



Conceptos y procedimientos avanzados de AMS

Guía de usuario avanzada de AMS



Version October 3, 2025

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Guía de usuario avanzada de AMS: Conceptos y procedimientos avanzados de AMS

Copyright © 2025 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

¿Qué es AWS Managed Services?	1
Acerca de esta guía	2
Planes de operaciones	2
Acelere el plan de operaciones	3
Plan de operaciones avanzado	3
Introducción	4
Términos clave	4
Descripción del servicio	10
Características del plan operativo avanzado de AWS Managed Services (AMS) AMS	11
Lo que hacemos, lo que no hacemos	17
Matriz de responsabilidad de AMS (RACI)	18
Componentes básicos del entorno AMS	42
Límites de cuentas AMS	45
Objetivos de nivel de servicio de AMS (SLOs)	48
AWS Servicios compatibles	49
Configuraciones admitidas	53
Sistemas operativos no compatibles	55
Interfaces avanzadas AMS	56
Puntos de conexión de la VPC	57
Espacios de nombres protegidos por AMS	58
Prefijos reservados AMS	60
Ventana de mantenimiento de AMS	61
Recursos de información de AMS	61
Conformidad con AMS	62
AMS apoya las normas de conformidad	62
Responsabilidad compartida	68
Imágenes de máquinas AMS Amazon (AMIs)	68
Seguridad mejorada AMIs	71
Cómo funciona la integración entre AD FS y AMS	71
Active Directory gestionado por AMS	73
Implementaciones de aplicaciones	76
Administración de servicios	78
Gobierno de cuentas	78
Inicio del servicio	79

Gestión de relaciones con los clientes (CRM)	79
Proceso de CRM	80
Reuniones de CRM	81
Organización de reuniones de CRM	82
Informes mensuales de CRM	83
Optimización de costos	84
Marco de optimización de costos	84
Matriz de responsabilidad de optimización de costes	87
Horas de servicio	89
Obtener ayuda	89
Gestión de eventos planificados	90
Criterios AMS PEM	90
Tipos de PEM	90
El proceso AMS PEM	91
PEM FAQs	91
Arquitectura de redes	93
Arquitectura de red MALZ	93
Acerca de la arquitectura de red de landing zone multicuenta	93
Elegir un solo MALZ o varios MALZs	96
Cuentas multicuenta de Landing Zone	101
Arquitectura de red SALZ	136
Servicios compartidos de zona de aterrizaje con una sola cuenta de AMS	137
Configuración de AMS	139
Configuración predeterminada de AMS	140
Valores predeterminados de resolución de DNS (MALZ)	140
EC2 Perfil de instancia de IAM	141
Alertas del monitoreo de referencia en AMS	148
Valores predeterminados de retención y rotación de registros	166
Uso de las consolas AMS	166
Uso de la API y la CLI de AMS	168
Puntos finales HTTP de la API AMS para llamadas REST	168
Instalación o actualización de la CLI de AMS	169
Uso de la API AMS en CLI, Ruby, Python y Java	170
AMS trae tu propio EPS	180
Activa el BYOEPS en tu cuenta	182
Recibir notificaciones de AMS	185

Notificaciones AMI de AMS con SNS	186
Notificaciones de servicio	190
Notificaciones de cambio de estado de RFC	191
Configuración de DNS públicos y privados	195
Gestión del tráfico de salida AMS	196
Implementación de recursos de IAM	197
Aprovisionamiento automatizado de IAM	198
Configuración de permisos con roles y perfiles de IAM	223
Solicitar un nuevo perfil de instancia o rol de usuario de IAM	223
Restrinja los permisos con las declaraciones de política de funciones de IAM	224
Restrinja los permisos con los perfiles de instancia de Amazon EC2 IAM	225
Regla de notificación de AD FS y configuración de SAML	226
Configuraciones de reglas de reclamación de ADFS	226
Consola web	227
Acceso a API y CLI con SAML	227
Restringir con ACL de red	231
AMS en Outposts	232
AWS Outposts administración de la instalación y las operaciones	232
Aprovisionamiento de recursos gestionados por AMS en AWS Outposts	235
Limitaciones de AMS en AWS Outposts	235
AWS Outposts AMS sobre el cumplimiento	237
AMS está activada AWS Outposts FAQs	238
Uso de etiquetas	240
Etiquetado automático de infraestructuras AMS	241
Etiquetas recomendadas por AMS	243
Etiquete las notas de actualización masiva	247
Programador de recursos	249
Implementación del programador de recursos	250
Personalización del programador de recursos	250
Uso del programador de recursos	251
Estimador de costos de AMS Resource Scheduler	252
Mejores prácticas de AMS Resource Scheduler	253
AWS Systems Manager en AMS Advanced	255
Documentos AMS Advanced SSM disponibles	256
Versiones de documentos AMS Advanced SSM	256
Precios de Systems Manager	257

Cuentas AMS externas	257
Abandonar las cuentas de landing zone con una sola cuenta	258
Abandonar las cuentas multicuenta de landing zone	262
Modos de administración de cambios	286
Descripción general de los modos	287
Tipos de modos y cuentas en AMS	288
Modos y aplicaciones o cargas de trabajo AMS	291
Casos de uso reales para los modos AMS	300
Modo RFC	303
Más información sobre RFCs	304
¿Qué son los tipos de cambios?	345
Solución de problemas de errores de RFC	358
Modo de cambio directo	370
Cómo empezar con el modo Direct Change	370
Seguridad y conformidad	373
Gestión de cambios en el modo Direct Change	378
Creación de pilas mediante el modo de cambio directo	381
Casos de uso del modo de cambio directo	384
Modo desarrollador	385
Cómo empezar con el modo Desarrollador	386
Seguridad y conformidad	388
Administración de cambios	390
Aprovisionamiento de la infraestructura	396
Controles de detección	397
Registro, supervisión y gestión de eventos	397
Administración de incidentes	397
Administración de parches	398
Gestión de la continuidad	398
Gestión de seguridad y acceso	398
Modo de aprovisionamiento de autoservicio en AMS	399
Cómo empezar con el modo SSP en AMS	400
Amazon API Gateway	400
Alexa for Business	401
Amazon AppStream 2.0	403
Amazon Athena	406
Amazon Bedrock	407

Amazon CloudSearch	408
Amazon CloudWatch Synthetics	409
Amazon Cognito	410
Amazon Comprehend	412
Amazon Connect	413
Amazon Data Firehose	416
El DevOps gurú de Amazon	417
Amazon DocumentDB (con compatibilidad con MongoDB)	418
Amazon DynamoDB	419
Amazon Elastic Container Registry	420
EC2 Image Builder	421
Amazon ECS en AWS Fargate	423
Amazon EKS en AWS Fargate	426
Amazon EMR	429
Amazon EventBridge	432
Amazon Forecast	434
Amazon FSx	437
Amazon FSx para OpenZFS	439
Amazon FSx para NetApp ONTAP	441
Amazon Inspector Classic	442
Amazon Kendra	444
Amazon Kinesis Data Streams	444
Amazon Kinesis Video Streams	445
Amazon Lex	446
Amazon MQ	447
Amazon Managed Service para Apache Flink	448
Transmisión gestionada de Amazon para Apache Kafka	450
Servicio administrado por Amazon para Prometheus	451
Amazon Personalize	452
Amazon QuickSight	455
Amazon Rekognition	456
Amazon SageMaker AI	458
Amazon Simple Email Service	461
Amazon Simple Workflow Service	462
Amazon Textract	463
Amazon Transcribe	464

Amazon WorkSpaces	466
Servicios de códigos AMS	468
AWS Amplify	471
AWS AppSync	472
AWS App Mesh	473
AWS Audit Manager	474
AWS Batch	475
AWS Certificate Manager	476
AWS Private Certificate Authority	478
AWS CloudEndure	481
AWS CloudHSM	482
AWS CodeBuild	484
AWS CodeCommit	485
AWS CodeDeploy	487
AWS CodePipeline	488
AWS Compute Optimizer	490
AWS DataSync	491
AWS Device Farm	493
AWS Elastic Disaster Recovery	493
AWS Elemental MediaConvert	495
AWS Elemental MediaLive	496
AWS Elemental MediaPackage	497
AWS Elemental MediaStore	498
AWS Elemental MediaTailor	499
AWS Global Accelerator	500
AWS Glue	501
AWS Lake Formation	502
AWS Lambda	504
AWS License Manager	505
AWS Migration Hub	506
AWS Outposts	507
AWS Resilience Hub	508
AWS Secrets Manager	509
AWS Security Hub	512
AWS Service Catalog AppRegistry	513
AWS Shield	514

AWS Snowball Edge	515
AWS Step Functions	517
AWS Systems Manager Almacén de parámetros	518
AWS Systems Manager Automation	519
AWS Transfer Family	523
AWS Transit Gateway	524
AWS WAF	525
AWS Well-Architected Tool	526
AWS X-Ray	527
VM Import/Export	528
Modo gestionado por el cliente	530
Cómo empezar con el modo Customer Managed	530
Catálogo de servicios de AMS y AWS	531
Introducción a Service Catalog	531
Service Catalog en AMS antes de empezar	532
Encontrar los datos que necesita (SKMS)	536
¿Qué es la gestión del conocimiento de los servicios?	536
Encuentra VPC IDs	537
Encuentra una subred IDs	539
Encuentra AMI IDs	542
Encuentra un grupo de seguridad (SG) IDs	543
Encuentra entidades de IAM	544
Encuentra una pila IDs	544
Encuentra direcciones IP IDs o de instancia	546
Encuentra ARNs	549
Encuentra recursos por ARN	551
Encuentra la configuración de la cuenta	552
Encuentra FQDNs	554
Encuentra zonas de disponibilidad (AZs)	554
Encuentra temas de SNS	555
Encuentra la configuración de copia de seguridad	556
Administración de accesos	557
¿Qué es la gestión de acceso?	557
¿Por qué y cuándo accedemos a su cuenta	558
¿Cómo y cuándo usar root	563
Consola AMS Advanced y EC2 acceso a Amazon	564

