MF/PA/Egress
  - PARouteTableConnectionsByAZ
  - PAUnhealthyByInstance
  - PAUnhealthyAggregatedByAZ
  - PAHealthCheckLockState
- Firewall generado
  - Espacio de nombres:/AMS/MF/PA/Egress<instance-id>
    - DataPlaneCPUUtilizationPacto
    - DataPlanePacketBuffferUtilization
    - dolor GPGateway UtilizationPct
    - panSessionActive
    - panSessionUtilization

CloudWatch Integración de registros

CloudWatch La integración de los registros reenvía los registros de los firewalls a CloudWatch registros, lo que reduce el riesgo de perder los registros debido al uso del almacenamiento local. Los registros se rellenan en tiempo real a medida que los firewalls los generan y se pueden ver bajo demanda a través de la consola o la API.

Las consultas complejas se pueden crear para el análisis de registros o se pueden exportar a CSV mediante CloudWatch Insights. Además, el CloudWatch panel de control personalizado de AMS Managed Firewall también mostrará una vista rápida de consultas específicas del registro de tráfico y una visualización gráfica de las repercusiones del tráfico y las políticas a lo largo del tiempo. El uso de CloudWatch registros también permite la integración nativa con otros servicios de AWS, como AWS Kinesis.

> **Note**
>
> Los registros de PA no se pueden reenviar directamente a un recopilador de Syslog existente en las instalaciones o a un recopilador de Syslog externo. La solución AMS Managed Firewall proporciona el envío en tiempo real de los registros de las máquinas PA a AWS CloudWatch Logs. Puede utilizar la función CloudWatch Logs Insight para ejecutar consultas ad hoc. Además, los registros se pueden enviar a la solución de gestión Panorama de Palo Alto. CloudWatch Los registros también se pueden reenviar a otros destinos mediante los filtros de

CloudWatch suscripción. Obtenga más información sobre Panorama en la siguiente sección. Para obtener más información sobre Splunk, consulte Integración con Splunk.

Integración de Panorama

El firewall gestionado por AMS se puede integrar, de forma opcional, con su Panorama existente. Esto le permite ver las configuraciones del firewall desde Panorama o reenviar los registros del firewall al Panorama. La integración de Panorama con el Firewall gestionado por AMS es de solo lectura y no se permiten cambios de configuración en los firewalls desde Panorama. Panorama está completamente gestionado y configurado por usted, AMS solo se encargará de configurar los firewalls para comunicarse con él.

Licencias

El precio del firewall gestionado por AMS depende del tipo de licencia que se utilice, del tipo de licencia que se utilice por hora o con licencia propia (BYOL) y del tamaño de la instancia en la que se ejecute el dispositivo. Debe solicitar el tamaño de las instancias y las licencias del firewall de Palo Alto que prefiera a través de AWS Marketplace.

- Licencias Marketplace: acepte los términos y condiciones del paquete 1 de firewalls de próxima generación de la serie VM desde la cuenta de red de MALZ.
- Licencias BYOL: acepte los términos y condiciones del firewall de próxima generación (BYOL) de la serie VM desde la cuenta de red de MALZ y comparta con AMS el «código de autenticación BYOL» obtenido tras la compra de la licencia.

Limitaciones

En este momento, AMS es compatible con los firewalls de las series VM-300 o VM-500. Las configuraciones se encuentran aquí: modelos de la serie VM en instancias de AWS EC2 ,

> **Note**
>
> La solución AMS se ejecuta en modo Active-Active, ya que cada instancia de PA de su AZ gestiona el tráfico de salida de su AZ correspondiente. Por lo tanto, con dos AZs, cada instancia de PA gestiona el tráfico de salida de hasta 5 Gbps y proporciona de forma efectiva un rendimiento total de 10 Gbps en dos de ellas. AZs Lo mismo ocurre con todos los límites de cada zona de disponibilidad. Si la comprobación de estado del AMS no se realiza

correctamente, cambiamos el tráfico de la AZ con el PA defectuoso a otra AZ y, durante la sustitución de la instancia, la capacidad se reduce hasta los AZs límites restantes. Actualmente, AMS no admite otros paquetes de Palo Alto disponibles en AWS Marketplace; por ejemplo, no puede solicitar el «paquete de firewalls de próxima generación de la serie VM 2". Tenga en cuenta que la solución de firewall administrado por AMS que utiliza Palo Alto actualmente solo ofrece una oferta de filtrado del tráfico de salida, por lo que el uso de paquetes avanzados de la serie VM no proporcionaría funciones ni ventajas adicionales.

Requisitos de incorporación

- Debe revisar y aceptar los términos y condiciones del firewall de próxima generación de la serie VM de Palo Alto en AWS Marketplace.
- Debe confirmar el tamaño de la instancia que quiere usar en función de la carga de trabajo prevista.
- Debe proporcionar un bloqueo CIDR de /24 horas que no entre en conflicto con las redes de su entorno de zona de destino multicuenta o local. Debe ser de la misma clase que la VPC de salida (la solución proporciona una extensión de VPC /24 a la VPC de salida).

Precios

Los costes de la infraestructura básica del firewall gestionado por AMS se dividen en tres factores principales: la EC2 instancia que aloja el firewall de Palo Alto, la licencia de software, las licencias de la serie VM de Palo Alto y CloudWatch las integraciones.

Los siguientes precios se basan en los firewalls de la serie VM-300.

- EC2 Instancias: el firewall de Palo Alto se ejecuta en un modelo de alta disponibilidad de 2 a 3 EC2 instancias, en el que la instancia se basa en las cargas de trabajo esperadas. El costo de la instancia depende de la región y del número de AZs
  - Por ejemplo, us-east-1, m5.xlarge, 3 AZs
    - 0,192$ * 24 * 30 * 3 = 414,72$
  - https://aws.amazon.com/ec2/precios/bajo demanda/
- Licencias de Palo Alto: el costo de la licencia de software de un firewall Palo Alto VM-300 de próxima generación depende del número de zonas de disponibilidad y del tipo de instancia.
  - Por ejemplo, us-east-1, m5.xlarge, 3 AZs

    - 0,87$ * 24 * 30 * 3 = 1879,20$
    - https://aws.amazon.com/marketplace/pp/B083M7JPKB? ref_=srh_res_product_title #pdp - pricing
- CloudWatch Integración de registros: la integración de registros utiliza SysLog servidores (- t3.medium), NLB y CloudWatch registros. EC2 CloudWatch El costo de los servidores depende de la región y el número de servidores AZs, y el costo de los NLB/CloudWatch registros varía según la utilización del tráfico.
    - Por ejemplo, us-east-1, t3.medium, 3AZ
        - 0,0416$ * 24 * 30 * 3 = 89,86$
    - https://aws.amazon.com/ec2/precios/bajo demanda/
    - https://aws.amazon.com/cloudwatch/precios/

VPC perimetral (DMZ)

La VPC perimetral, o DMZ, contiene los recursos necesarios para que los ingenieros de operaciones de AMS accedan a las redes de AMS. Contiene subredes públicas de 2 a 3 AZs, con hosts SSH Bastions en un grupo de Auto Scaling (ASG) para que los ingenieros de operaciones de AMS puedan iniciar sesión o recorrer un túnel. Los grupos de seguridad adjuntos a los bastiones de la DMZ contienen reglas de entrada del puerto 22 de Amazon Corp Networks.

Rango CIDR de VPC DMZ: al crear una VPC, debe especificar un rango de IPv4 direcciones para la VPC en forma de bloque de enrutamiento entre dominios sin clase (CIDR); por ejemplo, 10.0.16.0/24. Se trata del bloque de CIDR principal de la VPC.

> **Note**
>
> El equipo de AMS recomienda el rango de 24 (con más direcciones IP) para proporcionar un búfer en caso de que se desplieguen otros recursos, como un firewall, en el futuro.

AWS Transit Gateway

AWS Transit Gateway (TGW) es un servicio que le permite conectar sus Amazon Virtual Private Clouds (VPCs) y sus redes locales a una única puerta de enlace. Transit Gateway es la columna vertebral de la red que gestiona el enrutamiento entre las redes de cuentas AMS y las redes externas. Para obtener información sobre Transit Gateway, consulte AWS Transit Gateway.

Proporcione la siguiente entrada para crear este recurso:

- Número ASN de Transit Gateway *: proporciona el número de sistema autónomo (ASN) privado de tu pasarela de transporte. Este debe ser el ASN para el lado AWS de una sesión de protocolo de gateway fronteriza (BGP). El rango es de 64512 a 65534 para 16 bits. ASNs

Cuenta de Shared Services

La cuenta de servicios compartidos sirve como centro central para la mayoría de los servicios del plano de datos de AMS. La cuenta contiene la infraestructura y los recursos necesarios para la gestión del acceso (AD) y la gestión de la seguridad de los puntos finales (Trend Micro) y contiene los bastiones de clientes (SSH/RDP). En el siguiente gráfico se muestra una descripción general de los recursos contenidos en la cuenta de Shared Services.

La VPC de Shared Services está compuesta por la subred AD, la subred EPS y la subred de bastiones del cliente en las tres zonas de disponibilidad (). AZs Los recursos creados en la VPC de Shared Services se enumeran a continuación y requieren su participación.

- Rango CIDR de VPC de Shared Services: al crear una VPC, debe especificar un rango de direcciones IPv4 para la VPC en forma de bloque de enrutamiento entre dominios sin clase (CIDR); por ejemplo, 10.0.1.0/24. Se trata del bloque de CIDR principal de la VPC.

  > **Note**
  >
  > El equipo de AMS recomienda el rango de /23.

- Detalles de Active Directory: Microsoft Active Directory (AD) se utiliza para la user/resource administración, la autenticación/autorización y el DNS en todas sus cuentas de zona de landing zone multicuenta de AMS. AMS AD también está configurado con una conexión unidireccional a Active Directory para una autenticación basada en la confianza. Se requiere la siguiente entrada para crear el AD:
  - Nombre de dominio completo (FQDN) del dominio: el nombre de dominio completo del directorio de Microsoft AD administrado por AWS. El dominio no debe ser un dominio existente ni un dominio secundario de un dominio existente en su red.
  - Nombre NetBIOS del dominio: si no especifica un nombre NetBIOS, AMS utilizará el nombre predeterminado en la primera parte del DNS de su directorio. Por ejemplo, corp para el directorio DNS corp.example.com.

- Trend Micro: protección de puntos finales (EPS): la protección de puntos finales (EPS) de Trend Micro es el componente principal de AMS para la seguridad de los sistemas operativos. El sistema está compuesto por Deep Security Manager (DSM), EC2 instancias, instancias de retransmisión EC2 y un agente presente en todos los planos de datos y en las EC2 instancias de los clientes.

  Debe asumir que está `EPSMarketplaceSubscriptionRole` en la cuenta de Shared Services y suscribirse a la AMI de Trend Micro Deep Security (BYOL) o a Trend Micro Deep Security (Marketplace).

  Se requieren las siguientes entradas predeterminadas para crear el EPS (si desea cambiar las opciones predeterminadas):

  - Tipo de instancia de retransmisión: valor predeterminado: m5.large
  - Tipo de instancia de DSM: valor predeterminado: m5.xlarge
  - Tamaño de la instancia de base de datos: valor predeterminado: 200 GB
  - Tipo de instancia de RDS: valor predeterminado: db.m5.large

- Bastiones de clientes: se le proporcionan bastiones SSH o RDP (o ambos) en la cuenta de servicios compartidos para acceder a otros hosts de su entorno AMS. Para acceder a la red AMS como usuario (SSH/RDP), you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/VPNa la pasarela de tránsito (TGW) y, a continuación, se enruta a la VPC de servicios compartidos. Una vez que pueda acceder al bastión, podrá pasar a otros hosts del entorno AMS, siempre que se haya concedido la solicitud de acceso.
  - Los bastiones SSH requieren las siguientes entradas.
    - Capacidad de instancia deseada del bastión SSH: valor predeterminado: 2.
    - Número máximo de instancias de SSH Bastion: valor predeterminado: 4.
    - Instancias mínimas de SSH Bastion: valor predeterminado -2.
    - Tipo de instancia de SSH Bastion: valor predeterminado: m5.large (se puede cambiar para ahorrar costes; por ejemplo, un t3.medium).
    - Entrada de SSH Bastion CIDRs: rangos de direcciones IP desde los que los usuarios de la red acceden a SSH Bastions.
  - Los bastiones RDP de Windows requieren las siguientes entradas.
    - Tipo de instancia de bastión RDP: valor predeterminado: t3.medium.
    - Sesiones mínimas deseadas de RDP Bastion: valor predeterminado: 2.
    - Número máximo de sesiones de RDP: valor predeterminado -10.

- Tipo de configuración de RDP Bastion: puede elegir una de las siguientes configuraciones
  - SecureStandard = Un usuario recibe un bastión y solo un usuario puede conectarse al bastión.
  - SecureHA = Un usuario recibe dos bastiones en dos zonas de disponibilidad diferentes a los que conectarse y solo un usuario puede conectarse al bastión.
  - SharedStandard = Un usuario recibe un bastión al que conectarse y dos usuarios pueden conectarse al mismo bastión a la vez.
  - sharedHA = Un usuario recibe dos bastiones en dos zonas de disponibilidad diferentes para conectarse y dos usuarios pueden conectarse al mismo bastión a la vez.
- Entrada de RDP del cliente CIDRs: rangos de direcciones IP desde los que los usuarios de su red accederán a RDP Bastions.

Actualizaciones de los servicios compartidos: Multi-Account Landing Zone

AMS publica los planos de datos a las cuentas gestionadas mensualmente, sin previo aviso.

AMS utiliza la unidad organizativa principal para proporcionar servicios compartidos, como el acceso, las redes, el EPS, el almacenamiento de registros y la agregación de alertas en su zona de destino multicuenta. AMS es responsable de abordar las vulnerabilidades, los parches y las implementaciones de estos servicios compartidos. AMS actualiza periódicamente los recursos utilizados para proporcionar estos servicios compartidos para que los usuarios tengan acceso a las funciones y actualizaciones de seguridad más recientes. Las actualizaciones suelen realizarse mensualmente. Los recursos que forman parte de estas actualizaciones son:

- Cuentas que forman parte de la OU principal.

  La cuenta de administración, la cuenta de servicios compartidos, la cuenta de red, la cuenta de seguridad y la cuenta de archivo de registros tienen recursos para los bastiones de RDP y SSH, los proxies, los hosts de administración y la seguridad de los terminales (EPS), que normalmente se actualizan todos los meses. AMS utiliza EC2 despliegues inmutables como parte de la infraestructura de servicios compartidos.
- El nuevo AMS AMIs incorpora las últimas actualizaciones.

> **Note**
>
> Los operadores del AMS utilizan un tipo de cambio de supresión de alarmas (CT) interno al ejecutar los cambios en el plano de datos y la RFC correspondiente a ese CT aparece en su lista de RFC. Esto se debe a que, a medida que se implementa la versión del plano de datos, es posible que varias infraestructuras se cierren, se reinicien o se desconecten, o que se produzcan picos de CPU u otros efectos derivados del despliegue que activen alarmas que, durante el despliegue del plano de datos, son ajenas. Una vez finalizada la implementación, se comprueba que toda la infraestructura funciona correctamente y se vuelven a activar las alarmas.

Cuenta de Log Archive

La cuenta Log Archive sirve como centro central para archivar los registros en su entorno de landing zone multicuenta de AMS. Hay un bucket de S3 en la cuenta que contiene copias de los archivos de registro de AWS CloudTrail y AWS Config de cada una de las cuentas del entorno de landing zone multicuenta de AMS. Puede usar esta cuenta para su solución de registro centralizado con AWS Firehose o Splunk, etc. El acceso de AMS a esta cuenta está limitado a unos pocos usuarios y está restringido a los auditores y los equipos de seguridad para las investigaciones forenses y de conformidad relacionadas con la actividad de la cuenta.

Cuenta de seguridad

La cuenta de seguridad es el eje central de las operaciones relacionadas con la seguridad de la vivienda y el punto principal desde el que se canalizan las notificaciones y alertas a los servicios del plano de control de la AMS. Además, la cuenta de seguridad incluye la cuenta de administración de Amazon Guard Duty y el agregador de AWS Config.

Tipos de cuentas de aplicaciones

Las cuentas de aplicación son cuentas de AWS dentro de la arquitectura de landing zone administrada por AMS que se utilizan para alojar las cargas de trabajo. AMS ofrece tres tipos de cuentas de aplicaciones:

- Cuentas de aplicaciones administradas por AMS
- Cuentas AMS Accelerate

- Cuentas de aplicaciones administradas por el cliente

Las cuentas de aplicación se agrupan de OUs forma diferente en AWS Organizations según el tipo de cuenta de aplicación:

- Unidad organizativa raíz:
  1. Aplicaciones: OU
     - OU gestionada: cuentas gestionadas por AMS
     - OU de desarrollo: cuentas administradas por AMS con el modo de desarrollador habilitado
  2. Accelerate OU: AMS Accelerate Application cuentas
  3. OU gestionada por el cliente: cuentas de aplicaciones gestionadas por el cliente

Las cuentas de aplicación se aprovisionan mediante una RFC enviada desde la cuenta de administración:

- Crear una cuenta de aplicación con VPC ct-1zdasmc2ewzrs
- Crear una cuenta de Accelerate ct-2p93tyd5angmi
- Crear una cuenta de aplicación gestionada por el cliente ct-3pwbixz27n3tn

Cuentas de aplicaciones administradas por AMS

Las cuentas de aplicaciones gestionadas íntegramente por AMS se denominan cuentas de aplicaciones gestionadas por AMS, en las que AMS realiza algunas o todas las tareas operativas, como la gestión de solicitudes de servicio, la gestión de incidentes, la gestión de la seguridad, la gestión de la continuidad (copias de seguridad), la gestión de parches, la optimización de costes o la supervisión y gestión de eventos de la infraestructura.

La cantidad de tareas que realiza AMS depende del modo de gestión de cambios que seleccione. Las cuentas gestionadas por AMS admiten distintos modos de gestión de cambios:

- Modo RFC
- Modo de cambio directo en AMS
- Catálogo de servicios de AMS y AWS
- Modo AMS Advanced Developer
- Modo de aprovisionamiento de autoservicio en AMS

Para obtener más información sobre la gestión de cambios y los diferentes modos, consulte. Modos de administración de cambios

Hay algunos servicios de AWS que puede usar en su cuenta administrada por AMS sin la administración de AMS. La lista de estos servicios de AWS y cómo añadirlos a su cuenta de AMS se describen en la sección Aprovisionamiento de autoservicio.

Cuentas AMS Accelerate

AMS Accelerate es el plan de operaciones de AMS que permite operar la infraestructura de AWS que soporta cargas de trabajo. Puede beneficiarse de los servicios operativos de AMS Accelerate, como la supervisión y las alertas, la gestión de incidentes, la gestión de la seguridad y la gestión de copias de seguridad, sin tener que pasar por una nueva migración, sufrir tiempos de inactividad ni cambiar la forma en que utiliza AWS. AMS Accelerate también ofrece un complemento de parches opcional para cargas de trabajo EC2 basadas que requieren la aplicación de parches con regularidad.

Con AMS Accelerate, tiene la libertad de usar, configurar e implementar todos los servicios de AWS de forma nativa o con las herramientas que prefiera. Utilizará los mecanismos de acceso y cambio que prefiera, mientras que AMS aplica constantemente prácticas comprobadas que le ayudan a ampliar su equipo, optimizar los costes, aumentar la seguridad y la eficiencia y mejorar la resiliencia.

> **Note**
>
> Las cuentas AMS Accelerate de AMS Advanced no cuentan con la administración de cambios de AMS (RFCs) ni con la consola AMS Advanced. En cambio, tienen la consola y la funcionalidad AMS Accelerate.

Las cuentas de Accelerate solo se pueden aprovisionar desde tu cuenta de AMS multicuenta de landing zone Management. Accelerate ofrece diferentes capacidades operativas. Para obtener más información, consulte la descripción del servicio Accelerate.

- Seguirás disfrutando de algunas de las funciones de las cuentas principales de multicuenta landing zone (MALZ), como el registro centralizado, la facturación única, el Config Aggregator en la cuenta de seguridad y. SCPs
- AMS Accelerate no ofrece algunos servicios avanzados de AMS, como el EPS, la gestión de accesos, la gestión de cambios y el aprovisionamiento. Le recomendamos que siga los siguientes pasos para acceder a la pasarela de tránsito (TGW) y configurarla.

Para obtener más información sobre Accelerate, consulta Qué es Accelerate.

Cómo crear su cuenta de Accelerate

Para crear una cuenta de Accelerate, siga los pasos que se describen aquí Crear una cuenta de Accelerate.

Acceder a su cuenta de Accelerate

Después de aprovisionar una cuenta de Accelerate en tu cuenta multicuenta de landing zone (MALZ), tendrás que asumir un rol con permisos de acceso administrativo en la cuenta. `AccelerateDefaultAdminRole`

Para acceder a la nueva cuenta de Accelerate:

1. Inicie sesión en la consola de IAM de la cuenta de administración con el `CustomerDefaultAssumeRole` rol.
2. En la consola de IAM, en la barra de navegación, elige tu nombre de usuario.
3. Elija Switch Role. Si es la primera vez que elige esta opción, aparecerá una página con más información. Después de leerla, elija Switch Role (Cambiar rol). Si borra las cookies del navegador, esta página podría aparecer de nuevo.
4. En la página Switch Role, escriba el ID de cuenta de Accelerate y el nombre del rol que se va a asumir:`AccelerateDefaultAdminRole`.

Ahora que tiene acceso, puede crear nuevos roles de IAM para seguir accediendo a su entorno. Si desea aprovechar la federación de SAML para su cuenta de Accelerate, consulte Permitir que los usuarios federados de SAML 2.0 accedan a la consola de administración de AWS.

Cómo conectar tu cuenta de Accelerate con Transit Gateway

AMS no administra la configuración de red de una cuenta de Accelerate. Tiene la opción de gestionar su propia red mediante AWS APIs (consulte Networking Solutions) o conectarse a la red MALZ gestionada por AMS, mediante la Transit Gateway (TGW) existente implementada en AMS MALZ.

> **Note**
>
> Solo puede tener una VPC asociada al TGW si la cuenta Accelerate se encuentra en la misma región de AWS. Para obtener más información, consulte Transit Gateways.

Para añadir tu cuenta de Accelerate a Transit Gateway, solicita una nueva ruta mediante el tipo de cambio Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59) e incluye esta información:

- Agujero negro: True para indicar que el objetivo de la ruta no está disponible. Haga esto cuando Transit Gateway vaya a eliminar el tráfico de la ruta estática. Es False para enrutar el tráfico al ID de adjunto de TGW especificado. El valor predeterminado es “false” (falso).
- DestinationCidrBlock: el rango IPV4 CIDR utilizado para las coincidencias de destino. Las decisiones de direccionamiento se basan en la coincidencia más específica. Ejemplo: 10.0.2.0/24.
- TransitGatewayAttachmentId: El identificador adjunto de TGW que servirá como objetivo de la tabla de rutas. Si Blackhole es falso, este parámetro es obligatorio; de lo contrario, deje este parámetro en blanco. Ejemplo: tgw-attach-04eb40d1e14ec7272.
- TransitGatewayRouteTableId: El ID de la tabla de rutas de TGW. Ejemplo: tgw-rtb-06ddc751c0c0c881c.

Cree rutas en las tablas de rutas de TGW para conectarse a esta VPC:

1. De forma predeterminada, esta VPC no podrá comunicarse con ninguna otra de la red VPCs MALZ.
2. Decida con su arquitecto de soluciones con qué VPCs quiere que se comunique esta VPC de Accelerate.
3. Envíe una implementación | Managed landing zone | Cuenta de red | Agregue el tipo de cambio de ruta estática (ct-3r2ckznmt0a59) e incluya esta información:
   - Agujero negro: Su valor es verdadero para indicar que el objetivo de la ruta no está disponible. Haga esto cuando Transit Gateway vaya a eliminar el tráfico de la ruta estática. Es False para enrutar el tráfico al ID de adjunto de TGW especificado. El valor predeterminado es “false” (falso).
   - DestinationCidrBlock: el rango IPV4 CIDR utilizado para las coincidencias de destino. Las decisiones de direccionamiento se basan en la coincidencia más específica. Ejemplo: 10.0.2.0/24.
   - TransitGatewayAttachmentId: El identificador adjunto de TGW que servirá como objetivo de la tabla de rutas. Si Blackhole es falso, este parámetro es obligatorio; de lo contrario, deje este parámetro en blanco. Ejemplo: tgw-attach-04eb40d1e14ec7272.
   - TransitGatewayRouteTableId: El ID de la tabla de rutas de TGW. Ejemplo: tgw-rtb-06ddc751c0c0c881c.

Conexión de una nueva VPC de una cuenta de Accelerate a la red de zonas de aterrizaje multicuenta de AMS (creación de un adjunto de VPC de TGW):

1. En su cuenta de red de landing zone con varias cuentas, abra la consola de Amazon VPC.
2. En el panel de navegación, elija Transit Gateways (Puertas de enlace de tránsito). Registre el identificador de TGW de la pasarela de tránsito que ve.
3. En su cuenta de Accelerate, abra la consola de Amazon VPC.
4. En el panel de navegación, seleccione Adjuntos de Transit Gateway > Crear adjunto de Transit Gateway. Haga estas elecciones:
   - Para el ID de Transit Gateway, elige el ID de Transit Gateway que registraste en el paso 2.
   - En Tipo de vinculación, elija VPC.
   - En VPC Attachment (Vinculación de VPC), puede escribir un nombre para la Attachment name tag (Etiqueta de nombre de vinculación).
   - Elija si desea habilitar DNS Support and IPv6 Support.
   - En VPC ID (ID de VPC), elija la VPC que desee asociar a la puerta de enlace de tránsito. Esta VPC debe tener una subred asociada como mínimo.
   - En Subred IDs, seleccione una subred para cada zona de disponibilidad que utilizará la puerta de enlace de tránsito para enrutar el tráfico. Debe seleccionar al menos una subred. Solo puede seleccionar una subred por zona de disponibilidad.
5. Elija Create attachment (Crear vinculación). Registre el ID del adjunto TGW recién creado.

Asociar el accesorio del TGW a una tabla de rutas:

1. Decida a qué tabla de enrutamiento de TGW quiere asociar la VPC. Recomendamos crear una nueva tabla de rutas de aplicaciones para la cuenta Accelerate VPCs mediante el tipo de cambio Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup).
2. Envíe un RFC de Management | Managed landing zone | Cuenta de red | Asocie el adjunto de TGW (ct-3nmhh0qr338q6) a la cuenta de red para asociar el adjunto de VPC o TGW a la tabla de enrutamiento que seleccione.

Cree rutas en las tablas de rutas de TGW para conectarse a esta VPC:

1. De forma predeterminada, esta VPC no podrá comunicarse con ninguna otra VPCs de tu red de landing zone multicuenta.

2. Decida con su arquitecto de soluciones con qué VPCs desea que se comunique esta VPC de cuenta de Accelerate.
3. Envíe un RFC de despliegue | Managed landing zone | Cuenta de red | Agregue un RFC de ruta estática (ct-3r2ckznmt0a59) a la cuenta de red para crear las rutas de TGW que necesite.

Configuración de las tablas de rutas de VPC para que apunten a la pasarela de tránsito multicuenta de AMS para la zona de aterrizaje:

1. Decida con su arquitecto de soluciones qué tráfico quiere enviar a la pasarela de tránsito de la zona de aterrizaje multicuenta de AMS.
2. Envíe un RFC de despliegue | Managed landing zone | Cuenta de red | Agregue un RFC de ruta estática (ct-3r2ckznmt0a59) a la cuenta de red para crear las rutas de TGW que necesite.

Cuentas de aplicaciones administradas por el cliente

Puede crear cuentas que AMS no administre de la manera estándar. Estas cuentas se denominan cuentas gestionadas por el cliente y te permiten gestionar por tu cuenta la infraestructura de las cuentas y, al mismo tiempo, disfrutar de las ventajas de la arquitectura centralizada gestionada por AMS.

Las cuentas gestionadas por el cliente no tienen acceso a la consola AMS ni a ninguno de los servicios que ofrecemos (parches, copias de seguridad, etc.).

Las cuentas gestionadas por el cliente solo se pueden aprovisionar desde tu cuenta de gestión de zonas de landing zone multicuenta de AMS.

Los distintos modos de AMS funcionan de forma diferente con las cuentas de aplicación; para obtener más información sobre los modos, consulte los modos de AWS Managed Services.

Para crear su cuenta de aplicación administrada por el cliente, consulte Cuenta de administración | Crear una cuenta de aplicación administrada por el cliente.

Para eliminar una cuenta de aplicación gestionada por el cliente, utilice Cuenta de gestión | Cuenta de aplicación externa. (El Código de Confirmación de Offboarding no se aplica a las cuentas de aplicaciones administradas por el cliente).

Acceder a tu cuenta gestionada por el cliente

Tras aprovisionar una cuenta gestionada por el cliente (CMA) en una zona de aterrizaje multicuenta (MALZ)`CustomerDefaultAdminRole`, se asigna a la cuenta un rol de administrador que debes asumir, mediante la federación de SAML, para configurar la cuenta.

Para acceder a la CMA:

1. Inicie sesión en la consola de IAM de la cuenta de administración con el CustomerDefaultAssumeRolerol.
2. En la consola de IAM, en la barra de navegación, elige tu nombre de usuario.
3. Elija Switch Role. Si es la primera vez que elige esta opción, aparecerá una página con más información. Después de leerla, elija Switch Role (Cambiar rol). Si borra las cookies del navegador, esta página podría aparecer de nuevo.
4. En la página Switch Role, escriba el ID de la cuenta gestionada por el cliente y el nombre del rol que se va a asumir: CustomerDefaultAdminRole.

Ahora que tiene acceso, puede crear nuevos roles de IAM para seguir accediendo a su entorno. Si desea aprovechar la federación de SAML para su cuenta de CMA, consulte Permitir que los usuarios federados de SAML 2.0 accedan a la consola de administración de AWS.

Cómo conectar tu CMA con Transit Gateway

AMS no administra la configuración de red de las cuentas administradas por el cliente (CMAs). Tiene la opción de gestionar su propia red mediante AWS APIs (consulte Networking Solutions) o conectarse a la red de landing zone multicuenta gestionada por AMS, mediante la Transit Gateway (TGW) existente implementada en AMS MALZ.

> **Note**
>
> Solo puede tener una VPC conectada al TGW si la CMA se encuentra en la misma región de AWS. Para obtener más información, consulte Transit Gateways.

Para añadir su CMA a Transit Gateway, solicite una nueva ruta con la cuenta de red | Añadir ruta estática (ct-3r2ckznmt0a59) cambie de tipo e incluya esta información:

- Agujero negro: Verdadero para indicar que el objetivo de la ruta no está disponible. Haga esto cuando Transit Gateway vaya a eliminar el tráfico de la ruta estática. Es False para enrutar el tráfico al ID de adjunto de TGW especificado. El valor predeterminado es “false” (falso).
- DestinationCidrBlock: el rango IPV4 CIDR utilizado para las coincidencias de destino. Las decisiones de direccionamiento se basan en la coincidencia más específica. Ejemplo: `10.0.2.0/24`.
- TransitGatewayAttachmentId: El identificador adjunto de TGW que servirá como objetivo de la tabla de rutas. Si Blackhole es falso, este parámetro es obligatorio; de lo contrario, deje este parámetro en blanco. Ejemplo: `tgw-attach-04eb40d1e14ec7272`.
- TransitGatewayRouteTableId: El ID de la tabla de rutas de TGW. Ejemplo: `tgw-rtb-06ddc751c0c0c881c`.

Conexión de una nueva VPC gestionada por el cliente a la red de zonas de destino multicuenta de AMS (creación de un adjunto de VPC de TGW):

1. En su cuenta de red de landing zone con varias cuentas, abra la consola de Amazon VPC.
2. En el panel de navegación, elija Transit Gateways. Registra el identificador de TGW de la pasarela de transporte que veas.
3. En tu cuenta gestionada por el cliente, abre la consola de Amazon VPC.
4. En el panel de navegación, seleccione Adjuntos de Transit Gateway > Crear adjunto de Transit Gateway. Haga estas elecciones:
    a. Para el ID de Transit Gateway, elige el ID de Transit Gateway que registraste en el paso 2.
    b. En Tipo de vinculación, elija VPC.
    c. En VPC Attachment (Vinculación de VPC), puede escribir un nombre para la Attachment name tag (Etiqueta de nombre de vinculación).
    d. Elija si desea habilitar DNS Support and IPv6 Support.
    e. En VPC ID (ID de VPC), elija la VPC que desee asociar a la puerta de enlace de tránsito. Esta VPC debe tener una subred asociada como mínimo.
    f. En Subred IDs, seleccione una subred para cada zona de disponibilidad que utilizará la puerta de enlace de tránsito para enrutar el tráfico. Debe seleccionar al menos una subred. Solo puede seleccionar una subred por zona de disponibilidad.
5. Elija Create attachment (Crear vinculación). Registre el ID del adjunto TGW recién creado.

Asociar el accesorio del TGW a una tabla de rutas:

Decida a qué tabla de enrutamiento de TGW quiere asociar la VPC. Recomendamos crear una nueva tabla de rutas de aplicaciones para Customer Managed VPCs mediante el envío de un RFC sobre despliegue | Managed landing zone | Cuenta de red | Crear tabla de rutas de pasarela de tránsito (ct-3dscwaeyi6cup). Para asociar el adjunto de VPC o TGW a la tabla de rutas que seleccione, envíe un RFC de despliegue | Managed landing zone | Cuenta de red | Asociar adjunto de TGW (ct-3nmhh0qr338q6) en la cuenta de red.

Cree rutas en las tablas de rutas de TGW para conectarse a esta VPC:

1. De forma predeterminada, esta VPC no podrá comunicarse con ninguna otra de su red de zonas VPCs de destino multicuenta.
2. Decida con su arquitecto de soluciones con qué VPCs quiere que se comunique esta VPC gestionada por el cliente. Envíe un RFC de despliegue | Managed landing zone | Cuenta de red | Agregue un RFC de ruta estática (ct-3r2ckznmt0a59) a la cuenta de red para crear las rutas de TGW que necesite.

> **Note**
>
> Este CT (ct-3r2ckznmt0a59) no permite agregar rutas estáticas a la tabla de rutas principal EgressRouteDomain; si su CMA necesita permitir el tráfico de salida, envíe un RFC de administración | Otros | Otros (MOO) con el ct-0xdawir96cy7k.

Configuración de las tablas de rutas de VPC para que apunten a la pasarela de tránsito de la zona de aterrizaje multicuenta de AMS:

Decida con su arquitecto de soluciones qué tráfico quiere enviar a la pasarela de tránsito de la zona de aterrizaje multicuenta de AMS. Actualice las tablas de rutas de la VPC para enviar el tráfico al adjunto de TGW creado anteriormente

Obtener ayuda operativa con sus cuentas gestionadas por el cliente

AMS puede ayudarle a gestionar las cargas de trabajo que ha desplegado en sus cuentas gestionadas por el cliente al incorporar la cuenta a AMS Accelerate. Con AMS Accelerate, puede beneficiarse de servicios operativos como la supervisión y las alertas, la gestión de incidentes, la gestión de la seguridad y la gestión de las copias de seguridad, sin tener que pasar por una nueva migración, sufrir tiempos de inactividad o cambiar su forma de utilizar. AWS AMS Accelerate también ofrece un complemento de parches opcional para las cargas de trabajo EC2 basadas en bases que requieren la aplicación de parches con regularidad. Con AMS Accelerate, podrá seguir utilizando, configurando e implementando todos los AWS servicios de forma nativa o con las herramientas que prefiera, tal y como hace con las cuentas gestionadas por clientes de AMS Advanced. Usted utiliza los mecanismos de acceso y cambio que prefiera, mientras que AMS aplica prácticas comprobadas que ayudan a ampliar su equipo, optimizar los costes, aumentar la seguridad y la eficiencia y mejorar la resiliencia. Para obtener más información, consulte la descripción del servicio Accelerate.

Para incorporar su cuenta gestionada por el cliente a Accelerate, póngase en contacto con su CSDM y siga los pasos que se indican en Cómo empezar a utilizar AMS Accelerate.

> **Note**
>
> Las cuentas AMS Accelerate de AMS Advanced no cuentan con la gestión de cambios (solicitudes de cambio o RFCs) de AMS ni con la consola AMS Advanced. En su lugar, cuentan con la consola y la funcionalidad AMS Accelerate.

Cuenta AMS Tools (migración de cargas de trabajo)

Su cuenta de herramientas de zona de destino multicuenta (con VPC) ayuda a acelerar los esfuerzos de migración, aumenta su posición de seguridad, reduce los costes y la complejidad y estandariza su patrón de uso.

Una cuenta de herramientas proporciona lo siguiente:

- Un límite bien definido para el acceso a las instancias de replicación para los integradores de sistemas ajenos a sus cargas de trabajo de producción.
- Le permite crear una cámara aislada para comprobar si una carga de trabajo contiene malware o rutas de red desconocidas antes de colocarla en una cuenta con otras cargas de trabajo.
- Al tratarse de una configuración de cuenta definida, agiliza la incorporación y la preparación para la migración de las cargas de trabajo.

- Rutas de red aisladas para proteger el tráfico desde las instalaciones -> -> Cuenta de herramientas CloudEndure -> imagen ingerida por AMS. Una vez ingerida una imagen, puede compartirla con la cuenta de destino mediante un RFC de AMS Management | Advanced stack components | AMI | Share (ct-1eiczxw8ihc18).

Diagrama de arquitectura de alto nivel:

Utilice el tipo de cambio Deployment | Managed landing zone | Management Account | Create tools account (con VPC) (ct-2j7q1hgf26x5c) para implementar rápidamente una cuenta de herramientas e instanciar un proceso de ingestión de carga de trabajo en un entorno de zona de aterrizaje multicuenta. Consulte Cuenta de administración, Cuenta de herramientas: creación (con VPC).

> **Note**
>
> Recomendamos tener dos zonas de disponibilidad (AZs), ya que se trata de un centro de migración.
> De forma predeterminada, AMS crea los siguientes dos grupos de seguridad (SGs) en cada cuenta. Confirme que estos dos SGs estén presentes. Si no están presentes, abra una nueva solicitud de servicio con el equipo de AMS para solicitarlos.
>
> - SentinelDefaultSecurityGroupPrivateOnlyEgressAll
> - InitialGarden-SentinelDefaultSecurityGroupPrivateOnly
>
> Asegúrese de que las instancias de CloudEndure replicación se creen en la subred privada donde hay rutas de regreso a la red local. Puede confirmarlo asegurándose de que las tablas de enrutamiento de la subred privada tengan una ruta predeterminada de regreso a TGW. Sin embargo, si se realiza un corte de CloudEndure máquina, se debe utilizar una subred privada «aislada», donde no hay ninguna ruta de regreso a la red local y solo se permite el tráfico saliente de Internet. Es fundamental garantizar que la transición se produzca en la subred aislada para evitar posibles problemas con los recursos locales.

Requisitos previos:

1. Nivel de soporte Plus o Premium.
2. La cuenta de aplicación IDs de la clave KMS en la que AMIs se despliegan.

3. La cuenta de herramientas, creada como se describió anteriormente.

AWS Servicio de migración de aplicaciones (AWS MGN)

AWS El Servicio de migración de aplicaciones (AWS MGN) se puede utilizar en su cuenta de MALZ Tools mediante la función de `AWSManagedServicesMigrationRole` IAM que se crea automáticamente durante el aprovisionamiento de la cuenta de Tools. Puede usar AWS MGN para migrar aplicaciones y bases de datos que se ejecutan en versiones compatibles de los sistemas operativos Windows y Linux.

Para up-to-date obtener más información sobre el Región de AWS soporte, consulte la Lista de servicios AWS regionales.

Si MGN no admite actualmente su preferido Región de AWS o si AWS MGN no admite actualmente el sistema operativo en el que se ejecutan sus aplicaciones, considere la posibilidad de utilizar la CloudEndure migración en su cuenta de herramientas. AWS

Solicitar AWS la inicialización de MGN

AMS debe inicializar AWS MGN antes del primer uso. Para solicitarlo para una nueva cuenta de Herramientas, envíe un RFC de administración | Otros | Otros desde la cuenta de Herramientas con estos detalles:

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:

    https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using
 all default values
    to 'Create template' and complete the initialization process.
```

Una vez que AMS complete correctamente la RFC e inicialice AWS MGN en su cuenta de Tools, podrá utilizarla `AWSManagedServicesMigrationRole` para editar la plantilla predeterminada según sus necesidades.

Habilitar el acceso a la nueva cuenta de AMS Tools

Una vez creada la cuenta de herramientas, AMS le proporciona un identificador de cuenta. El siguiente paso es configurar el acceso a la nueva cuenta. Siga estos pasos.

1. Actualice los grupos de Active Directory correspondientes a la cuenta correspondiente IDs.

Las nuevas cuentas creadas por AMS se aprovisionan con la política de funciones, así como con una ReadOnly función que permite a los usuarios archivar archivos. RFCs

La cuenta Tools también tiene un rol de IAM y un usuario adicionales disponibles:

- Rol de IAM: `AWSManagedServicesMigrationRole`
- Usuario de IAM: `customer_cloud_endure_user`

2. Solicite políticas y funciones que permitan a los miembros del equipo de integración de servicios configurar el siguiente nivel de herramientas.

   Navegue hasta la consola AMS y archive lo siguiente RFCs:

   a. Cree una clave KMS. Utilice Crear clave KMS (auto) o Crear clave KMS (se requiere revisión).

      Al usar KMS para cifrar los recursos ingeridos, el uso de una única clave KMS que se comparte con el resto de las cuentas de la aplicación MultiAccount Landing Zone proporciona seguridad a las imágenes ingeridas, ya que se pueden descifrar en la cuenta de destino.

   b. Comparta la clave KMS.

      Utilice el tipo de cambio Management | Advanced stack components | KMS key | Share (es necesario revisar) (ct-05yb337abq3x5) para solicitar que la nueva clave KMS se comparta con las cuentas de la aplicación en las que residirá la ingestión. AMIs

Ejemplo gráfico de la configuración final de una cuenta:

Ejemplo de política de CloudEndure IAM preaprobada por AMS

Para ver una CloudEndure política de IAM preaprobada por AMS: desempaquete el archivo de ejemplo de zona de aterrizaje de WIGS Cloud Endure y abra el. `customer_cloud_endure_policy.json`

Prueba de la conectividad y la end-to-end configuración de la cuenta de AMS Tools

1. Comience por configurar CloudEndure e instalar el CloudEndure agente en un servidor que se replicará en AMS.
2. Cree un proyecto en CloudEndure.
3. Introduzca las AWS credenciales compartidas cuando realizó los requisitos previos, a través del administrador de secretos.

4. En la configuración de replicación:
   a. Seleccione los dos grupos de seguridad «Sentinel» de AMS (solo privados y EgressAll) en la opción Elija los grupos de seguridad que desee aplicar a los servidores de replicación.
   b. Defina las opciones de transición para las máquinas (instancias). Para obtener información, consulte el paso 5. Corte
   c. Subred: subred privada.
5. Grupo de seguridad:
   a. Seleccione los dos grupos de seguridad AMS «Sentinel» (solo privados y EgressAll).
   b. Las instancias de transición deben comunicarse con el Active Directory (MAD) administrado por AMS y con los puntos finales públicos: AWS
      i. IP elástica: ninguna
      ii. IP pública: no
      iii. Función de IAM: customer-mc-ec perfil de 2 instancias
   c. Configure las etiquetas según su convención de etiquetado interna.
6. Instale el CloudEndure agente en la máquina y busque la instancia de replicación que aparecerá en su cuenta de AMS en la EC2 consola.

El proceso de ingestión de AMS:

Higiene de cuentas de AMS Tools

Querrá limpiar una vez que haya terminado en la cuenta, haya compartido la AMI y ya no necesite las instancias replicadas:

- Tras la WIGs ingestión de instancias:
  - Instancia de transición: como mínimo, detenga o finalice esta instancia, una vez que se haya completado el trabajo, a través de la consola de AWS
  - Respaldos de AMI previos a la ingesta: elimínelos una vez que la instancia se haya ingerido y la instancia local haya terminado
  - Instancias ingeridas por AMS: apague la pila o finalice una vez que se haya compartido la AMI
  - Ingeridas por AMS AMIs: se eliminan una vez que se haya completado el uso compartido con la cuenta de destino

- Limpieza final de la migración: documenta los recursos desplegados a través del modo Desarrollador para garantizar que la limpieza se realice de forma periódica, por ejemplo:
  - Grupos de seguridad
  - Recursos creados mediante la formación de nubes
  - ACK de red
  - Subred
  - VPC
  - Tabla de enrutamiento
  - Roles
  - Usuarios y cuentas

Migración a gran escala - Migration Factory

Consulte Presentación de la solución AWS CloudEndure Migration Factory.

MALZ: Incorporación de cuentas principales

Las tareas clave que deberá realizar al incorporarse a una cuenta principal de landing zone AWS multicuenta son las siguientes:.

Temas

- Crea una AWS cuenta principal de landing zone con varias cuentas en AMS
- Cree un rol de IAM para que AMS acceda a su cuenta
- Proteja la nueva cuenta con autenticación multifactor (MFA) para el usuario raíz en AMS
- Suscríbase a AWS Marketplace Trend Micro Endpoint Protection (EPS)
- Configurar redes
- Configurar la administración de acceso

Si tiene preguntas sobre la incorporación, póngase en contacto con su arquitecto de nube.

Crea una AWS cuenta principal de landing zone con varias cuentas en AMS

La zona de aterrizaje multicuenta de AMS requiere el aprovisionamiento de una nueva cuenta de Amazon Web Services (AWS) para que actúe como cuenta de gestión en el entorno de zona de

aterrizaje de cuentas múltiples de AMS. Para crear una Cuenta de AWS, sigue estas step-by-step instrucciones: ¿Cómo creo y activo una nueva cuenta de Amazon Web Services?

Los pasos sencillos son: ve a Crear una cuenta, haz clic en Registrarse ahora y, en la página que se abre, haz clic en Crear una nueva Cuenta de AWS. Sigue las instrucciones que aparecen en pantalla, que incluyen recibir una llamada telefónica e introducir un PIN con el teclado del teléfono. También tendrás que introducir una tarjeta de crédito. AMS usa esta cuenta como cuenta de administración, o cuenta de pago, para tu nueva landing zone multicuenta.

Note

Una vez que se haya incorporado, hable con su administrador de prestación de servicios en la nube (CSDM) sobre la posibilidad de trasladar la facturación de su tarjeta de crédito a un sistema de facturación. Se requerirá la siguiente información:

- Nombre de la empresa de facturación
- Nombre del contacto de facturación
- Número de teléfono de contacto de facturación
- Correo electrónico de contacto de facturación
- Dirección de facturación

Su CSDM le ayudará con esta actualización. Una vez completada, y para cambiar el método de pago, consulta Administrar tus métodos de AWS pago.

Note

No vincule su nueva cuenta a una cuenta de administración o de pago existente. Asegúrese de que su cuenta no forma parte de una cuenta existente AWS Organizations; para obtener más información, consulte ¿Qué es? AWS Organizations

Important

Es muy importante que se asegure de tener una dirección de correo electrónico (una lista de distribución, no la dirección de correo electrónico de una persona) y un número de teléfono asociados a la cuenta para recibir respuestas a posibles incidentes de seguridad. El número

de teléfono y la dirección de correo electrónico de la cuenta no se pueden cambiar sin restablecer la contraseña de la cuenta, lo cual es una tarea importante para una cuenta root de AMS. Para garantizar que estos valores se mantengan estables, es fundamental seleccionar información de contacto que no esté asociada a personas físicas, ya que puede cambiar. Elige un alias de correo electrónico que pueda apuntar a un grupo. Siga esta misma práctica al seleccionar un número de teléfono: elija un número que pueda apuntar a un grupo o a un número que sea propiedad de la empresa y no de un individuo.

Para obtener más información sobre las preguntas que se te harán para incorporar tu cuenta principal a la zona de aterrizaje multicuenta de AMS, consultaApéndice: lista de consideraciones para la incorporación de múltiples cuentas a una zona de landing zone (MALZ).

Cree un rol de IAM para que AMS acceda a su cuenta

Ahora que ha creado correctamente su nueva cuenta Cuenta de AWS, el siguiente paso del proceso es permitir que AMS acceda a la nueva cuenta para crear y configurar su entorno de AMS y atender las solicitudes de cambio y aprovisionamiento en curso. Para obtener más información, consulte Delegar el acceso a todas AWS las cuentas mediante funciones de IAM.

AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso de sus usuarios a AWS los recursos. La IAM se utiliza para controlar quién puede utilizar AWS los recursos (autenticación), qué recursos pueden utilizar y de qué forma (autorización).

Activar el acceso de IAM a la consola AWS

1. Inicie sesión en la consola AWS de administración con las credenciales de su cuenta raíz (el correo electrónico y la contraseña que utilizó para crear las suyas Cuenta de AWS). No inicie sesión con otras credenciales de IAM. Se abre la página de inicio de la consola de AWS administración.
2. En la barra de navegación superior, abre el menú desplegable del nombre de tu cuenta y, a continuación, selecciona Cuenta. Se abre la página de inicio de facturación.
3. Desplázate hacia abajo hasta el acceso de usuario y rol de IAM a Información de facturación y selecciona Editar. Se abre un área de acceso de Activate IAM.
4. Seleccione la casilla de verificación y, a continuación, elija Actualizar. Ahora puede utilizar las políticas de IAM para controlar a qué páginas puede acceder un usuario.

Cree un rol de IAM para que lo utilice AMS

1. Obtenga un archivo JSON o YAML que defina un rol de IAM para que AMS lo utilice para crear su infraestructura. Con cualquiera de las siguientes opciones:
   - Su arquitecto de nube (CA) de AMS le proporciona un archivo JSON o YAML.
   - Puede descargar onboarding_iam_roles.zip y elegir una de las siguientes opciones:
     - onboarding_role_admin.json (más corto, otorga acceso de administrador completo)
     - onboarding_role_minimal.json (más largo, otorga menos privilegios)
2. Inicia sesión en /cloudformation y abre la consola. Consola de administración de AWSCloudFormation https://console.aws.amazon.com
3. Elija Crear pila. Verá la página siguiente.
4. Selecciona Cargar un archivo de plantilla, carga el archivo JSON o YAML del rol de IAM y, a continuación, selecciona Siguiente. Verás la página siguiente.
5. **`ams-onboarding-role`**Entra en la sección del nombre de la pila y continúa desplazándote hacia abajo y seleccionando Siguiente hasta llegar a esta página.
6. Asegúrese de que la casilla de verificación esté seleccionada y, a continuación, seleccione Crear pila.
7. Asegúrese de que la pila se creó correctamente.

Proteja la nueva cuenta con autenticación multifactor (MFA) para el usuario raíz en AMS

Esta sección se ha redactado porque contiene información confidencial relacionada con la seguridad de AMS. Esta información está disponible en la documentación de la consola AMS. Para acceder a AWS Artifact, puede ponerse en contacto con su CSDM para obtener instrucciones o ir a Introducción a AWS Artifact.

Suscríbase a AWS Marketplace Trend Micro Endpoint Protection (EPS)

Trend Micro Endpoint Protection (EPS) es el componente principal de AMS para la seguridad de los sistemas operativos. Para configurar el EPS una vez que se haya iniciado la creación de la zona de landing zone de AMS, debe iniciar sesión en la cuenta principal de servicios compartidos y suscribirse a la AMI de Trend Micro Deep Security en AWS Marketplace. Su CSDM o CA le asesorarán.

1. Inicie sesión en la AWS consola con el rol o el usuario que especificó en el cuestionario de incorporación para `CustomerEPSSubscriptionIAMRoleOrUser`
2. Navegue hasta la pantalla Cambiar rol.

   - Cuenta: proporcionada por AMS
   - Rol: `EPSMarketplaceSubscriptionRole`
   - Nombre para mostrar: Sesión de suscripción a EPS

   Para suscribirse a Trend Micro Deep Security en AWS Marketplace, siga estos pasos después de cambiar de rol en la consola:

   1. Navegue hasta AWS Marketplace.
   2. En Buscar AWS Marketplace productos que se adapten a sus necesidades, seleccione las siguientes opciones:
      a. Proveedores: Trend Micro
      b. Plan de precios: traiga su propia licencia si tiene una licencia o de Hosts Billing
      c. Métodos de entrega: Amazon Machine Image
   3. Haz clic en Continuar para suscribirte en el panel derecho.
   4. Revisa los términos y condiciones y haz clic en Aceptar términos en la esquina superior derecha.
   5. Cierre sesión en la cuenta y confirme con su Cloud Architect que el procedimiento se ha completado.

En este punto, AMS despliega la infraestructura en su entorno de AMS y el entorno está listo para que lo utilice una vez que haya conectado la red y configurado el acceso.

Configurar redes

Las redes en el entorno AMS se gestionan principalmente en la cuenta principal de la red.

Hay varios procesos que deben completarse para configurar las redes de AWS Managed Services (AMS):

- Asignación de espacio IP para su entorno AMS
- Establecer una conectividad de red privada para AWS
- Configurar el firewall para permitir las operaciones de AMS

Asignación de espacio IP para su entorno AMS

Al rellenar el cuestionario de incorporación, ya debería haber trabajado con su arquitecto de nube para definir el espacio IP de su entorno AMS.

Establecer la conectividad de la red privada AWS en AMS

AWS ofrece conectividad privada mediante conectividad VPN y líneas dedicadas a través de AWS Direct Connect. La conectividad privada se puede configurar de dos maneras:

- Conectividad perimetral centralizada mediante Transit Gateway
- Conexión de Direct Connect and/or VPN a la cuenta VPCs

Conectividad perimetral centralizada mediante Transit Gateway

AWS Transit Gateway es un servicio que le permite conectar sus Amazon Virtual Private Clouds (VPCs) y sus redes locales a una única puerta de enlace. Transit Gateway se puede utilizar para consolidar su conectividad perimetral existente y enrutarla a través de un único ingress/egress punto. Para obtener más información, consulte AWS Transit Gateway.

Conexión de Direct Connect a Transit Gateway

Puedes usar tu conexión Direct Connect existente o crear una nueva conexión Direct Connect en una de tus AWS cuentas existentes. La conexión Direct Connect debe ser una conexión dedicada o alojada que funcione a 1 Gbps o más.

> **Note**
>
> Para obtener información sobre el uso de Direct Connect con AWS los servicios, consulte Cómo comenzar en una ubicación de AWS Direct Connect.

Para usar una conexión dedicada de Direct Connect existente, la conexión no debe tener más de 3 interfaces virtuales de tránsito creadas en ella. Esto se debe Direct Connect a que las conexiones dedicadas tienen un límite de 4 interfaces virtuales de tránsito por conexión.

Para obtener información adicional sobre los límites de Direct Connect, consulte Límites de AWS Direct Connect.

Una vez que la conexión Direct Connect esté disponible, ocurre lo siguiente:

1. AMS crea una puerta de enlace Direct Connect en la cuenta de red. Debe proporcionar un número de sistema autónomo (ASN) para la puerta de enlace de Direct Connect y los prefijos que se deben anunciar desde la puerta de enlace de Direct Connect. Esta ASN se utiliza como ASN de Amazon.
2. Debe crear un nuevo Transit VIF y establecer el propietario de la interfaz virtual como la cuenta de red.
3. AMS inicia sesión en la cuenta de red y acepta la propuesta de conexión.
4. AMS asocia la pasarela de tránsito con la pasarela Direct Connect.
5. AMS asocia el adjunto a la tabla de enrutamiento local de Transit Gateway.

> **Note**
>
> El ASN proporcionado para la puerta de enlace Direct Connect y la Transit Gateway debe ser diferente.

Para aumentar la resiliencia de su conectividad, se recomienda conectar al menos 2 interfaces virtuales de tránsito, desde diferentes ubicaciones de AWS Direct Connect, a la puerta de enlace Direct Connect. Para obtener más información, consulte la recomendación de Direct Connect resiliencia.

Conexión de la VPN a Transit Gateway

Para asociar una conexión de VPN a la puerta de enlace de tránsito, debe especificar la puerta de enlace de cliente. Para obtener más información sobre los requisitos de una pasarela de clientes, consulte Requisitos para su pasarela de clientes en la Guía para administradores de redes de Amazon VPC.

Deberá proporcionar el número ASN BGP, la dirección IP pública estática y la opción de enrutamiento (estática o dinámica). Una vez proporcionados estos detalles, AMS crearía el adjunto de la VPN y lo asociaría a la tabla de enrutamiento local de Transit Gateway.

Para obtener más información sobre los archivos adjuntos de Transit Gateway, consulte Adjuntos de VPN de Transit Gateway.

Conexión de Direct Connect and/or VPN a la cuenta VPCs

También puedes conectarte directamente VPCs a Direct Connect o a una VPN. El tráfico fluye directamente desde Direct Connect o VPN sin atravesar la puerta de enlace de tránsito. VPCs

> **Note**
>
> La VPC de servicios compartidos y la cuenta VPCs de la aplicación deben estar conectadas a una conexión Direct Connect o VPN para establecer una conectividad privada.

Direct Connect configuración en AMS

Configure una Direct Connect para comunicarse entre su VPC administrada por AMS y su red interna.

> **Note**
>
> Para obtener información sobre el uso de Direct Connect con AWS los servicios, consulte Cómo empezar en una Direct Connect ubicación.

Para configurar una conexión Direct Connect, complete los siguientes pasos:

1. Regístrese en Amazon Web Services (AWS)

2. Envíe una solicitud de Direct Connect conexión.
3. Complete Cross Connect.
4. (Opcional) Configure las conexiones redundantes con Direct Connect.
5. Realizado por AMS: cree una interfaz virtual.
6. Realizado por AMS: descarga la configuración del router.
7. Verifique su interfaz virtual.

Configuración de VPN

Los pasos básicos que sigue AMS para configurar una VPN que se comunique entre la VPC gestionada por AMS y la red interna.

> **Note**
>
> Para obtener información general sobre el uso de una VPN con AWS servicios, consulte Qué es una AWS Site-to-Site VPN y su puerta de enlace con el cliente (su dispositivo VPN).

Seguimos las AWS secciones Cómo empezar y Probar la conexión Site-to-Site VPN de la Guía del usuario de la VPN para completar los siguientes pasos:

1. En su AWS VPC, cree una pasarela de clientes.
2. En su AWS VPC, cree una puerta de enlace privada virtual.
3. En su AWS VPC, habilite la propagación de rutas en su tabla de rutas.
4. En su AWS VPC, actualice su grupo de seguridad para habilitar el acceso entrante SSH, RDP e ICMP.
5. En su red interna, cree una conexión VPN y configure la puerta de enlace del cliente.
6. Pruebe la conectividad VPN entre la VPC y su red interna.

Configurar la administración de acceso

El uso de una red gestionada por AWS Managed Services (AMS) significa conceder a AMS acceso para gestionar su infraestructura de nube. Deberá configurar un medio de conexión segura entre su red privada y AMS. Esto comienza con algunas decisiones:

- Acceso a AMS API/CLI y consola: querrá instalar la CLI de AMS (las instrucciones se proporcionan en este documento). Utiliza la API de gestión de cambios de AMS para realizar solicitudes de cambio en AMS y la API SKMS de AMS para obtener información sobre los recursos gestionados por AMS. Con los Servicios de federación de Active Directory (AD FS), puede acceder a la consola AMS.
- Acceso de los usuarios: se debe establecer la conectividad entre AD, por parte de AMS (mediante los servicios de directorio), y el directorio que se utiliza para administrar los usuarios.
- Acceso a las instancias: el acceso a nivel de instancia se logra mediante una configuración de confianza unidireccional. Los servicios de directorio confían en las credenciales de su CORP AD, lo que permite iniciar sesión con las credenciales de CORP en pilas integradas en el AMS.

> **Note**
>
> El Active Directory (AD) en el que AMS establece la confianza debe ser el directorio que contenga las cuentas de los usuarios autorizados por usted para acceder a los recursos de AWS.

Establecer una confianza en Active Directory

Para establecer una confianza, AMS requiere que el controlador de dominio disponga de políticas locales -> Opciones de seguridad -> Acceso a la red: canalizaciones denominadas a las que se puede acceder de forma anónima. Incluya las canalizaciones Netlogon y lsarpc en la lista. Estas canalizaciones aparecen en la lista de forma predeterminada, pero a veces se eliminan por motivos de seguridad. Una vez establecida la confianza, se pueden volver a eliminar de la lista.

Configurar el reenviador condicional

1. En el Administrador de DNS de AD -> Crear un nuevo reenviador condicional, en Dominio DNS: utilice el nombre de dominio que AMS le proporcionó; por ejemplo, A523434123.Amazonaws.com (cámbielo por el nombre de dominio seleccionado en el cuestionario de incorporación).
2. En Direcciones IP de los servidores maestros: añade las direcciones IP proporcionadas por el AMS. Asegúrese de que no haya ningún problema de conexión validando ambas direcciones.
3. Seleccione Guardar este reenviador condicional en Active Directory y replique de la siguiente manera: Todos los servidores DNS de este dominio y pulse Aceptar.

Configurar la confianza de AD

Siga este artículo de Microsoft AD Cree una confianza forestal entrante unidireccional para un lado de la confianza mediante la configuración y las opciones que se describen en esta sección.

1. Abra el cuadro de diálogo Inicio -> Herramientas administrativas -> Dominios y confianzas de Active Directory. Haga clic con el botón derecho en el nodo del dominio con el que desee establecer una confianza y, a continuación, haga clic en Propiedades -> Confianzas -> Nueva confianza para abrir el asistente de nueva confianza. Introduzca el nombre de dominio que le proporcionó AMS para el nombre de confianza y pulse Siguiente.
2. En Tipo de confianza, seleccione el nivel de confianza adecuado (por ejemplo, Forest Trust). Pulse Siguiente.
3. En Dirección de confianza, selecciona Unidireccional: entrante. Pulse Siguiente.
4. En Sides of Trust, selecciona Solo este dominio. Pulse Siguiente.
5. En Contraseña de confianza, escribe la contraseña que desees. Pulse Siguiente.
6. Para completar las selecciones de confianza y completar la creación de confianza, pulse Siguiente.
7. En Confirmar confianza entrante, seleccione No, no confirme la confianza entrante. Pulse Siguiente.
8. En Completado el asistente de nueva confianza, selecciona Finalizar y, a continuación, Aceptar para cerrar.
9. Proporcione la contraseña de confianza (póngase en contacto con nosotros a través del número de teléfono de su CSDM por motivos de seguridad). AMS completará la configuración de confianza.

Sitios y servicios de Active Directory

Para reducir la latencia de inicio de sesión, añada el rango CIDR de VPC a sus sitios y servicios de Active Directory (Inicio -> Herramientas administrativas -> Sitios y servicios de Active Directory). Agregue el rango CIDR de VPC a un sitio de Active Directory que contenga los controladores de dominio más cercanos a AWS.

Proporcione a su CSDM el nombre del sitio de AD que ha dedicado a AMS. AMS cambiará el nombre del sitio predeterminado en la parte de AMS de AD para que coincida con el nombre proporcionado.

Enrutamiento de sufijos de nombres de Active Directory

Una vez establecida la confianza unidireccional en el bosque, complete los siguientes pasos para validar el enrutamiento de los sufijos:

1. En Inicio > Todos los programas > Herramientas administrativas, haga clic en Dominios y confianzas de Active Directory.

   Se abre la consola de dominios y confianzas de Active Directory.
2. Haga clic con el botón derecho en el dominio corporativo y haga clic en Propiedades

   Se abre el cuadro de diálogo de propiedades de ese dominio.
3. Haga clic en la pestaña Confianzas.

   Se abre la página de fideicomisos.
4. Haz clic en el nombre de dominio de Amazon y, a continuación, en Propiedades.

   Se abre la página de propiedades de la confianza de dominios de Amazon.
5. Haga clic en Name Suffix Routing y, a continuación, en Actualizar.

   Asegúrese de que no haya conflictos para garantizar que los nombres principales del servicio (SPNs) se puedan resolver a través de la confianza.

Federe su Active Directory con las funciones de IAM de AMS

El objetivo de federar su directorio con las funciones de IAM de AMS es permitir a los usuarios corporativos utilizar sus credenciales corporativas para interactuar con la consola de AWS y la AWS y APIs, por lo tanto, con la consola de AMS y. APIs

Ejemplo de proceso de federación

En este ejemplo se utilizan los Servicios de federación de Active Directory (AD FS); sin embargo, se admite cualquier tecnología compatible con AWS IAM Federation. Para obtener más información sobre la federación de IAM compatible con AWS, consulte Socios de IAM y proveedores de identidad y federación. Su CSDM le ayudará en este proceso, que implica un esfuerzo conjunto con su equipo de AD y AMS.

Para obtener información detallada sobre la integración de SAML para el acceso a las API, consulte este blog de AWS, Cómo implementar el acceso federado a las API y CLI mediante SAML 2.0 y AD FS.

Para ver un ejemplo en el que se instalan la CLI y el SAML de AMS, consulte el Apéndice: regla de notificación de AD FS y configuración de SAML.

Configuración de la federación en la consola AMS (MALZ)

Las funciones de IAM y el proveedor de identidad de SAML (entidad de confianza) que se detallan en la siguiente tabla se han aprovisionado como parte de la infraestructura de AMS. Estas funciones le permiten auditar y ver las cuentas principales de AMS.

Rol	Permisos
AWSManagedServicesReadOnlyRole	Le permite ver la infraestructura de AMS en las cuentas principales.
AWSManagedServicesCaseRole	Le permite ver los recursos de su nueva cuenta de aplicación y archivar los incidentes y las solicitudes de servicio de AMS.
AWSManagedServicesChangeManagementRole	Le permite ver la infraestructura de AMS en las cuentas principales, archivar tickets de AWS Support y solicitar algunos RFCs.

Para ver la lista completa de los roles disponibles en las diferentes cuentas, consulteFunción de usuario de IAM en AMS.

Verificar el acceso a la consola

Una vez que haya configurado ADFS y disponga de la URL de AMS para utilizarla en la autenticación, siga estos pasos.

Con una configuración del Servicio federado de Active Directory (ADFS), puede seguir estos pasos:

1. Abra una ventana del navegador y vaya a la página de inicio de sesión proporcionada para su cuenta. Se abre la IdpInitiatedSignOnpágina ADFS de su cuenta.
2. Selecciona el botón de radio situado junto a Iniciar sesión en uno de los siguientes sitios. Se activa la lista de selección de sitios para iniciar sesión.
3. Selecciona el sitio signin.aws.amazon.com y haz clic en Iniciar sesión. Se abren las opciones para introducir sus credenciales.

4. Introduzca sus credenciales de CORP y haga clic en Iniciar sesión. Se Consola de administración de AWS abre.
5. Pegue en la barra de direcciones la URL de la consola AMS y pulse Entrar. Se abre la consola AMS.

Verificar el acceso a la API

AMS usa la API de AWS, con algunas operaciones específicas de AMS sobre las que puede leer en la referencia de la API de AMS.

AWS proporciona varios a los SDKs que puede acceder en Tools for Amazon Web Services. Si no desea utilizar un SDK, puede realizar llamadas directas a la API. Para obtener información sobre la autenticación, consulte Firmar solicitudes de API de AWS. Si no utiliza un SDK o no realiza solicitudes directas a la API HTTP, puede utilizar el AMS CLIs para la gestión de cambios (CM) y el SKMS.

Instale el AMS CLIs

La AWS CLI es un requisito previo para utilizar el AMS CLIs (Change Management y SKMS).

1. Para instalar la CLI de AWS, consulte Instalación de la interfaz de línea de comandos de AWS y siga las instrucciones correspondientes. Tenga en cuenta que al final de esa página hay instrucciones para usar diferentes instaladores: Linux, MS Windows, macOS, Virtual Environment, Bundled Installer (Linux, macOS o Unix).
2. Tras la instalación, ejecuta aws help para comprobar la instalación.
3. Una vez instalada la CLI de AWS, para instalar o actualizar la CLI de AMS, descargue el archivo zip distribuible de AMS y descomprímalo. Puede acceder a los distribuibles de la CLI de AMS a través del enlace de documentación situado en la barra de navegación izquierda de la consola de AMS o solicitar al administrador de prestación de servicios en la nube (CSDM) que le envíe el archivo zip.
4. Abra el directorio Managed Cloud Distributables -> CLI -> Windows o Managed Cloud Distributables -> CLI -> Linux/macOS, según su sistema operativo, y:
5. Para Windows, ejecute el instalador adecuado (este método solo funciona en sistemas Windows de 32 o 64 bits):

   - 32 bits: ManagedCloud API_x86.msi
   - 64 bits: ManagedCloud API_x64.msi

6. Para Mac/Linux, ejecute el archivo denominado: MC_CLI.sh ejecutando este comando: sh MC_CLI.sh. Tenga en cuenta que los directorios amscm y amsskms y su contenido deben estar en el mismo directorio que el archivo MC_CLI.sh.
7. Si sus credenciales corporativas se utilizan mediante la federación con AWS (la configuración predeterminada de AMS), debe instalar una herramienta de administración de credenciales que pueda acceder a su servicio de federación. Por ejemplo, puede utilizar este blog de seguridad de AWS sobre cómo implementar el acceso federado a las API y CLI mediante SAML 2.0 y AD FS como ayuda para configurar sus herramientas de administración de credenciales.
8. Tras la instalación, ejecute `aws amscm help` y consulte los comandos y `aws amsskms help` las opciones.

MALZ: Incorporación de cuentas de aplicaciones

Debe tener un entorno de AWS Managed Services (AMS) de varias cuentas configurado con cuentas principales antes de solicitar una nueva cuenta de aplicación. Estos son los pasos que debe seguir después de configurar su entorno.

Temas

- Solicitar una nueva cuenta de aplicación
- Configuración de Active Directory para federar el acceso a las funciones de AMS IAM
- Configuración de la red con la nueva cuenta de la aplicación
- Configuración adicional VPCs en la cuenta de la aplicación

Si tiene preguntas sobre la incorporación, póngase en contacto con su administrador de prestación de servicios en la nube (CSDM). Consulte también Cuentas de aplicaciones: administradas por AMS, en modo desarrollo y administradas por el cliente. Para obtener información general sobre los modos, consulte Modos AMS. Administración de servicios en AWS Managed Services

Para obtener información sobre los distintos modos de las cuentas de aplicación, consulte Cuentas de aplicación: administradas por AMS, en modo de desarrollo y administradas por el cliente. Para obtener información general sobre los modos, consulte Modos AMS.

Solicitar una nueva cuenta de aplicación

Debe tener un entorno de AWS Managed Services (AMS) de varias cuentas configurado con cuentas principales antes de solicitar una nueva cuenta de aplicación. Para obtener información sobre cómo

configurar un entorno de múltiples cuentas con cuentas principales, consulte. MALZ: Incorporación de cuentas principales

Puede elegir uno de los siguientes tipos de Amazon VPC para la VPC inicial de la cuenta de la aplicación:

- Privada: esta VPC no tiene ninguna puerta de enlace de Internet conectada. Esto es adecuado para aplicaciones privadas que no requieren acceso a to/from Internet.
- Pública: esta VPC tiene una puerta de enlace a Internet conectada y tiene subredes públicas y privadas. Esto es adecuado para aplicaciones públicas que requieren acceso a Internet to/from .

Para solicitar una nueva cuenta de aplicación, envíe un RFC de implementación | Managed landing zone | Cuenta de administración | Cree una cuenta de aplicación (con VPC) (ct-1zdasmc2ewzrs) y proporcionando los siguientes valores en la RFC:

- Nombre de cuenta: nombre personalizado para la cuenta. Tenga en cuenta que el nombre de la cuenta tiene una longitud máxima de 50 caracteres.
- Correo electrónico de la cuenta: el correo electrónico de la lista de distribución de la cuenta. Este ID de correo electrónico se utiliza para crear la cuenta de AWS.
- Nivel de soporte: el nivel de AWS Support, Premium o Plus.
- Nombre de la VPC: nombre de la VPC.
- Número de zonas de disponibilidad (AZs): 2 o 3.
- CIDR de VPC: el bloque CIDR de la VPC.
- Tipo de ruta: puede ser o. `routable` `isolated` `Routable`significa que la aplicación VPCs asociada a la tabla de enrutamiento de aplicaciones de Transit Gateway (TGW) puede conectarse a esta VPC. `Isolated`significa que la aplicación VPCs asociada a la tabla de enrutamiento de aplicaciones de TGW no puede conectarse a esta VPC. El valor predeterminado es `routable`.
- Tabla de rutas de la aplicación Transit Gateway: tabla de rutas de Transit Gateway a la que se debe asociar la VPC de la cuenta de la aplicación. Si no se proporciona ningún valor, `defaultAppRouteDomain` se utiliza el valor predeterminado, lo que significa que esta cuenta podrá comunicarse con todas las demás cuentas de la misma tabla de enrutamiento.
- PublicSubnetAZ *<1-3>* CIDRCIDR para la subred pública en la AZ 1: El CIDR para la subred pública en la zona de disponibilidad 1.
- PrivateSubnet*<1-10>*AZ *<I-3>* CIDRCIDR para la subred pública en AZ 1: El CIDR para la subred pública en la zona de disponibilidad 1.

En este punto, AMS implementa una nueva cuenta de aplicación en su cuenta de administración de AMS, con la configuración de VPC especificada.

Configuración de Active Directory para federar el acceso a las funciones de AMS IAM

Federe su directorio con las funciones de IAM de AMS para que los usuarios corporativos puedan usar sus credenciales corporativas para interactuar con la consola de AWS y AWS APIs, y con la consola de AMS y AMS. APIs

Ejemplo de proceso de federación

En este ejemplo se utilizan los Servicios de federación de Active Directory (ADFS). Sin embargo, se admite cualquier tecnología compatible con AWS IAM Federation. Para obtener más información sobre la federación de IAM compatible con AWS, consulte Socios de IAM y proveedores de identidad y federación. Su CSDM le ayudará en este proceso, que implica un esfuerzo conjunto con su equipo de AD y AMS.

Para obtener información detallada sobre la integración de SAML para el acceso a las API, consulte este blog de AWS, Cómo implementar el acceso federado a las API y CLI mediante SAML 2.0 y AD FS.

Para ver un ejemplo en el que se instalan la CLI y el SAML de AMS, consulte el Apéndice: Regla de notificación de AD FS y configuración de SAML en la Guía del usuario de AMS.

Configuración de la federación en la consola AMS

Las funciones de IAM y el proveedor de identidad de SAML (entidad de confianza) que se detallan en la siguiente tabla se aprovisionan en la nueva cuenta de la aplicación. Estas funciones le permiten acceder a la nueva cuenta y al archivo de la aplicación RFCs, escribir en los buckets de S3 y realizar otras acciones.

Rol	Permisos
AWSManagedServicesReadOnlyRole	Le permite ver los recursos de su nueva cuenta de aplicación.

Rol	Permisos
AWSManagedServicesCaseRole	Le permite ver los recursos de su nueva cuenta de aplicación y archivar los tickets de AWS Support.
AWSManagedServicesChangeManagementRole	Le permite ver la infraestructura de AMS en las cuentas de la aplicación, archivar RFCs, archivar los tickets de AWS Support, escribir en buckets S3, gestionar los secretos de Secrets Manager y gestionar las instancias reservadas de Amazon Elastic Compute Cloud (Amazon EC2).
AWSManagedServicesSecurityOpsRole	Le permite ver la infraestructura de AMS en las cuentas de la aplicación, gestionar los secretos de Secrets Manager, gestionar las reglas de Web Application Firewall, gestionar los certificados y archivar los tickets de AWS Support.
AWSManagedServicesAdminRole	Le permite ver la infraestructura de AMS en las cuentas de las aplicaciones, gestionar las suscripciones a Marketplace, gestionar los secretos de Secrets Manager, gestionar las reglas de Web Application Firewall, gestionar certificados, crear RFCs, gestionar EC2 instancias reservadas de Amazon, escribir en buckets de S3, archivar tickets de AWS Support y gestionar acuerdos de AWS Artifacts.

Envío de la solicitud de federación a AMS

Si es su primera cuenta, trabaje con sus arquitectos de and/or nube de CSDM para proporcionar el archivo XML de metadatos a su proveedor de identidad.

Si va a incorporar una cuenta o un proveedor de identidad adicional y tiene acceso a la cuenta de administración o a la cuenta de aplicación que desee, siga estos pasos.

1. Cree una solicitud de servicio desde la consola AMS.

> **Note**
>
> - Si va a crear un proveedor de identidad para una cuenta de aplicación, envíe esta solicitud desde la propia cuenta de la aplicación o desde la cuenta de administración.
> - Si va a crear un proveedor de identidad para una cuenta principal de AMS, envíe esta solicitud desde la cuenta de administración.
> - Si va a crear un proveedor de identidad para la cuenta de administración, envíe esta solicitud desde la cuenta de administración o póngase en contacto con su CSDM para obtener ayuda.

   En la solicitud de servicio, proporciona los detalles necesarios para añadir el proveedor de identidad:

   - AccountId de la cuenta en la que se creará el nuevo proveedor de identidad.
   - Si no se proporciona el nombre del proveedor de identidad deseado, el predeterminado será customer-saml; normalmente, debe coincidir con los ajustes configurados en el proveedor de la federación.
   - En el caso de las cuentas existentes, indica si el nuevo proveedor de identidades debe propagarse a todas las funciones de consola existentes o proporciona una lista de funciones que deben confiar en el nuevo proveedor de identidades.
   - Adjunta el archivo XML de metadatos exportado por tu agente de federación a la solicitud de servicio como archivo adjunto.
2. Desde la misma cuenta en la que creó la solicitud de servicio, cree una nueva RFC con el CT-ID ct-1e1xtak34nx76 (Administración | Otros | Otros | Crear) con la siguiente información.

   - <Name>Título: «IDP SAML integrado para la cuenta < >». AccountId
   - AccountId de la cuenta en la que se creará el proveedor de identidad.
   - Nombre del proveedor de identidad.
   - Para las cuentas existentes: si el proveedor de identidades debe propagarse a todas las funciones de consola existentes o a la lista de funciones que deben confiar en el nuevo proveedor de identidades.

- Identificador de caso de la solicitud de servicio creada en el paso 1, donde se adjunta el archivo XML de metadatos.

Verificar el acceso a la consola

Una vez que haya configurado AD FS y disponga de la URL de AMS para utilizarla en la autenticación, puede realizar el siguiente procedimiento.

Con una configuración del Servicio federado de Active Directory (AD FS), puede seguir estos pasos:

1. Abra una ventana del navegador y vaya a la página de inicio de sesión proporcionada para su cuenta. Se abre la IdpInitiatedSignOn página AD FS de tu cuenta.
2. Selecciona el botón de radio situado junto a Iniciar sesión en uno de los siguientes sitios. La lista de sitios de inicio de sesión se activa.
3. Selecciona el sitio signin.aws.amazon.com y selecciona Iniciar sesión. Se abren las opciones para introducir sus credenciales.
4. Introduzca sus credenciales de CORP y seleccione Iniciar sesión. Se abre la consola de administración de AWS.
5. Pegue en la barra de direcciones la URL de la consola AMS y pulse Entrar. Se abre la consola AMS.

Verificar el acceso a la API

AMS usa la API de AWS, con algunas operaciones específicas de AMS sobre las que puede leer en la referencia de la API de AMS.

AWS proporciona varios a los SDKs que puede acceder en Tools for Amazon Web Services. Si no desea utilizar un SDK, puede realizar llamadas directas a la API. Para obtener información sobre la autenticación, consulte Firmar solicitudes de API de AWS. . Si no utiliza un SDK ni realiza solicitudes directas a la API HTTP, puede utilizar el AMS CLIs for Change Management (CM) y el SKMS.

Configuración de la red con la nueva cuenta de la aplicación

La configuración de la red para la cuenta de la aplicación incluye la configuración de las reglas de firewall y, posiblemente, la configuración de tablas de rutas de Transit Gateway (TGW) adicionales.

Configuración del firewall

Para usar las aplicaciones implementadas en su entorno AMS, debe crear algunas reglas de firewall. No necesita estas reglas para acceder a sus instancias, sino que puede saltar a través de los bastiones hasta llegar a las instancias.

Reglas de firewall para el acceso a las aplicaciones

Debe abrir los siguientes puertos para el tráfico a través del firewall:

- Desde su red local hasta su nueva CIDRs VPC de aplicaciones, tanto en la dirección de entrada como de salida.
- Desde su nueva VPC de aplicaciones CIDRs hasta su red local, tanto en la dirección de entrada como de salida (si las aplicaciones en la nube necesitan llegar a las aplicaciones locales).

Puerto	Protocolo	Servicio	Desde/Hasta	Hacia y desde
80	TCP	Acceso web HTTP	Red local	Aplicación AMS VPC
443	TCP	Acceso web HTTPS	Red local	Aplicación AMS VPC

Configuración de tablas de rutas de aplicaciones de pasarela de tránsito adicionales

Las redes de AWS Managed Services (AMS) son flexibles y admiten una variedad de casos de uso de redes.

- Comunicación entre aplicaciones VPCs de la misma cuenta.
- Comunicación entre aplicaciones VPCs en cuentas diferentes.
- Aislamiento entre aplicaciones VPCs en diferentes cuentas.
- Aislamiento entre aplicaciones VPCs en las mismas cuentas.

Si tiene unique/special requisitos de red, póngase en contacto con su arquitecto de nube de AMS y ellos desarrollarán un plan para que la arquitectura de red de AMS satisfaga sus requisitos.

En función de la decisión de red tomada para la cuenta de aplicación VPCs, puede crear varias tablas de rutas de aplicaciones de Transit Gateway (TGW) enviando un RFC de despliegue | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup).

El tipo de cambio requiere que especifique `TransitGatewayRouteTableName` (un nombre significativo para la tabla de rutas de TGW), y. `TransitGatewayId` `TGWRouteTableType`

> **Note**
>
> Si se selecciona createCustomRoute Dominio para TGWRouteTableType, la tabla de rutas creada está vacía. Debe presentar una RFC con el tipo de cambio Deployment | Managed landing zone | Networking account | Add static route (ct-3r2cknmt0a59).

Configuración adicional VPCs en la cuenta de la aplicación

Para solicitar una VPC de cuenta de aplicación adicional, envíe un RFC sobre despliegue | Managed landing zone | Cuenta de aplicación | Creación de VPC (ct-1j3503fres5a5).

Esto funciona de la misma manera que configurar una VPC para una nueva cuenta de aplicación. Para obtener información, consulte Solicitar una nueva cuenta de aplicación.

Apéndice: lista de consideraciones para la incorporación de múltiples cuentas a una zona de landing zone (MALZ)

Hay una serie de consideraciones clave que tendrás que tener en cuenta a la hora de planificar el despliegue de una zona de landing zone con varias cuentas de AMS. Sus elecciones proporcionarán a AMS la información necesaria para determinar los componentes de infraestructura que necesitará. Su arquitecto de nube (CA) le proporcionará un cuestionario para ayudarlo en este trabajo.

Temas

- Configuración de cuentas AMS multicuenta en la zona de landing zone
- Alertas de monitoreo de zonas de landing zone con varias cuentas de AMS
- Configuración de red
- Configuración de Active Directory
- Protección de endpoints de Trend Micro (EPS)

- Acceso: Bastions, SSH y RDP
- Federación

> **Note**
>
> Para obtener más información sobre los tipos de instancias, consulta Amazon EC2 Instance Types.
> Para obtener más información sobre los tipos de instancias de bases de datos, consulte Tipos de instancias de Amazon RDS.
> Si necesitas Direct Connect, consulta la Guía de incorporación de una sola cuenta de AMS en la zona de landing zone para crear una conexión Direct Connect.

Su administrador de prestación de servicios en la nube (CSDM) le enviará un cuestionario de incorporación con preguntas sobre los ajustes de configuración que desee para su cuenta. Trabaje con su CSDM para completar el cuestionario antes de continuar.

Configuración de cuentas AMS multicuenta en la zona de landing zone

- ID de cuenta nueva

  El Cuenta de AWS ID que creaste para la zona de aterrizaje multicuenta de AMS. No debe formar parte de una AWS organización.
- Región de servicio

  La región principal en la que se desplegará el entorno de zona de landing con múltiples cuentas de AMS.
- Los correos electrónicos de la cuenta principal para recibir notificaciones. (todos deben estar en el mismo dominio). Proporcione una dirección de correo electrónico para cada uno de ellos:
  - Cuenta de Shared Services
  - Cuenta de red
  - Cuenta de registro
  - Cuenta de seguridad
- Tu tipo de servicio, Premium o Plus

  Esto determina los acuerdos de nivel de servicio (SLAs) para resolver los problemas en su entorno

Alertas de monitoreo de zonas de landing zone con varias cuentas de AMS

El AMS permite recibir alertas directas (en lugar de recibir notificaciones del servicio AMS) sobre determinadas alertas de monitoreo. Para suscribirse, asegúrese de que su Cloud Architect (CA) o Cloud Service Delivery Manager (CSDM) reciba la siguiente información:

Correo electrónico de alertas directas: estas son las direcciones de correo electrónico a las que desea que AMS envíe determinadas alertas basadas en los recursos. Para obtener más información sobre qué alertas se envían directamente al correo electrónico, consulte las alertas de la supervisión básica en AMS en la Guía de usuario avanzada de AMS. Para obtener más información sobre la supervisión de AMS, consulte la gestión de la supervisión en la Guía del usuario de AMS para zonas de destino con una sola cuenta.

Configuración de red

- Número ASN de Transit Gateway

  Este es el número de sistema autónomo (ASN) de la sesión de AWS de una sesión de Border Gateway Protocol (BGP), debe ser único y no puede ser el mismo que se utiliza para Direct Connect o VPN. El rango es de 64512 a 65534 (ambos incluidos) para 16 bits. ASNs
- Sus rangos de VPC CIDR de infraestructura de zonas de landing zone de múltiples cuentas de AMS.

  Estos rangos de CIDR no pueden superponerse con su red local

  Puede incluir un rango de CIDR de /22 o proporcionar cada CIDR de VPC de forma individual. Tenga en cuenta que solo se permiten estos rangos de CIDR:

  - 10.0.0.0 - 10.255.255.255 (prefijo 10/8)
  - 172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)
  - 192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)

  Tenga en cuenta que no se puede usar el rango de IP 198.18.0.0/15 (lo reserva AWS Directory Service).

  - Rango CIDR de VPC de infraestructura principal (se recomienda un rango /22)
  - Rango CIDR de VPC para redes (se recomienda un rango /24)
  - Rango CIDR de VPC de Shared Services (se recomienda rango /23)
  - Rango DMZ VPC CIDR (se recomienda rango /25)

- VPN ECMP (activar o desactivar)

  En VPN ECMP support (Soporte ECMP de VPN), elija enable (habilitar) si necesita soporte de direccionamiento mediante varias rutas de igual costo (ECMP) entre las conexiones de VPN. Si las conexiones anuncian lo mismo CIDRs, el tráfico se distribuye equitativamente entre ellas.

Lista de control de acceso a la red (NACL)

Una lista de control de acceso a la red (NACL) es una capa de seguridad opcional para su VPC que actúa como firewall para controlar el tráfico que entra y sale de una o más subredes. Puede configurar una red ACLs con reglas similares a las de sus grupos de seguridad para añadir una capa de seguridad adicional a su VPC. Para obtener más información sobre las diferencias entre los grupos de seguridad y la red ACLs, consulte Comparación de grupos de seguridad y redes ACLs.

Sin embargo, en la zona de aterrizaje multicuenta de AMS, para que AMS pueda gestionar y supervisar la infraestructura de forma eficaz, el uso de NACLs se limita al siguiente ámbito:

- NACLs no se admiten en las cuentas principales de varias cuentas de landing zone: administración, redes, servicios compartidos, registro y seguridad.
- NACLs se admiten en las cuentas de aplicaciones multicuenta de landing zone siempre que solo se utilicen como una lista de «Denegados». Además, deben tener configurada la opción «Permitir todo» para garantizar las operaciones de supervisión y gestión de AMS.

En entornos de múltiples cuentas a gran escala, también puedes aprovechar funciones como los firewalls de salida centralizados para controlar el tráfico saliente o las tablas de enrutamiento de AWS Transit Gateway en la landing zone multicuenta de AMS para segregar el tráfico de red entre ellas. VPCs

Configuración de Active Directory

FQDN de dominio para Active Directory administrado por AMS

Protección de endpoints de Trend Micro (EPS)

- Tamaños de instancia para sus EC2 instancias y grupos de Auto Scaling

  Trend Micro Endpoint Protection (EPS) es el componente principal de AMS para la seguridad de los sistemas operativos. El sistema está compuesto por instancias de Deep Security Manager

(DSM), EC2 instancias de retransmisión EC2 y un agente presente en todo el plano de datos de AMS y en sus EC2 instancias.

  - El tipo de instancia de retransmisión (el mínimo admitido por AMS es m5.large)
  - Tamaño de la instancia de base de datos (se recomiendan 200 GB)
  - Tipo de instancia RDS (solo se permiten db.m5.large o db.m5.xlarge)
- Tipo de licencia DSM (Marketplace o BYOL)

  Si ya tiene una licencia, elija BYOL (traiga su propia licencia). AMS se pondrá en contacto con usted para obtener la información necesaria sobre la licencia.
- AWS Nombre de recurso de Amazon (ARN) de usuario o rol de IAM para la suscripción a Trend Micro Deep Security (ARN del rol: arn:aws:iam: ::role/) *ACCOUNT_ID ROLE_NAME*

  Indíquenos un rol de IAM, un ARN o un ARN de usuario de IAM de uno de Cuentas de AWS sus actuales a los que tenga acceso. AMS crea un rol de IAM, en su cuenta de AMS, zona de aterrizaje multicuenta, Shared Services y añade el rol o usuario proporcionado en la confianza de un rol de IAM en Shared Services para que usted pueda asumir el rol al suscribirse a Trend Micro Deep Security en. AWS Marketplace