Acceso a la consola AWS de administración y a la consola AMS	565
Acceso temporal a la consola AMS	565
Acceso a las instancias mediante bastiones	566
Nombres de bastiones compatibles con DNS	568
Ahorro de costes en los bastiones de las zonas de landing zone con una sola cuenta (SALZ)	569
Uso de direcciones IP de bastión	570
Ejemplos de acceso a instancias	571
Control de acceso basado en equipos o roles en una cuenta AMS	582
Configuración de EC2 instancias automatizada	583
Requisitos previos para la configuración automatizada de instancias	583
Instalación automática de SSM Agent	584
Requisitos previos	584
Solicite la instalación automática del agente SSM	585
Cómo funciona la instalación automática de SSM Agent	586
Cambios automatizados	586
Actualice automáticamente el código en las instancias de Linux	586
Actualice automáticamente PBIS en instancias de Linux	587
Actualice automáticamente la versión mínima de SSM y CloudWatch de los agentes	588
CloudWatch archivos de configuración, detalles de actualización	589
Registros configurados automáticamente	590
Supervisión y gestión de eventos	592
¿Qué es la monitorización?	593
¿Qué monitorea el sistema de monitoreo AMS?	594
Supervisión proactiva de Active Directory Trust en la zona de destino con una sola cuenta .	595
Cómo funciona la supervisión	595
EC2 notificaciones agrupadas por instancias	597
Notificación de alertas basada en etiquetas	598
Visualización de la configuración de supervisión de una cuenta	599
Cambiar la configuración de supervisión de una cuenta	600
Notificaciones de incidentes compatibles con las aplicaciones en AMS	600
AppRegistry Aprovisiona en su cuenta AMS y cree aplicaciones	601
Cree etiquetas para permitir el enriquecimiento de mayúsculas y minúsculas	601
Personalice la gravedad de los casos de soporte de AMS para sus aplicaciones	601
Revisa los permisos necesarios	602
Usando OpsCenter	603

Notificaciones de alerta	604
Recibir alertas	604
Notificaciones de alertas basadas en etiquetas	605
Remediación automática de alertas por parte de AMS	606
Creación de CloudWatch alarmas adicionales	614
Creación de CloudWatch métricas y alarmas personalizadas	616
Uso de CloudWatch Application Insights para .Net y SQL Server	617
Router de eventos AMS	618
Amazon EventBridge Managed Rules implementadas por AMS	618
Creación de reglas administradas para AMS	619
Edición de reglas gestionadas para AMS	619
Eliminar reglas administradas para AMS	619
Remediador de confianza	619
Ventajas principales	620
Cómo funciona Trusted Remediator	620
Términos clave	621
Comience con Trusted Remediator	622
Recomendaciones de Compute Optimizer compatibles	626
Comprobaciones compatibles Trusted Advisor	630
Configure la corrección de comprobaciones	691
Flujo de trabajo de decisiones en modo ejecución	696
Configure los tutoriales de corrección	696
Trabaje con las soluciones	698
Registros de remediación	703
Prácticas recomendadas	706
FAQs	706
Administración de registros:	709
¿Qué es la administración de registros?	709
Cómo funciona el registro de AMS	709
Acceder a sus registros de	710
Registros de servicios agregados de AMS	710
Registros de servicios compartidos de AMS	727
Amazon Elastic Compute Cloud (Amazon EC2): registros a nivel de sistema	730
Integración con Splunk	732
Personalización de la configuración de registros	732
Alterar la retención de CloudWatch registros	732

Habilitar el registro para los servicios compatibles	733
Administración de la seguridad	734
Protección de datos en AMS	734
Amazon Macie	735
GuardDuty	737
Firewall DNS Amazon Route 53 Resolver	740
AWS Certificate Manager Certificado (ACM)	741
Cifrado de datos en AMS	742
Identity and Access Management	743
La IAM de Multi-Account Landing Zone (MALZ) protege	744
Autenticación con identidades	744
Registro y supervisión de eventos de seguridad	766
Seguridad de terminales (EPS)	766
Proceso de mitigación de malware	771
Seguridad de Amazon Inspector	773
Respuesta a incidentes de AMS	775
Validación de conformidad	776
Zona de destino multicuenta: visualización del estado de cumplimiento de su Reglas de	
AWS Config	777
Restricciones de la política de control del servicio de landing zone multicuenta de AMS	778
Resiliencia	778
Seguridad de la infraestructura	778
Prácticas recomendadas de seguridad	811
Configuración no predeterminada del EPS de la zona de landing zone multicuenta de	
AMS	811
Barandillas AMS	811
Políticas de control del servicio MALZ	812
Respuesta a incidentes de seguridad	812
Funcionamiento	813
Preparación	813
Detect	814
Análisis	815
Contención	816
Erradicación	818
Recuperar	819
Informe posterior al incidente	819

Guías de respuesta a incidentes de seguridad	820
Revisiones de seguridad de solicitudes de cambio en AMS Advanced	827
Proceso de gestión de riesgos de seguridad del cliente	827
Estándares técnicos AMS Advanced	828
Controles estándar en AMS Advanced	828
Cambios que introduzcan riesgos de seguridad altos o muy altos en su entorno	856
Gestión de la continuidad	859
¿Qué es la gestión de la continuidad?	859
Cómo funciona la gestión de la continuidad	859
Planes de copia de seguridad	860
Almacenes de copias de seguridad	864
Tipos de cambios de Backup	865
Supervisión e informes de las copias de seguridad	866
Respuesta de recuperación ante desastres	866
Planificación de la recuperación ante desastres	867
Multisitio o de alta disponibilidad (HA)	868
Espera semiactiva	868
Luz piloto	870
Copia de seguridad y restauración	871
Administración de parches	876
AMS Patch Orchestrator: un modelo de parches basado en etiquetas	877
Uso de Patch Orchestrator	879
Requisitos previos de Patch Orchestrator	883
Ventanas de parches	884
Notificaciones de parches	885
líneas de base de revisiones	888
Etiquetas reservadas de Patch Orchestrator	888
Aplicación de parches bajo demanda	889
Parqueo estándar AMS	889
Sistemas operativos compatibles	891
Parches compatibles	891
Diseño de parches e infraestructura	894
Cómo funcionan los parches estándar AMS	894
Fallos de parqueo estándar AMS	900
Acciones que puede realizar en la aplicación de parches estándar de AMS	900
Parqueo estándar AMS FAQs	904

Compromisos de servicio de parcheo	906
Aplicación de parches estándar	906
Parches críticos	908
Informes y opciones	912
Informes a petición	912
Informes de parches de AMS	913
Informes de AMS Backup	922
Informes de Top Talkers prevenidos y seguimiento	925
Informe de detalles de cargos de facturación	927
Informes de Trusted Remediator	929
Informes de autoservicio	932
Operaciones de API internas	933
Informe de parches (diario)	937
Informe de Backup (diario)	947
Informe de incidentes (semanal)	952
Informe de facturación (mensual)	956
Informes agregados	959
Paneles de informes de autoservicio de AMS	961
Política de conservación de los datos	969
Fuera de SSR	969
Cómo obtener ayuda	971
Administración de incidentes	971
¿Qué es la gestión de incidentes?	973
Compromisos del servicio de gestión de incidentes	974
Ejemplos de gestión de incidentes	977
Gestión de solicitudes de servicio	983
Cuándo utilizar una solicitud de servicio	984
Cómo funciona la administración de solicitudes de servicio	985
Probar una solicitud de servicio	986
Crear una solicitud de servicio	986
Supervisión y actualización de las solicitudes de servicio	989
Responder a una solicitud de servicio generada por AMS	990
Preguntas sobre facturación	991
Operaciones bajo demanda	992
Solicitar AMS Operations On Demand	1002
Realizar cambios en las ofertas de Operations on Demand	1003

Historial de documentos 1004

Actualizaciones anteriores 1023

..... mlv

¿Qué es AWS Managed Services?

Bienvenido a AWS Managed Services (AMS), administración de operaciones de infraestructura para Amazon Web Services (AWS). AMS es un servicio empresarial que proporciona una gestión continua de su AWS infraestructura.

Esta guía del usuario está destinada a profesionales de TI y desarrolladores de aplicaciones. Se presupone tener un conocimiento básico de los términos y prácticas de funcionalidad de TI, redes e implementación de aplicaciones.

AMS implementa las mejores prácticas y mantiene su infraestructura para reducir los gastos operativos y los riesgos. AMS proporciona servicios durante todo el ciclo de vida para aprovisionar, ejecutar y respaldar su infraestructura, y automatiza las actividades comunes, como las solicitudes de cambios, la supervisión, la administración de parches, la seguridad y los servicios de respaldo. AMS aplica sus políticas de infraestructura corporativa y de seguridad y le permite desarrollar soluciones y aplicaciones utilizando el enfoque de desarrollo que prefiera.

Para comprender mejor la arquitectura AMS, consulte [estos diagramas](#).

Temas

- [Acerca de esta guía de usuario de AMS](#)
- [Planes de operaciones de AMS](#)
- [Introducción a AWS Managed Services](#)
- [Términos clave de AMS](#)
- [Descripción del servicio](#)
- [Recursos de información de AMS](#)
- [Conformidad con AMS](#)
- [Imágenes de máquinas AMS Amazon \(AMIs\)](#)
- [Cómo funciona la integración entre AD FS y AMS](#)
- [Active Directory gestionado por AMS](#)
- [Implementaciones de aplicaciones AMS](#)

 Note

Regiones de AWS Los nuevos se añaden con frecuencia. Para conocer los sistemas operativos compatibles con AMS más recientes y los más recientes compatibles con AMS Regiones de AWS, consulte. [Configuraciones admitidas](#)
[Para obtener más información, consulte Regiones de AWS Administración. Regiones de AWS](#)

AMS busca mejorar continuamente nuestros servicios en función de sus comentarios. Utilizamos varios mecanismos para facilitar el autoservicio, automatizar las tareas repetitivas e implementar nuevas Servicios de AWS funciones a medida que se lanzan. Puede enviar una solicitud de servicio de AMS en cualquier momento para sugerir nuevas funciones o mejoras en las funciones.