Acceso: Bastions, SSH y RDP

- Configuración de SSH Bastion

  AMS proporciona bastiones SSH en su cuenta de Shared Services para acceder a los hosts del entorno AMS. Para acceder a la red AMS como usuario de SSH, debe utilizar SSH Bastions como punto de entrada. La ruta de red se origina en la red local, pasa por la puerta de enlace de tránsito (TGW) y, DX/VPN a continuación, se enruta a la VPC de Shared Services. Una vez que pueda acceder al bastión, podrá ir a otros hosts de su entorno AMS, siempre que se haya concedido la solicitud de acceso adecuada.

  - Número de instancias deseado (se recomiendan 2)
  - Número máximo de instancias (se recomiendan 4)
  - Instancias mínimas (se recomiendan 2)
  - Tipo de instancia (se recomienda m5.large)
  - Entrada CIDRs: rangos de direcciones IP desde los que los usuarios de tu red accederán a SSH Bastions (rango de IP 1, rango de IP 2, rango de IP 3,... etc.)
- Configuración de RDP Bastion

AMS proporciona opcionalmente bastiones RDP en su cuenta de Shared Services para acceder a los hosts del entorno AMS. Para acceder a la red AMS como usuario de RDP, debe utilizar RDP Bastions como punto de entrada. La ruta de red se origina en la red local, pasa por el TGW y, DX/VPN a continuación, se enruta a la VPC de Shared Services. Una vez que pueda acceder al bastión, podrá pasar a otros hosts del entorno AMS, siempre que se haya concedido la solicitud de acceso adecuada.

  - Tipo de instancia (se recomienda t3.medium)
  - Sesiones mínimas deseadas (se recomiendan 2)
  - Número máximo de sesiones deseado (se recomiendan 10)
- Tipo de configuración RDP Bastion, estándar compartido o HA compartido (el valor predeterminado es estándar compartido)

  SecureStandard = Un usuario recibe un bastión y solo un usuario puede conectarse al bastión.

  SecureHA = Un usuario recibe dos bastiones en dos zonas de disponibilidad diferentes a los que conectarse y solo un usuario puede conectarse al bastión.

  SharedStandard = Un usuario recibe un bastión al que conectarse y dos usuarios pueden conectarse al mismo bastión a la vez.

  sharedHA = Un usuario recibe dos bastiones en dos zonas de disponibilidad diferentes para conectarse y dos usuarios pueden conectarse al mismo bastión a la vez.

Federación

Nombre del proveedor de identidad (IDP)

El valor predeterminado es `customer-saml`

Incorporación de AMS Single-Account Landing Zone (SALZ)

Proceso de incorporación de AMS SALZ

Para incorporar cuentas AMS single-account landing zone (SALZ), debes seguir los siguientes pasos:

1. Cree una nueva cuenta de AWS que AMS configure como cuenta de red para alojar el firewall. Cree la nueva cuenta en su organización de AWS, si tiene una. AMS seguirá el procedimiento de creación de una cuenta AMS normal, por lo que deberá recopilarse toda la información necesaria (por ejemplo, el CIDR, las licencias de EPS y los usuarios). Nota: Una asignación de CIDR de /24 es buena.
2. Especifique si desea o no eliminar las puertas de enlace de Internet (IGWs) de las cuentas de tráfico de salida.
3. Determine sus dominios aprobados. AMS permite filtrar los destinos manteniendo una lista de dominios aprobados; la lista se puede modificar más adelante.
4. Confirme el tamaño de la instancia que quiere usar en función del rendimiento esperado. De forma predeterminada, la instancia se crea en una instancia m4.xlarge en la que hemos comprobado que el rendimiento del firewall es de 350 Mbps. AMS puede aumentar el tamaño a una instancia C4.8xlarge en la que el rendimiento esperado es de 1,25 Gbps.
5. Configure las redes entre AMS y su red privada. Esto implica varias tareas:
    a. Asigne espacio IP
    b. Establezca una conectividad de red privada con AWS
    c. Configure su firewall
    d. Configure la administración de acceso
    e. Programe copias de seguridad
6. Proporcione acceso a la cuenta creada a AMS.
7. Valide que el servicio AMS funcione correctamente.

AMS podrá realizar la creación (incorporación) de su cuenta en un plazo de 2 semanas (10 días laborables) a partir de la fecha de solicitud inicial. Cualquier actividad de seguimiento se puede realizar mediante la gestión de eventos planificados (PEM) de AMS.

Note

- EE.UU. Este (Virginia)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- Este de EE. UU. (Ohio)
- Canadá (centro)
- América del Sur (São Paulo)
- UE (Irlanda)
- UE (Fráncfort)
- UE (Londres)
- EU West (París)
- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)

Se añaden nuevas regiones con frecuencia. Para ver la lista más actualizada, consulte las regiones y zonas de disponibilidad de AWS.

Arquitectura de red SALZ

El siguiente diagrama muestra el diseño de la red de VPC de la zona de aterrizaje (SALZ) de cuenta única de AWS Managed Services (AMS) y es un ejemplo de la configuración de alta disponibilidad.

AMS configura automáticamente todos los aspectos de la red en función de nuestras plantillas estándar y de las opciones que haya seleccionado durante la incorporación. Se aplica un diseño de red de AWS estándar a su cuenta de AWS y se crea una nube privada virtual (VPC) para usted que se conecta a AMS mediante VPN o Direct Connect. Obtenga más información sobre Direct

Connect en AWS Direct Connect. VPCsLos estándares incluyen la DMZ, los servicios compartidos y una subred de aplicaciones. Durante el proceso de incorporación, es VPCs posible que se soliciten y creen más en función de sus necesidades (por ejemplo, divisiones de clientes o socios). Tras la incorporación, recibirá un diagrama de red, un documento de entorno en el que se explica cómo se ha configurado la red.

> **Note**
>
> Para obtener más información sobre los límites y las restricciones de servicio predeterminados para todos los servicios activos, consulte la documentación sobre los límites de servicio de AWS.

El diseño de nuestra red se basa en el «Principio de Privilegio Mínimo» de Amazon. Para lograrlo, enrutamos todo el tráfico, entrante y saliente, a través de pasarelas, excepto el tráfico que proviene de una red confiable. La única red de confianza es la que se configura entre el entorno local y la VPC mediante el uso de una and/or VPN y AWS Direct Connect (DX). El acceso se concede mediante el uso de instancias bastión, lo que impide el acceso directo a cualquier recurso de producción. Todas sus aplicaciones y recursos residen en subredes privadas a las que se puede acceder mediante balanceadores de carga públicos. El tráfico de salida público fluye a través de nuestros proxies de reenvío al Internet Gateway y luego a Internet. Como alternativa, el tráfico puede fluir a través de su VPN o Direct Connect a su entorno local.

Servicios compartidos de zona de aterrizaje con una sola cuenta de AMS

Las subredes de servicios compartidos contienen AMS Directory Services, el host de administración que automatiza el aprovisionamiento y las tareas comunes, el servidor de administración del antivirus (TrendMicro) y los hosts bastiones internos:

- AMS Directory Services = controlador de dominio AD

  Crea un Active Directory en las cuentas de AMS, crea el dominio AMS y une las pilas gestionadas al dominio en el momento del lanzamiento.
- Hosts de administración = host de administración de AMS (automatiza el aprovisionamiento y las tareas comunes)

  Actúa como punto final de la API para modificar Directory Service e interactuar con los controladores Directory Service de dominio.

- Servicios de seguridad: servidor de administración de antivirus (TrendMicro) = EPS DSM + EPS Relay

  Utiliza el software Deep Security (DSM) de Trend Micro™, funciona según un modelo cliente-servidor y tiene una base de datos interna que incluye administradores, agentes y relés de Deep Security.

- Hosts bastiones internos = bastiones de clientes

  Servidores de propósito especial diseñados para ser el punto de acceso principal desde Internet y actuar como proxy para tus otras EC2 instancias de Amazon.

SALZ: Crea una nueva AWS cuenta para AMS

Los cinco pasos para crear una nueva AWS cuenta para AWS Managed Services (AMS) son:

1. Crea un Cuenta de AWS
2. Configure la facturación consolidada: vincule la nueva cuenta a la cuenta del pagador
3. Configure su Cuenta de AWS acceso a AMS
4. Proteja la nueva cuenta con autenticación multifactor (MFA) para el usuario raíz en AMS
5. Suscríbase a AWS Marketplace para EPS

Si tiene alguna duda, póngase en contacto con su gerente de prestación del servicio de atención al cliente (CSDM).

Crea un Cuenta de AWS

El programa AMS requiere el aprovisionamiento de una nueva cuenta de Amazon Web Services (AWS). Las instrucciones paso a paso están disponibles en el siguiente vídeo: ¿Cómo creo y activo una nueva cuenta de Amazon Web Services? Los pasos sencillos son los siguientes:

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión Consola de administración de AWScomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

> **Note**
>
> Si ya tiene una cuenta, puede ir a la página de AWS precios y hacer clic en Crear una cuenta gratuita. Asegúrese de suscribirse al EC2 Servicio, como mínimo. Al suscribirse a un servicio, podrá acceder a todos los servicios de AWS. Solo se le cobrará por los servicios que utilice. Si planea vincular su nueva cuenta a una cuenta de pagador a efectos de facturación unificada, no necesita introducir la información del método de pago cuando se le solicite. En

su lugar, cuando llegues a la pantalla para introducir la información de la tarjeta de crédito, simplemente navega hasta allí. Necesitarás la dirección de correo electrónico asociada a la cuenta del pagador para enviar una solicitud de billing/linked cuenta consolidada, que se detalla en la siguiente sección.

Important

Es fundamental que se asegure de que haya una dirección de correo electrónico y un número de teléfono asociados a la cuenta para poder recibir respuestas a posibles incidentes de seguridad. El número de teléfono y la dirección de correo electrónico de la cuenta no se pueden cambiar sin restablecer la contraseña de la cuenta, lo cual es una tarea importante para una cuenta raíz de AMS. Para garantizar que estos valores se mantengan estables, es fundamental seleccionar información de contacto que no esté asociada a personas físicas, ya que puede cambiar. Elige un alias de correo electrónico que pueda apuntar a un grupo. Siga esta misma práctica recomendada para seleccionar un número de teléfono: elija un número que pueda apuntar a un grupo o a un número que sea propiedad de la empresa y no de un individuo.

Configure la facturación consolidada: vincule la nueva cuenta a la cuenta del pagador

Si quieres que tu nueva Cuenta de AWS factura gestionada por AMS se incorpore al pago de una cuenta de AWS Organizations administración existente, tienes que configurar la facturación unificada y vincular las cuentas. Para obtener más información sobre cómo hacerlo, consulte

- Facturación unificada AWS Organizations y estrategia de facturación AWS multicuenta.
- Invitar a un hombre Cuenta de AWS a unirse a su organización

Note

Puede realizar estos pasos antes de transferir la cuenta a AMS. Tras la transferencia, los pasos para unirse a su organización (descritos anteriormente) se pueden realizar mediante el proceso de gestión de cambios. Consulte con su administrador de prestación de servicios en la nube (CSDM) o con su arquitecto de nube (CA) si necesita ayuda.

Para obtener información general sobre facturación, incluida la gestión de la facturación unificada, consulte Qué es AWS la facturación. Para AWS Organizations obtener información general sobre cómo las cuentas pueden funcionar juntas, consulta Qué es AWS Organizations. Para obtener una guía prescriptiva sobre las cuentas AWS Organizations de administración, consulte La cuenta de administración, el acceso de confianza y los administradores delegados

Configure su Cuenta de AWS acceso a AMS

Una vez completados los pasos anteriores, ha asegurado satisfactoriamente su nuevo coste Cuenta de AWS y se ha asegurado de que los costes asociados se facturen adecuadamente. El último paso del proceso consiste en permitir que AMS acceda a la nueva cuenta para la configuración inicial de la pila y para tramitar las solicitudes de cambio y aprovisionamiento en curso. Para obtener más información, consulte Delegar el acceso a todas AWS las cuentas mediante funciones de IAM. Los pasos básicos se describen en esta sección.

Activar el acceso al AWS sitio web

Para permitir que los usuarios de IAM accedan a la información y las herramientas de facturación de su cuenta, debe activar la funcionalidad.

Siga estos pasos:

1. Inicie sesión Consola de administración de AWS con las credenciales de su cuenta raíz (el correo electrónico y la contraseña que utilizó para crear la suya Cuenta de AWS). No inicie sesión con las credenciales de usuario de IAM.

   Se abre la página de Consola de administración de AWS inicio.
2. En la barra de navegación superior, abre el menú desplegable del nombre de tu cuenta y, a continuación, selecciona Mi cuenta.

   Se abre la página de inicio de facturación.
3. Desplázate hacia abajo hasta el área Acceso de los usuarios de IAM a la información de facturación y haz clic en Editar en la parte derecha. *`The area does not appear unless you are logged in with root credentials`*.

   Se abre un área de acceso de Activate IAM.
4. Seleccione la casilla de verificación y haga clic en Actualizar.

   Ahora puede utilizar las políticas de IAM para controlar a qué páginas puede acceder un usuario.

Para obtener más información sobre este proceso AWS, consulte Descripción general de la administración de los permisos de acceso.

Cree un rol de IAM con acceso al sitio web AWS

AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso de sus usuarios a AWS los recursos. La IAM se utiliza para controlar quién puede utilizar AWS los recursos (autenticación), qué recursos pueden utilizar y de qué forma (autorización).

1. Vaya a la consola de administración de IAM y haga clic en Funciones en el panel de navegación izquierdo.

   Se abre la página de administración de roles con información sobre los roles de IAM, la opción Crear rol y una lista de los roles existentes.

2. Haz clic en Crear rol.

   Se abre la página Crear rol y seleccionar el tipo de entidad de confianza. Haga clic en Otro Cuenta de AWS y se abrirá un área de configuración debajo.

   Introduzca el ID de cuenta de confianza de AMS que le proporcionó AMS. Deje las opciones Requerir ID externo y Requerir MFA sin seleccionar.

3. Haga clic en Next: Permissions (Siguiente: Permisos).

   Se abre la página Crear políticas de permisos para adjuntar roles con opciones para crear una nueva política, actualizar la página y buscar políticas existentes. Se proporciona una lista de las políticas existentes.

4. Seleccione la AdministratorAccesspolítica y, a continuación, haga clic en Siguiente: revisar.

   Se abre la página Crear revisión de roles.

5. Asigne al nuevo rol el nombre aws_managedservices_onboarding_role y escriba «AMS Onboarding Role» en la descripción del rol. Revise la configuración del nuevo rol y, si está satisfecho, haga clic en Crear rol.

Se abre la página de administración de roles con su nuevo rol en la lista.

Suscríbase a AWS Marketplace para EPS

Los cambios recientes en AMS Endpoint Security (EPS) requieren que se suscriba a TrendMicro Deep Security AWS Marketplace y acepte las condiciones del software.

TrendMicro ofrece dos modelos de licencia: Per Protected Instance Hour y Bring your own License (BYOL).

- BYOL:
  1. Utiliza su propia licencia que ha adquirido a través de canales externos.
  2. Debe proporcionar todas las claves de licencia a AMS para construir la infraestructura de EPS. Puede proporcionar un código de activación que otorgue licencias a todos los módulos o códigos de activación individuales que otorguen licencias a un determinado conjunto de módulos. AMS crea solo los archivos de licencia que se corresponden con los códigos de activación que usted proporciona. Dado que la activación de la licencia se produce durante la incorporación, en presencia de un ingeniero jefe de AMS y del CSDM, podrá compartir esa información en ese momento.
  3. Además, debe suscribirse a la suscripción AMI de BYOL TrendMicro Market Place. Consulte Trend Micro Deep Security (BYOL).
- Por hora de instancia protegida:
  1. En esta suscripción, no es necesario que tenga ninguna licencia de Trend previamente adquirida.
  2. Sin embargo, debes suscribirte a la suscripción a Marketplace.
  3. En este modelo no es necesario compartir la clave de licencia con AMS, ya que el uso de Trend se mide automáticamente, incluida la licencia de software y el uso de la EC2 infraestructura. Consulte Trend Micro Deep Security.

Para suscribirse a Trend Micro, siga estos pasos:

1. Inicie sesión en su Cuenta de AWS.
2. Vaya a la página del producto de Trend Micro Deep Security (BYOL o por hora de instancia protegida).
3. Haga clic en Continuar para suscribirse en el panel derecho.

4. Haz clic en Aceptar condiciones en la esquina superior derecha.

Habilite IDS e IPS en Trend Micro Deep Security

Puede solicitar que AMS habilite en su cuenta el Sistema de Detección de Intrusiones (IDS) y los Sistemas de Protección contra Intrusiones (IPS) de Trend Micro, funciones no predeterminadas.

Para ello, envíe una solicitud de actualización (Administración | Otros | Otros | Actualización) e incluya una lista de direcciones de correo electrónico para recibir las notificaciones de IDS e IPS. Estas direcciones se añaden a un tema de SNS de su cuenta, que AMS crea para usted.

> **Note**
>
> AMS no puede añadir ningún servicio de Trend Micro que pueda interferir con nuestra capacidad de prestar otros servicios de AMS.

Paso siguiente: Proteja la nueva cuenta con autenticación multifactor (MFA) para el usuario raíz en AMS

Suscríbase a AWS Marketplace para CentOS 7.6

AMS ahora ofrece la HVM CentOS 7 (x86_64), con actualizaciones, vendida por CentOS.org, como AMI de AMS. Para utilizar esta AMI, debe optar por la licencia GRATUITA de Cent OS y aceptar la licencia en todas sus cuentas de AMS.

Para suscribirse, vaya a AWS Marketplacey siga las instrucciones para suscribirse.

No incurrirá en cargos de software por el uso de este producto, pero seguirá siendo responsable de otros AWS cargos, incluido el uso. EC2 Si se trata de un producto con licencia propia, debe disponer de una licencia de software válida para poder utilizarlo.

Puede revisar la información de este software en CentOS 7 (x86_64), con Updates HVM.

Proteja la nueva cuenta con autenticación multifactor (MFA) para el usuario raíz en AMS

Esta sección se ha redactado porque contiene información confidencial relacionada con la seguridad de AMS. Esta información está disponible en la documentación de la consola AMS. Para acceder

a AWS Artifact, puede ponerse en contacto con su CSDM para obtener instrucciones o ir a Introducción a AWS Artifact.

SALZ: Configurar redes

Hay varios procesos que deben completarse para configurar las redes de AWS Managed Services (AMS):

1. Asignación de espacio IP para su entorno AMS
2. Establecer la conectividad de red privada con AWS
3. Configuración del firewall para permitir las operaciones de AMS

Asigne espacio IP para su entorno AMS

AMS se diseñó y probó utilizando un bloque CIDR de /16 como asignación de red recomendada. Es importante que la red de confianza conectada a AMS utilice un bloque CIDR que no se superponga con el bloque CIDR asignado a AMS. Estas direcciones son necesarias para configurar la nube privada virtual (VPC) y las subredes. Para obtener más información sobre AWS VPCs, consulte Amazon VPC Limits y Amazon VPC. FAQs

Si bien un bloque CIDR /16 puede parecer una gran cantidad de direcciones IP, una VPC, una vez creada, no se puede expandir. Por lo tanto, esta asignación garantiza que su VPC gestionada por AMS pueda funcionar durante un período considerable. Dentro del bloque CIDR, debe asignar rangos de direcciones IP para, al menos, dos subredes privadas y dos subredes públicas.

AWS acepta la conectividad con el entorno AMS mediante la funcionalidad nativa de la red privada virtual (VPN) de AWS. Por su parte, esto puede lograrse mediante AWS Direct Connect (DX), una VPN de hardware o una VPN de software. Por el lado de AMS, utilizamos la funcionalidad de puerta de enlace virtual de VPCs.

Componentes básicos del entorno

Opciones de conectividad Network-to-Amazon de VPC de usuario	
VPN de hardware	Establece una conexión VPN de hardware desde su equipo de red en una red remota a un equipo de red administrado por AMS conectado a su VPC.

Opciones de conectividad Network-to-Amazon de VPC de usuario	
AWS Direct Connect (DX)	Establece una conexión privada y lógica (o cifrada si se usa con una VPN) desde su red remota a la Amazon VPC, mediante AWS Direct Connect.
Software: VPN	Establece una conexión VPN desde su equipo en una red remota a un dispositivo VPN de software administrado por el usuario que se ejecuta dentro de una Amazon VPC.

> **Note**
>
> AMS recomienda conexiones redundantes de VPN privadas a DX. Su administrador de servicios de atención al cliente (CSDM) le ayudará a configurarlo cuando incorpore su cuenta.

Establezca una conectividad de red privada con AWS

Agregue AMS a su Active Directory corporativo para establecer la conectividad. Es posible que desee realizar acciones administrativas o acceder a los usuarios a través de una conexión de red privada. AWS ofrece conectividad VPN y líneas dedicadas a través de Direct Connect. En los siguientes pasos se explica cómo trabajar con AMS para establecer uno de los dos medios de conectividad (o ambos).

Configuración de VPN

En esta sección se describen los pasos básicos para configurar una VPN que se comunique entre la VPC gestionada por AMS y la red interna.

> **Note**
>
> Para obtener información general sobre el uso de una VPN con los servicios de AWS, consulte Qué es AWS Site-to-Site VPN y Todo sobre Your Customer Gateway (su dispositivo VPN).

Siga las secciones Introducción y Prueba de la conexión Site-to-Site VPN de la Guía del usuario de AWS VPN para completar los siguientes pasos.

- Paso 1: Cree una pasarela de clientes en su VPC de AWS
- Paso 2: Cree una puerta de enlace privada virtual en su VPC de AWS
- Paso 3: En su VPC de AWS, habilite la propagación de rutas en su tabla de rutas
- Paso 4: En su VPC de AWS, actualice su grupo de seguridad para habilitar el acceso entrante por SSH, RDP e ICMP
- Paso 5: En su red interna, cree una conexión VPN y configure la puerta de enlace del cliente
- Paso 6: Pruebe la conectividad VPN entre la VPC y su red interna

Direct Connect Configuración

En esta sección se describen los pasos básicos para configurar una Direct Connect (DX) para la comunicación entre la VPC administrada por AMS y la red interna.

> **Note**
>
> Para obtener información sobre el uso de una DX con los servicios de AWS, consulte Cómo empezar en una Direct Connect ubicación.

Para configurar una conexión DX, debe completar los siguientes pasos:

1. Inscríbase en Amazon Web Services
2. Enviar una solicitud de conexión de AWS Direct Connect
3. Completa el Cross Connect
4. (opcional) Configure las conexiones redundantes con AWS Direct Connect
5. Realizado por AMS: cree una interfaz virtual
6. Realizado por AMS: descarga la configuración del router
7. Verifique su interfaz virtual

Configura tu firewall

Esta sección se ha redactado porque contiene información confidencial relacionada con la seguridad de AMS. Esta información está disponible en la documentación de la consola AMS. Para acceder a AWS Artifact, puede ponerse en contacto con su CSDM para obtener instrucciones o ir a Introducción a AWS Artifact.

Opciones de AMS Bastion durante las migraciones o la incorporación de aplicaciones

Con el fin de proporcionarle la mejor experiencia durante los esfuerzos de migración, estas son las posibles opciones que AMS podría aprovechar actualmente:

- Opción 1: Evita los bastiones únicamente para realizar tareas de migración (debes aprobarla por motivos de seguridad y como medida temporal).

  Nota: Se seguirán utilizando las funciones de auditoría para garantizar que AMS pueda ver todas las solicitudes.
- Opción 2: crear túneles SSH con la herramienta que prefiera; por ejemplo, PuTTy, como se muestra en la ilustración.

  Los componentes del entorno descritos ya deberían estar implementados para esta opción.

  AMS proporcionaría notas e instrucciones adicionales.

Pasos de tunelización SSH con Pu: TTy

En PuTTY, crearía una sesión SSH con la IP pública del host del bastión, proporcionaría la clave PEM en la sección AUTH y, a continuación, crearía un túnel. El puerto de origen del túnel debería ser un puerto local no utilizado (por ejemplo, 5000) y la IP sería la IP del host de destino (la caja de Windows a la que intenta acceder) con el puerto RDP adjunto (3389). Asegúrese de guardar la configuración, ya que no querrá tener que hacerlo cada vez que inicie sesión en la casilla. Conéctese al host del bastión e inicie sesión. A continuación, inicie una sesión RDP para localhost:5000 (o el puerto que elija).

1. Establezca el nombre de host o la IP pública del host bastión

2. En SSH ->Auth, configure el archivo de clave privada en formato.ppk

3. En SSH ->Tunnels, agrega el nuevo puerto reenviado. El puerto de origen debe ser el puerto arbitrario no utilizado y el de destino debe ser la IP del servidor de destino situado detrás del host bastión, con el puerto RDP adjunto.

4. Conéctate al host del bastión mediante PuTTY e inicia sesión.

5. Inicie una sesión RDP en localhost:5000 para llegar al servidor de destino.

SALZ: configurar la gestión de acceso

El uso de una red gestionada por AWS Managed Services (AMS) significa conceder a AMS acceso para gestionar su infraestructura de nube. Deberá configurar un medio de conexión segura entre su red privada y AMS. Para empezar, debes tomar algunas decisiones sobre los tipos de acceso que deseas proporcionar:

- Para el acceso a AMS API/CLI y a la consola: querrá instalar la CLI de AMS (las instrucciones se proporcionan en este documento). Utiliza la API de gestión de cambios de AMS para realizar solicitudes de cambio en AMS y la API SKMS de AMS para obtener información sobre los recursos gestionados por AMS. Con los Servicios de federación de Active Directory (AD FS), puede acceder a la consola AMS.

  > **Note**
  >
  > Si va a configurar su propio ITSM, necesitará usar la API de AWS Support (SAPI) para las solicitudes de servicio y los informes de incidentes. La SAPI está documentada en la AWS Support API Reference.

- Para el acceso de los usuarios: ya sea que administre los usuarios con Windows Active Directory (AD) o con una Linux/LDAP solución, debe establecerse la conectividad entre AD por parte de AMS (a través de los servicios de directorio) y su directorio.
- Por ejemplo, el acceso: el acceso a nivel de instancia se logra mediante una configuración unidireccional de Forest Trust. Los servicios de directorio confían en las credenciales de su CORP AD, lo que permite iniciar sesión con las credenciales de CORP dentro del lado AMS.

Tenga en cuenta que el Active Directory (AD) en el que AMS ha configurado la confianza debe ser el directorio que contenga las cuentas de los usuarios autorizados por usted para acceder a sus recursos de AWS.

> **Important**
>
> Para configurar un fideicomiso en Forest, AMS requiere que el controlador de dominio disponga de políticas locales -> Opciones de seguridad -> Acceso a la red: canalizaciones denominadas a las que se puede acceder de forma anónima. Incluya las canalizaciones Netlogon y lsarpc en la lista. Estas tuberías aparecen en la lista de forma predeterminada, pero a veces se eliminan por motivos de seguridad. Una vez establecida la confianza, se pueden volver a eliminar de la lista.

Establecer una confianza en Active Directory (AD)

Antes de empezar a establecer una confianza de Active Directory (AD) para su cuenta de AWS Managed Services (AMS), asegúrese de que estén abiertos los puertos de firewall correspondientes.

La confianza del Active Directory administrado por AMS y de su servicio de directorio corporativo le permite usar sus credenciales administradas por la empresa para acceder a las instancias administradas por AMS con el fin de realizar funciones de desarrollo, pruebas o administrativas.

La creación de una conexión de confianza consta de dos partes:

En primer lugar, configure un reenvío condicional, una configuración de DNS para que las consultas de DNS sepan a qué servidor DNS deben ir.

En segundo lugar, configure una confianza, una estructura de Active Directory (AD) para permitir el acceso de los usuarios de un dominio para utilizar los recursos de otro dominio.

Configurar el reenviador condicional

Siga este artículo de Microsoft AD Asigne un reenviador condicional para un nombre de dominio y utilice estas opciones y configuraciones:

1. En el Administrador de DNS de AD -> Crear un nuevo reenviador condicional, en Dominio DNS: utilice el nombre de dominio que AMS le proporcionó; por ejemplo,. *A523434123.amazonaws.com*

2. En las direcciones IP de los servidores maestros: añada las direcciones IP proporcionadas por el AMS. Asegúrese de que no haya ningún problema de conexión validando ambas direcciones.
3. Seleccione Guardar este reenviador condicional en Active Directory y replique de la siguiente manera: Todos los servidores DNS de este dominio y pulse Aceptar.

Configurar la confianza

Para configurar la confianza de su cuenta de AWS Managed Services (AMS), consulte este artículo de MicroSoft AD sobre cómo crear una confianza forestal entrante unidireccional para una parte de la confianza mediante los ajustes y las opciones que se describen en esta sección.

1. Abra el cuadro de diálogo Inicio -> Herramientas administrativas -> Dominios y confianzas de Active Directory. Haga clic con el botón derecho en el nodo del dominio con el que desee establecer una confianza y, a continuación, haga clic en Propiedades -> Confianzas -> Nueva confianza para abrir el asistente de nueva confianza. Introduzca el nombre de dominio que le proporcionó AMS para el nombre de confianza y pulse Siguiente.
2. En Tipo de confianza, seleccione Forest Trust. Pulse Siguiente.
3. En Dirección de confianza, selecciona Unidireccional: entrante. Pulse Siguiente.
4. En Sides of Trust, selecciona Solo este dominio. Pulse Siguiente.
5. En Contraseña de confianza, escribe la contraseña que desees. Pulse Siguiente.
6. Para completar las selecciones de confianza y completar la creación de confianza, pulse Siguiente.
7. En Confirmar confianza entrante, seleccione No, no confirme la confianza entrante. Pulse Siguiente.
8. En Completado el asistente de nueva confianza, selecciona Finalizar y, a continuación, Aceptar para cerrar.
9. Proporcione la contraseña de confianza (póngase en contacto con nosotros a través del número de teléfono de su CSDM por motivos de seguridad). AMS completará la configuración de confianza.

Sitios y servicios de Active Directory

Para reducir la latencia de inicio de sesión, añada el rango CIDR de VPC a sus sitios y servicios de Active Directory (Inicio -> Herramientas administrativas -> Sitios y servicios de Active Directory).

Agregue el rango CIDR de VPC a un sitio de Active Directory que contenga los controladores de dominio más cercanos a AWS.

Enrutamiento de sufijos de nombres de Active Directory

Una vez que se haya establecido el fideicomiso forestal unidireccional, complete los pasos adicionales.

1. En Inicio > Todos los programas > Herramientas administrativas, haga clic en Dominios y confianzas de Active Directory.

   Se abre la consola de dominios y confianzas de Active Directory.
2. Haga clic con el botón derecho en el dominio corporativo y haga clic en Propiedades

   Se abre el cuadro de diálogo de propiedades de ese dominio.
3. Haga clic en la pestaña Confianzas.

   Se abre la página de fideicomisos.
4. Haz clic en el nombre de dominio de Amazon y, a continuación, en Propiedades.

   Se abre la página de propiedades de la confianza de dominios de Amazon.
5. Haga clic en Name Suffix Routing y, a continuación, en Actualizar.

   Estos pasos garantizan que los nombres principales del servicio (SPNs) puedan resolverse a través de la confianza.

Solución de problemas

Algunas cosas que puede probar si tiene problemas:

- El grupo de seguridad saliente de Active Directory administrado por AMS debe poder conectarse a través del bloque CIDR (por ejemplo, 10.27.0.0/16) al controlador de dominio.
- Rastree la ruta en la consola de AWS de un controlador de dominio a otro comprobando todos los grupos de seguridad a lo largo del camino.
- Asegúrese de poder hacer ping a los controladores de dominio de Active Directory administrados por AMS si está permitido el Protocolo de mensajes de control de Internet (ICMP).
- Asegúrese de que su controlador de dominio pueda comunicarse con AWS Directory Services.
- Asegúrese de que los reenviadores condicionales se resuelvan y estén validados.

- Si no ve Forest Trust en el asistente New Trust, es posible que sus reenviadores condicionales no funcionen correctamente:
  - Utilice nslookup para probar la resolución
  - Intente reiniciar el controlador de dominio

Active Directory gestionado por AMS

AMS ofrece ahora un nuevo servicio denominado Active Directory administrado (también conocido como Managed AD) que permite a AMS ocuparse de las operaciones de la infraestructura de Active Directory (AD) y, al mismo tiempo, mantener el control de la administración de Active Directory.

La compatibilidad de AMS con Managed AD es similar a la compatibilidad de AMS con Amazon Relational Database Service (Amazon RDS). En ambos casos AWS (incluido AMS), permite crear y gestionar la infraestructura en la que se ejecuta el servicio, además de realizar el control de acceso y todas las funciones de administración. Este modelo presenta las siguientes ventajas:

- Limita los riesgos de seguridad: AWS además, AMS no necesita privilegios administrativos en tu dominio.
- Integraciones directas: puedes usar tu modelo de autorización actual e integrarlo con AD sin necesidad de interactuar con AMS.

Notas:

- Ni AMS ni usted tendrán acceso a sus controladores de dominio de AD gestionados, por lo que no se podrá instalar ningún software en los controladores de dominio. Esto es importante porque no se permiten soluciones de terceros que requieran la instalación de software en los controladores de dominio.

  El acceso funciona así:

  - AWS Equipo de Directory Service: tiene acceso a los controladores de dominio.
  - AMS: tiene acceso a Directory Service APIs para realizar determinadas acciones en el dominio. Estas acciones incluyen tomar instantáneas de AD, cambiar el esquema de AD y otras acciones.
  - Tú: tienes acceso al dominio (AD) para crear usuarios, grupos, etc.
- Te recomendamos que realices una prueba de concepto del AD gestionado antes de migrar tu AD corporativo, ya que no todas las funciones de un entorno de AD tradicional están disponibles en un entorno de AD gestionado.

- AMS no gestionará ni proporcionará orientación sobre la gestión de su AD. Por ejemplo, AMS no proporcionará orientación sobre la estructura de las unidades organizativas, la estructura de las políticas de grupo, las convenciones de nomenclatura de los usuarios de AD, etc.

Funciona así:

1. AMS incorpora una nueva cuenta Cuenta de AWS para usted, independiente de su cuenta de AMS y además de ella, y aprovisiona un entorno de Active Directory (AD) a través de AWS Directory Service (consulte también ¿Qué es AWS Directory Service?).

   La siguiente es la información que un integrador de sistemas tendría que recopilar sobre usted para que AMS incorpore Managed AD:

   - Información de la cuenta
     - ID de cuenta Cuenta de AWS que se creó para su AD gestionado por AMS: número Cuenta de AWS
     - Región en la que incorporar su AD gestionado: Región de AWS
   - Información de Active Directory administrado:
     - Edición Microsoft AD: estándar/empresarial. AWS Microsoft AD (edición estándar) incluye 1 GB de almacenamiento de objetos de directorio. Esta capacidad puede admitir hasta 5000 usuarios o 30 000 objetos de directorio, incluidos usuarios, grupos y ordenadores. AWS Microsoft AD (Enterprise Edition) incluye 17 GB de almacenamiento de objetos de directorio, que puede admitir hasta 100 000 usuarios o 500 000 objetos.

       Para obtener más información, consulte AWS Directory Service FAQs.
     - FQDN de dominio: el FQDN de su dominio de AD gestionado por AMS.
     - Nombre NetBIOS del dominio: el nombre NetBIOS de su dominio de AD gestionado por AMS.
     - Números de cuenta de las cuentas estándar de AMS con las que desea integrar el AD gestionado (AMS configura una confianza unidireccional entre el AD de la cuenta estándar de AMS y el AD gestionado)
     - ¿Es necesario modificar el esquema de Active Directory y, de ser así, qué modificaciones?
     - De forma predeterminada, se aprovisionan dos controladores de dominio. ¿Necesita más? Si es así, ¿cuántos necesita y por qué motivo?
   - Información sobre redes para Active Directory administrado:
     - CIDR de VPC de AD administrado para controladores de dominio (un CIDR en su rango de subredes privadas para los controladores de dominio de AD administrados):

- Subred CIDR 1 para controladores de dominio: [su CIDR debe formar parte del CIDR de VPC AD gestionado por AMS]
- Subred CIDR 2 para controladores de dominio: [su CIDR debe formar parte del CIDR de VPC AD gestionado por AMS]

Por ejemplo:

- CIDR de VPC AD gestionado: 192.168.0.0/16
- CIDR 1 para controladores de dominio: 192.168.1.0/24
- CIDR 2 para controladores de dominio: 192.168.2.0/24

Para evitar conflictos de direcciones IP, asegúrese de que el CIDR de VPC de AD administrado que especifique no entre en conflicto con ningún otro CIDR de subred privada que utilice en la red corporativa.

- Tecnología VPN (opcional): [Direct Connect/Direct Connect y VPN]
  - Número de sistema autónomo (ASN) BGP de su puerta de enlace: [ASN proporcionado por el cliente]
  - La dirección IP enrutable por Internet de la interfaz exterior de la puerta de enlace, debe ser estática: [Dirección IP proporcionada por el cliente]
  - Si su conexión VPN requiere o no rutas estáticas: [sí/no]

2. AMS le proporciona la contraseña de la cuenta de administrador para el entorno de AD y le pide que restablezca la contraseña para que los ingenieros de AMS ya no puedan acceder a su entorno de AD.
3. Para restablecer la contraseña de la cuenta de administrador, conéctese a su entorno de Active Directory mediante Active Directory Users and Computers (ADUC). El ADUC y otras herramientas de administración remota de servidores (RSAT) deben instalarse y ejecutarse en los hosts administrativos que usted haya aprovisionado en una infraestructura que no sea de AMS. Microsoft tiene las mejores prácticas para proteger dichos hosts administrativos. Para obtener más información, consulte Implementación de hosts administrativos seguros. El entorno de Active Directory se administra mediante estos hosts administrativos.
4. En las operaciones diarias, AMS gestiona todo lo Cuenta de AWS relacionado con el AWS Directory Service; por ejemplo, la configuración de la VPC, las copias de seguridad de AD, la creación y eliminación de la confianza de AD, etc. Usted usa y administra su entorno de AD; por ejemplo, la creación de usuarios, la creación de grupos, la creación de políticas de grupo, etc.

Para ver la tabla RACI más reciente, consulte la sección «Funciones y responsabilidades» de la descripción del servicio See.

Federe su Active Directory con las funciones de AMS AWS Identity and Access Management

El objetivo de federar su directorio con las funciones de IAM de AMS es permitir a los usuarios corporativos utilizar sus credenciales corporativas para interactuar con la consola AMS Consola de administración de AWS y, por lo tanto AWS APIs, con ella. APIs

Ejemplo de proceso de federación

En este ejemplo se utilizan los Servicios de federación de Active Directory (AD FS); sin embargo, se admite cualquier tecnología que admita AWS Identity and Access Management la federación. Para obtener más información sobre la federación de IAM AWS compatible, consulte Socios de IAM y proveedores de identidad y federación. Su CSDM le ayudará en este proceso, que implica un esfuerzo conjunto con su equipo de AD y AMS.

Para obtener información detallada sobre la integración de SAML para el acceso a las API, consulte este AWS blog, Cómo implementar el acceso federado a las API y CLI mediante SAML 2.0 y AD FS.

> **Note**
>
> Para ver un ejemplo que instala la CLI de AMS y el SAML, consulte. Apéndice: Regla de notificación de ActiveDirectory Federation Services (ADFS) y configuración de SAML

Configuración de la federación en la consola AMS (SALZ)

Las funciones de IAM y el proveedor de identidad de SAML (entidad de confianza) que se detallan en la siguiente tabla se han proporcionado como parte de la incorporación de su cuenta. Estas funciones te permiten enviar y supervisar RFCs solicitudes de servicio e informes de incidentes, así como obtener información sobre tus cuentas. VPCs

Rol	Proveedor de identidades	Permisos
Cliente_ _Role ReadOnly	SAML	Para cuentas AMS estándar. Permite enviar solicitudes de servicio e RFCs incidentes para realizar cambios en la infraestructura gestionada por AMS, así como crear solicitudes de servicio e incidentes.
customer_managed_ad_user_role	SAML	Para cuentas de Active Directory administradas por AMS. Permite iniciar sesión en la consola AMS para crear solicitudes de servicio e incidentes (no RFCs).

Para ver la lista completa de las funciones disponibles en las diferentes cuentas, consulteFunción de usuario de IAM en AMS.

Un miembro del equipo de incorporación carga el archivo de metadatos de su solución de federación al proveedor de identidades preconfigurado. Utiliza un proveedor de identidades de SAML cuando quiere establecer confianza entre un IdP (proveedor de identidades) compatible con SAML, como Shibboleth o Active Directory Federation Services, de modo que los usuarios de su organización puedan acceder a los recursos de AWS. Los proveedores de identidad SAML en IAM se utilizan como principales en una política de confianza de IAM con las funciones anteriores.

Mientras que otras soluciones de federación proporcionan instrucciones de integración para AWS, AMS tiene instrucciones independientes. En la siguiente entrada del blog, Enabling Federation to AWS Using Windows Active Directory, AD FS y SAML 2.0, junto con las modificaciones que se indican a continuación, permitirán a los usuarios corporativos acceder a varias cuentas de AWS desde un único navegador.

Tras crear el fideicomiso de la parte de confianza según se indica en la entrada del blog, configure las reglas de reclamaciones de la siguiente manera:

- NameId: Sigue la entrada del blog.

- RoleSessionName: Utilice los siguientes valores:
  - Nombre de la regla de reclamación: RoleSessionName
  - Almacén de atributos: Active Directory
  - Atributo de LDAP: SAM-Account-Name
  - Tipo de reclamación saliente: atributos/ https://aws.amazon.com/SAML/ RoleSessionName
- Obtenga grupos de anuncios: siga la publicación del blog.
- Reclamación de rol: sigue la entrada del blog, pero para la regla personalizada, usa lo siguiente:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
 => issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-",
 "arn:aws:iam::$1:saml-provider/customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Al usar AD FS, debe crear grupos de seguridad de Active Directory para cada rol en el formato que se muestra en la siguiente tabla (customer_managed_ad_user_role es solo para las cuentas AD administradas por AMS):

Grupo	Rol
AWS- [AccountNo] ReadOnly -Cliente_ _Rol	Cliente_ _Rol ReadOnly
AWS- [AccountNo] -customer_managed_ ad_user_role	custome_managed_ad_user_role

Para obtener más información, consulte Configuración de las aserciones de SAML para la respuesta de autenticación.

> **Tip**
>
> Para ayudarte a solucionar problemas, descarga el complemento SAML Tracer para tu navegador.

Envío de la solicitud de federación a AMS

Si es su primera cuenta, trabaje con sus arquitectos de and/or nube de CSDM para proporcionar el archivo XML de metadatos a su proveedor de identidad.

Si va a incorporar una cuenta o un proveedor de identidad adicional y tiene acceso a la cuenta de administración o a la cuenta de aplicación que desee, siga estos pasos.

1. Cree una solicitud de servicio desde la consola AMS y proporcione los detalles necesarios para añadir el proveedor de identidad:
   - AccountId de la cuenta en la que se creará el nuevo proveedor de identidad.
   - Si no se proporciona el nombre del proveedor de identidad deseado, el predeterminado será customer-saml; normalmente, debe coincidir con los ajustes configurados en el proveedor de la federación.
   - En el caso de las cuentas existentes, indica si el nuevo proveedor de identidades debe propagarse a todas las funciones de consola existentes o proporciona una lista de funciones que deben confiar en el nuevo proveedor de identidades.
   - Adjunta el archivo XML de metadatos exportado por tu agente de federación a la solicitud de servicio como archivo adjunto.
2. Desde la misma cuenta en la que creó la solicitud de servicio, cree una nueva RFC con el CT-ID ct-1e1xtak34nx76 (Administración | Otros | Otros | Crear) con la siguiente información.
   - <Name>Título: «IDP SAML integrado para la cuenta < >». AccountId
   - AccountId de la cuenta en la que se creará el proveedor de identidad.
   - Nombre del proveedor de identidad.
   - Para las cuentas existentes: si el proveedor de identidades debe propagarse a todas las funciones de consola existentes o a la lista de funciones que deben confiar en el nuevo proveedor de identidades.
   - Identificador de caso de la solicitud de servicio creada en el paso 1, donde se adjunta el archivo XML de metadatos.

Verificar el acceso a la consola

Una vez que haya configurado ADFS y disponga de la URL de AMS para utilizarla en la autenticación, siga estos pasos.

Con una configuración del Servicio federado de Active Directory (ADFS), puede seguir estos pasos:

1. Abra una ventana del navegador y vaya a la página de inicio de sesión proporcionada para su cuenta. Se abre la IdpInitiatedSignOnpágina ADFS de su cuenta.
2. Selecciona el botón de radio situado junto a Iniciar sesión en uno de los siguientes sitios. Se activa la lista de selección de sitios para iniciar sesión.
3. Selecciona el sitio signin.aws.amazon.com y haz clic en Iniciar sesión. Se abren las opciones para introducir sus credenciales.
4. Introduzca sus credenciales de CORP y haga clic en Iniciar sesión. Se Consola de administración de AWS abre.
5. Pegue en la barra de direcciones la URL de la consola AMS y pulse Entrar. Se abre la consola AMS.

Verificar el acceso a la API

AMS usa la API de AWS, con algunas operaciones específicas de AMS sobre las que puede leer en la referencia de la API de AMS.

AWS proporciona varios a los SDKs que puede acceder en Tools for Amazon Web Services. Si no desea utilizar un SDK, puede realizar llamadas directas a la API. Para obtener información sobre la autenticación, consulte Firmar solicitudes de API de AWS. Si no utiliza un SDK o no realiza solicitudes directas a la API HTTP, puede utilizar el AMS CLIs para la gestión de cambios (CM) y el SKMS.

Instale el AMS CLIs

Para ver un ejemplo de cómo instalar la CLI de AWS Managed Services (AMS) para usarla con SAML, consulteApéndice: Regla de notificación de ActiveDirectory Federation Services (ADFS) y configuración de SAML.

Si necesita acceso temporal, para obtener e instalar AWS Managed Services (AMS) SDKs, consulte Acceso temporal a la consola AMS.

> **Note**
>
> Debe tener credenciales de administrador para este procedimiento.

La AWS CLI es un requisito previo para utilizar AWS Managed Services (AMS) CLIs (Change Management y SKMS).

1. Para instalar la CLI de AWS, consulte Instalación de la interfaz de línea de comandos de AWS y siga las instrucciones correspondientes. Tenga en cuenta que al final de esa página hay instrucciones para usar diferentes instaladores: Linux, MS Windows, macOS, Virtual Environment, Bundled Installer (Linux, macOS o Unix).

   Tras la instalación, ejecute `aws help` para verificar la instalación.

2. Una vez instalada la CLI de AWS, para instalar o actualizar la CLI de AMS, descargue el archivo zip distribuible de la CLI de AMS o del SDK de AMS y descomprímalo. Puede acceder a los distribuibles de la CLI de AMS a través del enlace Recursos para desarrolladores en la barra de navegación izquierda de la consola AMS.

3. El archivo README proporciona instrucciones para cualquier instalación.

   Abra una de las siguientes opciones:

   - CLI zip: proporciona únicamente la CLI de AMS.
   - SDK zip: proporciona todo el AMS APIs y la AMS CLI.

   Para Windows, ejecute el instalador adecuado (solo sistemas de 32 o 64 bits):

   - 32 bits: ManagedCloudAPI_x86.msi
   - 64 bits: ManagedCloudAPI_x64.msi

   Para Mac/Linux, ejecute el archivo denominado: AWSManagedServices_InstallCLI.sh ejecutando este comando:. `sh AWSManagedServices_InstallCLI.sh` Tenga en cuenta que los directorios amscm y amsskms y su contenido deben estar en el mismo directorio que el archivo.sh. AWSManagedServices_InstallCLI

4. Si sus credenciales corporativas se utilizan mediante la federación con AWS (la configuración predeterminada de AMS), debe instalar una herramienta de administración de credenciales que pueda acceder a su servicio de federación. Por ejemplo, puede utilizar este blog de seguridad de AWS sobre cómo implementar el acceso federado a las API y CLI mediante SAML 2.0 y AD FS como ayuda para configurar sus herramientas de administración de credenciales.

5. Tras la instalación, ejecute `aws amscm help` y consulte los comandos y `aws amsskms help` las opciones.

> **Note**
>
> La CLI de AMS debe estar instalada para que estos comandos funcionen. Para instalar la API o CLI de AMS, vaya a la página de recursos para desarrolladores de la consola AMS. Para obtener material de referencia sobre la API AMS CM o la API AMS SKMS, consulte la sección Recursos de información de AMS en la Guía del usuario. Puede que necesite añadir una `--profile` opción de autenticación; por ejemplo,`aws amsskms` *`ams-cli-command`* `--profile SAML`. Es posible que también tengas que añadir la `--region` opción, ya que todos los comandos de AMS se ejecutan desde us-east-1, por ejemplo. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

Programación de copias de seguridad de AMS a nivel de VPC

La programación de copias de seguridad de AWS Managed Services (AMS) en la VPC, donde se asignan las instancias de destino, se crea durante la incorporación de la cuenta con una etiqueta predeterminada en el esquema de creación de la VPC. El sistema de respaldo programa la ejecución de las instantáneas en función de esa etiqueta de VPC. La modificación de la programación se puede realizar mediante la creación de una solicitud de servicio. Para obtener más información, consulte Etiqueta y valores predeterminados de VPC.

Para ver los valores predeterminados de las copias de seguridad, consulte Descripción de los valores predeterminados de AMS

SALZ: configuración predeterminada

Su red de AWS Managed Services (AMS) está configurada de forma estandarizada con valores predeterminados para la mayoría de los servicios.

En esta sección se describen los ajustes predeterminados que AMS utiliza para la administración de la seguridad, el acceso, la supervisión, el registro, la continuidad y la aplicación de parches.

Para ver un ejemplo de los costes de infraestructura, consulte Componentes básicos.

Las reglas de firewall se proporcionan en Configura tu firewall

Seguridad de terminales (EPS)

Los recursos que aprovisione en su entorno AMS Advanced incluyen automáticamente la instalación de un cliente de supervisión de Endpoint Security (EPS). Este proceso garantiza que los recursos gestionados por AMS Advanced se supervisen y admitan las 24 horas del día, los 7 días de la semana. Además, AMS Advanced supervisa toda la actividad de los agentes y, si se detecta algún incidente de seguridad, se crea un incidente.

> **Note**
>
> Los incidentes de seguridad se tratan como incidentes; para obtener más información, consulte Respuesta a los incidentes.

Endpoint Security proporciona protección antimalware. En concreto, admite las siguientes acciones:

- EC2 las instancias se registran con EPS
- EC2 las instancias se dan de baja del EPS
- EC2 instancias de protección antimalware en tiempo real
- Latidos cardíacos iniciados por un agente EPS
- EPS restaura el archivo en cuarentena
- Notificación de eventos EPS
- Informes de EPS

AMS Advanced utiliza Trend Micro para la seguridad de terminales (EPS). Estos son los ajustes de EPS predeterminados. Para obtener más información sobre Trend Micro, consulte el Centro de ayuda de Trend Micro Deep Security; tenga en cuenta que los enlaces que no son de Amazon pueden cambiar sin previo aviso.

La configuración predeterminada de la zona de aterrizaje multicuenta avanzada (MALZ) de AMS se describe en las siguientes secciones; para ver la configuración de EPS de la zona de aterrizaje multicuenta de AMS no predeterminada, consulte la configuración no predeterminada de la EPS de la zona de aterrizaje multicuenta de AMS Advanced.

> **Note**
>
> Puedes traer tu propio EPS, consulta AMS trae tu propio EPS.

Configuración general del EPS

Configuración general de red de Endpoint Security.

Valores predeterminados de EPS

Opción	Valor predeterminado
Puertos de firewall (grupo de seguridad de las instancias)	Los agentes de EPS Deep Security Manager (DSMs) deben tener el puerto 4120 abierto Agent/Relay para la comunicación con el administrador y el puerto 4119 para la consola Manager. Los relés EPS deben tener el puerto 4122 abierto para poder comunicarse con el Manager/Agent relé. No debe haber ningún puerto específico abierto para la comunicación entrante de la instancia del cliente, ya que los agentes inician todas las solicitudes.
Dirección de comunicación	Agente o dispositivo iniciado
Intervalo de latidos	Diez minutos
Número de latidos cardíacos perdidos antes de una alerta	Dos
Variación (diferencia) máxima permitida entre los horarios de los servidores	Sin límite
Genera errores de desconexión en las máquinas virtuales inactivas (registradas, pero no conectadas)	No
Política predeterminada	Política base (que se describe a continuación)

Opción	Valor predeterminado
Activación de varios ordenadores con el mismo nombre de host	Está permitida
Se generan alertas de actualizaciones pendientes	Después de siete días
Calendario de actualizaciones	AMS prevé un ciclo de publicación mensual para las actualizaciones de software de Trend Micro Deep Security Manager (DSM) y Deep Security Agent (DSA). Sin embargo, AMS no mantiene un SLA para las actualizaciones. Los equipos de desarrolladores de AMS realizan las actualizaciones en toda la flota durante una implementación. Las actualizaciones de DSA/DSA se registran en los eventos del sistema DSM de Trend Micro que AMS conserva localmente de forma predeterminada durante 13 semanas. Para ver la documentación del proveedor, consulte los eventos del sistema en el Centro de ayuda de Trend Micro Deep Security. Los registros también se exportan al grupo de registros/aws/ams/eps/var/log/DSM.log en Amazon CloudWatch.
Fuente de actualización	Servidor de actualizaciones de Trend Micro (https://ipv6-iaus.trendmicro.com/iau_server.dll/)
Eliminación de datos de eventos o registros	Los eventos y los registros se eliminan de la base de datos de DSM después de siete días.
Se conservan las versiones del software del agente	Hasta cinco

Opción	Valor predeterminado
Se mantienen las actualizaciones de reglas más recientes	Hasta diez
Almacenamiento de registros	De forma predeterminada, los archivos de registro se almacenan de forma segura en Amazon S3, pero también puede archivarlos en Amazon Glacier para cumplir con los requisitos de auditoría y conformidad.

Política básica

Configuración predeterminada de la política básica de seguridad de terminales.

Política base de EPS

Opción	Valor predeterminado
Módulos habilitados	Antimalware
Módulos deshabilitados	Reputación web
	Firewall
	Protección contra intrusiones
	Supervisión de integridad
	Inspección de registros
	Control de aplicaciones

Antimalware

Configuración antimalware de Endpoint Security.

Valores predeterminados de antimalware de EPS

Opción	Valor predeterminado	Notas
Escaneo en tiempo real	Escanea todo Todos los Day/All días (24 horas)	Ponga en cuarenten a todos los virus sospechosos. IntelliTr ap Activación y spyware/grayware protección. El spyware y el grayware activan el antimalware y provocan que el artículo quede en cuarentena.
Escaneo manual	Escanea todo	Debe solicitarse y, a continuación, sigue la configuración de escaneo en tiempo real predeterminada.
Escaneo programado	Escanea todo	Programado para el último domingo de cada mes, a las 6 de la mañana.
Protección inteligente	Deshabilitado	N/A
Archivos en cuarentena	Administrador de seguridad profunda (DSM) de Trend Micro	Aproximadamente 1 GB de disco reservado para la cuarentena.
Limitación de escaneo	Trend Micro DSM	Escanee archivos de todos los tamaños.

Opción	Valor predeterminado	Notas
Se permite el spyware o el grayware	Ninguno	N/A
Notificación de eventos locales	Sí	N/A

Grupos de seguridad

En AWS VPCs, los grupos de seguridad de AWS actúan como firewalls virtuales y controlan el tráfico de una o más pilas (una instancia o un conjunto de instancias). Cuando se lanza una pila, se asocia a uno o más grupos de seguridad, que determinan qué tráfico puede llegar a ella:

- En el caso de las pilas de las subredes públicas, los grupos de seguridad predeterminados aceptan el tráfico de HTTP (80) y HTTPS (443) procedente de todas las ubicaciones (Internet). Las pilas también aceptan tráfico SSH y RDP interno de su red corporativa y de los bastiones de AWS. Luego, esas pilas pueden salir a Internet a través de cualquier puerto. También pueden salir a las subredes privadas y a otras pilas de la subred pública.
- Las pilas de tus subredes privadas pueden salir a cualquier otra pila de tu subred privada, y las instancias de una pila pueden comunicarse completamente entre sí a través de cualquier protocolo.

Important

El grupo de seguridad predeterminado para las pilas de las subredes privadas permite que todas las pilas de la subred privada se comuniquen con otras pilas de esa subred privada. Si desea restringir las comunicaciones entre las pilas de una subred privada, debe crear nuevos grupos de seguridad que describan la restricción. Por ejemplo, si desea restringir las comunicaciones a un servidor de base de datos para que las pilas de esa subred privada solo puedan comunicarse desde un servidor de aplicaciones específico a través de un puerto específico, solicite un grupo de seguridad especial. En esta sección se describe cómo hacerlo.

Grupos de seguridad predeterminados

MALZ

En la siguiente tabla se describe la configuración predeterminada del grupo de seguridad entrante (SG) para sus pilas. El SG se denomina «SentinelDefaultSecurityGroupPrivateOnly-VPC-ID» y es *ID* un ID de VPC en tu cuenta de zona de landing zone multicuenta de AMS. Se permite que todo el tráfico salga a «mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly» a través de este grupo de seguridad (se permite todo el tráfico local dentro de las subredes apiladas).

Un segundo grupo de seguridad "» permite que todo el tráfico salga a 0.0.0.0/0. SentinelDefaultSecurityGroupPrivateOnly

> **Tip**
>
> Si elige un grupo de seguridad para un tipo de cambio de AMS, como EC2 crear o OpenSearch crear un dominio, debe utilizar uno de los grupos de seguridad predeterminados que se describen aquí o un grupo de seguridad que haya creado. Puede encontrar la lista de grupos de seguridad, por VPC, en la consola de AWS o en la EC2 consola de VPC.

Hay otros grupos de seguridad predeterminados que se utilizan con fines internos de AMS.

Grupos de seguridad predeterminados de AMS (tráfico entrante)

Tipo	Protocolo	Intervalo de puertos	Origen
Todo el tráfico	Todos	Todos	SentinelDefaultSecurityGroupPrivateOnly (restringe el tráfico saliente a los miembros del mismo grupo de seguridad)
Todo el tráfico	Todos	Todos	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (no restringe el tráfico saliente)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (fuente 0.0.0.0/0)	SentinelDefaultSecurityGroupPublic (no restringe el tráfico saliente)

Tipo	Protocolo	Intervalo de puertos	Origen
		Se permite el acceso SSH y RDP desde los bastiones	
Bastiones de MALZ:			
SSH	TCP	22	SharedServices CIDR de VPC y CIDR de VPC DMZ, además de entornos locales proporcionados por el cliente CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
Bastiones de SALZ:			
SSH	TCP	22	mc-initial-garden- SG LinuxBastion
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- SG WindowsBastion
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

SALZ

En la siguiente tabla se describe la configuración predeterminada del grupo de seguridad entrante (SG) para sus pilas. El SG se denomina «mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly -*ID*» y *ID* es un identificador único. Se permite que todo el tráfico salga a «mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly» a través de este grupo de seguridad (se permite todo el tráfico local dentro de las subredes apiladas).

Un segundo grupo de seguridad, "- -», permite que todo el tráfico salga a 0.0.0.0/0. mc-initial-garden SentinelDefaultSecurityGroupPrivateOnlyEgressAll *ID*

> **Tip**
>
> Si elige un grupo de seguridad para un tipo de cambio de AMS, como EC2 crear o OpenSearch crear un dominio, debe utilizar uno de los grupos de seguridad predeterminados que se describen aquí o un grupo de seguridad que usted haya creado. Puede encontrar la lista de grupos de seguridad, por VPC, en la consola de AWS o en la EC2 consola de VPC.

Hay otros grupos de seguridad predeterminados que se utilizan con fines internos de AMS.

Grupos de seguridad predeterminados de AMS (tráfico entrante)

Tipo	Protocolo	Intervalo de puertos	Origen
Todo el tráfico	Todos	Todos	SentinelDefaultSecurityGroupPrivateOnly (restringe el tráfico saliente a los miembros del mismo grupo de seguridad)
Todo el tráfico	Todos	Todos	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (no restringe el tráfico saliente)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (fuente 0.0.0.0/0) Se permite el acceso SSH y RDP desde los bastiones	SentinelDefaultSecurityGroupPublic (no restringe el tráfico saliente)
Bastiones de MALZ:			
SSH	TCP	22	SharedServices CIDR de VPC y CIDR de VPC DMZ, además de entornos locales proporcionados por el cliente CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	

Tipo	Protocolo	Intervalo de puertos	Origen
Bastiones de SALZ:			
SSH	TCP	22	mc-initial-garden- SG LinuxBastion
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden- SG WindowsBastion
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZSG

Crear, cambiar o eliminar grupos de seguridad

Puede solicitar grupos de seguridad personalizados. En los casos en que los grupos de seguridad predeterminados no satisfagan las necesidades de sus aplicaciones o de su organización, puede modificar o crear nuevos grupos de seguridad. Esta solicitud se consideraría necesaria para su aprobación y sería examinada por el equipo de operaciones de AMS.

Para crear un grupo de seguridad fuera de las pilas VPCs, envíe una RFC con el tipo de `Deployment | Advanced stack components | Security group | Create (review required)` cambio (ct-1oxx2g2d7hc90).

Para las modificaciones de los grupos de seguridad de Active Directory (AD), utilice los siguientes tipos de cambios:

- Para añadir un usuario: envíe un RFC mediante Management | Directory Service | Usuarios y grupos | Añadir usuario al grupo [ct-24pi85mjtza8k]
- Para eliminar un usuario: envíe un RFC mediante Management | Directory Service | Users and groups | Eliminar usuario del grupo [ct-2019s9y3nfml4]

> **Note**
>
> Cuando utilice la opción «revisión obligatoria» CTs, AMS recomienda que utilice la opción de programación lo antes posible (elija ASAP en la consola y deje en blanco la hora de inicio y finalización en la API/CLI), ya que CTs requiere que un operador de AMS examine la RFC y, posiblemente, se comunique con usted antes de que pueda aprobarse y ejecutarse. Si las

programa RFCs, asegúrese de esperar al menos 24 horas. Si la aprobación no se produce antes de la hora de inicio programada, la RFC se rechaza automáticamente.

Busque grupos de seguridad

Para buscar los grupos de seguridad adjuntos a una pila o instancia, utilice la EC2 consola. Tras encontrar la pila o la instancia, podrá ver todos los grupos de seguridad asociados a ella.

Para obtener información sobre cómo buscar grupos de seguridad en la línea de comandos y filtrar los resultados, consulte `describe-security-groups`.

EC2 Perfil de instancia de IAM

Un perfil de instancia es un contenedor para un rol de IAM que puedes usar para pasar la información del rol a una EC2 instancia cuando se inicia la instancia.

MALZ

Hay dos perfiles de instancia predeterminados de AMS `customer-mc-ec2-instance-profile` y`customer-mc-ec2-instance-profile-s3`. Estos perfiles de instancia proporcionan los permisos que se describen en la siguiente tabla.

Descripciones de políticas

Perfil	Políticas
`customer-mc-ec2-instance-profile`	`AmazonSSMManagedInstanceCore` : Permite que las instancias Ec2 utilicen el agente SSM.
	`AMSInstanceProfileLoggingPolicy` : Permite que las instancias de Ec2 envíen registros a S3 y. CloudWatch
	`AMSInstanceProfileManagementPolicy` : Permite que las instancias de Ec2 realicen acciones de arranque, como unirse a Active Directory.

Perfil	Políticas
	`AMSInstanceProfileMonitoringPolicy` : Permite a las instancias de Ec2 informar de los hallazgos a los servicios de monitoreo de AMS.
	`AMSInstanceProfilePatchPolicy` : Permite que las instancias de Ec2 reciban parches.
`customer-mc-ec2-instance-profile-s3`	`AMSInstanceProfileBYOEPSPolicy` : Permite que las instancias de Ec2 utilicen AMS y traigan su propio EPS.
	`AMSInstanceProfileLoggingPolicy` : Permite que las instancias de Ec2 envíen registros a S3 y. CloudWatch
	`AMSInstanceProfileManagementPolicy` : Permite que las instancias de Ec2 realicen acciones de arranque, como unirse a Active Directory.
	`AMSInstanceProfileMonitoringPolicy` : Permite a las instancias de Ec2 informar de los hallazgos a los servicios de monitoreo de AMS.
	`AMSInstanceProfilePatchPolicy` : Permite que las instancias de Ec2 reciban parches.
	`AMSInstanceProfileS3WritePolicy` : Permite que las instancias de Ec2 lleguen read/write a los buckets S3 del cliente.

SALZ

Hay un perfil de instancia predeterminado de AMS que concede permisos desde la política de instancias de IAM. `customer-mc-ec2-instance-profile` `customer_ec2_instance_profile_policy` Este perfil de instancia proporciona los permisos

que se describen en la siguiente tabla. El perfil concede permisos a las aplicaciones que se ejecutan en la instancia, no a los usuarios que inician sesión en la instancia.

Las políticas suelen incluir varias sentencias, cada una de las cuales concede permisos a un conjunto diferente de recursos o los concede con una condición específica.

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).

EC2 permisos de perfil de instancia de IAM predeterminados

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).			
Declaración de la política	Efecto	Actions	Descripción y recurso (ARN)
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 Acciones de mensajes	Permitir	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages, SendReply	Permite acciones de mensajería de EC2 Systems Manager en su cuenta.
Ec2 Describa	Permitir	* (Todos)	Permite que la consola muestre los detalles de configuración EC2 de una cuenta.
Soy Get Role ID	Permitir	GetRole	Permite EC2 obtener su ID de IAM de `aws:iam::*:role/customer-*` y. `aws:iam::*:role/customer_*`
Instancia para cargar eventos de registro	Permitir	Crear grupo de registros	Permite crear registros en: `aws:logs:*:*:log-group:i-*`

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).			
Declaración de la política	Efecto	Actions	Descripción y recurso (ARN)
		Crear flujo de registro	Permite que los registros se transmitan a: `aws:logs:*:*:log-group:i-*`
CW para MMS	Permitir	DescribeAlarms, PutMetricAlarm, PutMetricData	Permite CloudWatch recuperar las alarmas de su cuenta. Permite a CW crear o actualizar una alarma y asociarla a la métrica especificada. Permite a CW publicar puntos de datos métricos en su cuenta.
Etiquetas Ec2	Permitir	CreateTags, DescribeTags,	Permite añadir, sobrescribir y describir etiquetas en las instancias especificadas de su cuenta.
Denegar explícitamente los registros de CW	Denegar	DescribeLogStreams, FilterLogEvents, GetLogEvents	No permite enumerar, filtrar ni obtener las secuencias de registro de: `aws:logs:*:*:log-group:/mc/*`
Amazon EC2 Simple Systems Manager (SSM)			

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).			
Declaración de la política	Efecto	Actions	Descripción y recurso (ARN)
Acciones de SSM	Permitir	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Permite una variedad de funciones de SSM en su cuenta.
Acceso a SSM en S3	Permitir	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadPorts, ListBucketMultipartUploads	Permite al SSM del sistema EC2 obtener y actualizar objetos y abortar la carga de objetos de varias partes y enumerar los puertos y depósitos disponibles para cargas de varias partes. `aws:s3:::mc-*-internal-*/aws/ssm*`
Amazon EC2 Simple Storage Service (S3)			
Obtenga el objeto en S3	Permitir	Get Enumeración	Permite a EC2 las aplicaciones recuperar y enumerar los objetos de los depósitos de S3 de su cuenta.
Acceso al registro cifrado por el cliente (S3)	Permitir	PutObject	Permite a EC2 las aplicaciones actualizar los objetos en `aws:s3:::mc-*-logs-*/encrypted/app/*`

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).			
Declaración de la política	Efecto	Actions	Descripción y recurso (ARN)
Parche Data Put Object S3	Permitir	PutObject	Permite a EC2 las aplicaciones cargar los datos de los parches a sus depósitos de S3 en `aws:s3:::awsms-a*-patch-data-*`
Carga de registros propios a S3	Permitir	PutObject	Permite a EC2 las aplicaciones cargar registros personalizados en: `aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`
Denegar explícitamente los registros de MC Namespace S3	Denegar	GetObject* Pone*	No permite que EC2 las aplicaciones obtengan o coloquen objetos desde o hacia: `aws:s3:::mc-*-logs-*/encrypted/mc*` , `aws:s3:::mc-*-logs-*/mc/*`, `aws:s3:::mc-a*-logs-*-audit/*`
Denegar explícitamente la eliminación de S3	Denegar	* (todos)	No permite que EC2 las aplicaciones realicen ninguna acción sobre los objetos de: `aws:s3:::mc-a*-logs-*/*` , `aws:s3:::mc-a*-internal-*/*` ,

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).			
Declaración de la política	Efecto	Actions	Descripción y recurso (ARN)
Denegar explícitamente el bucket CFN de S3	Denegar	Delete*	No permite que EC2 las aplicaciones eliminen ningún objeto de: `aws:s3:::cf-templates-*`
Denegar explícitamente List Bucket S3	Denegar	ListBucket	No le permite incluir ningún objeto cifrado, de registro de auditoría o reservado (mc) de: `aws:s3:::mc-*-logs-*`
AWS Secrets Manager en Amazon EC2			

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).			
Declaración de la política	Efecto	Actions	Descripción y recurso (ARN)
Acceso secreto a Trend Cloud One	Permitir	GetSecretValue	Permite EC2 a Amazon acceder a los secretos de la migración de Trend Cloud One: `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `arn:aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-activation-token*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-guid*`
AWS Key Management Service en Amazon EC2			
Clave de descifrado de Trend Cloud One	Permitir	Decrypt	Permita EC2 que Amazon descifre la AWS KMS clave con el alias/-migration ams/eps/cloudone `arn:aws:kms:*:*:alias/ams/eps/cloudone-migration`

Si no estás familiarizado con las políticas de Amazon IAM, consulta Descripción general de las políticas de IAM para obtener información importante.

> **Note**
>
> Las políticas suelen incluir varias declaraciones, en las que cada declaración concede permisos a un conjunto diferente de recursos o concede permisos bajo una condición específica.

Valores predeterminados de las métricas monitorizadas

En la siguiente tabla se muestra lo que se supervisa y los umbrales de alerta predeterminados. Puede cambiar los valores predeterminados con una solicitud de cambio (RFC) de la administración de cambios.

> **Note**
>
> CloudWatch lanzó la retención ampliada de métricas el 1 de noviembre de 2016. Para obtener más información, consulte CloudWatch Límites.

Alertas del monitoreo de referencia

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
En el caso de las alertas destacadas (*), AMS evalúa el impacto de forma proactiva y las corrige cuando es posible; si no es posible remediarlas, AMS crea un incidente. Si la automatización no corrige el problema, AMS le informa del caso del incidente y contrata a un ingeniero de AMS. Además, estas alertas se pueden enviar directamente a su correo electrónico (si ha optado por el tema de las Direct-Customer-Alerts redes sociales).			
Instancia de Application Load	No	RejectedConnectionCount suma > 0 durante 1 minuto, 5 veces consecutivas.	CloudWatch alarma si el número de conexiones que se rechazaron porque el balanceador de carga alcanzó su máximo.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
Balancer (ALB)			
Objetivo de Application Load Balancer (ALB)	No	TargetConnectionErrorCount suma > 0 durante 1 minuto, 5 veces consecutivas.	CloudWatch se emitirá una alarma si el número de conexiones entre el balanceador de cargas y las instancias registradas no se estableció correctamente.
EC2 Instancia de Amazon: Windows	No	SecureChannelFailure > 0.0 para 10 de los últimos 15 puntos de datos.	CloudWatch alarma en las instancias de Windows para avisar cuando se produce un error en la conexión Secure a Channel.
Instancia Aurora	No	CPUUtilization > 85% durante 5 minutos, 2 veces consecutivas.	CloudWatch alarma.
AWS Backup	Sí	DeleteRecoveryPoint Un director de rol de IAM o un usuario principal de IAM inesperado ha eliminado un punto de AWS Backup recuperación.	CloudWatch evento. Se emite cuando se elimina un punto de recuperación de una copia de seguridad.
AWS Outposts	Sí	AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% durante 5 minutos, 12 veces consecutivas.	CloudWatch alarma en la familia de instancias, capacidad y disponibilidad del AWS Outposts recurso.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% durante 5 minutos, 12 veces consecutivas.	CloudWatch alarma sobre el tipo de instancia, la capacidad y la disponibilidad del AWS Outposts recurso.
		AMSOutpostsConnectedStatusConnectedStatus < 1 durante 5 minutos, 1 vez consecutiva.	CloudWatch alarma en la conexión AWS Outposts del enlace de servicio, se ha averiado menos de 1 cuenta.
		AMSOutpostsCapacityExceptionCapacityExceptions 0 durante 5 minutos, 1 vez consecutiva.	CloudWatch alarma por errores de capacidad insuficiente (por ejemplo, lanzamientos de AWS Outposts un recurso) .
EC2 instancia: todos OSs	No	CPUUtilization* >= 95% durante 5 minutos, 6 veces consecutivas.	CloudWatch alarma. El uso elevado de la CPU es un indicador de un cambio en el estado de la aplicación, como bloqueos muertos, bucles infinitos, ataques maliciosos y otras anomalías.
		StatusCheckFailed > 0 durante 5 minutos, 3 veces consecutivas.	CloudWatch alarma.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		Uso del volumen raíz >= 95% durante 5 minutos, 6 veces consecutivas.	
		Uso de volúmenes sin root > 85% durante 5 minutos, 2 veces consecutivas. Desactivado de forma predeterminada; para obtener más información, consulte https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	
		Libre de memoria* MemoryFree < 5% durante 5 minutos, 6 veces consecutivas.	
	Sí	Malware EPS Se encontró malware en una instancia.	CloudWatch evento.
EC2 Instancia de Amazon: Linux	No	Uso del inodo del volumen raíz Promedio superior al 95% durante 5 minutos, 6 veces consecutivas.	CloudWatch alarma. Se aplica solo a instancias de Linux.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		Sin intercambios* Intercambio de memoria inferior al 5% durante 5 minutos, 6 veces consecutivas.	
ElastiCache Clúster	No	CurrConnections = 65000	Esta alarma notifica a AMS el límite máximo de conexión de un ElastiCache host. CloudWatch Alarma. Si desea actualizar este umbral, póngase en contacto con el servicio de asistencia de AMS.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
ElastiCache Nodo	No	CPUUtilization Promedio > valor predefinido durante 15 minutos, 2 veces consecutivas.	CloudWatch alarma. El valor predeterminado es 90. Si es Redis, usa uno de los siguientes valores según el tipo de instancia : • cache.t1.micro: 90% • cache.m1.small: 90% • cache.m1.medium: 90% • cache.m1.large: 45% • cache.m1.xlarge: 22,5% • cache.m2.xlarge: 45% • cache.m2.4xlarge: 11,25% • cache.c1.xlarge: 11,25% • cache.t2.micro: 90% • cache.t2.small: 90% • cache.t2.medium: 45% • cache.m3.medium: 90% • cache.m3.large: 45% • cache.m3.xlarge: 22,5% • cache.m3.2xlarge: 11,25% • cacher.3.large: 45% • cache.r3.xlarge: 22,5% • cache.r3.2xlarge: 11,25% • cache.r3.4xlarge: 5,625% • cacher.3.8x grande: 2.8125%

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
ElastiCache Nodo: memcached	No	SwapUsage máximo > 50 000 000 bytes durante 5 minutos, 5 veces consecutivas.	CloudWatch alarma. Se aplica solo a memcached.
OpenSearch clúster	No	ClusterStatus.red el máximo es >= 1 durante 1 minuto, 1 vez consecutiva. Cuando se activa esta alerta, AMS toma medidas proactivas para reducir el impacto operativo.	CloudWatch alarma. Al menos una partición principal y sus réplicas no están asignados a un nodo. Para obtener más información, consulte Red Cluster Status.
Dominio OpenSearch	No	KMSKeyError >= 1 durante 1 minuto, 1 vez consecutiva.	CloudWatch alarma. La clave de cifrado de KMS que se utiliza para cifrar los datos en reposo en el dominio está deshabilitada. Vuelva a habilitarla para restablecer las operaciones normales. Para obtener más información, consulte Cifrado de datos en reposo para OpenSearch Service Service.
		ClusterStatus.amarillo el máximo es >= 1 durante 1 minuto, 1 vez consecutiva Cuando se activa esta alerta, AMS toma medidas proactivas para reducir el impacto operativo.	Al menos una partición de réplica no está asignada a un nodo. Para obtener más información, consulte Estado del clúster amarillo.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		FreeStorageSpace el mínimo es <= 20480 durante 1 minuto, 1 vez consecutiva Cuando se activa esta alerta, AMS toma medidas proactivas para reducir el impacto operativo.	El espacio de almacenamiento disponible de un nodo en su clúster se redujo hasta los 20 GiB. Para obtener más información, consulte Falta de espacio de almacenamiento disponible.
		ClusterIndexWritesBlocked >= 1 durante 5 minutos, 1 vez consecutiva Cuando se activa esta alerta, AMS toma medidas proactivas para reducir el impacto operativo.	El clúster bloquea las solicitudes de escritura. Para obtener más información, consulte ClusterBlockException.
		Nodos el mínimo es < x durante 1 día, 1 vez consecutiva Cuando se activa esta alerta, AMS toma medidas proactivas para reducir el impacto operativo.	x es el número de nodos del clúster. Esta alarma indica que al menos un nodo del clúster se mantuvo inaccesible durante un día. Para obtener más información, consulte Nodos de clúster fallidos.
		CPUUtilization el promedio es >= 80% durante 15 minutos, 3 veces consecutivas Cuando se activa esta alerta, AMS toma medidas proactivas para reducir el impacto operativo.	Es habitual utilizar el 100% de la CPU, pero los promedios altos y sostenidos son problemáticos. Considere la posibilidad de utilizar tipos de instancias más grandes o de agregar instancias.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		JVMMemoryPresión el máximo es >= 80% durante 5 minutos, 3 veces consecutivas Cuando se activa esta alerta, AMS toma medidas proactivas para reducir el impacto operativo.	El clúster podría encontrar errores de memoria insuficiente si aumenta el uso. Considere el escalado vertical. Amazon ES utiliza la mitad de la RAM de una instancia para el montón de Java, hasta un tamaño de pila de 32 GiB. Puede escalar las instancias verticalmente hasta 64 GiB de RAM y después escalarlas horizontalmente mediante el agregado de instancias.
		Maestro CPUUtilization el promedio es >= 50% durante 15 minutos, 3 veces consecutivas Cuando se activa esta alerta, AMS toma medidas proactivas para reducir el impacto operativo.	Considere la posibilidad de utilizar tipos de instancias más grandes para sus nodos maestros dedicados. Debido a su función en la estabilidad y blue/green las implementaciones de los clústeres, los nodos maestros dedicados deberían tener un uso medio de CPU inferior al de los nodos de datos.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		Presión maestra JVMMemory el máximo es >= 80% durante 15 minutos, 1 vez consecutiva Cuando se activa esta alerta, AMS toma medidas proactivas para reducir el impacto operativo.	Considere la posibilidad de utilizar tipos de instancias más grandes para sus nodos maestros dedicados. Debido a su función en la estabilidad y blue/green las implementaciones de los clústeres, los nodos maestros dedicados deberían tener un uso medio de CPU inferior al de los nodos de datos.
OpenSearch instancia	No	AutomatedSnapshotFailure el máximo es >= 1 durante 1 minuto, 1 vez consecutiva.	CloudWatch alarma. Se produjo un error en una instantánea automatizada. Este error suele ser el resultado de un estado rojo del clúster. Consulte el estado del clúster rojo.
Instancia de Elastic Load Balancing	No	SurgeQueueLength > 100 durante 1 minuto, 15 veces consecutivas.	CloudWatch alarma si hay un número excesivo de solicitudes pendientes de enrutamiento.
		HTTPCode_ELB_5xx_Count suma > 0 durante 5 minutos, 3 veces consecutivas.	CloudWatch alarma por un número excesivo de códigos de respuesta HTTP 5XX que se originan en el balanceador de cargas.
		SpilloverCount > 1 durante 1 minuto, 15 veces consecutivas.	CloudWatch alarma si hay un número excesivo de solicitudes rechazadas porque la cola de espera está llena.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
GuardDuty servicio	Sí	No aplicable; se supervisan todos los hallazgos (con fines de amenaza). Cada hallazgo corresponde a una alerta. Cambios en los GuardDuty hallazgos. Entre estos cambios se incluyen los resultados recién generados, y todos los casos posteriores de resultados.	La lista de tipos de GuardDuty hallazgos compatibles se encuentra en GuardDuty Active Finding Types.
Estado	Varía	Panel de AWS Health	Las notificaciones se envían cuando hay cambios en el estado de los eventos Panel de AWS Health (AWS Health) en relación con los servicios de referencia compatibles con AMS. Para obtener más información, consulte Servicios compatibles.
AWS Managed Microsoft AD	No	Estado de Active Directory AWS Managed Microsoft AD la instancia envía un evento de estado activo.	Evento de servicio. Se emite cuando el directorio funciona normalmente después de un evento.
		Estado del directorio deteriorado AWS Managed Microsoft AD la instancia envía un evento de estado de directorio dañado.	Evento de servicio. Se emite cuando el directorio se ejecuta en un estado degradado. Se han detectado uno o varios problemas y no todas las operaciones de directorios pueden funcionar con plena capacidad operativa.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		Estado del directorio inoperable AWS Managed Microsoft AD la instancia envía un evento de estado inoperable.	Evento de servicio. Se emite cuando el directorio no funciona. Todos los puntos de enlace del directorio han informado de la existencia de problemas.
		Eliminar el estado del directorio AWS Managed Microsoft AD la instancia envía un evento de eliminación del estado del directorio.	Evento de servicio. Se emite cuando el directorio se está borrando actualmente.
		Estado del directorio fallido AWS Managed Microsoft AD la instancia envía un evento de estado fallido.	Evento de servicio. Se emite cuando no se ha podido crear el directorio.
		RestoreFailed Estado del directorio AWS Managed Microsoft AD la instancia envía un evento de restauración fallida del estado del directorio.	Evento de servicio. Se emite cuando se produce un error al restaurar el directorio a partir de una instantánea.
Instancia de Amazon RDS	No	La alerta de bajo nivel de almacenamiento se activa cuando se agota el almacenamiento asignado a la instancia de base de datos.	RDS-EVENT-0007, consulte los detalles en Uso de la notificación de eventos de Amazon RDS.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		Fallo en la instancia de base Se ha producido un error en la instancia de base de datos debido a una configuración incompatible o a un problema de almacenamiento subyacente. Comience a point-in-time-restore para la instancia de base de datos.	Evento de servicio. RDS-EVENT-0031, categorías de eventos y mensajes de eventos de Amazon RDS.
		No se intentó la conmutación por error Amazon RDS no está intentando realizar la conmutación por error solicitada porque recientemente se ha producido una conmutación por error en la instancia de base de datos.	Evento de servicio. RDS-EVENT-0034, categorías de eventos y mensajes de eventos de Amazon RDS.
		Parámetros no válidos de la instancia de base Por ejemplo, MySQL no se pudo iniciar porque un parámetro relacionado con la memoria está establecido en un valor demasiado alto para esta clase de instancia , por lo que la acción del cliente consistiría en modificar el parámetro de memoria y reiniciar la instancia de base de datos.	Evento de servicio. RDS-EVENT-0035, categorías de eventos y mensajes de eventos de Amazon RDS.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		Instancia de base IDs de datos de subred no válida La instancia de base de datos está en una red incompatible. Algunas de las subredes especificadas no IDs son válidas o no existen.	Evento de servicio. RDS-EVENT-0036, categorías de eventos y mensajes de eventos de Amazon RDS.
		Error de lectura y réplica de la instancia de base Se ha producido un error en el proceso de replicación de una réplica de lectura. Para obtener más información, consulte el mensaje del evento. Para obtener información sobre la solución de errores de réplica de lectura, consulte Solución de problemas de réplica de lectura de MySQL.	Evento de servicio. RDS-EVENT-0045, categorías de eventos y mensajes de eventos de Amazon RDS.
		Finalizó la replicación de lectura de la instancia de base Se ha finalizado la replicación en la réplica de lectura.	Evento de servicio. RDS-EVENT-0057, categorías de eventos y mensajes de eventos de Amazon RDS.
		Error al crear la cuenta de usuario de statspack Error al crear la cuenta del usuario PERFSTAT de Statspack. Elimine la cuenta antes de añadir la opción Statspack.	Evento de servicio. RDS-EVENT-0058, categorías de eventos y mensajes de eventos de Amazon RDS.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		Inicio de recuperación de instancias de base de datos La instancia de base de datos de SQL Server está restableciendo su imagen reflejada. El desempeño se degradará hasta que se restablezca la imagen reflejada. Se ha encontrado una base de datos con un modelo de recuperación no completa (non-FULL). El modelo de recuperación volvió a ser COMPLETO y se inició la recuperación duplicada. (<dbname>: <recovery model found>[,...]).	Evento de servicio. RDS-EVENT-0066, categorías de eventos y mensajes de eventos de Amazon RDS.
		Ha fallado la conmutación por error de un clúster de bases de datos.	RDS-EVENT-0069, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		Depósito de S3 de recuperación de permisos no válidos El rol de IAM que se utiliza para obtener acceso al bucket de Amazon S3 para las operaciones nativas de copia de seguridad y restauración de SQL Server se ha configurado incorrectamente. Para obtener más información, consulte Configuración de Native Backup and Restore.	Evento de servicio. RDS-EVENT-0081, categorías de eventos y mensajes de eventos de Amazon RDS.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		Aurora no ha podido copiar los datos de copia de seguridad de un bucket de Amazon S3.	RDS-EVENT-0082, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		Alerta de almacenamiento bajo cuando la instancia de base de datos ha consumido más del 90% del almacenamiento asignado	RDS-EVENT-0089, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		El servicio de notificaciones cuando se produce un error de escalado en el clúster de base de datos Aurora Serverless.	RDS-EVENT-0143, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		La instancia de base de datos se encuentra en un estado no válido. No es necesaria ninguna acción. El escalado automático se volverá a intentar más tarde.	RDS-EVENT-0219, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		La instancia de base de datos alcanzó el umbral de almacenamiento completo y se cerró la base de datos.	RDS-EVENT-0221, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		Este evento indica que el escalado automático del almacenamiento de la instancia de RDS no puede escalarse. Es posible que el escalado automático no se pueda escalar por varios motivos.	RDS-EVENT-0223, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		El escalado automático del almacenamiento ha desencadenado una tarea de escala de almacenamiento pendiente que alcanzaría el umbral máximo de almacenamiento.	RDS-EVENT-0224, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		La instancia de base de datos tiene un tipo de almacenamiento que no está disponible actualmente en la zona de disponibilidad. El escalado automático se volverá a intentar más tarde.	RDS-EVENT-0237, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		RDS no ha podido aprovisionar capacidad para el proxy porque no hay suficientes direcciones IP disponibles en las subredes.	RDS-EVENT-0243, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		El almacenamiento de su cuenta de AWS ha superado la cuota de almacenamiento permitida.	RDS-EVENT-0254, consulte los detalles en las categorías de eventos y los mensajes de eventos de Amazon RDS.
		CPUUtilization Utilización media de la CPU superior al 90% durante 15 minutos, 2 veces consecutivas.	CloudWatch alarma.
		DiskQueueDepth La suma es > 75 durante 1 minuto, 15 veces consecutivas.	

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		FreeStorageSpace Promedio < 1.073.741.824 bytes durante 5 minutos, 2 veces consecutivas.	
		SwapUsage Promedio = 104.857.600 bytes durante 5 minutos, 2 veces consecutivas.	
Clúster de Amazon Redshift	No	RedshiftClusterStatus El estado del clúster cuando no está en modo de mantenimiento es inferior a 1 durante 5 minutos.	1 representa un clúster en buen estado.
Amazon Macie	Sí	Alertas recién generadas y actualizaciones de las alertas existentes. Macie encuentra cualquier cambio en los resultados. Entre estos cambios se incluyen los resultados recién generados, y todos los casos posteriores de resultados.	Alerta de Amazon Macie. Para obtener una lista de los tipos de alertas de Macie compatibles, consulte Análisis de los hallazgos de Amazon Macie. Tenga en cuenta que Macie no está activado para todas las cuentas.

Valores predeterminados de retención y rotación de registros

En esta sección se describen los valores predeterminados de administración de registros de AMS; para obtener más información, consulte Administración de registros.

- Rotación = rotación de registros dentro de las instancias

- Retención = período de tiempo que guardamos los registros en Amazon CloudWatch Logs y Amazon Simple Storage Service (S3)

Los registros se conservan en CloudWatch Logs según sea necesario (puede configurarlo) y en S3. No caducan ni se eliminan y están sujetos a la durabilidad del servicio. Para obtener información detallada sobre la durabilidad del S3, consulte Protección de datos en Amazon S3.

Puede solicitar un cambio en la retención de registros para todos los registros, excepto los AWS CloudTrail registros, que se conservan indefinidamente por motivos de auditoría y seguridad.

La rotación de registros se configura dentro de las instancias. De forma predeterminada, los registros del sistema operativo y de seguridad rotan cada hora si superan los 100 MB. Esto se hace para garantizar que no te quedes sin espacio en disco en las instancias.

El agente de registro de las instancias carga el registro en línea en CloudWatch Logs, desde donde se archivan en S3.

Los registros se almacenan en CloudWatch Logs y S3 en el formato original en el que se generan, sin procesamiento previo.

Valores predeterminados de administración de continuidad

En esta sección se describen los valores predeterminados de la gestión de la continuidad de AMS; para obtener más información sobre las copias de seguridad de AMS, consulte el capítulo sobre la gestión de la continuidad de la guía del usuario de AMS.

La configuración de Backup se realiza en el momento de la incorporación. Esta es la configuración de copia de seguridad predeterminada (recomendada).

Etiqueta de VPC y valores predeterminados

Para obtener la información más actualizada sobre las copias de seguridad de AMS, consulte Administración de la continuidad.

> **Important**
>
> De forma predeterminada, las copias de seguridad EC2 apiladas están deshabilitadas (Backup = False). Puedes habilitar las copias de seguridad de las EC2 instancias en el momento de la creación añadiendo una etiqueta `Key: Backup, Value: True` al solicitar una EC2 pila mediante una RFC (CT ct-14027q0sjyt1h). Si quieres añadir la etiqueta una vez

creada la instancia, envía una RFC a Management | Advanced stack components | instance stack | Update CT (ct-38s4s4tm4ic4u). EC2

EC2 etiqueta de instancia y valores predeterminados

La etiqueta de respaldo de la EC2 pila especifica si la pila requiere una instantánea de los volúmenes de EBS adjuntos o no.

Etiqueta `Key: Backup`

Etiqueta `Value: True, False`

De forma predeterminada, el valor es que `False` la etiqueta de copia de seguridad no está presente y la pila no tiene copias de seguridad programadas.

Cambie la etiqueta `Key: Backup` `Value: True` a para habilitar las copias de seguridad, que luego se realizan según la programación establecida con la etiqueta de copia de seguridad de VPC.

> **Note**
>
> El significado del valor de la etiqueta (solo el valor) es insensible, por lo que True/true o todos False/false son aceptables.

Copia de seguridad y valores predeterminados de la instancia RDS

Los valores predeterminados de Amazon Relational Database Service (RDS) se definen en las plantillas de pila:

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

Valores predeterminados de aplicación de parches

En esta sección se describen los ajustes predeterminados de los parches de AMS; para obtener más información sobre los parches de AMS, consulte el capítulo sobre la gestión de parches de la Guía del usuario de AMS.

AMS publica parches AMIs mensualmente; todas las solicitudes de pila nuevas deben configurarse con la AMI de AMS más reciente.

> **Important**
>
> AMS Patch Orchestrator, el parcheo basado en etiquetas, utiliza la funcionalidad de AWS Systems Manager (SSM) para que pueda etiquetar instancias o hacer que AMS etiquete sus instancias y parchear esas instancias mediante una línea base y una ventana que usted configure. Para obtener más información, consulte Patch Orchestrator: un modelo de parches basado en etiquetas.

Parcheo estándar de AMS, basado en cuentas: para cada cuenta con pilas que reciba parches de forma automática, se enviará una notificación de los próximos parches aplicables poco después del «martes de parches». La notificación contiene una lista de todas las pilas y los parches aplicables, así como la ventana de parches sugerida. En el caso de los parches críticos, el plazo se establece con no más de 10 días de antelación y, para los parches estándar, con no más de 14 días de antelación. Si no responde a la notificación, no se procederá a aplicar los parches. Si desea excluir algunos parches, responda a la notificación o envíe una solicitud de servicio. Si respondes con tu consentimiento a la aplicación de parches, pero no solicitas específicamente un calendario diferente, los parches se aplicarán tal y como se describe en la notificación que recibas.

> **Note**
>
> La notificación del servicio de parches es un correo electrónico que se envía a los contactos de la cuenta y contiene un enlace a la consola de AWS Support. Puede responder a través de la consola de AWS Support o a través de la página de solicitud de servicio de AMS, donde la notificación aparece como una notificación de servicio.

Durante el proceso de aplicación de parches estándar de AMS, AMS realiza lo siguiente:

1. Se le envía una notificación del servicio de aplicación de parches catorce días antes de la fecha de aplicación de parches propuesta. La notificación del servicio de aplicación de parches se envía por correo electrónico a la dirección de correo electrónico de contacto que tiene registrada en su cuenta.
2. Identifica todas las EC2 instancias accesibles de la pila en función de la lista de pilas proporcionada en la notificación de aplicación de parches. En este caso, «Accesible» se refiere

a las instancias que están en EC2 estado «En ejecución» y que tienen el agente Run Command en EC2 pleno funcionamiento.

3. AMS aplica los parches de forma que se garantice que se estén ejecutando simultáneamente un número suficiente de EC2 instancias (configuradas mediante la `healthy-host-threshold` configuración) para que la pila se mantenga en buen estado.
4. Una vez finalizada la operación de aplicación de parches en todas las EC2 instancias, AMS actualiza la RFC con el estado de aplicación del parche: correcto, parcial o fallido. Si el estado no es correcto, se crea un ticket para que un operador haga un seguimiento de los resultados de la aplicación de los parches y tome las medidas correctivas necesarias.

Valide el servicio AMS (SALZ)

Para comprobar que el servicio AWS Managed Services (AMS) funciona según lo previsto, en este capítulo se describen algunos ejercicios que puede realizar.

Encuentra la configuración de la cuenta AMS

Configuración de la cuenta que se utiliza para crear AMS RFCs, establecer horarios y determinar quién recibe las notificaciones.

Algunos ajustes se crean durante la incorporación y requieren una solicitud de servicio para cambiarlos. Debes anotar estos detalles de la cuenta porque los usarás cuando te comuniques con AMS:

- Credenciales: si necesita recuperar su nombre de usuario o contraseña de AMS, póngase en contacto con el administrador de TI local. AMS utiliza su Active Directory corporativo.
- Gerente de prestación de servicios en la nube (CSDM): esta persona es su enlace con AMS y está disponible para responder a las preguntas sobre el servicio. Se le proporciona la información de contacto de esta persona en el momento de la incorporación y debe mantenerla disponible para todos los miembros de su organización que interactúen con AMS. Puede esperar recibir informes mensuales sobre su servicio de AMS por parte de esta persona.
- Acceso a la consola: accedes a la consola AMS desde una URL configurada específicamente para tu cuenta. Puede obtener la URL desde su CSDM.
- CLI de AMS: puede obtener la CLI de AMS a través de la página de recursos para desarrolladores de la consola AMS o del paquete de productos distribuibles que obtiene de su CSDM. Una vez que

tenga el paquete distribuible, siga los pasos descritos en Instalación o actualización de la CLI de AMS.

- Periodo de mantenimiento: el intervalo de mantenimiento determina cuándo se aplican los parches a las instancias EC2 . La ventana de mantenimiento de AWS Managed Services (o ventana de mantenimiento) realiza actividades de mantenimiento para los servicios gestionados de AWS (AMS) y se repite el segundo jueves de cada mes, de 15:00 a 16:00, hora del Pacífico. AMS puede cambiar el período de mantenimiento con 48 horas de antelación. Es posible que haya elegido un período diferente al incorporarse; lleve un registro del período de mantenimiento que haya elegido.
- Supervisión: AMS proporciona un conjunto de CloudWatch métricas de forma predeterminada, pero también puede solicitar métricas adicionales. Si lo hace, lleve un registro de las mismas.
- Registros: de forma predeterminada, los registros se almacenan en ams-a- *ACCOUNT_ID* -log-management-, que *REGION* es la región en la *REGION* que se generó el registro.
- Mitigación: en el momento de la incorporación, AMS registra la acción de mitigación que elijas en caso de que se identifique un ataque de malware contra tus recursos. Por ejemplo, ponte en contacto con determinadas personas. Mantenga esta información disponible para todos los miembros de su organización que interactúen con AMS.
- Región: puede consultar la página de detalles de la VPC en la consola AMS. También puede ejecutar este comando después de instalar la CLI AMS SKMS (este comando usa un perfil SAML, elimínelo si el método de autenticación es diferente):

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

Los puntos de enlace AMS API/CLI (amscm y amsskms) se encuentran en la región de AWS del Norte de Virginia,. `us-east-1` En función de cómo esté configurada su autenticación y de la región de AWS en la que se encuentren su cuenta y sus recursos, es posible que tenga que `--region us-east-1` añadirlos al emitir comandos. Es posible que también necesite añadirlo`--profile saml`, si ese es su método de autenticación.

Buscar FQDNs en AMS

Los tipos de cambio de acceso a AWS Managed Services (AMSCTs) requieren el nombre de dominio completo, o FQDN, de su dominio de confianza de AMS, en forma de. `C844273800838.amazonaws.com` Para descubrir su AWS FQDN, realice una de las siguientes acciones:

- Consola de AWS: busque en la consola de AWS Directory Service, en la columna del nombre del directorio.
- CLI: utilice estos comandos mientras esté conectado a su dominio:

  Windows (devuelve el usuario y el FQDN):