El horario de atención de AMS es las 24 horas del día, los 7 días de la semana, los 365 días del año.

AMS sigue un conjunto de prácticas para la gestión de servicios de TI (ITSM) que se centran en alinear los servicios de TI con las necesidades de su empresa.

Acerca de esta guía de usuario de AMS

Esta guía del usuario está destinada a los clientes de AMS Advanced con una zona de aterrizaje con varias cuentas o con una sola cuenta. Para obtener más información sobre las ofertas de zonas de aterrizaje de AMS, consulte los [términos clave de AMS](#); consulte también la arquitectura de zonas de [aterrizaje multicuenta y la arquitectura de zonas](#) de [aterrizaje de cuentas únicas](#).

Planes de operaciones de AMS

AWS Managed Services (AMS) está disponible con dos planes de operaciones: AMS Accelerate y AMS Advanced. Un plan de operaciones ofrece un conjunto específico de características y tiene diferentes niveles de servicio, capacidades técnicas, requisitos, precios y restricciones. Nuestros planes de operaciones le ofrecen la flexibilidad de seleccionar las capacidades operativas del tamaño adecuado para cada una de sus cargas de AWS trabajo. En esta sección, se describen las capacidades y las diferencias, así como las responsabilidades, características y beneficios asociados a cada plan, para que pueda entender qué plan de operaciones es el mejor para sus cuentas.

Para ver una comparación detallada de las características de los dos planes de operaciones, consulte [Características de AWS Managed Services](#).

Plan de operaciones de AMS Accelerate

AMS Accelerate es el plan de operaciones de AMS que le ayuda a gestionar la day-to-day infraestructura de su AWS entorno nuevo o existente. AMS Accelerate ofrece servicios operativos, como supervisión, gestión de incidentes y seguridad. AMS Accelerate también ofrece un complemento de parche opcional para las cargas de trabajo EC2 basadas en Amazon que requieren parches periódicos.

Con AMS Accelerate, usted decide cuáles Cuentas de AWS quiere que opere AMS Accelerate, las regiones de AWS en las que quiere que opere AMS Accelerate, los complementos que necesita y los acuerdos de nivel de servicio (SLAs) que necesita. Para obtener más información, consulte [Uso del plan de operaciones y la descripción del servicio de AMS Accelerate](#).

Plan de operaciones de AMS Advanced

AMS Advanced proporciona servicios de ciclo de vida completo para aprovisionar, ejecutar y dar soporte a su infraestructura. Además de los servicios operativos proporcionados por AMS Accelerate, AMS Advanced también incluye servicios adicionales, como la gestión de las zonas de aterrizaje, los cambios y el aprovisionamiento de la infraestructura, la gestión del acceso y la seguridad de los terminales.

AMS Advanced despliega una landing zone a la que migras tus AWS cargas de trabajo y recibes los servicios operativos de AMS. Nuestras zonas de destino gestionadas con múltiples cuentas vienen preconfiguradas con la infraestructura necesaria para facilitar la autenticación, la seguridad, la creación de redes y el registro.

AMS Advanced también incluye un sistema de gestión de cambios y accesos que protege sus cargas de trabajo al impedir el acceso no autorizado o la implementación de cambios riesgosos en su infraestructura. AWS Los clientes deben crear una solicitud de cambio (RFC) mediante nuestro sistema de gestión de cambios para implementar la mayoría de los cambios en sus cuentas de AMS Advanced. Puede crear cambios RFCs a partir de una biblioteca de cambios automatizados previamente examinados por nuestros equipos de seguridad y operaciones, o bien solicitar cambios manuales que son revisados e implementados por nuestro equipo de operaciones si los considera seguros y compatibles con AMS Advanced.

AMS Advanced también ofrece diferentes opciones. SLAs Para obtener más información, consulte la [descripción del servicio AWS Managed Services AMS Advanced](#).

Introducción a AWS Managed Services

Para obtener información sobre cómo empezar a utilizar el servicio AMS de zona de aterrizaje multicuenta, consulte la Introducción a la [incorporación de AWS Managed Services](#). Las dos guías de incorporación proporcionan descripciones del servicio y preguntas que debe tener en cuenta para ayudarle a empezar. Consulte el conjunto de [funciones, las características de AWS Managed Services](#) y los recursos actuales en [AWS Managed Services Resources](#).

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.

Descripción del servicio

AMS Advanced (AMS) es un plan operativo del servicio AWS Managed Services para gestionar las operaciones de su AWS infraestructura. AMS Advanced proporciona operaciones de infraestructura rutinarias, como la gestión de parches, la gestión de la continuidad, la gestión de la seguridad y los procesos de gestión de TI, como la gestión de incidentes, cambios y solicitudes de servicio. Para obtener una lista de los servicios compatibles, consulte [AWS Servicios compatibles](#).

YouTube Vídeo: [¿Cómo puede ayudarme AMS a lograr la excelencia operativa en la nube?](#)

Temas

- [Características del plan operativo avanzado de AWS Managed Services \(AMS\) AMS](#)
- [Lo que hacemos, lo que no hacemos](#)
- [Matriz de responsabilidad de AMS \(RACI\)](#)
- [Componentes básicos del entorno AMS](#)
- [Límites de cuentas AMS](#)
- [Objetivos de nivel de servicio de AMS \(SLOs\)](#)
- [AWS Servicios compatibles](#)
- [Configuraciones admitidas](#)
- [Capacidades para sistemas operativos no compatibles en AMS](#)
- [Interfaces avanzadas AMS](#)
- [Puntos finales de VPC de AMS](#)
- [Espacios de nombres protegidos por AMS](#)
- [Prefijos reservados AMS](#)
- [Ventana de mantenimiento de AMS](#)

Características del plan operativo avanzado de AWS Managed Services (AMS) AMS

AMS Advanced ofrece las siguientes funciones para AWS los servicios compatibles:

- Registro, monitoreo, banderas y administración de eventos:

AMS configura y supervisa su entorno gestionado para registrar la actividad y define las alertas en función de una variedad de comprobaciones de estado. AMS investiga las alertas de los servicios de AWS aplicables y las que afectan negativamente al uso de esos servicios provocan incidentes. AMS agrega y almacena todos los registros generados como resultado de todas las operaciones y los registros del sistema en Amazon S3. CloudWatch CloudTrail Puede solicitar que se pongan en marcha alertas adicionales. Además de los controles preventivos de AMS, AMS implementa banderas de configuración y controles de detección para protegerlo continuamente contra errores de configuración que podrían reducir la integridad operativa y de seguridad de las cuentas gestionadas, a fin de reforzar sus controles, como el etiquetado y el cumplimiento. Cuando

se detecta un control supervisado, se genera una alarma que provoca la notificación, modificación o cancelación de los recursos en función de los valores predeterminados de AMS predefinidos que usted puede modificar.

- Administración de la continuidad (Backup and Restore):

AMS proporciona copias de seguridad de los recursos mediante la funcionalidad de AWS Backup estándar existente en un intervalo programado que usted determine. AMS puede realizar acciones de restauración a partir de instantáneas específicas con su RFC. Usted es responsable de realizar copias de seguridad de los cambios en los datos que se produzcan entre los intervalos de las instantáneas. Puede enviar una RFC para las solicitudes de copias de seguridad o instantáneas fuera de los intervalos programados. En caso de que la zona de disponibilidad (AZ) no esté disponible en una AWS región, con su permiso, AMS restaura el entorno gestionado mediante la recreación de nuevas pilas en función de las plantillas y las instantáneas de EBS disponibles de las pilas afectadas.

- Administración de seguridad y acceso:

AMS proporciona seguridad para terminales (EPS), por ejemplo, configurando la protección antivirus y antimalware. También puede utilizar sus propias herramientas y procesos de EPS y no utilizar AMS para EPS mediante una función llamada traiga su propio EPS (BYOEPS). AMS también configura las capacidades de AWS seguridad predeterminadas que usted aprueba durante la incorporación, como las funciones AWS Identity and Access Management (IAM) y los grupos de EC2 seguridad de Amazon, y utiliza AWS herramientas estándar (por ejemplo, Amazon AWS Security Hub Macie o Amazon GuardDuty) para supervisar y responder a los problemas de seguridad. Usted administra sus usuarios a través de un servicio de directorio aprobado que usted proporciona. Para obtener una lista de los servicios de directorio aprobados, consulte [Configuraciones admitidas](#).

AMS incluye seguridad para terminales (EPS), que incluye antivirus (AV), y protección antimalware, detección de malware e intrusiones (Trend Micro). Los grupos de seguridad se definen por plantilla de pila y se modifican en el momento del lanzamiento en función de la visibilidad de los grupos de seguridad de la aplicación (públicos o privados).

El acceso a los sistemas se solicita mediante las solicitudes de cambio de la administración de cambios (RFCs). La administración de acceso proporciona acceso a distintos recursos, como EC2 las instancias de Amazon AWS Management Console, y APIs. Tras establecer una confianza unidireccional con una implementación de Microsoft Active Directory de AMS durante la

incorporación y la federación a AWS, puede utilizar sus credenciales corporativas actuales para todas las interacciones.

- Administración de parches:

AMS aplica e instala actualizaciones en las EC2 instancias de los sistemas operativos compatibles (OSs) y en el software preinstalado con los sistemas operativos compatibles. Para obtener una lista de los sistemas operativos compatibles, consulte. [Configuraciones admitidas](#)

AMS ofrece dos modelos de parches:

- El parche estándar de AMS para la aplicación tradicional de parches basada en cuentas, y
- AMS Patch Orchestrator, para parches basados en etiquetas.

En el parche estándar de AMS, usted elige un período de mantenimiento mensual para que AMS lleve a cabo la mayoría de las actividades de aplicación de parches. AMS aplica las actualizaciones de seguridad críticas fuera del período de mantenimiento seleccionado (con las notificaciones correspondientes) y las actualizaciones importantes durante el período de mantenimiento seleccionado. AMS también aplica las actualizaciones a las herramientas de administración de la infraestructura durante el período de mantenimiento seleccionado. Si lo desea, puede excluir las pilas de la administración de parches o rechazar las actualizaciones.

Con AMS Patch Orchestrator, usted define un período de mantenimiento predeterminado por cuenta para que AMS lleve a cabo las actividades de aplicación de parches. Puede programar períodos de mantenimiento personalizados adicionales para que AMS repare con etiquetas un conjunto específico de instancias que haya definido. AMS aplica todas las actualizaciones disponibles, pero puede filtrarlas o rechazarlas creando una línea base de parches personalizada. En ambos modelos, si apruebas o rechazas una actualización proporcionada en el marco de la gestión de parches, pero cambias de opinión más adelante, eres responsable de iniciar la actualización mediante una RFC. AMS hace un seguimiento del estado de los parches de los recursos y resalta los sistemas que no están actualizados en la revisión empresarial mensual. La administración de parches se limita a las pilas del entorno gestionado, incluidas todas las aplicaciones gestionadas por AMS y los servicios de AWS compatibles con funciones de aplicación de parches (por ejemplo, RDS). Para admitir todos los tipos de configuraciones de infraestructura cuando se publica una actualización, AMS a) actualiza la EC2 instancia y b) proporciona una AMI de AMS actualizada para que la utilice. Es su responsabilidad instalar, configurar, aplicar parches y supervisar cualquier aplicación adicional que no se haya mencionado específicamente anteriormente.

- Administración de cambios:

La gestión de cambios de AMS es el mecanismo que le permite controlar los cambios en su entorno gestionado. AMS utiliza una combinación de controles preventivos y de detección para facilitar este proceso y proporciona diferentes niveles de control y riesgo asociado en función del modo AMS seleccionado.

Todas las acciones de su entorno AMS están registradas. AWS CloudTrail

Para obtener más información sobre la gestión de cambios de AMS y los diferentes modos, consulte la [guía de gestión de cambios de AMS y los modos de AMS](#).

- Gestión de aprovisionamiento automatizada y de autoservicio:

Puede aprovisionar recursos de AWS en AMS Advanced de varias maneras:

- Envíe solicitudes de cambio de aprovisionamiento y configuración () RFCs
 - Implemente mediante AWS Service Catalog
 - Implemente mediante el [modo Direct Change](#)
 - Implemente mediante [el modo Desarrollador](#). Recuerde que AMS no administra los recursos creados mediante el modo Desarrollador.
 - Configure los servicios de AWS directamente mediante el aprovisionamiento de autoservicio para seleccionar Servicios de AWS (consulte [AWS Servicios compatibles](#)).
- Gestión de incidentes:

AMS le notifica de forma proactiva los incidentes detectados por AMS. AMS responde tanto a los incidentes enviados por los clientes como a los generados por AMS y los resuelve en función de la prioridad de los incidentes. A menos que indique lo contrario, los incidentes que AMS determine que representan un riesgo para la seguridad de su entorno gestionado y los incidentes relacionados con la disponibilidad de AMS y otros servicios de AWS se toman medidas de forma proactiva. AMS tomará medidas en relación con todos los demás incidentes una vez que reciba su autorización. Los incidentes recurrentes se abordan mediante el proceso de gestión de problemas.

- Gestión de problemas:

AMS realiza un análisis de tendencias para identificar e investigar los problemas e identificar la causa raíz. Los problemas se solucionan con una solución alternativa o permanente que evite que se repita un impacto similar en el servicio en el futuro. Se puede solicitar un informe posterior al incidente (PIR) para cualquier incidente «grave», una vez resuelto el problema. El PIR recoge la causa raíz y las medidas preventivas adoptadas, incluida la implementación de medidas preventivas.

- **Presentación de informes:**

AMS le proporciona un informe de servicio mensual en el que se resumen las principales métricas de rendimiento de AMS, que incluye un resumen ejecutivo y perspectivas, las métricas operativas, los recursos gestionados, el cumplimiento del acuerdo de nivel de servicio (SLA) de AMS y las métricas financieras relacionadas con los gastos, el ahorro y la optimización de costes. Los informes los entrega el gestor de prestación de servicios en la nube (CSDM) de AMS que se le asigne.

- **Gestión de solicitudes de servicio:**

Para solicitar información sobre su entorno gestionado, su AMS o sus ofertas de AWS servicios, envíe las solicitudes de servicio mediante la consola de AMS. Puede enviar una solicitud de servicio si tiene preguntas prácticas sobre AWS los servicios y las funciones o para solicitar servicios AMS adicionales.

- **Mesa de servicio:**

AMS dota de personal de operaciones de ingeniería a empleados de Amazon a tiempo completo para cumplir con las solicitudes no automatizadas, incluida la gestión de incidentes, la gestión de solicitudes de servicio y la gestión de cambios. La mesa de servicio funciona las 24 horas del día, los 7 días de la semana, los 365 días del año.

- **Recursos designados:**

A cada cliente se le asigna un administrador de prestación de servicios en la nube (CSDM) y un arquitecto de nube (CA).

- CSDMs se puede contactar directamente. Realizan revisiones de los servicios y proporcionan informes e información a lo largo de todas las fases del ciclo de vida de la implementación, la migración y las operaciones. CSDMs realizan revisiones empresariales mensuales y detallan aspectos como el gasto financiero, las recomendaciones de ahorro de costes, la utilización de los servicios y los informes de riesgos. Profundizan en las estadísticas de rendimiento operativo y proporcionan recomendaciones sobre las áreas de mejora.
- CAs puede ponerse en contacto directamente con nosotros y proporcionarle conocimientos técnicos que le ayuden a optimizar el uso de la AWS nube. Algunas de las actividades de CA incluyen seleccionar las cargas de trabajo para la migración, ayudar a incorporar cuentas y cargas de trabajo adicionales, actuar como líder técnico en las actividades operativas, como los días de juego, las pruebas de recuperación ante desastres, la gestión de problemas y el asesoramiento técnico para aprovechar al máximo AMS y. AWS CAs Impulse los debates

técnicos en todos los niveles de su organización y ayude a gestionar los incidentes, hacer concesiones, establecer las mejores prácticas y mitigar los riesgos técnicos.

- Modo desarrollador:

Esta función le permite iterar diseños e implementaciones de infraestructura rápidamente dentro de las cuentas configuradas por AMS [1] al permitir el acceso directo al servicio de AWS y a APIs la consola de AWS, además del acceso al proceso de administración de cambios de AMS. La gestión de los recursos aprovisionados o configurados con permisos en modo desarrollador fuera del proceso de gestión de cambios es responsabilidad suya (consulte la sección «Gestión del aprovisionamiento automatizada y de autoservicio»). Los recursos aprovisionados mediante el proceso de gestión de cambios de AMS son compatibles, al igual que otras cargas de trabajo aprovisionadas por la gestión de cambios en AMS.

- Soporte de AWS:

Los clientes de AMS pueden elegir el nivel de AWS Support que necesitan para complementar su plan de operaciones de AMS. Las cuentas inscritas en AMS se pueden suscribir a Business Support o Enterprise Support. Para obtener más información sobre las diferencias entre los planes de soporte, consulte los [planes de AWS Support](#).

- Cuenta gestionada por el cliente:

Esta función le permite solicitar cuentas de AWS en el mismo entorno gestionado, pero las operaciones continuas de las cargas de trabajo y los recursos de AWS dentro de esas cuentas son su responsabilidad. AMS aprovisiona cuentas administradas por los clientes, pero una vez creadas las cuentas, no se les proporciona ninguna otra función o servicio de AMS. AWS no inscribirá las cuentas administradas por los clientes en el soporte premium de nivel empresarial. Será su responsabilidad inscribir las cuentas administradas por el cliente en AWS Support con la tasa de soporte que elija.

- Administración de firewalls:

AMS ofrece una solución de firewall gestionado opcional para los servicios de firewall compatibles, que permite filtrar el tráfico de salida con destino a Internet para las redes de su entorno gestionado. Esto excluye los servicios públicos que no utilizan la infraestructura de red de AWS y cuyo tráfico va directamente a Internet. La solución combina la tecnología de firewall líder del sector con las capacidades de administración de la infraestructura de AMS para implementar, monitorear, administrar, escalar y restaurar la infraestructura de firewall.

Cuando incorpore AMS, recibirá una lista completa de su infraestructura de red AMS. Para obtener en cualquier momento una lista actualizada de los servicios que se están ejecutando en apoyo de su infraestructura de AMS, presente una solicitud de servicio con información específica sobre la información que desee. Para solicitar un cambio en el diseño de la red, cree una solicitud de servicio que describa los cambios que desea realizar, por ejemplo, agregar una VPC o solicitar un cambio en las reglas de un grupo de seguridad.

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.

Matriz de responsabilidad de AMS (RACI)

Note

Para cumplir con sus obligaciones en el momento oportuno, AWS Managed Services (AMS) puede requerir su opinión para decidir el curso de acción adecuado. AMS se pondrá en contacto con la persona de contacto designada por el cliente para solicitar cualquier aclaración e información al respecto. AMS esperará recibir una respuesta a dichas consultas en un plazo de 24 horas laborables. En caso de que no reciba respuesta en un plazo de 24 horas laborables, AMS podrá elegir una acción en su nombre.