  ```
  whoami /upn
  ```

  o (DC+DC+DC=FQDN)

  ```
  whoami /fqdn
  ```

  Linux:

  ```
  hostname --fqdn
  ```

> **Note**
>
> Los puntos de enlace AMS API/CLI (amscm y amsskms) se encuentran en la región de AWS del Norte de Virginia,. `us-east-1` En función de cómo esté configurada su autenticación y de la región de AWS en la que se encuentren su cuenta y sus recursos, es posible que tenga que `--region us-east-1` añadirlos al emitir comandos. Es posible que también necesite añadirlo`--profile saml`, si ese es su método de autenticación.

Encuentra las zonas de disponibilidad en AMS AZs

Zona de disponibilidad: todas las cuentas tienen al menos dos zonas de disponibilidad. Para encontrar con precisión los nombres de las zonas de disponibilidad, primero debe conocer el ID de subred asociado.

- Consola AMS: en el panel de navegación VPCs, haga clic y, a continuación, en la VPC correspondiente, si es necesario. En la página de VPCs detalles, seleccione la subred correspondiente en la tabla de subredes para abrir la página de detalles de la subred con el nombre de la zona de disponibilidad asociada.
- API/CLI DE AMS SKMS:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

> **Note**
>
> Los puntos de enlace AMS API/CLI (amscm y amsskms) se encuentran en la región de AWS del Norte de Virginia,. `us-east-1` En función de cómo esté configurada su autenticación y de la región de AWS en la que se encuentren su cuenta y sus recursos, es posible que tenga que `--region us-east-1` añadirlos al emitir comandos. Es posible que también necesite añadirlo`--profile saml`, si ese es su método de autenticación.

Encuentre temas de SNS en AMS

Sus temas de SNS determinan a quién se notifica en diversas circunstancias. AMS proporciona temas de SNS para notificaciones de AMI (consulte Notificaciones de AMI de AMS con SNS), CloudWatch alarmas y EC2 recursos (consulte Recepción de alertas generadas por AMS) y más. Para descubrir sus temas de SNS actuales:

- Consola AWS: utilice la consola de SNS para ver todos los temas, aplicaciones y suscripciones, así como un gráfico de los mensajes. También cree, elimine, suscríbase y publique temas.
- API/CLI (si ha iniciado sesión en su cuenta de AMS, requiere la CLI de AWS):

  Enumere sus temas de SNS:

```
aws sns list-topics
```

  Enumere sus suscripciones de SNS:

```
aws sns list-subscriptions
```

> **Note**
>
> Los puntos de enlace AMS API/CLI (amscm y amsskms) se encuentran en la región de AWS del Norte de Virginia,. `us-east-1` En función de cómo esté configurada su autenticación y de la región de AWS en la que se encuentren su cuenta y sus recursos, es posible que tenga que `--region us-east-1` añadirlos al emitir comandos. Es posible que también necesite añadirlo`--profile saml`, si ese es su método de autenticación.

Encuentre la configuración de copia de seguridad en AMS

AMS gestiona las copias de seguridad y las instantáneas a través del AWS Backupservicio nativo.

La configuración se gestiona mediante AWS Backup planes. Puede tener varios AWS Backup planes que asocien los recursos etiquetados con los programas de respaldo y las políticas de retención. Para encontrar la AWS Backup configuración de su cuenta AMS, utilice la consola https://console.aws.amazon.com/backup o la AWS CLI Command Reference para los comandos de backup.

Para obtener más información sobre AMS AWS Backup, consulte Continuity Management.

Buscar un ID de instancia o una dirección IP

Necesitas una dirección IP de la instancia para iniciar sesión en ella.

- Para solicitar acceso a una instancia, iniciar sesión en una instancia o crear una AMI, debe tener el ID de la instancia. Para una EC2 instancia (ya sea una instancia independiente o una parte de una pila) o una instancia de base de datos, puede encontrar el ID de varias maneras diferentes:
  - La consola AMS para una instancia de una pila de ASG: busca en la página de detalles de la RFC la RFC que creó la pila. En la sección Execution Output, encontrará el ID de pila para la pila ASG y, a continuación, podrá ir a la página de grupos de Auto Scaling de la EC2 consola y buscar ese ID de pila y encontrar instancias para él. Cuando encuentres la instancia, selecciónela y se abrirá un área en la parte inferior de la página con detalles, incluida la dirección IP.

- La consola AMS para una instancia independiente EC2 o de base de datos (DB): busque en la página de detalles del RFC el RFC que creó la EC2 pila o la instancia de base de datos. En la sección Resultado de la ejecución, encontrará el ID de la instancia y la dirección IP.
- EC2 Consola AWS:
  1. En el panel de navegación, seleccione Instances (Instancia[s]). Se abre la página de instancias.
  2. Haga clic en la instancia para la que desee obtener el ID. Se abre la página de detalles de la instancia y muestra el ID y la dirección IP.
- Consola de bases de datos de AWS:
  1. En la página de inicio, seleccione Instancias de base de datos. Se abre la página de instancias.
  2. Filtre la instancia de base de datos para la que desea obtener el ID. Se abre la página de detalles de la instancia y muestra el ID.
- AMS CLI/API.

> **Note**
>
> La CLI de AMS debe estar instalada para que estos comandos funcionen. Para instalar la API o CLI de AMS, vaya a la página de recursos para desarrolladores de la consola AMS. Para obtener material de referencia sobre la API AMS CM o la API AMS SKMS, consulte la sección Recursos de información de AMS en la Guía del usuario. Puede que necesite añadir una `--profile` opción de autenticación; por ejemplo,`aws amsskms` *`ams-cli-command`* `--profile SAML`. Es posible que también tengas que añadir la `--region` opción, ya que todos los comandos de AMS se ejecutan desde us-east-1, por ejemplo. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

> **Note**
>
> Los puntos de enlace AMS API/CLI (amscm y amsskms) se encuentran en la región de AWS del Norte de Virginia,. `us-east-1` En función de cómo esté configurada su autenticación y de la región de AWS en la que se encuentren su cuenta y sus recursos, es posible que tenga que `--region us-east-1` añadirlos al emitir

comandos. Es posible que también necesite añadirlo`--profile saml`, si ese es su método de autenticación.

Ejecuta el siguiente comando para obtener los detalles del resultado de la ejecución de la pila:

```
aws amsskms get-stack --stack-id STACK_ID
```

El resultado tiene un aspecto similar al siguiente y InstanceId aparece cerca de la parte inferior, debajo `Outputs` (los valores que se muestran son ejemplos):

```
{
    "Stack": {
        "StackId": "stack-7fa52bd5eb8240123",
        "Status": {
            "Id": "CreateCompleted",
            "Name": "CreateCompleted"
        },
        "VpcId": "vpc-01234567890abcdef",
        "Description": "Amazon",
        "Parameters": [
            {
                "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
                "Key": "SecurityGroups"
            },
            {
                "Value": "subnet-01234567890abcdef",
                "Key": "InstanceSubnetId"
            },
            {
                "Value": "t2.large",
                "Key": "InstanceType"
            },
            {
                "Value": "ami-01234567890abcdef",
                "Key": "InstanceAmiId"
            }
        ],
        "Tags": [],
        "Outputs": [
            {
                "Value": "i-0b22a22eec53b9321",
```

```
                "Key": "InstanceId"
            },
            {
                "Value": "10.0.5.000",
                "Key": "InstancePrivateIP"
            }
        ],
        "StackTemplateId": "stm-s6xvs000000000000",
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
}
```

Nombres de bastiones compatibles con DNS

MALZ

Para Multi-account Landing Zone (MALZ), los registros DNS se crean para los bastiones en el FQDN del Active Directory administrado por AMS. AMS reemplaza a los bastiones de Linux y Windows según sea necesario. Por ejemplo, si se debe implementar una nueva AMI de bastión, los registros DNS del bastión se actualizan dinámicamente para apuntar a bastiones nuevos y válidos.

1. Para acceder a los bastiones de SSH (Linux), utilice registros DNS como los siguientes: `sshbastion`*`(1-4)`*`.`*`Your_Domain`*`.com`

   Por ejemplo, donde el dominio está: `Your_Domain`

   - `sshbastion1.`*`Your_Domain`*`.com`
   - `sshbastion2.`*`Your_Domain`*`.com`
   - `sshbastion3.`*`Your_Domain`*`.com`
   - `sshbastion4.`*`Your_Domain`*`.com`

2. Para acceder a los bastiones de RDP (Windows), utilice registros DNS como estos:. `rdp-`*`Username`*`.`*`Your_Domain`*`.com`

   Por ejemplo, si el nombre de usuario es`alex`, `test` demobob, o y el dominio es: *`Your_Domain`*`.com`

   - `rdp-alex.`*`Your_Domain`*`.com`

- rdp-test.*Your_Domain*.com
- rdp-demo.*Your_Domain*.com
- rdp-bob.*Your_Domain*.com

SALZ

La zona de landing de cuenta única (SALZ) reemplaza a los bastiones de Linux y Windows según sea necesario. Por ejemplo, si se debe implementar una nueva AMI de bastión, los registros DNS del bastión se actualizan dinámicamente para apuntar a bastiones nuevos y válidos.

1. Para acceder a los bastiones de SSH (Linux), utilice registros DNS como los siguientes: sshbastion*(1-4)*.A*AccountNumber*.amazonaws.com.

   Por ejemplo, dónde 123456789012 está el número de cuenta:

   - sshbastion1.A123456789012.amazonaws.com
   - sshbastion2.A123456789012.amazonaws.com
   - sshbastion3.A123456789012.amazonaws.com
   - sshbastion4.A123456789012.amazonaws.com

2. Para acceder a los bastiones RDP (Windows), utilice registros DNS como estos:. rdpbastion*(1-4)*.A*ACCOUNT_NUMBER*.amazonaws.com

   Por ejemplo, dónde 123456789012 está el número de cuenta:

   - rdpbastion1.A123456789012.amazonaws.com
   - rdpbastion2.A123456789012.amazonaws.com
   - rdpbastion3.A123456789012.amazonaws.com
   - rdpbastion4.A123456789012.amazonaws.com

Búsqueda de direcciones IP de bastión

Los clientes de AMS pueden usar bastiones SSH y RDP, ya sean las Nombres de bastiones compatibles con DNS descritas anteriormente, o bien direcciones IP de bastión.

Para encontrar las direcciones IP de bastión, SSH y RDP, para su cuenta:

1. Solo para landing zone con varias cuentas: inicie sesión en la cuenta de Shared Services.
2. Abra la EC2 consola y elija Instancias en ejecución.

   Se abre la página de instancias.
3. En el cuadro de filtros de la parte superior, introduzca ssh-bastion o rdp-bastion.

   En el cuadro de filtros de la parte superior, introduce customer-ssh o customer-rdp.

   Aparecen los bastiones SSH RDP de tu cuenta. and/or

   Tenga en cuenta que, además de los bastiones de SSH, en la lista puede ver los bastiones de la red perimetral AMS, que no están disponibles para esta función.
4. Seleccione un bastión SSH o RDP. Si utilizas un ordenador con Windows y quieres iniciar sesión en una instancia de Linux, utilizas un bastión de SSH. Si quieres iniciar sesión en una instancia de Windows, utilizas un bastión RDP. Si utilizas un sistema operativo Linux y quieres iniciar sesión en una instancia de Windows, utilizas un bastión SSH a través de un túnel RDP (esto te permite acceder al escritorio de Windows). Para acceder a una instancia de Linux desde un sistema operativo Linux, se utiliza un bastión de SSH.

EC2 instancias: creación

Puedes usar la consola AMS o API/CLI crear un Amazon EC2 y un Amazon EC2 con volúmenes adicionales.

Crea una pila

Crear una EC2 instancia con la consola

A continuación, se muestra este tipo de cambio en la consola AMS.

Cómo funciona:

1. Vaya a la página Crear RFC: en el panel de navegación izquierdo de la consola AMS, haga clic RFCspara abrir la página de RFCs listas y, a continuación, haga clic en Crear RFC.
2. Elija un tipo de cambio (CT) popular en la vista predeterminada de búsqueda de tipos de cambios o seleccione un CT en la vista Elegir por categoría.

- Busque por tipo de cambio: puede hacer clic en un CT popular en el área de creación rápida para abrir inmediatamente la página Ejecutar RFC. Tenga en cuenta que no puede elegir una versión antigua de CT con Quick Create.

  Para ordenar CTs, utilice el área Todos los tipos de cambios en la vista de tarjeta o de tabla. En cualquiera de las vistas, seleccione una CT y, a continuación, haga clic en Crear RFC para abrir la página Ejecutar RFC. Si corresponde, aparece la opción Crear con una versión anterior junto al botón Crear RFC.
- Elegir por categoría: seleccione una categoría, una subcategoría, un elemento y una operación, y se abrirá el cuadro de detalles del CT con la opción Crear con una versión anterior, si corresponde. Haga clic en Crear RFC para abrir la página Ejecutar RFC.

3. En la página Ejecutar RFC, abra el área del nombre del CT para ver el cuadro de detalles del CT. Se requiere un asunto (lo rellena automáticamente si elige su CT en la vista Buscar tipos de cambios). Abra el área de configuración adicional para añadir información sobre la RFC.

   En el área de configuración de ejecución, utilice las listas desplegables disponibles o introduzca valores para los parámetros necesarios. Para configurar los parámetros de ejecución opcionales, abra el área de configuración adicional.
4. Cuando haya terminado, haga clic en Ejecutar. Si no hay errores, aparecerá la página de la RFC creada correctamente con los detalles de la RFC enviada y el resultado inicial de la ejecución.
5. Abra el área de parámetros de ejecución para ver las configuraciones que envió. Actualice la página para actualizar el estado de ejecución de la RFC. Si lo desea, cancele la RFC o cree una copia de la misma con las opciones de la parte superior de la página.

Crear una EC2 instancia con la CLI

Cómo funciona:

1. Utilice la función de creación en línea (se emite un `create-rfc` comando con todos los parámetros de ejecución y RFC incluidos) o la de plantilla (se crean dos archivos JSON, uno para los parámetros de RFC y otro para los parámetros de ejecución) y ejecute el `create-rfc` comando con los dos archivos como entrada. Ambos métodos se describen aquí.
2. Envíe el `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con el ID de RFC devuelto.

   Supervise el comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a la parte de los parámetros de la RFC de la solicitud (no a los parámetros de ejecución). Para ver una lista de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

CREACIÓN EN LÍNEA:

Ejecute el comando create RFC con los parámetros de ejecución incluidos en línea (comillas de escape al proporcionar los parámetros de ejecución en línea) y, a continuación, envíe el ID de RFC devuelto. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
aws amscm create-rfc --change-type-id "ct-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

CREACIÓN DE PLANTILLA:

1. Envía los parámetros de ejecución de este tipo de cambio a un archivo JSON; en este ejemplo se denomina Create EC2 Params.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. Modifique y guarde el archivo Create EC2 Params. Por ejemplo, puede reemplazar el contenido por algo como esto:

```
{
  "Description": "Create a new EC2 Instance stack",
  "VpcId": "vpc-0a60eb65b4EXAMPLE",
  "Name": "My-EC2",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "InstanceAmiId": "ami-1234567890EXAMPLE",
    "InstanceDetailedMonitoring": false,
    "InstanceEBSOptimized": false,
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 3000,
    "InstanceRootVolumeType": "gp3",
    "InstanceType": "t2.large",
    "InstanceUserData": "",
    "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
    "EnforceIMDSV2": "false"
  }
}
```

3. Envía la plantilla RFC a un archivo de tu carpeta actual; en este ejemplo se llama Create EC2 RFC.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. Modifique y guarde el archivo Create EC2 RFC.json. Por ejemplo, puede reemplazar el contenido por algo como esto:.

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. Cree el RFC, especificando el archivo Create EC2 Rfc y el archivo Create EC2 Params:

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.json
```

Recibirá el ID del nuevo RFC en la respuesta y podrá utilizarlo para enviar y supervisar el RFC. Hasta que la envíe, la RFC permanece en estado de edición y no se inicia.