La matriz responsable, responsable, consultada e informada de AMS, o RACI (por sus siglas en inglés), asigna la responsabilidad principal al cliente o a AMS por una variedad de actividades.

AMS administra su infraestructura de AWS. La siguiente tabla proporciona un resumen de las responsabilidades del cliente y de AMS en relación con las actividades del ciclo de vida de una aplicación que se ejecuta en un entorno gestionado por AMS.

AMS no es responsable de ninguna de las siguientes actividades relacionadas con las cuentas gestionadas por el cliente ni con la infraestructura que se ejecuta en ellas; por lo tanto, esta RACI no es aplicable.

- R significa parte responsable que hace el trabajo para lograr la tarea.
- C significa consultada; parte cuya opinión se solicita, por lo general en calidad de expertos en la materia; y con la que existe comunicación bilateral.
- I significa informado; una parte que recibe información sobre el progreso, a menudo solo una vez finalizada la tarea o el producto final.

- El aprovisionamiento de autoservicio se refiere a los recursos que aprovisiona el cliente mediante el autoservicio a través de la AWS API o la consola, incluidos el modo de desarrollador y los servicios aprovisionados de autoservicio.

 Note

Algunas secciones contienen una «R» tanto para AMS como para Clientes. Esto se debe a que, en el modelo de responsabilidad AWS compartida, tanto AMS como los clientes asumen una propiedad conjunta para responder a los problemas de infraestructura y aplicaciones.

Para ofrecer capacidades de aprovisionamiento de autoservicio, AMS ha creado funciones de IAM más amplias con límites de permisos para limitar los cambios imprevistos derivados del acceso directo a los servicios. AWS Las funciones no impiden todos los cambios y usted es responsable de cumplir con sus controles internos y cumplir con las normas y de validar que todos los AWS servicios que utilice cumplan con las certificaciones requeridas. A esto lo denominamos modo de aprovisionamiento de autoservicio. [Para obtener más información sobre los requisitos AWS de conformidad, consulte AWS Cumplimiento.](#)

En el caso de los recursos que usted aprovisiona mediante el autoservicio, AMS proporciona gestión de incidentes, controles de detección y vigilancia, elaboración de informes, recursos designados (administrador de prestación de servicios en la nube y arquitecto de nube), seguridad y acceso, y asistencia técnica mediante 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.

Actividad	Cliente	AWS Managed Services (AMS)
Ciclo de vida de la aplicación		
Desarrollo de aplicaciones	R	I
Análisis y diseño de los requisitos de la infraestructura de aplicaciones	R	C

Actividad	Cliente	AWS Managed Services (AMS)
Diseño y optimización para pilas de AMS no estándar	R	C
Diseño y optimización de la pila estándar AMS	I	R
Implementación de aplicaciones	R	C
Implementación de la infraestructura de AWS	C	R
Supervisión de aplicaciones	R	I
Pruebas y optimización de aplicaciones	R	I
Guía de optimización de infraestructuras de AWS	I	R
Supervisión de la infraestructura de AWS	I	R
Solucione y resuelva los problemas de las aplicaciones	R	C
Solucionar y resolver problemas de red de AWS	C	R
Solucione y resuelva los problemas del sistema operativo y la infraestructura	C	R
Aprovisionamiento de autoservicio	R	C
Integración de aplicaciones e ITSM		
Integración de aplicaciones con ofertas de servicios de AWS	R	C
Integración de ITSM con la interfaz AWS Managed Services	R	C
Redes		

Actividad	Cliente	AWS Managed Services (AMS)
Configuración y configuración de VPC y VPC de entorno gestionado	C	R
Asigne espacio de direcciones privadas para (por ejemplo, VPCs /16)	R	C
Configurar y operar servicios gestionados ajenos a AWS, gestionados por el cliente Firewalls/Proxy/Bastions/HOSTs	R	C
Configure y utilice la seguridad de AWS Groups/NAT/Customer Bastions/NACL dentro del entorno gestionado	I	R
Configuración e implementación de redes (por ejemplo DirectConnect) dentro de la red del cliente	R	C
Configuración e implementación de redes en el entorno gestionado	C	R
Configuración del entorno gestionado		
Defina la configuración de Auto Scaling predeterminada para las plantillas de pila de referencia	I	R
Recomiende la optimización de RI	C	R
Adquiera capacidad de RI y PIOP	R	C
Elimine la capacidad cuando la capacidad esté sobreaprovisionada (cuando la aplicación del cliente lo admita)	C	R

Actividad	Cliente	AWS Managed Services (AMS)
Cree o actualice información específica del cliente de AWS para AWS Managed Services	C	R
Configuración de S3	C	R
Aprovisionamiento de autoservicio	R	C
Configuración de Glacier	C	R
Defina la política de archivado	R	C
Configuración de la política de archivado	C	R
Selección de la ventana de mantenimiento del cliente	R	I
Administración de AWS RDS		
Controle el estado de source/replica/RO la replicación	I	R
Identifique el RCA de la conmutación por error de origen	I	R
Configuración automática de instantáneas (copias de seguridad)	C	R
Aprovisionamiento de autoservicio	R	C
Coordine y programe la gestión de los parches del motor de base	C	R
Aprovisionamiento de autoservicio	R	C
Se recomienda el almacenamiento de bases de datos y la capacidad de PIOP	C	R
Aprovisionamiento de autoservicio	R	C

Actividad	Cliente	AWS Managed Services (AMS)
Recomiende el tamaño de las instancias para ejecutar bases de datos	C	R
	R	C
Aprovisionamiento de autoservicio		
Se recomienda la optimización de la RI para el entorno gestionado	C	R
	R	C
Aprovisionamiento de autoservicio		
Supervisión del rendimiento de RDS () CloudWatch	C	R
	R	C
Aprovisionamiento de autoservicio		
Configuración de suscripción a eventos (SNS) de RDS	C	R
	R	C
Aprovisionamiento de autoservicio		
Configuración del grupo de seguridad de RDS	C	R
	R	C
Aprovisionamiento de autoservicio		
Configuración del motor RDS parameter/option	R	C
Diseño de mesa DB	R	I
Indexación de bases de datos	R	I
Análisis de registros de bases de datos	R	I
Gestión de cambios en AMS		

Actividad	Cliente	AWS Managed Services (AMS)
Creación de clientes RFCs (por ejemplo, acceso a recursos, creating/updating/deleting managed stacks, deploying/updating aplicaciones, cambios en la configuración de las ofertas de AWS servicios)	R	I
Cliente aprobador RFCs	I	R
Creación de AWS Managed Services RFCs (por ejemplo, acceso a los recursos, creación de recursos en nombre del cliente, aplicación de actualizaciones al sistema operativo como parte de la administración de parches)	I	R
Aprobación de forma no automática RFCs	R	I
Enviar una solicitud de nuevos tipos de cambio	R	C
Crear nuevos tipos de cambio	I	R
Mantenimiento del calendario de cambios de la aplicación	R	C
Aviso de la próxima ventana de mantenimiento	I	R
AWS Service Catalog		
Cree carteras y productos	R	I
Distribuya los productos a los usuarios finales	R	I
Cree etiquetas y una biblioteca de opciones de etiquetas	R	C
Compartir carteras y productos con los usuarios finales	R	I

Actividad	Cliente	AWS Managed Services (AMS)
Revise o actualice carteras y productos	R	I
Cree y asigne restricciones a carteras y productos	R	C
Asocie las acciones de servicio a los productos	R	C
Actualice los recursos aprovisionados con la nueva versión del producto	R	I
Aprovisionando		
Adiciones específicas para cada cliente a la AMI básica de AWS Managed Services	R	C
Configure otros tipos de cambios aprobados que se utilizan para aprovisionar las plantillas de Stack	C	R
Lance las pilas gestionadas y los recursos de AWS asociados enviados mediante el proceso de gestión de cambios de AMS o AWS Service Catalog.	I	R
	R	I
Aprovisionamiento de autoservicio		
Install/Update aplicaciones personalizadas y de terceros en instancias aprovisionadas mediante el proceso de administración de cambios de AMS o AWS Service Catalog.	R	I
Aprovisionamiento: arquitectura Stack		

Actividad	Cliente	AWS Managed Services (AMS)
Proporcionar licencias de sistema operativo (incluidas las tarifas de uso de los servicios de AWS aplicables, por ejemplo, EC2 y RDS)	I	R
	R	I
Aprovisionamiento de autoservicio		
Defina plantillas de infraestructura básicas (pilas) para la implementación de aplicaciones mediante el sistema de gestión de cambios AMS.	I	R
	R	I
Aprovisionamiento de autoservicio		
Se aprobó la creación de la línea base 8 AMIs	I	R
Evalúe el inventario de aplicaciones de los clientes y determine si se ajustan a las plantillas de infraestructura disponibles (Stacks)	R	C
Defina pilas únicas que se sumen a las ofertas de plantillas básicas	R	C
Registro, supervisión y gestión de eventos		
Grabación de registros de cambios en la infraestructura de AWS	I	R
Registrar todos los registros de cambios de las aplicaciones	R	C
Instalación y configuración de agentes y scripts para la aplicación de parches, la seguridad , la supervisión, etc., de la infraestructura de AWS aprovisionada mediante el proceso de administración de cambios de AMS.	I	R
	R	C
Aprovisionamiento de autoservicio		

Actividad	Cliente	AWS Managed Services (AMS)
Defina los requisitos de supervisión e incidentes específicos del cliente	R	C
Configuración de alertas para el entorno gestionado	I	R
Supervisión de todas las alertas configuradas por AMS	I	R
	R	C
Aprovisionamiento de autoservicio		
Investigando las alertas de infraestructura para la notificación de incidentes	I	R
	R	C
Aprovisionamiento de autoservicio		
Investigando las alarmas de las aplicaciones	R	C
Gestión de incidentes		
Notifique de forma proactiva los incidentes en la infraestructura de AWS en función de la supervisión	I	R
	R	C
Aprovisionamiento de autoservicio		
Gestione los problemas y las interrupciones del rendimiento de las aplicaciones	R	I
Clasifique la prioridad de los incidentes	I	R
Proporcione una respuesta al incidente	I	R