Consejos

Grupos de seguridad

A partir de la versión 3.0 de este tipo de cambio, AMS no adjunta los grupos de seguridad AMS predeterminados si usted especifica sus propios grupos de seguridad. Si no especifica sus propios grupos de seguridad en la solicitud, AMS adjunta los grupos de seguridad predeterminados de AMS. En versiones anteriores, AMS adjuntaba los grupos de seguridad predeterminados independientemente de si proporcionaba sus propios grupos de seguridad o no.

Actualmente, si especifica grupos de seguridad personalizados, también debe especificar los grupos IDs de seguridad AMS predeterminados para su cuenta, `mc-initial-garden-SG-name` y`mc-initial-garden-SG-name`.

Tipos de instancias

AMS no recomienda los tipos t2.micro/t3.micro y t2.nano/t3.nano. Se trata de tipos de instancias más pequeños y pueden reducir el rendimiento de la aplicación y de las herramientas de AMS. EC2 las instancias necesitan capacidad suficiente para soportar herramientas de AMS, como EPS, SSM y Cloudwatch, además de la carga de trabajo de la aplicación. Para obtener más información, consulte Elegir el tipo de EC2 instancia adecuado para su aplicación.

Para crear una EC2 pila con volúmenes adicionales, consulte EC2 Stack | Create (with Additional Volumes).

Puede añadir hasta 50 etiquetas, pero para ello debe habilitar la vista de configuración adicional.

Si es necesario, consulte Error al crear la pila de EC2 instancias.

Crea una pila (con volúmenes adicionales)

Creación de una EC2 instancia y volúmenes adicionales con la consola

A continuación, se muestra este tipo de cambio en la consola AMS.

Cómo funciona:

1. Vaya a la página Crear RFC: en el panel de navegación izquierdo de la consola AMS, haga clic RFCspara abrir la página de RFCs listas y, a continuación, haga clic en Crear RFC.
2. Elija un tipo de cambio (CT) popular en la vista predeterminada de búsqueda de tipos de cambios o seleccione un CT en la vista Elegir por categoría.
   - Busque por tipo de cambio: puede hacer clic en un CT popular en el área de creación rápida para abrir inmediatamente la página Ejecutar RFC. Tenga en cuenta que no puede elegir una versión antigua de CT con Quick Create.

     Para ordenar CTs, utilice el área Todos los tipos de cambios en la vista de tarjeta o de tabla. En cualquiera de las vistas, seleccione una CT y, a continuación, haga clic en Crear RFC para abrir la página Ejecutar RFC. Si corresponde, aparece la opción Crear con una versión anterior junto al botón Crear RFC.
   - Elegir por categoría: seleccione una categoría, una subcategoría, un elemento y una operación, y se abrirá el cuadro de detalles del CT con la opción Crear con una versión anterior, si corresponde. Haga clic en Crear RFC para abrir la página Ejecutar RFC.
3. En la página Ejecutar RFC, abra el área del nombre del CT para ver el cuadro de detalles del CT. Se requiere un asunto (lo rellena automáticamente si elige su CT en la vista Buscar tipos de cambios). Abra el área de configuración adicional para añadir información sobre la RFC.

   En el área de configuración de ejecución, utilice las listas desplegables disponibles o introduzca valores para los parámetros necesarios. Para configurar los parámetros de ejecución opcionales, abra el área de configuración adicional.
4. Cuando haya terminado, haga clic en Ejecutar. Si no hay errores, aparecerá la página de la RFC creada correctamente con los detalles de la RFC enviada y el resultado inicial de la ejecución.
5. Abra el área de parámetros de ejecución para ver las configuraciones que envió. Actualice la página para actualizar el estado de ejecución de la RFC. Si lo desea, cancele la RFC o cree una copia de la misma con las opciones de la parte superior de la página.

Creación de una EC2 instancia y volúmenes adicionales con la CLI

Cómo funciona:

1. Utilice la función de creación en línea (se emite un `create-rfc` comando con todos los parámetros de ejecución y RFC incluidos) o la de plantilla (se crean dos archivos JSON, uno para los parámetros de RFC y otro para los parámetros de ejecución) y ejecute el `create-rfc` comando con los dos archivos como entrada. Ambos métodos se describen aquí.
2. Envíe el `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con el ID de RFC devuelto.

   Supervise el comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a la parte de los parámetros de la RFC de la solicitud (no a los parámetros de ejecución). Para ver una lista de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

CREACIÓN EN LÍNEA:

Ejecute el comando create RFC con los parámetros de ejecución incluidos en línea (comillas de escape al proporcionar los parámetros de ejecución en línea) y, a continuación, envíe el ID de RFC devuelto (el ejemplo muestra solo los parámetros obligatorios). Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
```

```
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

CREACIÓN DE PLANTILLA:

1. Envía los parámetros de ejecución de este tipo de cambio a un archivo JSON denominado Create EC2 AVParams .json.

```
aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
```

2. Modifique y guarde el EC2 AVParams archivo de creación (en el ejemplo se muestran la mayoría de los parámetros). Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
{
"Description":      "EC2-Create-1-Addl-Volumes",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-nn8v8ffhcal611bmo",
"Name":             "My-EC2-1-Addl-Volume",
"TimeoutInMinutes": 60,
"Parameters":   {
    "InstanceAmiId":    "AMI_ID",
    "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
    "InstanceCoreCount": 1,
    "InstanceThreadsPerCore": 2,
    "InstanceDetailedMonitoring": "true",
    "InstanceEBSOptimized": "false",
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 100,
    "InstanceRootVolumeName": "/dev/xvda",
    "InstanceRootVolumeSize": 50,
    "InstanceRootVolumeType": "io1",
    "RootVolumeKmsKeyId": "default",
    "InstancePrivateStaticIp": "10.27.0.100",
    "InstanceSecondaryPrivateIpAddressCount": 0,
    "InstanceTerminationProtection": "false",
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
```

```
    "Volume1Size":      "2 GiB",
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
    "InstanceSubnetId": "SUBNET_ID"
    }
}
```

3. Envía la plantilla RFC a un archivo de tu carpeta actual; en este ejemplo se llama Create EC2 AVRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. Modifique y guarde el archivo Create EC2 AVRfc .json. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. Cree el RFC, especificando el archivo de creación y el EC2 AVRfc archivo de creación EC2AVParams :

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.json
```

Recibirá el ID de la nueva RFC en la respuesta y podrá utilizarla para enviar y supervisar la RFC. Hasta que la envíe, la RFC permanece en estado de edición y no se inicia.

Consejos

> **Important**
>
> Hay una nueva versión de este tipo de cambio, la versión 4.0, que utiliza una versión diferente StackTemplateId (stm-nn8v8ffhcal611bmo). Esto es importante si envía la RFC con este tipo de cambio desde la línea de comandos. La nueva versión introduce dos parámetros nuevos (RootVolumeKmsKeyIdy CreditSpecification) y cambia el valor predeterminado de un parámetro existente (InstanceType).

Tipos de instancias

- Si decide especificar el número de núcleos o subprocesos, debe especificar valores para ambos. Utilice los parámetros `InstanceCoreCount` y`InstanceThreadsPerCore`. Para encontrar combinaciones válidas de núcleos o subprocesos, consulta Núcleos de CPU y subprocesos por núcleo de CPU por tipo de instancia.
- AMS no recomienda los tipos de instancia t2.micro/t3.micro o t2.nano/t3.nano. Son demasiado pequeñas para soportar las herramientas de AMS, como EPS, SSM y Cloudwatch, además de la carga de trabajo de su empresa. Para obtener más información, consulte Elegir el tipo de EC2 instancia adecuado para su aplicación.
- En la versión 4.0, el tipo predeterminado pasó de t2.large a t3.large. Las instancias T3 se lanzan con «créditos ilimitados» de forma predeterminada. La CPU no se agotará aunque la instancia consuma todos los créditos de la CPU. En su lugar, puedes elegir instancias T2 y usar la opción CreditSpecification ilimitada.
- Para obtener más información sobre Amazon EC2, incluidas las recomendaciones de tamaño, consulte la documentación de Amazon Elastic Compute Cloud.

Para actualizar tu EC2 pila con volúmenes adicionales una vez creados, consulta Pila de EC2 instancias: Actualización (con volúmenes adicionales)

Acceso, solicitud

Solicita acceso administrativo

Solicitar el acceso de administrador con la consola

A continuación se muestra este tipo de cambio en la consola AMS.

Cómo funciona:

1. Vaya a la página Crear RFC: en el panel de navegación izquierdo de la consola AMS, haga clic RFCspara abrir la página de RFCs listas y, a continuación, haga clic en Crear RFC.
2. Elija un tipo de cambio (CT) popular en la vista predeterminada de búsqueda de tipos de cambios o seleccione un CT en la vista Elegir por categoría.

- Busque por tipo de cambio: puede hacer clic en un CT popular en el área de creación rápida para abrir inmediatamente la página Ejecutar RFC. Tenga en cuenta que no puede elegir una versión antigua de CT con Quick Create.

  Para ordenar CTs, utilice el área Todos los tipos de cambios en la vista de tarjeta o de tabla. En cualquiera de las vistas, seleccione una CT y, a continuación, haga clic en Crear RFC para abrir la página Ejecutar RFC. Si corresponde, aparece la opción Crear con una versión anterior junto al botón Crear RFC.
- Elegir por categoría: seleccione una categoría, una subcategoría, un elemento y una operación, y se abrirá el cuadro de detalles del CT con la opción Crear con una versión anterior, si corresponde. Haga clic en Crear RFC para abrir la página Ejecutar RFC.

3. En la página Ejecutar RFC, abra el área del nombre del CT para ver el cuadro de detalles del CT. Se requiere un asunto (lo rellena automáticamente si elige su CT en la vista Buscar tipos de cambios). Abra el área de configuración adicional para añadir información sobre la RFC.

   En el área de configuración de ejecución, utilice las listas desplegables disponibles o introduzca valores para los parámetros necesarios. Para configurar los parámetros de ejecución opcionales, abra el área de configuración adicional.
4. Cuando haya terminado, haga clic en Ejecutar. Si no hay errores, aparecerá la página de la RFC creada correctamente con los detalles de la RFC enviada y el resultado inicial de la ejecución.
5. Abra el área de parámetros de ejecución para ver las configuraciones que envió. Actualice la página para actualizar el estado de ejecución de la RFC. Si lo desea, cancele la RFC o cree una copia de la misma con las opciones de la parte superior de la página.

Solicitud de acceso de administrador con la CLI

Cómo funciona:

1. Utilice la función de creación en línea (se emite un `create-rfc` comando con todos los parámetros de ejecución y RFC incluidos) o la de plantilla (se crean dos archivos JSON, uno para los parámetros de RFC y otro para los parámetros de ejecución) y ejecute el `create-rfc` comando con los dos archivos como entrada. Ambos métodos se describen aquí.
2. Envíe el `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con el ID de RFC devuelto.

   Supervise el comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a la parte de los parámetros de la RFC de la solicitud (no a los parámetros de ejecución). Para ver una lista de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

CREACIÓN EN LÍNEA:

Ejecute el comando create RFC con los parámetros de ejecución incluidos en línea (comillas de escape al proporcionar los parámetros de ejecución en línea) y, a continuación, envíe el ID de RFC devuelto. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
aws --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

CREACIÓN DE PLANTILLA:

1. Envía los parámetros de ejecución del esquema JSON para este tipo de cambio a un archivo; este ejemplo lo nombra GrantAdminAccessParams .json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantAdminAccessParams.json
   ```

   Modifique y guarde el GrantAdminAccessParams archivo. Por ejemplo, puede reemplazar el contenido por algo como esto:

```
{
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Username":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

Ten en cuenta que el valor predeterminado de la `TimeRequestedInHours` opción es de una hora. Puede solicitar un máximo de doce horas.

2. Envía la plantilla RFC a un archivo de tu carpeta actual; en este ejemplo se le asigna el nombre GrantAdminAccessRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
```

3. Modifique y guarde el GrantAdminAccessRfc archivo.json. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
{
"ChangeTypeId":         "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-Admin-Access-to-EC2-RFC"
}
```

4. Cree el RFC, especificando el GrantAdminAccessRfc archivo y el GrantAdminAcessParams archivo:

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.json
```

Recibirá el ID de la nueva RFC en la respuesta y podrá utilizarla para enviar y supervisar la RFC. Hasta que la envíe, la RFC permanece en estado de edición y no se inicia.

Para iniciar sesión en la instancia a través de un bastión, siga el siguiente procedimiento (Ejemplos de acceso a la instancia).

Consejos

> **Note**
>
> Puede enviar una actualización a su solicitud de acceso antes de que caduque. Para obtener más información, consulta Stack Admin Access | Update.
> Para iniciar sesión en una instancia que forma parte de un ASG, debes solicitar acceso a la pila de ASG, que te da acceso a todas las instancias asociadas.

Para ver un ejemplo sobre cómo solicitar ReadOnly acceso, consulta ReadOnly acceso: solicitud.

Solicita ReadOnly acceso

Solicitar el ReadOnly acceso con la consola

A continuación se muestra este tipo de cambio en la consola AMS.

Cómo funciona:

1. Vaya a la página Crear RFC: en el panel de navegación izquierdo de la consola AMS, haga clic RFCspara abrir la página de RFCs listas y, a continuación, haga clic en Crear RFC.
2. Elija un tipo de cambio (CT) popular en la vista predeterminada de búsqueda de tipos de cambios o seleccione un CT en la vista Elegir por categoría.
   - Busque por tipo de cambio: puede hacer clic en un CT popular en el área de creación rápida para abrir inmediatamente la página Ejecutar RFC. Tenga en cuenta que no puede elegir una versión antigua de CT con Quick Create.

     Para ordenar CTs, utilice el área Todos los tipos de cambios en la vista de tarjeta o de tabla. En cualquiera de las vistas, seleccione una CT y, a continuación, haga clic en Crear RFC para abrir la página Ejecutar RFC. Si corresponde, aparece la opción Crear con una versión anterior junto al botón Crear RFC.
   - Elegir por categoría: seleccione una categoría, una subcategoría, un elemento y una operación, y se abrirá el cuadro de detalles del CT con la opción Crear con una versión anterior, si corresponde. Haga clic en Crear RFC para abrir la página Ejecutar RFC.
3. En la página Ejecutar RFC, abra el área del nombre del CT para ver el cuadro de detalles del CT. Se requiere un asunto (lo rellena automáticamente si elige su CT en la vista Buscar tipos de cambios). Abra el área de configuración adicional para añadir información sobre la RFC.

En el área de configuración de ejecución, utilice las listas desplegables disponibles o introduzca valores para los parámetros necesarios. Para configurar los parámetros de ejecución opcionales, abra el área de configuración adicional.

4. Cuando haya terminado, haga clic en Ejecutar. Si no hay errores, aparecerá la página de la RFC creada correctamente con los detalles de la RFC enviada y el resultado inicial de la ejecución.
5. Abra el área de parámetros de ejecución para ver las configuraciones que envió. Actualice la página para actualizar el estado de ejecución de la RFC. Si lo desea, cancele la RFC o cree una copia de la misma con las opciones de la parte superior de la página.

Solicitud de ReadOnly acceso con la CLI

Cómo funciona:

1. Utilice la función de creación en línea (se emite un `create-rfc` comando con todos los parámetros de ejecución y RFC incluidos) o la de plantilla (se crean dos archivos JSON, uno para los parámetros de RFC y otro para los parámetros de ejecución) y ejecute el `create-rfc` comando con los dos archivos como entrada. Ambos métodos se describen aquí.
2. Envíe el `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con el ID de RFC devuelto.

   Supervise el comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a la parte de los parámetros de la RFC de la solicitud (no a los parámetros de ejecución). Para ver una lista de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

CREACIÓN EN LÍNEA:

Ejecute el comando create RFC con los parámetros de ejecución incluidos en línea (comillas de escape al proporcionar los parámetros de ejecución en línea) y, a continuación, envíe el ID de RFC devuelto. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
aws --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

CREACIÓN DE PLANTILLA:

1. Envía los parámetros de ejecución del esquema JSON para este tipo de cambio a un archivo; este ejemplo lo nombra GrantReadOnlyAccessParams .json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantReadOnlyAccessParams.json
   ```

   Modifique y guarde el GrantReadOnlyAccessParams archivo. Por ejemplo, puede reemplazar el contenido por algo como esto:

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   "StackIds":             [STACK_ID, STACK_ID],
   "TimeRequestedInHours": 12,
   "Usernames":             ["USERNAME", "USERNAME"],
   "VpcId":                "VPC_ID"
   }
   ```

   Ten en cuenta que el valor predeterminado de la `TimeRequestedInHours` opción es de una hora. Puede solicitar un máximo de doce horas.

2. Envía la plantilla RFC a un archivo de tu carpeta actual; en este ejemplo se le asigna el nombre GrantReadOnlyAccessRfc .json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
   ```

3. Modifique y guarde el GrantReadOnlyAccessRfc archivo.json. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
{
"ChangeTypeId":          "ct-199h35t7uz6jl",
"ChangeTypeVersion":     "3.0",
"Title":                 "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. Cree el RFC, especificando el GrantReadOnlyAccessRfc archivo y el GrantReadOnlyAcessParams archivo:

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.json
```

Recibirá el ID de la nueva RFC en la respuesta y podrá utilizarla para enviar y supervisar la RFC. Hasta que la envíe, la RFC permanece en estado de edición y no se inicia.

Para iniciar sesión en la instancia a través de un bastión, siga el siguiente procedimiento (Ejemplos de acceso a la instancia).

Consejos

> **Note**
>
> Puede enviar una actualización a su solicitud de acceso antes de que caduque. Para obtener más información, consulta Stack Read-Only Access | Update.
> Para iniciar sesión en una instancia que forma parte de un grupo de EC2 Auto Scaling (ASG), debe solicitar acceso a la pila de ASG, que le da acceso a todas las instancias asociadas.

Para ver un tutorial sobre cómo solicitar el acceso de administrador, consulta Acceso de administrador: solicitud.

Otros | Otros RFC, creación (CLI)

En este ejemplo se muestra cómo solicitar un cambio en la CTs dirección no disponible, mediante el CT Management | Other | Other | Create (ct-1e1xtak34nx76).

Utilice este CT cuando no pueda encontrar el tipo de cambio que busca; sin embargo, si no está seguro de especificar los parámetros en un CT existente, es mejor enviar una solicitud de servicio

para solicitar ayuda. Para obtener información sobre cómo enviar solicitudes de servicio, consulte los ejemplos de solicitudes de servicio.

Este tipo de RFC requiere aprobación, lo que significa que requiere la aprobación de AMS antes de poder implementarse. Tras enviar la RFC, un operador de AMS se pondrá en contacto con usted para hablar sobre la pila que desea implementar.

> **Note**
>
> Cuando utilice la opción «revisión obligatoria» CTs, AMS recomienda que utilice la opción de programación lo antes posible (elija ASAP en la consola y deje en blanco la hora de inicio y finalización en la API/CLI), ya que CTs requiere que un operador de AMS examine la RFC y, posiblemente, se comunique con usted antes de que pueda aprobarse y ejecutarse. Si las programa RFCs, asegúrese de esperar al menos 24 horas. Si la aprobación no se produce antes de la hora de inicio programada, la RFC se rechaza automáticamente.

DATOS NECESARIOS:

- `Comment`: Para qué sirve el RFC.
- `ChangeTypeIdyChangeTypeVersion`: Use Other | Create (`ct-1e1xtak34nx76`) para solicitar nuevos recursos, use Other | Update (`ct-0xdawir96cy7k`) para cambiar los recursos existentes; ambos son`v1`.

DATOS OPCIONALES`Priority`:: Los valores aceptables son `High`, `Medium`, o`Low`.

CREACIÓN EN LÍNEA:

- Ejecute el comando create RFC con los parámetros de ejecución proporcionados en línea (comillas de escape cuando se proporcionan los parámetros de ejecución en línea). El ejemplo usa Other | Create.

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- Envíe la RFC mediante el ID de RFC devuelto en la operación de creación de la RFC. Hasta que se envíe, la RFC permanece en ese `Editing` estado y no se toman medidas al respecto.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Supervise el estado de la RFC y vea el resultado de la ejecución:

```
aws amscm get-rfc --rfc-id RFC_ID
```

CREACIÓN DE PLANTILLA:

1. Cree y guarde un archivo JSON para los parámetros de ejecución; el ejemplo lo nombra OtherParams .json e incluye el `Priority` parámetro opcional:

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. Cree y guarde un archivo JSON para los parámetros de RFC; el ejemplo lo OtherRfc nombra .json.

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
"Title":                "TITLE"
}
```

3. Cree el RFC especificando el OtherRfc archivo y el archivo: OtherParams

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

   Recibirá el RfcId nuevo RFC en la respuesta. Por ejemplo:

```
{
"RfcId": "RFC-ID"
}
```

4. Envíe el RFC:

```
aws amscm submit-rfc --rfc-id RFC-ID
```

Si no se informa de ningún error, la operación se realizó correctamente.

5. Para supervisar el estado de la solicitud y ver el resultado de la ejecución:

```
aws amscm get-rfc --rfc-id RFC-ID
```

Cualquier pila: eliminar, reiniciar, iniciar, detener

Puede utilizar la consola AMS o API/CLI eliminar, reiniciar, iniciar o detener una pila AMS.

Eliminar pila

Eliminar una pila con la consola

Captura de pantalla de este tipo de cambio en la consola AMS:

Cómo funciona:

1. Vaya a la página Crear RFC: en el panel de navegación izquierdo de la consola AMS, haga clic RFCspara abrir la página de RFCs listas y, a continuación, haga clic en Crear RFC.
2. Elija un tipo de cambio (CT) popular en la vista predeterminada de búsqueda de tipos de cambios o seleccione un CT en la vista Elegir por categoría.
   - Busque por tipo de cambio: puede hacer clic en un CT popular en el área de creación rápida para abrir inmediatamente la página Ejecutar RFC. Tenga en cuenta que no puede elegir una versión antigua de CT con Quick Create.

     Para ordenar CTs, utilice el área Todos los tipos de cambios en la vista de tarjeta o de tabla. En cualquiera de las vistas, seleccione una CT y, a continuación, haga clic en Crear RFC para abrir la página Ejecutar RFC. Si corresponde, aparece la opción Crear con una versión anterior junto al botón Crear RFC.
   - Elegir por categoría: seleccione una categoría, una subcategoría, un elemento y una operación, y se abrirá el cuadro de detalles del CT con la opción Crear con una versión anterior, si corresponde. Haga clic en Crear RFC para abrir la página Ejecutar RFC.
3. En la página Ejecutar RFC, abra el área del nombre del CT para ver el cuadro de detalles del CT. Se requiere un asunto (lo rellena automáticamente si elige su CT en la vista Buscar tipos de cambios). Abra el área de configuración adicional para añadir información sobre la RFC.

En el área de configuración de ejecución, utilice las listas desplegables disponibles o introduzca valores para los parámetros necesarios. Para configurar los parámetros de ejecución opcionales, abra el área de configuración adicional.

4. Cuando haya terminado, haga clic en Ejecutar. Si no hay errores, aparecerá la página de la RFC creada correctamente con los detalles de la RFC enviada y el resultado inicial de la ejecución.
5. Abra el área de parámetros de ejecución para ver las configuraciones que envió. Actualice la página para actualizar el estado de ejecución de la RFC. Si lo desea, cancele la RFC o cree una copia de la misma con las opciones de la parte superior de la página.

Eliminar una pila con la CLI

Cómo funciona:

1. Utilice la función de creación en línea (se emite un `create-rfc` comando con todos los parámetros de ejecución y RFC incluidos) o la de plantilla (se crean dos archivos JSON, uno para los parámetros de RFC y otro para los parámetros de ejecución) y ejecute el `create-rfc` comando con los dos archivos como entrada. Ambos métodos se describen aquí.
2. Envíe el `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con el ID de RFC devuelto.

   Supervise el comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a la parte de los parámetros de la RFC de la solicitud (no a los parámetros de ejecución). Para ver una lista de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

CREACIÓN EN LÍNEA:

Ejecute el comando create RFC con los parámetros de ejecución incluidos en línea (comillas de escape al proporcionar los parámetros de ejecución en línea) y, a continuación, envíe el ID de RFC devuelto. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CREACIÓN DE PLANTILLA:

1. Envía la plantilla RFC a un archivo de tu carpeta actual; este ejemplo la nombra DeleteStackRfc .json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Modifique y guarde el DeleteStackRfc archivo.json.

   Las comillas internas de la extensión ExecutionParameters JSON deben ir precedidas de una barra invertida (\). Ejemplo sin hora de inicio y finalización:

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. Cree el RFC:

   ```
   aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
   ```

   Recibirá el ID del nuevo RFC en la respuesta y podrá utilizarlo para enviar y supervisar el RFC. Hasta que la envíe, la RFC permanece en estado de edición y no se inicia.

Consejos

> **Note**
>
> Si borras un depósito de S3, primero debes vaciarlo de objetos.

> **Important**
>
> Eliminar pilas puede tener consecuencias no deseadas e imprevistas. Para ver advertencias importantes, consulte la sección de solución de problemas de RFC para Delete StackRFCs .

Reinicie la pila

Reiniciar una pila con la consola

Captura de pantalla de este tipo de cambio en la consola AMS:

Cómo funciona:

1. Vaya a la página Crear RFC: en el panel de navegación izquierdo de la consola AMS, haga clic RFCspara abrir la página de RFCs listas y, a continuación, haga clic en Crear RFC.
2. Elija un tipo de cambio (CT) popular en la vista predeterminada de búsqueda de tipos de cambios o seleccione un CT en la vista Elegir por categoría.
   - Busque por tipo de cambio: puede hacer clic en un CT popular en el área de creación rápida para abrir inmediatamente la página Ejecutar RFC. Tenga en cuenta que no puede elegir una versión antigua de CT con Quick Create.

     Para ordenar CTs, utilice el área Todos los tipos de cambios en la vista de tarjeta o de tabla. En cualquiera de las vistas, seleccione una CT y, a continuación, haga clic en Crear RFC para abrir la página Ejecutar RFC. Si corresponde, aparece la opción Crear con una versión anterior junto al botón Crear RFC.
   - Elegir por categoría: seleccione una categoría, una subcategoría, un elemento y una operación, y se abrirá el cuadro de detalles del CT con la opción Crear con una versión anterior, si corresponde. Haga clic en Crear RFC para abrir la página Ejecutar RFC.

3. En la página Ejecutar RFC, abra el área del nombre del CT para ver el cuadro de detalles del CT. Se requiere un asunto (lo rellena automáticamente si elige su CT en la vista Buscar tipos de cambios). Abra el área de configuración adicional para añadir información sobre la RFC.

   En el área de configuración de ejecución, utilice las listas desplegables disponibles o introduzca valores para los parámetros necesarios. Para configurar los parámetros de ejecución opcionales, abra el área de configuración adicional.
4. Cuando haya terminado, haga clic en Ejecutar. Si no hay errores, aparecerá la página de la RFC creada correctamente con los detalles de la RFC enviada y el resultado inicial de la ejecución.
5. Abra el área de parámetros de ejecución para ver las configuraciones que envió. Actualice la página para actualizar el estado de ejecución de la RFC. Si lo desea, cancele la RFC o cree una copia de la misma con las opciones de la parte superior de la página.

Reiniciar una pila con la CLI

Cómo funciona:

1. Utilice la función de creación en línea (se emite un `create-rfc` comando con todos los parámetros de ejecución y RFC incluidos) o la de plantilla (se crean dos archivos JSON, uno para los parámetros de RFC y otro para los parámetros de ejecución) y ejecute el `create-rfc` comando con los dos archivos como entrada. Ambos métodos se describen aquí.
2. Envíe el `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con el ID de RFC devuelto.

   Supervise el comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a la parte de los parámetros de la RFC de la solicitud (no a los parámetros de ejecución). Para ver una lista

de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

CREACIÓN EN LÍNEA:

Ejecute el comando create RFC con los parámetros de ejecución incluidos en línea (comillas de escape al proporcionar los parámetros de ejecución en línea) y, a continuación, envíe el ID de RFC devuelto. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CREACIÓN DE PLANTILLA:

1. Envía la plantilla RFC a un archivo de tu carpeta actual. En este ejemplo se le asigna el nombre RebootStackRfc .json. Ten en cuenta que, dado que solo hay un parámetro de ejecución para detener (reiniciar o iniciar) una instancia, el parámetro de ejecución puede estar en el propio archivo JSON del esquema y no es necesario crear un archivo JSON de parámetros de ejecución independiente.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
   ```

2. Modifique y guarde el RebootStackRfc archivo.json.

   Las comillas internas de la extensión `ExecutionParameters` JSON deben ir precedidas de una barra invertida (\). Ejemplo:

   ```
   {
   "ChangeTypeId":          "ct-02u0hoaa9grat",
   "Title":                 "Reboot-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Cree el RFC:

   ```
   aws amscm create-rfc --cli-input-json file://RebootStackRfc.json
   ```

Recibirá el ID del nuevo RFC en la respuesta y podrá utilizarlo para enviar y supervisar el RFC. Hasta que la envíe, la RFC permanece en estado de edición y no se inicia.

Consejos

Para obtener información sobre los balanceadores de carga de aplicaciones, consulte Equilibradores de carga de aplicaciones.

Pila de inicio

Iniciar una pila con la consola

Captura de pantalla de este tipo de cambio en la consola AMS:

Cómo funciona:

1. Vaya a la página Crear RFC: en el panel de navegación izquierdo de la consola AMS, haga clic RFCspara abrir la página de RFCs listas y, a continuación, haga clic en Crear RFC.
2. Elija un tipo de cambio (CT) popular en la vista predeterminada de búsqueda de tipos de cambios o seleccione un CT en la vista Elegir por categoría.
   - Busque por tipo de cambio: puede hacer clic en un CT popular en el área de creación rápida para abrir inmediatamente la página Ejecutar RFC. Tenga en cuenta que no puede elegir una versión antigua de CT con Quick Create.

     Para ordenar CTs, utilice el área Todos los tipos de cambios en la vista de tarjeta o de tabla. En cualquiera de las vistas, seleccione una CT y, a continuación, haga clic en Crear RFC para abrir la página Ejecutar RFC. Si corresponde, aparece la opción Crear con una versión anterior junto al botón Crear RFC.
   - Elegir por categoría: seleccione una categoría, una subcategoría, un elemento y una operación, y se abrirá el cuadro de detalles del CT con la opción Crear con una versión anterior, si corresponde. Haga clic en Crear RFC para abrir la página Ejecutar RFC.
3. En la página Ejecutar RFC, abra el área del nombre del CT para ver el cuadro de detalles del CT. Se requiere un asunto (lo rellena automáticamente si elige su CT en la vista Buscar tipos de cambios). Abra el área de configuración adicional para añadir información sobre la RFC.

En el área de configuración de ejecución, utilice las listas desplegables disponibles o introduzca valores para los parámetros necesarios. Para configurar los parámetros de ejecución opcionales, abra el área de configuración adicional.

4. Cuando haya terminado, haga clic en Ejecutar. Si no hay errores, aparecerá la página de la RFC creada correctamente con los detalles de la RFC enviada y el resultado inicial de la ejecución.
5. Abra el área de parámetros de ejecución para ver las configuraciones que envió. Actualice la página para actualizar el estado de ejecución de la RFC. Si lo desea, cancele la RFC o cree una copia de la misma con las opciones de la parte superior de la página.

Inicio de una pila con la CLI

Cómo funciona:

1. Utilice la función de creación en línea (se emite un `create-rfc` comando con todos los parámetros de ejecución y RFC incluidos) o la de plantilla (se crean dos archivos JSON, uno para los parámetros de RFC y otro para los parámetros de ejecución) y ejecute el `create-rfc` comando con los dos archivos como entrada. Ambos métodos se describen aquí.
2. Envíe el `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con el ID de RFC devuelto.