Actividad	Cliente	AWS Managed Services (AMS)
Proporcione la resolución de incidentes o la restauración de la infraestructura  Note SLAs no se aplican a los recursos basados en instancias aprovisionados fuera de AMS Change Management, incluidos los aprovisionados mediante el aprovisionamiento de autoservicio y el modo de desarrollador.	C	R
Gestión de problemas		
Identifique los problemas en el entorno gestionado	C	R
Realice un RCA para los problemas en un entorno gestionado	C	R
Solución de problemas en un entorno gestionado	C	R
Identifique y solucione los problemas de las aplicaciones	R	I
Gestión de la seguridad		
Seguridad de la infraestructura del cliente: and/or establecimiento de una base para el proceso de cumplimiento de normas de seguridad, según lo determinado y acordado durante la incorporación del cliente.	C	R
	R	C
Aprovisionamiento de autoservicio		

Actividad	Cliente	AWS Managed Services (AMS)
Mantener licencias válidas para Managed EPS	R	C
Configure el EPS gestionado	I	R
Aprovisionamiento de autoservicio	R	C
Actualice el EPS gestionado	I	R
Aprovisionamiento de autoservicio	R	C
Supervisión del malware en las instancias aprovisionadas mediante el proceso AMS CM.	I	R
Aprovisionamiento de autoservicio	R	C
Mantenimiento y actualización de las firmas de virus.	I	R
Aprovisionamiento de autoservicio	R	C
Corregir las instancias infectadas con malware.	C	R
Aprovisionamiento de autoservicio	R	C
Gestión de eventos de seguridad	C	R
Seguridad: gestión de acceso		
Gestione el ciclo de vida de los usuarios y sus permisos para los servicios de directorio locales, que se utilizan para acceder a AWS Managed Services	R	I
Utilice sistemas de autenticación federada para que los clientes accedan a AWS la consola/ APIs	R	C

Actividad	Cliente	AWS Managed Services (AMS)
Acepte y mantenga la confianza de Active Directory (AD) desde AWS Managed Services AD hasta AD gestionado por el cliente	R	C
Durante la incorporación, cree funciones de administrador de IAM multicuenta en cada cuenta gestionada	R	C
Proteja la credencial AWS raíz de cada cuenta	I	R
Defina los recursos de IAM para el entorno gestionado	C	R
Administre las credenciales privilegiadas para el acceso al sistema operativo de los ingenieros de AMS	I	R
Administre las credenciales privilegiadas para el acceso al sistema operativo proporcionadas al cliente por AMS	R	I
Respuesta a un incidente de seguridad: prepárese		
Comunicaciones		
Proporcione los datos de contacto de seguridad del cliente para que AMS los utilice durante los eventos de seguridad, las notificaciones y las escaladas de seguridad	R	I
Guarde y gestione los datos de contacto de seguridad del cliente proporcionados para utilizarlos durante los eventos de seguridad y las escaladas de seguridad	CI	R
Entrenamiento		

Actividad	Cliente	AWS Managed Services (AMS)
Proporcione al cliente la documentación necesaria para respaldar a AMS durante el proceso de respuesta a incidentes	I	R
Practique la responsabilidad compartida durante los procesos de respuesta a incidentes mediante jornadas de juego sobre seguridad	RI	ARC
Administración de recursos		
Configure la gestión de seguridad compatible Servicios de AWS para las alertas, la correlación de alertas, la reducción del ruido y otras reglas	I	R
Mantenga un inventario de activos (AWS recursos) y conozca el valor y la criticidad de los activos. Esta información es útil durante la estrategia de contención de incidentes	R	CI
Emplee AWS etiquetas para identificar los recursos y las cargas de trabajo	R	CI
Defina y configure la retención y el archivado de registros	CI	R
Base de referencia segura de las configuraciones Cuenta de AWS, las políticas y la administración del acceso	CI	ARC
Respuesta a incidentes de seguridad: detectar		
Registro, indicadores y monitoreo		

Actividad	Cliente	AWS Managed Services (AMS)
Configure el registro y la supervisión para permitir la administración de eventos, por ejemplo, y las cuentas	CI	R
El monitor es compatible con Servicios de AWS las alertas de seguridad	I	R
Implemente y gestione herramientas de seguridad para terminales	CI	R
Supervise las instancias en busca de malware mediante una herramienta de seguridad para endpoints compatible con AMS	I	R
Notifique al cliente los eventos detectados mediante mensajes salientes	I	R
Envíe la notificación y cualquier actualización posterior a los responsables de la toma de decisiones para cuentas y cargas de trabajo específicas a fin de mejorar el tiempo de respuesta a los incidentes	R	CI
Defina, implemente y mantenga los servicios de detección estándar de AMS (por ejemplo, Amazon GuardDuty y AWS Config)	CI	R
Registre los registros AWS de cambios en la infraestructura	I	RC
Habilite y configure el registro y el monitoreo para habilitar la administración de eventos para la aplicación	R	C

Actividad	Cliente	AWS Managed Services (AMS)
Implemente y mantenga una lista de permitidos, una lista de denegaciones y detecciones personalizadas en los servicios de AWS seguridad compatibles (por ejemplo, Amazon GuardDuty)	RCI	R
Informes de eventos de seguridad		
Notifique a AMS de una actividad sospechosa o de una investigación de seguridad activa	R	CI
Notifique al cliente los incidentes y eventos de seguridad detectados	I	R
Notifique el evento planificado que pueda desencadenar el proceso de respuesta a incidentes de seguridad	R	CI
Respuesta a incidentes de seguridad: analice		
Investigación y análisis		
Realice una respuesta inicial a una alerta de seguridad compatible generada por una fuente de detección compatible	I	RC
Evalúe false/true los aspectos positivos utilizando los datos disponibles	RI	ARC
Genere una instantánea de las instancias afectadas para compartirla con el cliente si es necesario	I	R

Actividad	Cliente	AWS Managed Services (AMS)
Realice tareas forenses, como la cadena de custodia, el análisis del sistema de archivos, el análisis forense de la memoria y el análisis binario	R	CI
Recopile los registros de las aplicaciones para facilitar la investigación	R	I
Recopile datos y registros para ayudar a investigar las alertas de seguridad	RCI	RC
Participa SMEs Servicios de AWS en las investigaciones de seguridad	CI	R
Póngase en contacto con proveedores externos durante la investigación (por ejemplo, para que EPS investigue el antimalware y contacte con el equipo de TrendMicro soporte)	RCI	I
Comparta los registros de investigación del equipo de soporte con Servicios de AWS los clientes durante una investigación	I	R
¿Comunicación		
Envíe alertas y notificaciones desde las fuentes de detección de AMS para los recursos gestionados	I	R
Gestione las alertas y las notificaciones de los eventos de seguridad de las aplicaciones	R	I
Comuníquese con el punto de contacto de seguridad del cliente durante la investigación de un incidente de seguridad	R	I

Actividad	Cliente	AWS Managed Services (AMS)

Respuesta a un incidente de seguridad: contiene

Estrategia y ejecución de la contención

Decida la ejecución de la estrategia de contención acordada y acuerde las consecuencias que podrían afectar a la disponibilidad de los servicios durante el período de contención	R	CI
Haga una copia de seguridad de los sistemas afectados para su posterior análisis	CI	R
Contenga las aplicaciones y las cargas de trabajo (mediante la configuración específica de la aplicación o la actividad de respuesta)	R	CI
Defina la estrategia de contención en función del incidente de seguridad y del recurso afectado	CI	R
Habilite el cifrado y el almacenamiento seguro de las copias de seguridad puntuales de los sistemas afectados	CI	R
Ejecute las acciones de contención compatibles para AWS los recursos, incluidas las EC2 instancias, la red y la IAM	CI	R

Respuesta a los incidentes de seguridad: erradicar

Estrategia y ejecución de la erradicación

Defina las opciones de erradicación en función del incidente de seguridad y del recurso afectado en función de las cargas de trabajo de las aplicaciones de los clientes	R	CI

Actividad	Cliente	AWS Managed Services (AMS)
Decida la estrategia de erradicación acordada, el calendario de ejecución de la erradicación y las consecuencias	R	CI
Defina las medidas de erradicación en función del incidente de seguridad y del recurso afectado en las cargas de trabajo gestionadas por AMS	CI	R
Erradicar y reforzar los AWS recursos, incluidas las EC2 instancias, la red y la erradicación de la IAM	CI	R
Erradicar y reforzar las aplicaciones y las cargas de trabajo (mediante una configuración específica de la aplicación o una actividad de respuesta)	R	I
Respuesta a incidentes de seguridad: recuperación		
Preparación y ejecución de la recuperación		
Configure los planes y objetivos de respaldo según lo solicite el cliente	R	I
Revise los planes de respaldo para restaurar las cargas de trabajo gestionadas por AMS	CI	R
Realice actividades de restauración de copias de seguridad para obtener los recursos compatibles Servicios de AWS	I	R

Actividad	Cliente	AWS Managed Services (AMS)
Realice copias de seguridad de la aplicación del cliente, la configuración de la APLICACIÓN y los ajustes de implementación, y revise los planes de respaldo para restaurar las aplicaciones y cargas de trabajo del cliente después de un incidente	R	I
Restaurar las aplicaciones y las cargas de trabajo de los clientes (mediante pasos de restauración específicos de la aplicación)	R	I
Respuesta a un incidente de seguridad: informe posterior al incidente		
Informes posteriores al incidente		
Comparta las lecciones aprendidas y las medidas de acción apropiadas con el cliente después del incidente, según sea necesario	I	R
Administración de parches ⁹		
Supervise las actualizaciones aplicables al sistema operativo compatible y al software preinstalado con el sistema operativo compatible para EC2 las instancias.	I	R
	R	C
Aprovisionamiento de autoservicio		
Notifique al cliente de las próximas actualizaciones (solo se aplica al parche estándar de AMS)	I	R
Excluye determinadas actualizaciones (and/or determinadas pilas) de las actividades de aplicación de parches	R	I