   Supervise el comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a la parte de los parámetros de la RFC de la solicitud (no a los parámetros de ejecución). Para ver una lista de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

CREACIÓN EN LÍNEA:

Ejecute el comando create RFC con los parámetros de ejecución incluidos en línea (comillas de escape al proporcionar los parámetros de ejecución en línea) y, a continuación, envíe el ID de RFC devuelto. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CREACIÓN DE PLANTILLA:

1. Envía la plantilla RFC a un archivo de tu carpeta actual. En este ejemplo se le asigna el nombre StartInstanceRfc .json. Tenga en cuenta que, dado que solo hay un parámetro de ejecución para iniciar una pila, el parámetro de ejecución puede estar en el propio archivo JSON del esquema y no es necesario crear un archivo JSON de parámetros de ejecución independiente.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. Modifique y guarde el StartStackRfc archivo.json. Por ejemplo, puedes reemplazar el contenido por algo como esto:

   ```
   {
   "ChangeTypeId":          "ct-1h5xgl9cr4bzy",
   "Title":                 "Start-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Crea el RFC:

   ```
   aws amscm create-rfc --cli-input-json file://StartStackRfc.json
   ```

   Recibirá el ID del nuevo RFC en la respuesta y podrá utilizarlo para enviar y supervisar el RFC. Hasta que la envíe, la RFC permanece en estado de edición y no se inicia.

Consejos

Para obtener información sobre los balanceadores de carga de aplicaciones, consulte Equilibradores de carga de aplicaciones.

Detenga la pila

Detener una pila con la consola

Captura de pantalla de este tipo de cambio en la consola AMS:

Cómo funciona:

1. Vaya a la página Crear RFC: en el panel de navegación izquierdo de la consola AMS, haga clic RFCspara abrir la página de RFCs listas y, a continuación, haga clic en Crear RFC.
2. Elija un tipo de cambio (CT) popular en la vista predeterminada de búsqueda de tipos de cambios o seleccione un CT en la vista Elegir por categoría.
   - Busque por tipo de cambio: puede hacer clic en un CT popular en el área de creación rápida para abrir inmediatamente la página Ejecutar RFC. Tenga en cuenta que no puede elegir una versión antigua de CT con Quick Create.

     Para ordenar CTs, utilice el área Todos los tipos de cambios en la vista de tarjeta o de tabla. En cualquiera de las vistas, seleccione una CT y, a continuación, haga clic en Crear RFC para abrir la página Ejecutar RFC. Si corresponde, aparece la opción Crear con una versión anterior junto al botón Crear RFC.
   - Elegir por categoría: seleccione una categoría, una subcategoría, un elemento y una operación, y se abrirá el cuadro de detalles del CT con la opción Crear con una versión anterior, si corresponde. Haga clic en Crear RFC para abrir la página Ejecutar RFC.
3. En la página Ejecutar RFC, abra el área del nombre del CT para ver el cuadro de detalles del CT. Se requiere un asunto (lo rellena automáticamente si elige su CT en la vista Buscar tipos de cambios). Abra el área de configuración adicional para añadir información sobre la RFC.

   En el área de configuración de ejecución, utilice las listas desplegables disponibles o introduzca valores para los parámetros necesarios. Para configurar los parámetros de ejecución opcionales, abra el área de configuración adicional.
4. Cuando haya terminado, haga clic en Ejecutar. Si no hay errores, aparecerá la página de la RFC creada correctamente con los detalles de la RFC enviada y el resultado inicial de la ejecución.

5. Abra el área de parámetros de ejecución para ver las configuraciones que envió. Actualice la página para actualizar el estado de ejecución de la RFC. Si lo desea, cancele la RFC o cree una copia de la misma con las opciones de la parte superior de la página.

Detener una pila con la CLI

Cómo funciona:

1. Utilice la función de creación en línea (se emite un `create-rfc` comando con todos los parámetros de ejecución y RFC incluidos) o la de plantilla (se crean dos archivos JSON, uno para los parámetros de RFC y otro para los parámetros de ejecución) y ejecute el `create-rfc` comando con los dos archivos como entrada. Ambos métodos se describen aquí.
2. Envíe el `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con el ID de RFC devuelto.

   Supervise el comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Para comprobar la versión del tipo de cambio, utilice este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> Puede utilizar cualquier `CreateRfc` parámetro con cualquier RFC, forme o no parte del esquema del tipo de cambio. Por ejemplo, para recibir notificaciones cuando cambie el estado de la RFC, añada esta línea `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` a la parte de los parámetros de la RFC de la solicitud (no a los parámetros de ejecución). Para ver una lista de todos los CreateRfc parámetros, consulta la referencia de la API de administración de cambios de AMS.

CREACIÓN EN LÍNEA:

Ejecute el comando create RFC con los parámetros de ejecución incluidos en línea (comillas de escape al proporcionar los parámetros de ejecución en línea) y, a continuación, envíe el ID de RFC devuelto. Por ejemplo, puedes reemplazar el contenido por algo como esto:

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CREACIÓN DE PLANTILLA:

1. Envía la plantilla RFC a un archivo de tu carpeta actual. En este ejemplo se le asigna el nombre StopStackRfc .json. Ten en cuenta que, dado que solo hay un parámetro de ejecución para detener (reiniciar o iniciar) una instancia, el parámetro de ejecución puede estar en el propio archivo JSON del esquema y no es necesario crear un archivo JSON de parámetros de ejecución independiente.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
   ```

2. Modifique y guarde el StopStackRfc archivo.json. Por ejemplo, puedes reemplazar el contenido por algo como esto:

   ```
   {
   "ChangeTypeId":          "ct-3dgbnh6gpst4d",
   "Title":                 "Stop-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Crea el RFC:

   ```
   aws amscm create-rfc --cli-input-json file://StopInstanceRfc.json
   ```

   Recibirá el ID del nuevo RFC en la respuesta y podrá utilizarlo para enviar y supervisar el RFC. Hasta que la envíe, la RFC permanece en estado de edición y no se inicia.

Consejos

Las instancias detenidas permanecen detenidas a menos que haya programado los reinicios mediante el programador de recursos de AMS.

Si es necesario, consulta EC2 Instance Stack Stop Fail.

Ejemplos de acceso

Estos ejemplos muestran cómo iniciar sesión en una instancia a través de un bastión una vez que se te ha concedido el acceso mediante una RFC. Para obtener más información sobre cómo obtener el acceso, consulta Solicitudes de acceso.

> **Note**
>
> Una EC2 instancia creada a través de un grupo de Auto Scaling tendrá una dirección IP que entra y sale cíclicamente y tendrá que usar la EC2 consola para encontrar esa dirección IP.

Datos necesarios:

- Nombre descriptivo o dirección IP de DNS de Bastion: utilice un nombre descriptivo de DNS como se describe en Nombres de bastiones compatibles con DNS o busque direcciones IP de bastión como se describe en. Búsqueda de direcciones IP de bastión
- Nombre de usuario (por ejemplo, username@customerdomain.com) y contraseña: credenciales de la cuenta.
- Dirección IP de la pila: consulta la página de pilas de la consola AMS para ver la pila en la que quieres iniciar sesión y, a continuación, filtra el ID de pila en la EC2 consola de tu cuenta. Para una sola EC2 instancia, también puede utilizar el comando AMS SKMS. Para la referencia de la API AMS SKMS, consulte la pestaña Informes de la consola AWS Artifact. Para encontrar el ID de la pila y, a continuación, para obtener la referencia de la API AMS SKMS, consulte la pestaña Informes de la consola AWS Artifact. Para encontrar la dirección IP de la pila.

Acceda a la dirección IP del bastión, ya sea SSH o RDP, según corresponda, e inicie sesión mediante uno de los siguientes procedimientos.

De ordenador Linux a instancia de Linux

Usa SSH para conectarte al bastión de SSH y, después, a la instancia de Linux.

MALZ

Para obtener más información sobre los nombres fáciles de usar para los bastiones, consulta los bastiones de DNS.

Para conectarse a la instancia de Linux, primero debe conectarse a un bastión SSH.

1. Abre una ventana de shell e introduce:

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

Este sería el siguiente si tu dominio_FQDN es «corp.domain.com», tu número de cuenta es «123456789123», tu dominio es «amazonaws.com», eliges Bastion «4" y tu nombre de usuario es" «: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. Inicie sesión con sus credenciales corporativas de Active Directory.
3. Cuando aparezca un mensaje de Bash, inicie sesión con SSH en la instancia y, a continuación, introduzca:

```
ssh Domain_FQDN\\Username@Instance_IP
```

O bien, puedes usar el indicador de inicio de sesión (-l):

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

Para obtener más información sobre los nombres amigables de los bastiones, consulta los bastiones de DNS.

Para conectarse a la instancia de Linux, primero debe conectarse a un bastión SSH.

1. Abre una ventana de shell e introduce:

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
    or SSH_BASTION_IP
```

Se vería así si tu número de cuenta es 123456789123, eliges Bastion 4 y tu nombre de usuario es: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. Inicie sesión con sus credenciales corporativas de Active Directory.
3. Cuando aparezca un mensaje de Bash, inicie sesión con SSH en la instancia y, a continuación, introduzca:

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

O bien, puedes usar el indicador de inicio de sesión (-l):

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Instancia de ordenador Linux a Windows

Usa un túnel SSH y un cliente RDP para conectarte a una instancia de Windows desde tu ordenador Linux.

MALZ

Este procedimiento requiere un cliente de Conexión a Escritorio remoto para Linux; el ejemplo usa Microsoft Remote Desktop (un cliente UNIX de código abierto para conectarse a los Servicios de Escritorio remoto de Windows). Rdesktop es una alternativa.

> **Note**
>
> La forma de iniciar sesión en las instancias de Windows puede cambiar en función del cliente de escritorio remoto que se utilice.

Primero se establece un túnel SSH y, a continuación, se inicia sesión.

Para obtener más información sobre los nombres de los bastiones amistosos, consulte. Nombres de bastiones compatibles con DNS

Antes de empezar:

- Solicite acceso a la instancia a la que desee conectarse; para obtener más información, consulte Solicitudes de acceso.
- Elige un nombre de bastión DNS SSH fácil de entender al que conectarte; por ejemplo:

```
sshbastion(1-4).Your_Domain
```

Este sería el siguiente si tu Domain_FQDN es «corp.domain.com», tu Your_Domain gestionado por AMS es «amazonaws.com», eliges el bastión «4" y tu nombre de usuario es" «: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- Busca la dirección IP de la instancia a la que quieres conectarte; para obtener más información, consulta Cómo encontrar un ID de instancia o una dirección IP.

1. Configura RDP a través de un túnel SSH desde un escritorio Linux a una instancia de Windows. Para `ssh` ejecutar el comando con los valores correctos, hay dos maneras de proceder:

   - En el shell de Linux, defina las variables y, a continuación, introduzca el comando de conexión SSH:

     ```
     BASTION="sshbastion(1-4).Your_Domain""
     WINDOWS="Windows_Instance_Private_IP"
     AD="AD_Account_Number"
     USER="AD_Username"
     ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
     ```

     Por ejemplo, si se utilizan los siguientes valores:

     ```
     BASTION="sshbastion4.A123456789123.amazonaws.com"

     WINDOWS="172.16.3.254"

     AD="ACORP_example"

     USER="john.doe"
     ```

   - Añada los valores de las variables directamente al `ssh` comando.

   En cualquier caso, esto es lo que sería la solicitud renderizada (suponiendo el mismo conjunto de valores de variables):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. O bien: abra su cliente de escritorio remoto, introduzca la dirección y el puerto del bucle invertido 127.0.0. 1:3389 y, a continuación, abra la conexión.

   O bien, inicia sesión en la instancia de Windows desde una nueva consola de escritorio Linux. Si lo usas RDesktop, el comando tendrá el siguiente aspecto:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Aparece una ventana de escritorio remoto para la instancia de Windows en el escritorio de Linux.

   > **Tip**
   >
   > Si la sesión de escritorio remoto no se inicia, comprueba que la conectividad de red con la instancia de Windows desde el bastión SSH esté permitida en el puerto 3389 del shell en el paso 1 (`private_ip_address_of_windows_instance`sustitúyalo según corresponda):
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```
   >
   > Éxito:
   >
   > ```
   > nc 172.16.0.83 3389 -v -z
   >        Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
   >        netstat -anvp | grep 3389
   >        tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   > ```

SALZ

Este procedimiento para una zona de landing con una sola cuenta requiere un cliente de Conexión a Escritorio remoto para Linux; en el ejemplo se utiliza Microsoft Remote Desktop (un cliente UNIX de código abierto para conectarse a los Servicios de Escritorio Remoto de Windows). Rdesktop es una alternativa.

> **Note**
>
> La forma de iniciar sesión en las instancias de Windows puede cambiar en función del cliente de escritorio remoto que se utilice.

Primero se establece un túnel SSH y, a continuación, se inicia sesión.

Para obtener más información sobre los nombres de los bastiones amistosos, consulte. Nombres de bastiones compatibles con DNS

Antes de empezar:

- Solicite acceso a la instancia a la que desee conectarse; para obtener más información, consulte Solicitudes de acceso.
- Elige un nombre de bastión DNS SSH fácil de entender al que conectarte; por ejemplo:

  ```
  sshbastion(1-4).AAMSAccountNumber.amazonaws.com
  ```

  Este sería el siguiente si tu número de cuenta es 123456789123 y eliges el bastión 4:

  ```
  sshbastion4.A123456789123.amazonaws.com
  ```

- Busca la dirección IP de la instancia a la que quieres conectarte; para obtener más información, consulta Cómo encontrar un ID de instancia o una dirección IP.

1. Configura RDP a través de un túnel SSH desde un escritorio Linux a una instancia de Windows. Para `ssh` ejecutar el comando con los valores correctos, hay dos maneras de proceder:

   - En el shell de Linux, defina las variables y, a continuación, introduzca el comando de conexión SSH:

     ```
     BASTION="sshbastion(1-4).AAMSAccountNumber.amazonaws.com"
     WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
     AD="AD_ACCOUNT_NUMBER"
     USER="AD_USERNAME"
     ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
     ```

Por ejemplo, si se utilizan los siguientes valores:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"

WINDOWS="172.16.3.254"

AD="ACORP_example"

USER="john.doe"
```

- Añada los valores de las variables directamente al `ssh` comando.

En cualquier caso, esto es lo que sería la solicitud renderizada (suponiendo el mismo conjunto de valores de variables):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. O bien: abra su cliente de escritorio remoto, introduzca la dirección y el puerto del bucle invertido 127.0.0. 1:3389 y, a continuación, abra la conexión.

   O bien, inicia sesión en la instancia de Windows desde una nueva consola de escritorio Linux. Si lo usas RDesktop, el comando tendrá el siguiente aspecto:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Aparece una ventana de escritorio remoto para la instancia de Windows en el escritorio de Linux.

   > **Tip**
   >
   > Si la sesión de escritorio remoto no se inicia, comprueba que la conectividad de red con la instancia de Windows desde el bastión SSH esté permitida en el puerto 3389 del shell en el paso 1 (`private_ip_address_of_windows_instance`sustitúyalo según corresponda):
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```
   >
   > Éxito:

```
nc 172.16.0.83 3389 -v -z
        Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
        netstat -anvp | grep 3389
        tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

De un ordenador Windows a una instancia de Windows

Utilice el cliente de conexión a escritorio remoto de Windows para conectarse a una instancia de Windows desde un ordenador Windows.

MALZ

Para obtener más información sobre los nombres amigables de los bastiones, consulteNombres de bastiones compatibles con DNS.

1. Abra el programa Remote Desktop Connection, un programa estándar de Windows, e introduzca el nombre DNS descriptivo del bastión de Windows en el campo del nombre de host.

2. Elija Conectar. La conexión a escritorio remoto intenta establecer una conexión RDP con el bastión.

   Si se realiza correctamente, se abre un cuadro de diálogo de credenciales. Para obtener acceso, utilice sus credenciales corporativas de Active Directory, como lo haría con la instancia de Windows.

3. Abre el programa Remote Desktop Connection en el bastión e introduce la dirección IP de la instancia de Windows a la que te quieres conectar (por ejemplo, 10.0.0.100) y, a continuación, selecciona Connect. Vuelve a necesitar sus credenciales corporativas de Active Directory antes de conectarse a la instancia de Windows.

SALZ

Para obtener más información sobre los nombres descriptivos de los bastiones, consulteNombres de bastiones compatibles con DNS.

1. Abra el programa Remote Desktop Connection, un programa estándar de Windows, e introduzca el nombre DNS descriptivo del bastión de Windows en el campo del nombre de host; por ejemplo`rdpbastion`*`(1-4)`*`.A`*`AMSAccountNumber`*`.amazonaws.com`, que tendría este aspecto si su número de cuenta es 123456789123 y elige Bastion 4,. `rdpbastion4.A123456789123.amazonaws.com`

2. Elija Conectar. La conexión a escritorio remoto intenta establecer una conexión RDP con el bastión.

   Si se realiza correctamente, se abre un cuadro de diálogo de credenciales. Para obtener acceso, utilice sus credenciales corporativas de Active Directory, como lo haría con la instancia de Windows.

3. Abre el programa Remote Desktop Connection en el bastión e introduce la dirección IP de la instancia de Windows a la que te quieres conectar (por ejemplo, 10.0.0.100) y, a continuación, selecciona Connect. Vuelve a necesitar sus credenciales corporativas de Active Directory antes de conectarse a la instancia de Windows.

Instancia de ordenador Windows a Linux

Para realizar un RDP a un bastión de SSH desde un entorno Windows, sigue estos pasos.

MALZ

Antes de empezar:

- Solicita acceso a la instancia a la que quieres conectarte; para obtener más información, consulta Solicitudes de acceso.
- Elige un nombre de bastión DNS SSH fácil de entender al que conectarte; por ejemplo:

```
sshbastion(1-4).YOUR_DOMAIN
```

Este tendría este aspecto si «YOUR_DOMAIN» es «myamsaddomain.com» y eliges el bastión 4:

```
sshbastion4.myamsaddomain.com
```

- Busca la dirección IP de la instancia a la que quieres conectarte; para obtener más información, consulta Cómo encontrar un ID de instancia o una dirección IP.

Para conectarte a la instancia de Linux desde tu máquina Windows, primero debes conectarte a un bastión de SSH.

Utilice el cliente OpenSSH nativo de Windows o instale PuTTY en su máquina local. Para obtener más información sobre OpenSSH, consulte OpenSSH en Windows.

1. Usa el Windows nativo o abre PuTTY e ingresa el nombre de host del bastión SSH o la dirección IP del bastión SSH. Por ejemplo, 10.65.2.214 (22 es el puerto utilizado para SSH; se configurará de forma predeterminada).
2. OpenSSH o PuTTY intentan establecer una conexión SSH con el bastión y abrir una ventana de shell.
3. Use sus credenciales corporativas de Active Directory como lo haría con los hosts RDP para obtener acceso.
4. Cuando aparezca un mensaje de Bash, introduce SSH en la instancia. Escriba:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

Antes de empezar:

- Solicita acceso a la instancia a la que quieres conectarte; para obtener más información, consulta Solicitudes de acceso.
- Elige un nombre de bastión DNS SSH fácil de entender al que conectarte; por ejemplo:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

Este sería el siguiente si tu número de cuenta es 123456789123 y eliges el bastión 4:

```
sshbastion4.A123456789123.amazonaws.com
```

- Busca la dirección IP de la instancia a la que quieres conectarte; para obtener más información, consulta Cómo encontrar un ID de instancia o una dirección IP.

Para conectarte a la instancia de Linux desde tu máquina Windows, primero debes conectarte a un bastión de SSH.

Utilice el cliente OpenSSH nativo de Windows o instale PuTTY en su máquina local. Para obtener más información sobre OpenSSH, consulte OpenSSH en Windows.

1. Usa el Windows nativo o abre PuTTY e ingresa el nombre de host del bastión SSH o la dirección IP del bastión SSH. Por ejemplo, 10.65.2.214 (22 es el puerto utilizado para SSH; se configurará de forma predeterminada).
2. OpenSSH o PuTTY intentan establecer una conexión SSH con el bastión y abrir una ventana de shell.
3. Use sus credenciales corporativas de Active Directory como lo haría con los hosts RDP para obtener acceso.
4. Cuando aparezca un mensaje de Bash, introduce SSH en la instancia. Escriba:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

Reportar un incidente

Utilice la consola AMS para informar de un incidente. Es importante crear un incidente nuevo para cada problema o pregunta nuevos. Al abrir casos relacionados con consultas antiguas, es útil incluir el número de caso correspondiente para que podamos consultar la correspondencia anterior.

> **Note**
>
> Si la correspondencia del caso no coincide con la emisión original, un operador de AMS podría pedirte que denuncies un nuevo incidente.

Para informar de un incidente mediante la consola AMS:

1. En el panel de navegación de la izquierda, selecciona Incidentes

   Se abre la lista de incidentes:

   Si la lista de incidentes está vacía, la opción Borrar filtro restablece el filtro al estado Cualquier.

Si sabe que quiere usar el teléfono o el chat, haga clic en Crear incidente en Support Center para abrir la página Crear incidente en la consola del Support Center, que se rellena automáticamente con el tipo de servicio AMS.

> **Important**
>
> - Las llamadas telefónicas iniciadas con Soporte se graban para mejorar la respuesta. Si la llamada se interrumpe, debe volver a llamar a través del Support Center, no AWS tiene ningún mecanismo para devolverle la llamada.
> - El soporte telefónico y por chat está diseñado para ayudar con casos de asistencia, incidentes y solicitudes de servicio, no con RFC o problemas de seguridad.
> - Si tiene problemas con el RFC, utilice la opción de correspondencia de la página de detalles del RFC correspondiente para ponerse en contacto con un ingeniero de AMS.
> - Para problemas de seguridad, cree un caso de soporte de alta prioridad (P1 o P2). La función de chat en vivo no es para eventos de seguridad.

2. Si desea buscar un incidente existente, seleccione un filtro de estado del incidente en la lista desplegable.

	• Todos los incidentes que aún no se han resuelto. • Un incidente nuevo que aún no está asignado. • Un incidente que se ha asignado. • Un incidente que reabriste. • Un incidente complicado y asignado. • Incidentes que requieren tu opinión antes del siguiente paso. • Incidentes sobre los que has enviado información recientemente. • Un incidente que ha concluido.

- Todos los incidentes de la cuenta.

3. Seleccione Crear.

   Se abre la página Crear un incidente:

4. Seleccione una prioridad:

   - Bajo: las funciones no críticas de su servicio o aplicación empresarial relacionadas con los recursos de AWS/AMS se ven afectadas.
   - Medio: un servicio o aplicación empresarial relacionado con los recursos de AWS/AMS se ve afectado moderadamente y funciona en un estado degradado.
   - Alto: su empresa se ve afectada de forma significativa. Las funciones críticas de su aplicación relacionadas con los recursos de AWS/AMS no están disponibles. Reservado para las interrupciones más críticas que afectan a los sistemas de producción.

5. Seleccione una categoría.

   > **Note**
   >
   > Si va a probar la funcionalidad de los incidentes, añada la marca de no acción (AMSTestNoOpsActionRequired) al título del incidente.

6. Introduzca la información de:

   - Asunto: un título descriptivo para el informe del incidente.
   - Correos electrónicos CC: una lista de direcciones de correo electrónico de las personas a las que desea que se les informe sobre el informe y la resolución del incidente.
   - Detalles: una descripción completa del incidente, los sistemas afectados y el resultado esperado de la resolución. Responda a las preguntas preestablecidas o elimínelas e introduzca la información pertinente.

   Para añadir un adjunto, seleccione Añadir adjunto, busque el adjunto que desee y pulse Abrir. Para eliminar el archivo adjunto, haga clic en el icono Eliminar:

7. Elija Enviar.

Se abre una página de detalles con información sobre el incidente (como el tipo, el asunto, la creación, la identificación y el estado) y un área de correspondencia que incluye la descripción de la solicitud que has creado.

Haga clic en Responder para abrir un área de correspondencia y proporcionar detalles adicionales o actualizaciones del estado.

Haga clic en Cerrar caso cuando se haya resuelto el incidente.

Haga clic en Cargar más si hay más correspondencia de la que cabe en una página.

¡No olvides calificar la comunicación!

El incidente aparece en la página de lista de incidentes.

Crear una solicitud de servicio

Para crear una solicitud de servicio mediante la consola AWS Managed Services (AMS):

1. En el menú de navegación de la izquierda, seleccione Solicitudes de servicio.

   Se abre la lista de solicitudes de servicio.

   Si la lista de solicitudes de servicio está vacía, la opción Borrar filtro restablece el filtro al estado Cualquier.

   Si sabe que quiere usar el teléfono o el chat, haga clic en Crear solicitud de servicio en Support Center para abrir la página Crear solicitud de servicio en la consola del Support Center, que se rellena automáticamente con el tipo de servicio AMS.

   > **Note**
   >
   > Las llamadas telefónicas iniciadas en Soporte el centro se graban para mejorar la respuesta. Si la llamada se interrumpe, debe volver a llamar a través del Support Center, no AWS tiene ningún mecanismo para devolverle la llamada.

> **Important**
>
> El soporte telefónico y por chat está diseñado para ayudar con los casos de asistencia, los incidentes y las solicitudes de servicio. Si tiene problemas con el RFC, utilice la opción de correspondencia de la página de detalles del RFC correspondiente para ponerse en contacto con un ingeniero de AMS.

2. Si desea buscar una solicitud de servicio existente, seleccione un filtro de estado de la solicitud de servicio en la lista desplegable.

   - Todas las solicitudes de servicio que aún no se han resuelto.
   - Una nueva solicitud de servicio que aún no está asignada.
   - Una solicitud de servicio que se ha asignado.
   - Una solicitud de servicio que ha vuelto a abrir.
   - Una solicitud de servicio complicada y asignada.
   - Solicitudes de servicio que requieren tu opinión antes del siguiente paso.
   - Solicitudes de servicio para las que ha enviado información recientemente.
   - Una solicitud de servicio que ha finalizado.
   - Todas las solicitudes de servicio de la cuenta.

3. Seleccione Crear.

   Se abre la página Crear una solicitud de servicio.

4. Seleccione una categoría.

> **Note**
>
> Si va a probar la funcionalidad de la solicitud de servicio, añada el indicador de no acción,`AMSTestNoOpsActionRequired`. al título de la solicitud de servicio.

5. Introduzca la información de:

   - Asunto: Esto crea un enlace a los detalles de la solicitud de servicio en la página de la lista.
   - Correos electrónicos CC: estos correos electrónicos reciben correspondencia además de tus contactos de correo electrónico predeterminados.
   - Detalles: proporciona aquí tanta información como sea posible.

   Para agregar un archivo adjunto, seleccione Agregar archivo adjunto, busque el archivo adjunto que desee y haga clic en Abrir. Para eliminar el archivo adjunto, haga clic en el icono Eliminar:

6. Elija Enviar.

   Se abre una página de detalles con información sobre la solicitud de servicio (como el tipo, el asunto, la creación, el identificador y el estado) y un área de correspondencia que incluye la descripción de la solicitud que ha creado.

   Además, su solicitud de servicio aparece en la página de lista de solicitudes de servicio. Utilícela cuando reciba una alerta pero todavía no haya recibido noticias de AMS.

   Haga clic en Responder para abrir un área de correspondencia y proporcionar detalles adicionales o actualizaciones de estado.

   Haga clic en Resolver caso cuando se haya resuelto la solicitud de servicio.

   Haga clic en Cargar más para ver las correspondencias adicionales que no caben en la página inicial.

   ¡No olvides calificar la comunicación!

Para consultas relacionadas con la facturación, utilice la otra categoría en la consola de AMS, `ChangeTypeId ct-1e1xtak34nx76` en la API CM de AMS o `IssueType=AMS` en la API de AWS Support.

Pasos posteriores a la incorporación

Ahora que has creado una cuenta de AMS, querrás leer más documentación de AMS. Consulta estos documentos:

- A continuación, los tutoriales sobre cómo utilizar la pila HA de dos niveles CT para crear una WordPress pila completamente funcional ofrecen una experiencia AMS completa.
- Guía del usuario de AMS: la guía del usuario de AMS describe las funciones de AMS, enumera los términos clave, las operaciones y las interfaces y proporciona una descripción general de una arquitectura de infraestructura gestionada típica de AMS. Además, se proporcionan los detalles de la administración de acceso y los valores predeterminados de AMS. También se proporcionan descripciones detalladas de cómo utilizar el sistema de gestión de cambios AMS y se proporcionan varios tutoriales. También se describen conceptos de gestión adicionales.
- Referencia de la API de AMS: esta referencia de la API proporciona descripciones de todas las llamadas a la API, incluidas las solicitudes, las respuestas y algunos ejemplos.
- Guía de aplicaciones de AMS: la guía de aplicaciones de AMS describe diferentes opciones y métodos para implementar y mantener las aplicaciones en AMS.

Tutoriales

Los siguientes tutoriales detallan los pasos para crear una pila de dos niveles con el CT de alta disponibilidad (avanzado) (ct-06mjngx5flwto), mediante la CLI y la consola. Se proporciona un tutorial para implementar un grupo de Auto Scaling (ASG) de Linux y para implementar un ASG de Windows.

Las descripciones de todas las opciones de CT, incluidas, ChangeTypeId se encuentran en la referencia de tipos de cambio de AMS.

Tutorial de CLI: pila de dos niveles de alta disponibilidad (Linux/RHEL)

En esta sección se describe cómo implementar una pila de dos niveles de alta disponibilidad (HA) en un entorno AMS mediante la CLI de AMS.

> **Note**
>
> Este tutorial de implementación se ha probado en entornos AMZN Linux y RHEL.

Resumen de las tareas y requisitos: RFCs

1. Cree una infraestructura (pila de dos niveles de alta disponibilidad)
2. Cree un bucket de S3 para aplicaciones CodeDeploy
3. Cree el paquete de WordPress aplicaciones y cárguelo en el bucket de S3
4. Implemente la aplicación con CodeDeploy
5. Acceda al WordPress sitio e inicie sesión para validar la implementación

Antes de empezar

Deployment | Advanced Stack Components | High Availability Two Tier Stack Advanced | Create CT crea un grupo de Auto Scaling, un balanceador de cargas, una base de datos y un nombre de CodeDeploy aplicación y un grupo de implementación (con el mismo nombre que le dé a la aplicación). Para obtener más información, CodeDeploy consulte ¿Qué es? CodeDeploy

Este tutorial utiliza una RFC de dos niveles (avanzada) de alta disponibilidad que incluye UserData y también describe cómo crear un WordPress paquete que CodeDeploy se pueda implementar.

Lo que `UserData` se muestra en el ejemplo obtiene los metadatos de la instancia, como el ID de la instancia, la región, etc., de una instancia en ejecución consultando el servicio de metadatos de la EC2 instancia disponible en http://169.254.169.254/latest/meta-data/. Esta línea del script de datos de usuario:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, recupera el nombre de la zona de disponibilidad del servicio de metadatos y lo coloca en la variable $REGION de las regiones admitidas y lo usa para completar la URL del depósito de S3 donde se descarga el agente. CodeDeploy La IP 169.254.169.254 solo se puede enrutar dentro de la VPC (todos pueden consultar el servicio). VPCs Para obtener información sobre el servicio, consulte Metadatos de instancia y datos de usuario. Tenga en cuenta también que los scripts introducidos como UserData se ejecutan como usuario «root» y no necesitan usar el comando «sudo».

Este tutorial deja los siguientes parámetros en el valor predeterminado (que se muestra):

- Grupo Auto Scaling:`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.
- Load Balancer:. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Base de datos:`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Solicitud:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.
- Cubeta S3:`AccessControl=Private`.

AJUSTES ADICIONALES:

`RequestedStartTime`y `RequestedEndTime` si quieres programar tu RFC: puedes usar Time.is para determinar la hora UTC correcta. Los ejemplos proporcionados deben ajustarse adecuadamente. Una RFC no puede continuar si ha pasado la hora de inicio. Como alternativa, puede omitir esos valores para crear un RFC ASAP que se ejecute en cuanto se aprueben las aprobaciones.

> **Note**
>
> Hay muchos parámetros que puede elegir configurar de forma diferente a la que se muestra. Los valores de los parámetros que se muestran en el ejemplo se han probado, pero es posible que no sean adecuados para usted.

Cree la infraestructura

Si recopila los siguientes datos antes de empezar, la implementación será más rápida.

LOS DATOS NECESARIOS TIENEN UNA PILA:

- AutoScalingGroup:
  - `UserData`: Este valor se proporciona en este tutorial. Incluye comandos para configurar el recurso CodeDeploy e iniciar el CodeDeploy agente.
  - `AMI-ID`: Este valor determina qué tipo de EC2 instancias activará su grupo de Auto Scaling (ASG). Asegúrese de seleccionar una AMI en su cuenta que comience por «customer-» y que sea del sistema operativo que desee. Busque la AMI IDs con la referencia de la API SKMS de AMS, consulte la pestaña Informes de la consola AWS Artifact Console. Operation (CLI: list-amis) o en la consola AMS -> página de detalles. VPCs VPCs Este tutorial es para ASGs configurar el uso de una AMI de Linux.
- Base de datos:
  - Estos parámetros, `DBEngineEngineVersion`, y `LicenseModel` deben configurarse de acuerdo con su situación, aunque se han probado los valores que se muestran en el ejemplo.
  - Estos parámetros, `RDSSubnetIds` `DBNameMasterUsername`, y `MasterUserPassword` son necesarios para implementar el paquete de aplicaciones. Para RDSSubnet los identificadores, utilice dos subredes privadas.
- LoadBalancer:
  - Estos parámetros, `DBEngineEngineVersion`, y `LicenseModel` deben configurarse de acuerdo con su situación, aunque se han probado los valores que se muestran en el ejemplo.
  - `ELBSubnetIds`: Utilice dos subredes públicas.
- Aplicación: el `ApplicationName` valor establece el nombre de la CodeDeploy aplicación y el nombre del grupo de CodeDeploy implementación. Se usa para implementar la aplicación. Debe ser único en la cuenta. Para comprobar los CodeDeploy nombres de su cuenta, consulte la CodeDeploy consola. En el ejemplo se usa WordPress "" pero, si va a utilizar ese valor, asegúrese de que no esté ya en uso.

Este procedimiento utiliza el CT de pila de dos niveles (avanzado) de alta disponibilidad (ct-06mjngx5flwto) y el CT de almacenamiento Create S3 (ct-1a68ck03fn98r). Desde su cuenta autenticada, siga estos pasos en la línea de comandos.

1. Lanza la pila de infraestructuras.

a. Envía los parámetros de ejecución del esquema JSON de la pila de dos niveles de alta disponibilidad (CT) a un archivo de tu carpeta actual denominado CreateStackParams .json.

```
aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateStackParams.json
```

b. Modifique el esquema. *variables*Sustitúyala según proceda. Por ejemplo, utilice el sistema operativo que desee para las EC2 instancias que cree el ASG. Guárdelo`ApplicationName`, ya que lo usará más adelante para implementar la aplicación. Tenga en cuenta que puede añadir hasta 50 etiquetas.

```
{
"Description":      "HA two tier stack for WordPress",
"Name":             "WordPressStack",
"TimeoutInMinutes":  360,
"Tags": [
        {
            "Key": "ApplicationName",
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
            service httpd start \n
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
```

```
    },
    "Database":     {
        "DBEngine":             "MySQL",
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
    },
    "Application":  {
    "ApplicationName":  "WordPress"
        }
}
```

c. Envía la plantilla CreateRfc JSON a un archivo de tu carpeta actual denominado CreateStackRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. Modifique la plantilla RFC de la siguiente manera y guárdela; puede eliminar y reemplazar el contenido. Tenga en cuenta que `RequestedStartTime` ahora `RequestedEndTime` son opcionales; al excluirlos, se crea un RFC lo antes posible que se ejecuta tan pronto como se aprueba (lo que normalmente ocurre automáticamente). Para enviar una RFC programada, añada esos valores.

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. Cree el RFC especificando el CreateStackRfc archivo.json y el archivo de parámetros de ejecución CreateStackParams .json:

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

Recibirás el ID de RFC en la respuesta. Guarde el ID para los pasos siguientes.

f. Envíe el RFC:

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

Si la RFC es correcta, no recibirá ningún resultado.

g. Para comprobar el estado del RFC, ejecute

```
aws amscm get-rfc --rfc-id RFC_ID
```

Anote el ID de RFC.

2. Lance un bucket de S3

Si recopila los siguientes datos antes de empezar, la implementación será más rápida.

DEPÓSITO S3 DE DATOS NECESARIO:

- `VPC-ID`: Este valor determina dónde estará su bucket de S3. Use el mismo ID de VPC que utilizó anteriormente.
- `BucketName`: Este valor establece el nombre del bucket de S3, que se utiliza para cargar el paquete de aplicaciones. Debe ser único en toda la región de la cuenta y no puede incluir letras mayúsculas. No BucketName es obligatorio incluir tu ID de cuenta como parte de él, pero te permitirá identificar el segmento más adelante con más facilidad. Para ver qué nombres de bucket de S3 existen en la cuenta, vaya a la consola de Amazon S3 de su cuenta.

a. Genere los parámetros de ejecución del esquema JSON para el CT de creación del almacenamiento de S3 en un archivo JSON denominado CreateS3 StoreParams .json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3StoreParams.json
```

b. Modifique el esquema de la siguiente manera, puede eliminar y reemplazar el contenido. Reemplace *VPC_ID* adecuadamente. Los valores del ejemplo se han probado, pero es posible que no sean adecuados para usted.

> **Tip**
>
> `BucketName`Deben ser únicos en la región de la cuenta y no pueden incluir letras mayúsculas. No BucketName es obligatorio incluir tu ID de cuenta como parte de él, pero te permitirá identificar el segmento más adelante con más facilidad. Para ver qué nombres de bucket de S3 existen en la cuenta, vaya a la consola de Amazon S3 de su cuenta.

```
{
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. Envía la plantilla JSON CreateRfc a un archivo, en tu carpeta actual, denominado CreateS3 StoreRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. Modifique y guarde el archivo CreateS3 StoreRfc .json. Puede eliminar y reemplazar el contenido. Tenga en cuenta que `RequestedStartTime` ahora `RequestedEndTime` son opcionales; al excluirlos, se crea un RFC ASAP que se ejecuta tan pronto como se aprueba (lo que normalmente ocurre automáticamente). Para enviar una RFC programada, añada esos valores.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. Cree el RFC especificando el archivo CreateS3 StoreRfc .json y el archivo de parámetros de ejecución StoreParams CreateS3 .json:

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

Recibirá el nuevo RFC en RfcId la respuesta. Guarde el ID para los pasos siguientes.

f. Envíe el RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Si la RFC es correcta, no recibirá ningún resultado.

g. Para comprobar el estado del RFC, ejecute

```
aws amscm get-rfc --rfc-id RFC_ID
```

Crear, cargar e implementar la aplicación

En primer lugar, cree un paquete de WordPress aplicaciones y, a continuación, utilice el CodeDeploy CTs para crear e implementar la aplicación.

1. Descargue WordPress, extraiga los archivos y cree un. directorio /scripts.

   Comando de Linux:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: pégalo `https://github.com/WordPress/WordPress/archive/master.zip` en una ventana del navegador y descarga el archivo zip.

   Cree un directorio temporal en el que ensamblar el paquete.

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: cree un directorio WordPress «», utilizará la ruta del directorio más adelante.

2. Extraiga la WordPress fuente al directorio WordPress «» y cree un. directorio /scripts.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows: vaya al directorio «WordPress» que creó y cree allí un directorio de «scripts».

   Si se encuentra en un entorno Windows, asegúrese de establecer el tipo de interrupción de los archivos de script en Unix (LF). En Notepad ++, esta opción se encuentra en la parte inferior derecha de la ventana.

3. Cree el archivo CodeDeploy appspec.yml en el WordPress directorio (si va a copiar el ejemplo, compruebe la hendidura, cada espacio cuenta). IMPORTANTE: Asegúrese de que la ruta «fuente» sea correcta para copiar los WordPress archivos (en este caso, en su WordPress directorio) al destino esperado (/). var/www/html/WordPress En el ejemplo, el archivo appspec.yml está en el directorio con los WordPress archivos, por lo que solo se necesita «/». Además, aunque haya utilizado una AMI de RHEL para su grupo de Auto Scaling, deje la línea «os: linux» tal como está. Ejemplo de archivo appspec.yml:

   ```
   version: 0.0
   os: linux
   files:
     - source: /
       destination: /var/www/html/WordPress
   hooks:
     BeforeInstall:
       - location: scripts/install_dependencies.sh
         timeout: 300
         runas: root
     AfterInstall:
       - location: scripts/config_wordpress.sh
         timeout: 300
         runas: root
     ApplicationStart:
       - location: scripts/start_server.sh
         timeout: 300
   ```

```
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Cree scripts de archivos bash en. WordPress directorio /scripts.

   En primer lugar, cree `config_wordpress.sh` con el siguiente contenido (si lo prefiere, puede editar el archivo wp-config.php directamente).

> **Note**
>
> *DBName* Sustitúyalo por el valor indicado en el RFC de HA Stack (por ejemplo, `wordpress`).
> *DB_MasterUsername* Sustitúyalo por el `MasterUsername` valor indicado en el RFC de HA Stack (por ejemplo, `admin`).
> *DB_MasterUserPassword* Sustitúyalo por el `MasterUserPassword` valor indicado en el RFC de HA Stack (por ejemplo, `p4ssw0rd`).
> *DB_ENDPOINT* Sustitúyalo por el nombre DNS del punto final en los resultados de ejecución del RFC de la pila HA (por ejemplo, `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`). Puede encontrarlo en la GetRfcoperación (CLI: get-rfc --rfc-id RFC_ID) o en la página de detalles del RFC de la consola AMS para el RFC de la pila de alta disponibilidad que envió anteriormente.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. En `install_dependencies.sh` el mismo directorio, cree con el siguiente contenido:

```
#!/bin/bash
yum install -y php
```

```
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS se instala como parte de los datos del usuario en el momento del lanzamiento para permitir que las comprobaciones de estado funcionen desde el principio.

6. En el mismo directorio, cree `start_server.sh` con el siguiente contenido:

   - Para las instancias de Amazon Linux, usa lo siguiente:

   ```
   #!/bin/bash
   service httpd start
   ```

   - Para las instancias de RHEL, usa esto (los comandos adicionales son políticas que permiten que SELINUX las acepte): WordPress

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   setsebool -P  httpd_can_network_connect 1
   chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
   restorecon -Rv /var/www/html
   service httpd start
   ```

7. En el mismo directorio, cree `stop_server.sh` con el siguiente contenido:

   ```
   #!/bin/bash
   service httpd stop
   ```

8. Cree el paquete zip.

   Linux:

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

   Windows: Ve a tu directorio WordPress «», selecciona todos los archivos y crea un archivo zip, asegúrate de llamarlo wordpress.zip.

1. Cargue el paquete de aplicaciones en el bucket de S3.

   El paquete debe estar en su lugar para poder seguir desplegando la pila.

   Tendrá acceso automáticamente a cualquier instancia de bucket de S3 que cree. Puedes acceder a él a través de tus bastiones o a través de la consola S3 y cargar el WordPress paquete con el archivo zip drag-and-drop o buscarlo y seleccionarlo.

   También puedes usar el siguiente comando en una ventana de shell; asegúrate de tener la ruta correcta al archivo zip:

   ```
   aws s3 cp wordpress.zip s3://BUCKET_NAME/
   ```

2. Implemente el paquete de WordPress aplicaciones.

   Si recopila los siguientes datos antes de empezar, la implementación será más rápida.

   DATOS NECESARIOS:

   - `VPC-ID`: Este valor determina dónde estará su bucket de S3. Use el mismo ID de VPC que utilizó anteriormente.
   - `CodeDeployApplicationNameyCodeDeployApplicationName`: El `ApplicationName` valor que utilizó en el RFC de pila de 2 niveles de HA estableció el y el CodeDeployApplicationName . CodeDeployDeploymentGroupName En el ejemplo se utiliza «WordPress», pero es posible que haya utilizado un valor diferente.
   - `S3Location`: Para`S3Bucket`, usa el `BucketName` que creaste anteriormente. Los `S3BundleType` y `S3Key` son del paquete que pusiste en tu tienda S3.

   a. Genera el esquema JSON de los parámetros de ejecución para la CodeDeploy aplicación Deploy Params.json en un archivo JSON denominado Deploy CDApp Params.json.

      ```
      aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
       --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
       DeployCDAppParams.json
      ```

   b. Modifique el esquema de la siguiente manera y guárdelo como, puede eliminar y reemplazar el contenido.

      ```
      {
      ```

```
"Description":                          "DeployWPCDApp",
"VpcId":                                "VPC_ID",
"Name":                                 "WordPressCDAppDeploy",
"TimeoutInMinutes":                     60,
"Parameters":   {
    "CodeDeployApplicationName":                "WordPress",
    "CodeDeployDeploymentGroupName":            "WordPress",
    "CodeDeployIgnoreApplicationStopFailures":   false,
    "CodeDeployRevision": {
      "RevisionType": "S3",
      "S3Location": {
        "S3Bucket":     "BUCKET_NAME",
        "S3BundleType": "zip",
        "S3Key":        "wordpress.zip" }
        }
    }
}
```

c. Envía la plantilla JSON CreateRfc a un archivo, en tu carpeta actual, denominado Deploy CDApp RFC.json:

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. Modifica y guarda el archivo Deploy CDApp RFC.json. Puedes eliminar y reemplazar el contenido. Tenga en cuenta que `RequestedStartTime` ahora `RequestedEndTime` son opcionales; al excluirlos, se crea un RFC ASAP que se ejecuta tan pronto como se aprueba (lo que normalmente ocurre automáticamente). Para enviar una RFC programada, añada esos valores.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. Cree la RFC especificando el archivo CDApp Rfc de despliegue y el archivo de parámetros de ejecución de Deploy CDApp Params:

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

Recibirá el RfcId nuevo RFC en la respuesta. Guarde el ID para los pasos siguientes.

f. Envíe el RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Si la RFC es correcta, no recibirá ningún resultado.

g. Para comprobar el estado del RFC, ejecute

```
aws amscm get-rfc --rfc-id RFC_ID
```

Validar el despliegue de la aplicación

Navegue hasta el punto final (ELB CName) del balanceador de cargas creado anteriormente, con la ruta implementada:/. WordPress WordPress Por ejemplo:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Destruya la implementación de aplicaciones

Cuando termines con el tutorial, querrás desmantelar el despliegue para que no te cobren por los recursos.

La siguiente es una operación genérica de eliminación de pilas. Deberá enviarla dos veces, una para la pila de 2 niveles de alta disponibilidad y otra para la pila de cubos de S3. Como seguimiento final, envíe una solicitud de servicio para que se eliminen todas las instantáneas del bucket de S3 (incluya el ID de la pila de S3 en la solicitud de servicio). Se eliminan automáticamente al cabo de 10 días, pero eliminarlas anticipadamente supone un pequeño ahorro de costes.

Este tutorial proporciona un ejemplo del uso de la consola AMS para eliminar una pila S3; este procedimiento se aplica a la eliminación de cualquier pila mediante la consola AMS.

> **Note**
>
> Si borras un depósito de S3, primero debes vaciarlo de objetos.

DATOS NECESARIOS:

- `StackId`: La pila que se va a utilizar. Puedes encontrarlo consultando la página de pilas de consolas de AMS, disponible a través de un enlace en la barra de navegación izquierda. Con la API/CLI de AMS SKMS, ejecute la operación Para la referencia de la API de AMS SKMS, consulte la pestaña Informes de la AWS Artifact Console. (en la CLI). `list-stack-summaries`
- El identificador de tipo de cambio para este tutorial es que la versión es `ct-0q0bic0ywqk6c` «1.0". Para averiguar cuál es la versión más reciente, ejecute este comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

CREACIÓN EN LÍNEA:

- Ejecute el comando create RFC con los parámetros de ejecución proporcionados en línea (comillas de escape cuando se proporcionan los parámetros de ejecución en línea). E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- Envíe la RFC mediante el ID de RFC devuelto en la operación de creación de la RFC. Hasta que se envíe, la RFC permanece en ese `Editing` estado y no se toman medidas al respecto.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Supervise el estado de la RFC y vea el resultado de la ejecución:

```
aws amscm get-rfc --rfc-id RFC_ID
```

CREACIÓN DE PLANTILLA:

1. Envía la plantilla RFC a un archivo de tu carpeta actual; el ejemplo la nombra DeleteStackRfc .json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Modifique y guarde el DeleteStackRfc archivo.json. Como la eliminación de una pila solo tiene un parámetro de ejecución, los parámetros de ejecución pueden estar en el propio DeleteStackRfc

archivo.json (no es necesario crear un archivo JSON independiente con los parámetros de ejecución).

Las comillas internas de la extensión ExecutionParameters JSON deben ir precedidas de una barra invertida (\). Ejemplo sin hora de inicio y finalización:

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-0q0bic0ywqk6c",
"Title":                "Delete-My-Stack-RFC"
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"}"
}
```

3. Cree el RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

Recibirá el RfcId nuevo RFC en la respuesta. Por ejemplo:

```
{
"RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
}
```

Guarde el ID para los pasos siguientes.

4. Envíe el RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Si la RFC se realiza correctamente, no recibirá ninguna confirmación en la línea de comandos.

5. Para supervisar el estado de la solicitud y ver el resultado de la ejecución:

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

Tutorial de consola: pila de dos niveles de alta disponibilidad (Linux/RHEL)

En esta sección se describe cómo implementar un WordPress sitio de alta disponibilidad (HA) en un entorno AMS mediante la consola AMS.

> **Note**
>
> Este tutorial de implementación se ha probado en entornos AMZN Linux y RHEL.

Resumen de las tareas y requisitos: RFCs

1. Cree una infraestructura (pila de dos niveles de alta disponibilidad)
2. Cree un bucket de S3 para aplicaciones CodeDeploy
3. Cree el paquete de WordPress aplicaciones y cárguelo en el bucket de S3
4. Implemente la aplicación con CodeDeploy
5. Acceda al WordPress sitio e inicie sesión para validar la implementación
6. Destruya la implementación

Las descripciones de todas las opciones de tomografía computarizada ChangeTypeId, incluidas las disponibles, se encuentran en la referencia de cambios de tipo de AMS.

Antes de empezar

Deployment | Advanced Stack Components | High Availability Two Tier Stack | Create CT crea un grupo de Auto Scaling, un balanceador de cargas, una base de datos y un nombre de CodeDeploy aplicación y un grupo de implementación (con el mismo nombre que le dé a la aplicación). Para obtener más información, CodeDeploy consulte ¿Qué es? CodeDeploy

En este tutorial se utiliza una RFC de pila de dos niveles de alta disponibilidad que incluye `UserData` y también describe cómo crear un WordPress paquete que CodeDeploy se pueda implementar.

Lo que `UserData` se muestra en el ejemplo obtiene los metadatos de la instancia, como el ID de la instancia, la región, etc., de una instancia en ejecución consultando el servicio de metadatos de la EC2 instancia disponible en http://169.254.169.254/latest/meta-data/. Esta línea del script de datos de usuario:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, recupera el nombre de la zona de disponibilidad

del servicio de metadatos y lo coloca en la variable $REGION de las regiones admitidas y lo usa para completar la URL del depósito de S3 donde se descarga el agente. CodeDeploy La IP 169.254.169.254 solo se puede enrutar dentro de la VPC (todos pueden consultar el servicio). VPCs Para obtener información sobre el servicio, consulte Metadatos de instancia y datos de usuario. Tenga en cuenta también que los scripts introducidos como UserData se ejecutan como usuario «root» y no necesitan usar el comando «sudo».

Este tutorial deja los siguientes parámetros en el valor predeterminado (que se muestra):

- Grupo Auto Scaling:`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.
- Load Balancer:. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Base de datos:`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Solicitud:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.

Parámetros variables:

La consola proporciona una opción ASAP para la hora de inicio y en este tutorial se recomienda usarla. ASAP hace que la RFC se ejecute tan pronto como se aprueben las aprobaciones.

> **Note**
>
> Hay muchos parámetros que puede elegir configurar de forma diferente a la que se muestra. Los valores de los parámetros que se muestran en el ejemplo se han probado,

pero es posible que no sean adecuados para usted. En los ejemplos solo se muestran los valores obligatorios. Los valores de la *replaceable* fuente deben cambiarse, ya que son específicos de su cuenta.

Cree la infraestructura

Este procedimiento utiliza el CT de pila de dos niveles de alta disponibilidad seguido del CT de almacenamiento Create S3.

Si recopila los siguientes datos antes de empezar, la implementación será más rápida.

LOS DATOS NECESARIOS TIENEN UNA PILA:

- AutoScalingGroup:
  - UserData: Este valor se proporciona en este tutorial. Incluye comandos para configurar el recurso CodeDeploy e iniciar el CodeDeploy agente.
  - AMI-ID: este valor determina el sistema operativo de las EC2 instancias que activará su grupo de Auto Scaling (ASG). Seleccione una AMI en su cuenta que comience por «customer-» y que sea del sistema operativo que desee. Busque AMI IDs en la consola AMS VPCs -> página de VPCs detalles. Este tutorial es para ASGs configurar el uso de una AMI de Amazon Linux o RHEL.
- Base de datos:
  - Estos parámetros, DBEngineEngineVersion, y LicenseModeldeben configurarse de acuerdo con su situación, aunque se han probado los valores que se muestran en el ejemplo. El tutorial usa estos valores, respectivamente:*MySQL*,*8.0.16*,*general-public-license*.
  - Estos parámetros, DBNameMasterUserPassword, y MasterUsernameson necesarios al implementar el paquete de aplicaciones. El tutorial usa estos valores, respectivamente:*wordpressDB*,*p4ssw0rd*,*admin*. Tenga en cuenta que solo DBName puede contener caracteres alfanuméricos.
  - Cuando introduzca la MasterUsernamepara la base de datos de RDS, aparecerá en texto sin cifrar, así que inicie sesión en la base de datos lo antes posible y cambie la contraseña para garantizar su seguridad.
  - Para los RDSSubnetID, utilice dos subredes privadas. Introdúzcalas una por una, pulsando «Entrar» después de cada una. Busque la subred IDs con la referencia de la API SKMS de AMS, consulte la pestaña Informes de la consola AWS Artifact Console. Funcionamiento (CLI list-subnet-summaries:) o en la página de detalles de la consola AMS VPCs -> VPC.

- LoadBalancer:
  - Establezca este parámetro, Public, en true, porque el tutorial utiliza subredes ELB públicas.
  - ELBSubnetIdentificadores: utilice dos subredes públicas. Introdúzcalas una por una, pulsando «Entrar» después de cada una. Busque la subred IDs con la referencia de la API SKMS de AMS, consulte la pestaña Informes de la consola AWS Artifact Console. Funcionamiento (CLI list-subnet-summaries:) o en la página de detalles de la consola AMS VPCs -> VPC.
- Aplicación: el ApplicationNamevalor establece el nombre de la CodeDeploy aplicación y el nombre del grupo de implementación. CodeDeploy Se usa para implementar la aplicación. Debe ser único en la cuenta. Para comprobar los CodeDeploy nombres de su cuenta, consulte la CodeDeploy consola. El ejemplo usa *`WordPress`* pero, si va a usar ese valor, asegúrese de que aún no esté en uso.

1. Lance la pila de alta disponibilidad.

   a. En la página Crear RFC, seleccione de la lista la categoría Despliegue, la subcategoría Standard Stacks, el elemento Pila de dos niveles de alta disponibilidad y la operación Create.

   b. IMPORTANTE: Seleccione Avanzado y defina los valores tal y como se muestra.

      Solo tiene que introducir valores para las opciones marcadas con un asterisco (*); en el ejemplo se muestran los valores comprobados; puede dejar en blanco las opciones vacías que no sean obligatorias.

   c. Para la sección de descripción de la RFC:

      ```
      Subject: WP-HA-2-Tier-RFC
      ```

   d. En la sección de información sobre recursos, defina los parámetros para la base de datos AutoScalingGroupLoadBalancer, la aplicación y las etiquetas.

      Además, el objetivo de la clave de etiqueta AppName «» es poder buscar fácilmente las instancias de ASG en la EC2 consola; puede llamar a esta clave de etiqueta «Nombre» o cualquier otro nombre de clave que desee. Tenga en cuenta que puede añadir hasta 50 etiquetas.

      ```
      UserData:
          #!/bin/bash
      ```

```
    REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
 | sed 's/[a-z]$//')
    yum -y install ruby httpd
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:               AMI-ID
Description:         WP-HA-2-Tier-Stack

Database:
    LicenseModel:    general-public-license (USE RADIO BUTTON)
    EngineVersion:   8.0.16
    DBEngine:        MySQL
    RDSSubnetIds:    PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
    MasterUsername:      admin
    DBName:              wordpressDB

LoadBalancer:
    Public:              true (USE RADIO BUTTON)
    ELBSubnetIds:        PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:     WordPress

Tags:
    Name:                WP-Rhel-Stack
```

e. Haz clic en Enviar cuando hayas terminado.

2. Inicie sesión en la base de datos que creó y cambie la contraseña.

3. Lance un bucket Stack de S3.

   Si recopila los siguientes datos antes de empezar, la implementación será más rápida.

   DEPÓSITO S3 DE DATOS NECESARIO:

- VPC-ID: este valor determina dónde estará su bucket de S3. Busque la VPC IDs con la referencia para obtener información sobre la API SKMS de AMS, consulte la pestaña Informes de la consola AWS Artifact Console. Operation (CLI: list-vpc-summaries) o en la página de la consola AMS. VPCs
- BucketName: Este valor establece el nombre del bucket de S3, que se utiliza para cargar el paquete de aplicaciones. Debe ser único en toda la región de la cuenta y no puede incluir letras mayúsculas. No BucketName es obligatorio incluir tu ID de cuenta como parte de él, pero te permitirá identificar el segmento más adelante con más facilidad. Para ver qué nombres de bucket de S3 existen en la cuenta, vaya a la consola de Amazon S3 de su cuenta.

a. En la página Crear RFC, seleccione la categoría Implementación, la subcategoría Componentes de pila avanzados, el elemento S3 Storage y la operación Create en la lista de selección de RFC CT.

b. Mantenga la opción básica predeterminada y establezca los valores como se muestra.

```
Subject:              S3-Bucket-WP-HA-RFC
Description:          S3BucketForWordPressBundles
BucketName:           ACCOUNT_ID-BUCKET_NAME
AccessControl:        Private
VpcId:                VPC_ID
Name:                 S3-Bucket-WP-HA-Stack
TimeoutInMinutes:     60
```

c. Haga clic en Enviar cuando haya terminado. El depósito implementado con este tipo de cambio permite el read/write acceso total a toda la cuenta.

Crear, cargar e implementar la aplicación

En primer lugar, cree un paquete de WordPress aplicaciones y, a continuación, utilice el CodeDeploy CTs para crear e implementar la aplicación.

1. Descargue WordPress, extraiga los archivos y cree un. directorio /scripts.

   Comando de Linux:

```
wget https://github.com/WordPress/WordPress/archive/master.zip
```

Windows: pégalo `https://github.com/WordPress/WordPress/archive/master.zip` en una ventana del navegador y descarga el archivo zip.

Cree un directorio temporal en el que ensamblar el paquete.

Linux:

```
mkdir /tmp/WordPress
```

Windows: cree un directorio WordPress «», utilizará la ruta del directorio más adelante.

2. Extraiga la WordPress fuente al directorio WordPress «» y cree un. directorio /scripts.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows: vaya al directorio «WordPress» que creó y cree allí un directorio de «scripts».

   Si se encuentra en un entorno Windows, asegúrese de establecer el tipo de interrupción de los archivos de script en Unix (LF). En Notepad ++, esta opción se encuentra en la parte inferior derecha de la ventana.

3. Cree el archivo CodeDeploy appspec.yml en el WordPress directorio (si va a copiar el ejemplo, compruebe la hendidura, cada espacio cuenta). IMPORTANTE: Asegúrese de que la ruta «fuente» sea correcta para copiar los WordPress archivos (en este caso, en su WordPress directorio) al destino esperado (/). var/www/html/WordPress En el ejemplo, el archivo appspec.yml está en el directorio con los WordPress archivos, por lo que solo se necesita «/». Además, aunque haya utilizado una AMI de RHEL para su grupo de Auto Scaling, deje la línea «os: linux» tal como está. Ejemplo de archivo appspec.yml:

   ```
   version: 0.0
   os: linux
   files:
     - source: /
   ```

```
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Cree scripts de archivos bash en. WordPress directorio /scripts.

   En primer lugar, cree `config_wordpress.sh` con el siguiente contenido (si lo prefiere, puede editar el archivo wp-config.php directamente).

   > **Note**
   >
   > *DBName*Sustitúyalo por el valor indicado en el RFC de HA Stack (por ejemplo,`wordpress`).
   > *DB_MasterUsername*Sustitúyalo por el `MasterUsername` valor indicado en el RFC de HA Stack (por ejemplo,`admin`).
   > *DB_MasterUserPassword*Sustitúyalo por el `MasterUserPassword` valor indicado en el RFC de HA Stack (por ejemplo,`p4ssw0rd`).
   > *DB_ENDPOINT*Sustitúyalo por el nombre DNS del punto final en los resultados de ejecución del RFC de la pila HA (por ejemplo,`srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`). Puede encontrarlo en la GetRfcoperación (CLI: get-rfc --rfc-id RFC_ID) o en la página de detalles del RFC de la consola AMS para el RFC de la pila de alta disponibilidad que envió anteriormente.

```
#!/bin/bash
```

```
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. En `install_dependencies.sh` el mismo directorio, cree con el siguiente contenido:

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS se instala como parte de los datos del usuario en el momento del lanzamiento para permitir que las comprobaciones de estado funcionen desde el principio.

6. En el mismo directorio, cree `start_server.sh` con el siguiente contenido:

   - Para las instancias de Amazon Linux, usa lo siguiente:

   ```
   #!/bin/bash
   service httpd start
   ```

   - Para las instancias de RHEL, usa esto (los comandos adicionales son políticas que permiten que SELINUX las acepte): WordPress

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   setsebool -P  httpd_can_network_connect 1
   chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
   restorecon -Rv /var/www/html
   service httpd start
   ```

7. En el mismo directorio, cree `stop_server.sh` con el siguiente contenido:

```
#!/bin/bash
service httpd stop
```

8. Cree el paquete zip.

   Linux:

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

   Windows: Ve al directorio WordPress «», selecciona todos los archivos y crea un archivo zip, asegúrate de llamarlo wordpress.zip.

1. Cargue el paquete de aplicaciones en el bucket de S3

   El paquete debe estar en su lugar para poder seguir desplegando la pila.

   Tendrá acceso automáticamente a cualquier instancia de bucket de S3 que cree. Puede acceder a él a través de sus Bastions (consulte Acceso a las instancias) o a través de la consola S3 y cargar el CodeDeploy paquete con él drag-and-drop, o bien navegando hasta el archivo y seleccionándolo.

   También puede usar el siguiente comando en una ventana de shell; asegúrese de tener la ruta correcta al archivo zip:

   ```
   aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
   ```

2. Implemente el paquete WordPress CodeDeploy de aplicaciones

   DESPLIEGUE DE CÓDIGO DE DATOS REQUERIDO: DESPLIEGUE DE APLICACIONES:

   - CodeDeployApplicationName: el nombre que le diste a la CodeDeploy aplicación.
   - CodeDeployGroupName: Dado que tanto la CodeDeploy aplicación como el grupo se crearon a partir del nombre que le diste a la CodeDeploy aplicación en el RFC de la pila HA, es el mismo nombre que el CodeDeployApplicationName.
   - S3Bucket: el nombre que le diste al depósito S3.
   - S3 BundleType y S3Key: forman parte del paquete de WordPress aplicaciones que implementó.

- VpcId: El VPC correspondiente.

a. En la página Crear RFC, seleccione la categoría Despliegue, la subcategoría Aplicaciones, el elemento CodeDeploy Aplicación y operación Despliegue en la lista de selección de RFC CT.

b. Mantenga la opción básica predeterminada y establezca los valores como se muestra.

> **Note**
>
> Haga referencia a la CodeDeploy aplicación, el grupo de CodeDeploy implementación, el depósito de S3 y el paquete creados anteriormente.

```
Subject:                                WP-CD-Deploy-RFC
Description:                            DeployWordPress
S3Bucket:                               BUCKET_NAME
S3Key:                                  wordpress.zip
S3BundleType:                           zip
CodeDeployApplicationName:              WordPress
CodeDeployDeploymentGroupName:          WordPress
CodeDeployIgnoreApplicationStopFailures: false
RevisionType:                           S3



VpcId:                                  VPC_ID
Name:                                   WP-CD-Deploy-Op
TimeoutInMinutes:                       60
```

c. Haga clic en Enviar cuando haya terminado.

Validar el despliegue de la aplicación

Navegue hasta el punto final (LoadBalancerCName) del balanceador de cargas creado anteriormente, con la ruta implementada:/. WordPress WordPress Por ejemplo:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Deberías ver una página como esta:

Elimine la implementación de alta disponibilidad

Para reducir la implementación, debe enviar el Delete Stack CT, comparándolo con el conjunto de alta disponibilidad de dos niveles y el bucket S3, y puede solicitar que se eliminen las instantáneas de RDS (se eliminan automáticamente al cabo de diez días, pero mientras están ahí cuestan un pequeño importe). Reúna la pila IDs de alta disponibilidad y el depósito de S3 y, a continuación, siga estos pasos. Consulte Stack | Delete.

Apéndice: Cuestionario de incorporación de SALZ

Temas

- Resumen de despliegue
- Consideraciones sobre la arquitectura del entorno
- Alertas de monitoreo de zonas de aterrizaje con una sola cuenta
- Maintenance Window (Período de mantenimiento)
- Siguientes pasos

Esta es parte de la información que tendrás que tener en cuenta antes de incorporar una cuenta.

Resumen de despliegue

Descripción de la implementación. Por ejemplo:

- Esta cuenta es para el despliegue de una Line-of-Business aplicación (a diferencia del despliegue de una aplicación de producto).
- La implementación implica un ARP (proxy inverso autenticado) escalado automáticamente dentro de la subred pública o DMZ de la cuenta.
- Los servidores web y de aplicaciones se implementarán en la subred privada de la cuenta.
- También se implementará una instancia de RDS (Amazon Relational Database Service) en la subred privada de la cuenta.
- Los servidores (ARP, web, aplicación, base de datos, balanceador de carga, etc.) están separados en distintos grupos de seguridad.
- La cuenta requiere un diseño de alta disponibilidad (HA) distribuido en todas las zonas de disponibilidad (AZs), es decir, «Multi-AZ».

Consideraciones sobre la arquitectura del entorno

Tenga en cuenta los siguientes criterios al decidir cómo configurar el entorno y la arquitectura.

- ¿Se volverá a conectar su centro de datos virtual a la red corporativa?
  - ¿Tiene un AWS DirectConnect servicio existente o necesita uno nuevo DirectConnect ?
  - ¿Tiene una conexión VPN existente o necesita un nuevo servicio de VPN?
- ¿Cuál es el rango de direcciones internas del bloque CIDR disponible que podría asignar? (Se recomienda /16, no debe superponerse a los rangos de redes corporativas)
- ¿Su centro de datos virtual requerirá acceso a Internet?
- ¿Qué regiones piensa utilizar? (Sydney/N. Virginia/Dublin)
- ¿Necesitará una subred de Shared Services para alojar aplicaciones que tengan conectividad con todas las demás subredes?
- ¿Cuáles son las divisiones organizativas que desea que se alojen como subredes independientes? Para cada una de ellas:
  - ¿Qué conectividad con otras subredes necesita?
  - ¿La subred requiere acceso a Internet?
  - ¿Existe alguna restricción de despliegue de aplicaciones en esa subred?
  - ¿Hay algún requisito de red específico para esa subred?
- ¿Desea disponer de entornos de and/or pruebas de desarrollo separados? (Incluirá servicios compartidos duplicados para poder acceder a ellos en cualquier momento)
- ¿Cuáles son sus requisitos de copia de seguridad de instantáneas?
- ¿Tiene un proceso de mantenimiento existente o una o varias ventanas de revisión que le gustaría conservar?
- ¿Cuáles son los requisitos de registro de su dominio?
- ¿Tienes algún requisito de inicio de sesión único? (por ejemplo, AD, LDAP)
- ¿Cuáles son las expectativas generales del sistema operativo y los requisitos de capacidad previstos?

Alertas de monitoreo de zonas de aterrizaje con una sola cuenta

AMS te permite recibir alertas directas (en lugar de recibir notificaciones del servicio AMS) sobre determinadas alertas de supervisión. Para suscribirse, asegúrese de que su Cloud Architect (CA) o Cloud Service Delivery Manager (CSDM) reciba la siguiente información:

Correo electrónico de alertas directas: estas son las direcciones de correo electrónico a las que desea que AMS envíe determinadas alertas basadas en los recursos. Para obtener más información sobre qué alertas se envían directamente al correo electrónico, consulte Alertas de Baseline Monitoring en AMS en la Guía del usuario de AMS para zonas de destino con una sola cuenta. Para obtener más información sobre la supervisión de AMS, consulte la gestión de la supervisión en la Guía del usuario de AMS para zonas de destino con una sola cuenta.

Maintenance Window (Período de mantenimiento)

Querrá crear una ventana de mantenimiento que considere las diferentes necesidades de la aplicación Regiones de AWS, diferentes y diferentes períodos de stress. Su período de mantenimiento es el momento en el que AMS aplicará los parches. A continuación le presentamos algunas pautas:

- Para limitar el impacto en los usuarios, planifique el período de mantenimiento en función del lugar en el que Región de AWS se desplieguen sus entornos.
- Programe un período fuera del horario laboral habitual y en el momento en que se espera que haya menos tráfico en los servidores de producción.
- Por lo general, las pilas de infraestructura requieren actualizaciones mensuales.
- Programe un período de mantenimiento de al menos 300 minutos. La aplicación de parches al sistema operativo tarda entre 60 y 90 minutos, mientras que la aplicación de parches a la pila de infraestructuras tarda entre 180 y 300 minutos.

Siguientes pasos

El equipo de incorporación de AMS lo ayudará en cada paso de la incorporación de su cuenta a AMS. Estos son los requisitos de incorporación:

- Proporcione una nueva Cuenta de AWS para usar en AMS y proporcione una Cuenta de AWS identificación.
- Inscríbase para obtener el nivel de Support deseado.

- Cree una función de IAM multicuenta para conceder acceso a la cuenta de aprovisionamiento de AMS y proporcione el nombre de la función a AMS.
- Agregue la cuenta 753102745277 como entidad de confianza.

Apéndice: Regla de notificación de ActiveDirectory Federation Services (ADFS) y configuración de SAML

Para step-by-step obtener instrucciones detalladas sobre cómo instalar y configurar AD FS, consulte Habilitar la federación en AWS mediante Windows Active Directory, ADFS y SAML 2.0.

Configuraciones de reglas de reclamación de ADFS

Si ya tiene una implementación de ADFS, configure lo siguiente:

- Confiar en la confianza de una
- Normas de reclamación

Las normas de confianza y reclamaciones de la parte que confía se llevan a cabo desde Habilitar la federación hasta AWS con Windows Active Directory, AD FS y SAML 2.0 blog

- Reglas de reclamaciones:
  - Nameid: configuración por publicación de blog
  - RoleSessionName: Configure de la siguiente manera
    - Nombre de la regla de reclamación: **`RoleSessionName`**
    - Almacén de atributos: **`Active Directory`**
    - Atributo de LDAP: **`SAM-Account-Name`**
    - Tipo de reclamación saliente: **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**
    - Obtenga grupos de AD: configuración por publicación de blog
    - Afirmación de rol: configure de la siguiente manera

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-", "arn:aws:iam::$1:saml-provider/
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Consola web

Puede acceder a la consola web de AWS mediante el siguiente enlace y sustituirla *[ADFS-FQDN]* por el FQDN de su implementación de ADFS.

https://.aspx *[ADFS-FQDN]* adfs/ls/IdpInitiatedSignOn

Su departamento de TI puede implementar el enlace anterior entre la población de usuarios mediante una política de grupo.

Acceso a API y CLI con SAML

Cómo configurar el acceso a la API y a la CLI con SAML.

Los paquetes de Python provienen de las siguientes publicaciones de blog:

- NTLM: Cómo implementar el acceso federado a la API y a la CLI mediante SAML 2.0 y AD FS
- Formularios: cómo implementar una solución general para el acceso API/CLI federado mediante SAML 2.0
- PowerShell: Cómo configurar el acceso de la API federada a AWS mediante Windows PowerShell

Configuración de scripts

1. Con Notepad++, cambie la región predeterminada a la región correcta
2. Con Notepad++, deshabilite la verificación SSL para los entornos de prueba y desarrollo
3. Con Notepad++, configure idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
loginToRp=urn:amazon:webservices
```

Configuración de Windows

Las instrucciones que aparecen a continuación son para los paquetes de python. Las credenciales generadas serán válidas durante 1 hora.

1. Descargue e instale python (2.7.11)

2. Descargar e instalar las herramientas de AWS CLI
3. Instale la CLI de AMS:

   a. Descargue el archivo zip de productos distribuibles de AMS proporcionado por su administrador de prestación de servicios en la nube (CSDM) y descomprímalo.

      Hay varios directorios y archivos disponibles.

   b. Abra el directorio Managed Cloud Distributables -> CLI -> Windows o Managed Cloud Distributables -> CLI -> Linux/macOS, según su sistema operativo, y:

      Para Windows, ejecute el instalador adecuado (este método solo funciona en sistemas Windows de 32 o 64 bits):

      - 32 bits: ManagedCloud API_x86.msi
      - 64 bits: ManagedCloud API_x64.msi

      Para Mac/Linux, ejecute el archivo denominado: MC_CLI.sh. Puede hacerlo ejecutando este comando:. `sh MC_CLI.sh` Tenga en cuenta que los directorios amscm y amsskms y su contenido deben estar en el mismo directorio que el archivo MC_CLI.sh.

   c. Si sus credenciales corporativas se utilizan mediante la federación con AWS (la configuración predeterminada de AMS), debe instalar una herramienta de administración de credenciales que pueda acceder a su servicio de federación. Por ejemplo, puede utilizar este blog de seguridad de AWS sobre cómo implementar el acceso federado a las API y CLI mediante SAML 2.0 y AD FS como ayuda para configurar sus herramientas de administración de credenciales.

   d. Tras la instalación, ejecute `aws amscm help` y consulte los comandos y `aws amsskms help` las opciones.

4. Descargue el script de SAML necesario

   Descárguelo en c:\aws\scripts

5. Descargue PIP

   Descárguelo a c:\aws\downloads

6. Utilizando PowerShell, instale PIP

   <pythondir>. \ python.exe c:\aws\downloads\get -pip.py

7. Utilizando PowerShell, instale el módulo de arranque

<pythondir\ scripts>Usando, instale el módulo boto ----sep----pip install boto

8. Uso e instalación PowerShell del módulo de solicitudes

   <pythondir\ scripts>Uso del módulo de solicitudes de instalación ----sep----pip install requests

9. Uso PowerShell e instalación del módulo de seguridad de solicitudes

   <pythondir\ scripts>Uso del módulo de seguridad de solicitudes de instalación ----sep----pip install requests [security]

10. Usando PowerShell, instale el módulo beautifulsoup

    <pythondir\ scripts>Usando, instale el módulo beautifulsoup ----sep----pip instale beautifulsoup4

11. Usando PowerShell, cree una carpeta llamada .aws en el perfil del usuario (%userprofile%\ .aws)

    mkdir .aws

12. Con PowerShell, cree un archivo de credenciales en la carpeta .aws

    Archivo de credenciales de elemento nuevo: force

    El archivo de credenciales no debe tener una extensión

    El nombre del archivo debe estar todo en minúsculas y tener las credenciales del nombre

13. Abra el archivo de credenciales con el bloc de notas y pegue los siguientes datos, especificando la región correcta

    ```
    [default]
    output = json
    region = us-east-1
    aws_access_key_id =
    aws_secret_access_key =
    ```

14. Utilice el PowerShell script SAML y el inicio de sesión

    <pythondir>. \ python.exe c:\aws\scripts\samlapi.py

    Nombre de usuario: [NOMBRE DE USUARIO] @upn

    Elige el rol que te gustaría asumir

Configuración de Linux

Las credenciales generadas serán válidas durante 1 hora.

1. Con WinSCP, transfiera el script SAML
2. Con WinSCP, transfiera el certificado de CA raíz (ignorarlo para pruebas y desarrollo)
3. Agregue la CA RAÍZ a los certificados raíz de confianza (omítala para pruebas y desarrollo)

   $ openssl x509 -inform der -in [certname] .cer -out certificate.pem (ignorar para pruebas y desarrollo)

   Añada el contenido de certificate.pem al final del archivo/-bundle.crt (ignore para desarrolladores de pruebas) etc/ssl/certs/ca
4. Cree la carpeta.aws en home/ec2-user 5

   ```
   [default]
   output = json
   region = us-east-1
   aws_access_key_id =
   aws_secret_access_key =
   ```
5. Con WinSCP, transfiera el archivo de credenciales a la carpeta.aws
6. Instale el módulo de arranque

   $ sudo pip install boto
7. Instale el módulo de solicitudes

   Solicitudes de instalación de $ sudo pip
8. Instale el módulo beautifulsoup

   $ sudo pip instala beautifulsoup4
9. Copie el script a home/ec2-user

   Establezca los permisos necesarios

   Ejecute el script: samlapi.py

Historial del documento

En la siguiente tabla se describen los cambios importantes en la documentación desde la última versión de AMS.

- Versión de la API: 21 de mayo de 2019
- Última actualización de la documentación: 23 de septiembre de 2025

Cambio	Descripción	Fecha
Se actualizó el tipo de cambio para el escalado automático de puntos finales en SageMaker IA en la sección de preguntas frecuentes sobre AWS Managed Services	Utilice AMS SSP para aprovisionar Amazon SageMaker AI en su cuenta de AMS. Envíe una RFC con Management | Advanced stack components | Identity and Access Management (IAM) | Actualice la entidad o política (es necesario revisar) el tipo de cambio (ct-27tuth19k52b4) para aumentar los permisos de escalado automático de forma temporal o permanente, ya que el escalado automático requiere un acceso permisivo al servicio. CloudWatch	25 de septiembre de 2025
Referencias de tipos de cambio precisas	Crear, cambiar o eliminar grupos de seguridad. Para añadir un usuario: envíe una RFC mediante Management | Directory Service | Usuarios y grupos | Añadir usuario al grupo [ct-24pi85mjtza8k] y Para eliminar un usuario: Envíe una RFC mediante Management | Directory Service | Usuarios y grupos | Eliminar usuario del grupo [ct-2019s9y3nfml4]	8 de agosto de 2025
Se ha eliminado el enlace TOC	Se ha eliminado el enlace al AWS glosario de TOC.	8 de agosto de 2025

Cambio	Descripción	Fecha
Se agregó un enlace para obtener orientación sobre recetas	Configure la facturación consolidada: vincule la nueva cuenta a la cuenta del pagador.	08 de mayo de 2025
Instrucciones actualizadas para activar el acceso de IAM al Consola de administración de AWS	Se aclararon las instrucciones para activar el acceso de IAM al. Consola de administración de AWS	Activar el acceso de IAM a la consola AWS
Número actualizado de interfaces virtuales de tránsito permitidas en las conexiones dedicadas de Direct Connect	Las conexiones dedicadas de Direct Connect ahora tienen un límite de 4 interfaces virtuales de tránsito por conexión	Conexión de Direct Connect a Transit Gateway
Mejore la redacción.	Especificó que «solo se utiliza como lista de «Denegados» debe incluir «Permitir todo» para garantizar las operaciones de supervisión y gestión de AMS.	Configuración de red
Información adicional sobre el uso de la CLI de AMS.	«Se agregó una nota de que la `--region` opción puede ser necesaria para algunos comandos de CLI»	Instale el AMS CLIs
Actualizado: los encabezados de los capítulos han sido trasladados a secciones más apropiadas para garantizar una mayor coherencia y legibilidad	«Modos de gestión del cambio» es el nuevo título de «Gestión del cambio»	Modos de administración de cambios
Contenido actualizado	El modo AMS, anteriormente conocido como «modo de gestión de cambios» o «modo CM estándar», ahora se conoce como «modo RFC». Se ha ampliado la sección de modos.	Modo RFC.

Cambio	Descripción	Fecha
Contenido actualizado	El modo AMS, anteriormente conocido como «modo de gestión de cambios» o «modo CM estándar», ahora se conoce como «modo RFC». La sección de modos se ha abreviado y se han añadido enlaces a las secciones de la Guía de usuario avanzada del AMS sobre los modos.	Modos AMS.
MALZ: Diagrama de arquitectura de red actualizado	Arquitectura de cuentas de redm	16 de junio de 2022
Se ha movido la lista de temas a los párrafos iniciales	Introducción a la incorporación de AWS Managed Services	16 de junio de 2022
Contenido actualizado, iniciativa de lenguaje inclusivo	«Cuenta de administración», no «cuenta maestra».	Función de usuario de IAM en AMS, sección «Ejemplos de políticas»
Contenido actualizado, nombres de los roles de las cuentas de Tools	Se actualizó el nombre del rol CustomerMigrationAccessRole a AWSManagedServices MigrationRole.	AWS Servicio de migración de aplicaciones (AWS MGN)
SALZ: valores predeterminados de administración de continuidad	Se actualizó el enlace y se eliminó la información obsoleta de Etiqueta de VPC y valores predeterminados	28 de febrero de 2022

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.