Actividad	Cliente	AWS Managed Services (AMS)
Defina los períodos de mantenimiento predeterminados y personalizados, los cronogramas y otros parámetros (por ejemplo, la duración del período de mantenimiento) para aplicar los parches (se aplica a AMS Patch Orchestrator)	R	I
Defina líneas base de parches personalizadas para filtrar y excluir parches específicos (solo se aplica a AMS Patch Orchestrator)	R	I
Etiquete las instancias para asociarlas a ventanas de mantenimiento y líneas base de parches personalizadas (solo se aplica a AMS Patch Orchestrator)	R	I
Realice un seguimiento del estado de los parches de los recursos y destaque los sistemas que no estén actualizados en la revisión empresarial mensual.	C	R
Parchee el sistema operativo Windows y los paquetes de Microsoft instalados en el sistema operativo que se rigen por Windows Update	I	R
Aprovisionamiento de autoservicio	R	-
Parchee las aplicaciones instaladas, el software o las dependencias de aplicaciones no administradas por Windows Update	R	I
Aprovisionamiento de autoservicio	R	-

Actividad	Cliente	AWS Managed Services (AMS)
Aplica parches al sistema operativo Linux y a cualquier paquete que esté habilitado para su administración mediante el administrador de paquetes nativo del sistema operativo (por ejemplo, Yum, Apt o Zypper)	I	R
Aprovisionamiento de autoservicio	R	-
Parchee las aplicaciones instaladas, el software o las dependencias de aplicaciones no gestionadas por el administrador de paquetes nativo del sistema operativo Linux	R	I
Aprovisionamiento de autoservicio	R	-
Gestión de la continuidad		
Especifique los cronogramas de respaldo	R	I
Ejecute las copias de seguridad según la programación.	I	R
Aprovisionamiento de autoservicio	R	C
Valide los respaldos	R	I
Solicite actividades de restauración de copias de seguridad	R	I
Ejecute actividades de restauración de copias de seguridad.	I	R
Aprovisionamiento de autoservicio	R	C
Restablezca las pilas afectadas y VPCs	I	R
Aprovisionamiento de autoservicio	R	C

Actividad	Cliente	AWS Managed Services (AMS)
Restaurar la aplicación personalizada o de terceros afectada	R	C
Informes		
Prepare y entregue un informe de servicio mensual	I	R
	R	I
AMS activado AWS Outposts		
Configure y recupere el historial de auditorías de la API a pedido (CloudTrail).	I	R
	R	I
Aprovisionamiento de autoservicio		
Proporcione acceso al historial de incidentes a través de la interfaz AWS Managed Services	I	R
Proporcione acceso al historial de cambios a través de la interfaz AWS Managed Services.	I	R
	N/A	N/A
Aprovisionamiento de autoservicio		
Administración de solicitudes de servicio		
Solicite información mediante solicitudes de servicio	R	I
Responder a las solicitudes de servicio	I	R
Firewall gestionado		
Solicite el despliegue de un firewall administrado por AMS	R	I
Diseño y optimización de la arquitectura de firewall gestionado por AMS	I	R

Actividad	Cliente	AWS Managed Services (AMS)
Implementación de la infraestructura de AWS y del dispositivo de firewall administrado por AMS	I	R
Proporcionar licencias de firewall (incluidas las tarifas de uso de los servicios de AWS aplicables, por ejemplo EC2)	R	I
Defina la lista de dominios permitidos predeterminada	I	R
Solicitud para agregar, modificar y eliminar listas de permisos y políticas de seguridad personalizadas	R	I
Configuración de alertas para el firewall administrado por AMS	I	R
Supervisión de todas las alertas configuradas por el firewall gestionado por AMS	I	R
Ejecute copias de seguridad de la configuración del firewall	I	R
Solicite actividades de restauración de copias de seguridad	R	I
Actualice los recursos aprovisionados con una nueva versión del producto	I	R
Grabación de registros de firewall gestionados por AMS	I	R
Reenvíe los registros del firewall administrado por AMS a CloudWatch	I	R

Actividad	Cliente	AWS Managed Services (AMS)
Solicite cambios de configuración en el firewall administrado por AMS	R	I
Apruebe los cambios de configuración en el firewall administrado por AMS	I	R
Ejecute los cambios de configuración en el firewall administrado por AMS	I	R

- ⁸. AMS EC2 solo está AMIs disponible para Amazon.
- ⁹ AMS es responsable del final del ciclo de vida útil OSes únicamente cuando el cliente firma un acuerdo de soporte ampliado con el proveedor del sistema operativo

Componentes básicos del entorno AMS

Multi-Account Landing Zone

Se trata de una estimación de los componentes y los posibles costes de la infraestructura de las cuentas principales. Esto no incluye otros costes, como el ancho de banda, la supervisión CloudWatch detallada, el registro, las alarmas, Route53, Amazon S3, Simple Notification Service (Amazon SNS), las instantáneas o las instancias reservadas de Amazon. EC2

Usted paga por los componentes necesarios para la infraestructura de AWS landing zone administrada por AMS. Las estimaciones sitúan el coste de un entorno de landing zone multicuenta simple de AMS en 2.450\$ al mes y 50\$ en el caso de una cuenta de aplicación simple.

Para obtener información sobre los precios, consulte los [precios de AWS](#).

Componentes básicos del entorno

Componente	Est. Costo	Descripción
Cuenta de administración	60\$	Una cuenta de AWS Organizations Management; crea y administra financieramente las cuentas de los

Componente	Est. Costo	Descripción
		miembros. Contiene el marco de AWS Landing Zone (ALZ), conjuntos de conjuntos de configuraciones de cuentas y políticas de control de servicios de AWS Organization (SCPs). • Directory Service: 35 dólares • CloudTrail: 7\$ • CloudWatch: 6 dólares • Otros: 12 dólares
Cuenta de servicios compartidos	2.000 \$	Contiene la infraestructura y los recursos necesarios para la administración del acceso (es decir, Active Directory), la administración de la seguridad de los terminales (Trend Micro) y sus bastiones (SSH/RDP); la estimación es de 2400\$ al mes. Esta estimación no incluye el coste de las licencias de Trend Micro. • EC2: 800\$ (con el número mínimo de Bastions) • BARRAS: 300\$ (UNIDADES) • VPC (puntos finales): 400\$ • Directory Service: 300 dólares • CloudWatch: 100 dólares • GuardDuty : 15 dólares • Secrets Manager: 10 dólares • Transferencia de datos: 10 dólares • Config: 10\$ • Otros: 45 dólares

Componente	Est. Costo	Descripción
Cuenta de red	350 DÓLARES	El centro central para el enrutamiento de la red entre las cuentas de AMS, la red local y el tráfico de salida a Internet. Además, contiene bastiones DMZ públicos (el punto de entrada para que los ingenieros de AMS accedan a los hosts de su entorno de AMS). El precio puede aumentar según el tráfico que atraviese Transit Gateway y Direct Connect. • EC2: 250\$ (Bastions) • VPC: 80\$ • Otros: 20 dólares
Cuenta Log Archive	20 dólares	Un bucket de S3 con copias de los archivos de registro de AWS CloudTrail y AWS Config de cada una de sus cuentas de entorno AMS. Los costos aumentan a medida que se recopilan más registros. • S3: 10\$ • CloudWatch: 5 dólares • Otros: 5 dólares
Cuenta de seguridad	20 dólares	El eje central de las operaciones relacionadas con la seguridad y el punto principal para canalizar las notificaciones y alertas a los servicios del plano de control de AMS. Además, alberga la cuenta de administración de Amazon Guard Duty. Los costes aumentan a medida que se analizan más eventos con Amazon GuardDuty. • CloudWatch: 15\$ • Otros: 5 dólares

Single-Account Landing Zone

En la siguiente tabla se enumeran los componentes de un ejemplo de infraestructura administrada por AMS.

Componentes básicos del entorno, actualizados por última vez el 9 de julio de 2020

Nombre	Tipo de instancia	SO	Número de componentes	
mc-eps-dsm	m5.large	Linux	2	
mc-management	m5.large	Windows	2	
mc-bastion-dmz-ssh	m5.large	Linux	2	
mc-bastion-customer-rdp	m5.large	Windows	2	
mc-eps-relay	m5.large	Linux	2	
servicios de directorio	N/A	N/A		
componentes adicionales	N/A	N/A		

Para obtener información sobre los precios, consulte los [precios de AWS](#).

Límites de cuentas AMS

Hay tres tipos distintos de límites a tener en cuenta en la landing zone multicuenta de AMS: límites de API de AMS, límites de recursos de AMS y límites de AWS.

Hay dos tipos distintos de límites a tener en cuenta en la landing zone de una sola cuenta de AMS: los límites de la API de AMS y los límites de AWS.

Límites de las API de las cuentas AMS

En esta sección se describen los límites a nivel de cuenta a partir de los cuales AWS Managed Services (AMS) limita el servicio de API AMS SKMS. Esto significa que si llama a alguna de las opciones de la lista APIs más de 10 veces en un segundo, una de las llamadas se «limita» (recibe

una). `ThrottleException` En raras ocasiones, una dependencia externa o descendente podría limitar la API de AMS y, por lo tanto, AMS podría limitar las llamadas a la API a un ritmo posiblemente inferior.

 Note

Para obtener información sobre la API AMS SKMS, descargue la referencia en la pestaña Informes de la consola AWS Artifact.

Para cada API AMS SKMS de la lista, la operación se limita después de 10 TPS (transacciones por segundo):

- `GetStack`
- `GetSubnet`
- `GetVpc`
- `ListAmis`
- `ListStackSummaries`
- `ListSubnetSummaries`
- `ListVpcSummaries`

Límites de recursos de la cuenta AMS multicuenta en la zona de aterrizaje

Los límites de recursos de la cuenta se refieren a las cuentas y subredes de aplicaciones de zonas de landing zone multicuenta VPCs de AMS.

Límites de recursos de la cuenta de aplicación

Hay un límite flexible de 50 cuentas de aplicaciones por organización. Si tiene un caso de uso para más de 50 cuentas de aplicaciones, póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) para comunicarle sus requisitos.

VPCs y límites de recursos de las subredes.

Existe un límite flexible de 10 VPCs por cuenta de aplicación dentro de la región de AWS predefinida para la organización.

Cada VPC puede tener de 1 a 10 niveles de subred privada repartidos en 2 o 3 zonas de disponibilidad. Además, cada VPC puede tener de 0 a 5 niveles de subred pública repartidos en 2 o 3 zonas de disponibilidad. Si sus requisitos superan estos límites, informe a su CSDM o a Cloud Architect para revisar su caso de uso.

Relación entre solicitudes y cuentas de zonas de landing zone multicuentas de AMS

Se admite una cuenta por aplicación en la zona de aterrizaje multicuenta de AMS; sin embargo, cada cuenta de la aplicación tiene un coste reducido y se le cobrará por la cantidad de conexiones a la Transit Gateway por hora y por la cantidad de tráfico que fluya a través de AWS Transit Gateway. Por lo tanto, cuanto más segregadas estén las aplicaciones en cuentas VPCs, mayores serán los costos.

Para reducir los costes y, al mismo tiempo, garantizar una adecuada separación de funciones, AMS recomienda 1) agrupar las aplicaciones por equipos con procesos empresariales estrechamente relacionados, y 2) no mezclar aplicaciones que se encuentren en distintas etapas (de producción o no) o que estén gestionadas por equipos diferentes. De esta forma, tendrá menos cuentas, facilitará la gestión del acceso y la segregación de funciones y, además, se reducirán los costes de tráfico.

Por ejemplo: una empresa tiene en producción una aplicación de negociación y una aplicación de gestión de carteras; ambas aplicaciones son gestionadas por el equipo de TI de inversiones e intercambian mucho tráfico entre sí. En este escenario, la empresa puede beneficiarse de agrupar ambas aplicaciones en la misma cuenta y en la misma VPC, ya que el equipo de TI de Investments no tendrá que solicitar acceso a varias cuentas de aplicaciones y la empresa ahorrará en costes de tráfico. En este caso, la empresa debería crear otra cuenta para las mismas aplicaciones en la fase de desarrollo y proporcionar acceso al equipo de desarrollo.

En otro escenario, la empresa tiene en producción una aplicación de nómina y una aplicación de contabilidad, administradas por los equipos de TI de Recursos Humanos y TI de Contabilidad, respectivamente. Si bien la aplicación de nómina debe intercambiar información con la aplicación de contabilidad, recomendamos segregar ambas aplicaciones en cuentas diferentes, una por equipo, y establecer una conexión entre ambas aplicaciones VPCs mediante la cuenta de red. De esta forma, la empresa evitará que el equipo de TI de RRHH solicite cambios que afecten a la infraestructura de la aplicación de contabilidad y que ellos desconozcan.

Consejos sobre cómo agrupar cuentas en unidades organizativas (OUs). Una OU es un mecanismo lógico de agrupación que permite categorizar (agrupar) las cuentas y aplicarles políticas y configuraciones en función de esos grupos. El enfoque recomendado para crearlas OUs consiste en basarlas en políticas que deban aplicarse a un grupo específico de cuentas, no en la jerarquía

interna de los equipos dentro de la estructura jerárquica. Una unidad organizativa no equivale a una unidad organizativa de Active Directory, por lo que no se recomienda intentar replicar la estructura de la unidad organizativa de AD en ella, ya que resulta difícil mantener una estructura and/or operativa.

AWS Organizations

AWS límites de cuenta

AWS los límites de cuenta se aplican a sus cuentas de AWS Managed Services (AMS). El método más sencillo para determinar los límites predeterminados y actuales de AWS los servicios es aprovechar [AWS Service Quotas](#). AMS recomienda ajustar los límites de los servicios individuales al tamaño adecuado para ejecutar los servicios de la cuenta. Los límites actúan como barandillas para proteger sus cuentas por motivos de seguridad y reducir los costes. Si desea aumentar un límite específico, envíe una solicitud de servicio a AMS y AMS Operations aumentará el límite en su nombre. Por ejemplo, el límite (o cuota) predeterminado para las instancias de RDS es de 40; si su carga de trabajo requiere 50 instancias de RDS, envíe una solicitud de servicio a AMS Operations para aumentar el límite al valor que necesita.

Objetivos de nivel de servicio de AMS (SLOs)

En la siguiente tabla se describen los objetivos del servicio AWS Managed Services (AMS). Los acuerdos de nivel de servicio (SLAs) para otros aspectos del servicio de AMS, incluida la gestión de incidentes, se describen en el documento de acuerdo de nivel de servicio que le enviamos al suscribirse a AMS. Para obtener más información, póngase en contacto con su CSDM.

Objetivos de nivel de servicio de AMS

Característica	Indicador de rendimiento (PI)	Además (Business Days, M-F 8AM to 6PM local time)	Premium (Calendar Days, 24 x 7)
Administración de cambios	El tiempo que se tarda en programar o rechazar está automatizado RFCs	<=30 minutos	<=30 minutos
	Hora de inicio de la ejecución programad a RFCs en comparaci	<=1 minuto	<=1 minuto

Característica	Indicador de rendimiento (PI)	Además (Business Days, M-F 8AM to 6PM local time)	Premium (Calendar Days, 24 x 7)
	ón con la hora de ejecución programada		
	Tiempo transcurrido hasta approve/reject no ser automatizado RFCs, disponible en el catálogo de CT	<=48 horas	<=24 horas
	El tiempo transcurrido hasta que approve/reject no está automatizado RFCs no está disponible en el catálogo de CT	<=5 días	<=5 días
Administración de problemas	Tiempo necesario para completar el análisis de la causa raíz (RCA)	<=10 días	<=10 días
Gestión de solicitudes de servicio	Tiempo de respuesta de la primera respuesta y de todas las respuestas posteriores	<= 8 horas	<=4 horas

AWS Servicios compatibles

AWS Managed Services (AMS) proporciona servicios de soporte de administración operativa para los siguientes AWS servicios. Cada AWS servicio es distinto y, como resultado, el nivel de gestión operativa de AMS y el soporte varían según la naturaleza y las características del AWS servicio

subyacente. Los AWS servicios específicos se agrupan en función de la complejidad y el alcance del servicio de apoyo a la gestión operativa ofrecido por AMS.

Note

Los tres grupos, A, B y C, indican los precios como un porcentaje del gasto mensual total por cuenta en el servicio de AMS, según el plan de asistencia (Plus o Premium), para los clientes de AMS antes del 16 de marzo de 2021. Los clientes de AMS que se hayan incorporado después del 16 de marzo de 2021 deberán enviar una solicitud de servicio para obtener información adicional sobre los precios. El grupo A indica que no hay ningún cargo adicional. El grupo B indica un cargo adicional del 12% (Plus) o del 18% (Premium). El grupo C indica un cargo adicional del 25% (Plus) o del 42% (Premium).

Una estrella (*) indica los servicios que un cliente implementa en un entorno gestionado por AMS mediante la AWS consola y APIs. Consulte la sección «Gestión del aprovisionamiento automatizada y de autoservicio» en la sección [Características del plan operativo avanzado de AWS Managed Services \(AMS\) AMS](#) para obtener información adicional sobre las responsabilidades del cliente a la hora de aprovisionar y configurar los servicios de esta manera.

Dos estrellas (**) indican que Amazon EC2 on se AWS Outposts facturará como un servicio del grupo B; todos los demás recursos alojados en Amazon se AWS Outposts facturarán según su tarifa estándar.

Servicios compatibles AWS

Grupo A	Grupo B	Grupo C
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon CloudFront Amazon Elastic File System Amazon Glacier Amazon Simple Storage Service AWS Amplify* AWS AppMesh*	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon Bedrock* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect* Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic, application, and network; not gateway) Amazon ElastiCache

Grupo A	Grupo B	Grupo C
AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon EC2 Container Registry (ECR)* Amazon Elastic Container Service (ECS) on AWS Fargate* Amazon Elastic Kubernetes Service (EKS) on Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kendra* Amazon Kinesis Analytics* Amazon Kinesis Data Stream* Amazon Kinesis Firehose* Amazon Kinesis Video Streams* Amazon Lex* Amazon Managed Service for Prometheus* Amazon MQ* Amazon Personalize** Amazon Quantum Ledger Database (QLDB)* Amazon QuickSight* Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB*	Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift Amazon Relational Database Service Amazon Route 53 Amazon Route 53 Resolver DNS Firewall Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service AWS Systems Manager (SSM)

Grupo A	Grupo B	Grupo C
	Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkSpaces* AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Resilience Hub* AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Service Catalog AppRegistry* AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

Si solicita a AWS Managed Services que suministre servicios para cualquier software o servicio que no se identifique expresamente como compatible a continuación, todos los servicios gestionados

de AWS proporcionados para dichas configuraciones solicitadas por el cliente se tratarán como un «servicio beta» en virtud de las condiciones del servicio.

Configuraciones admitidas

Estas son las configuraciones que admite AWS Managed Services (AMS):

- Idioma: AMS está disponible en inglés.
- Servicios de firewall:
 - Firewall DNS Amazon Route 53 Resolver
 - Firewall de próxima generación de la serie VM de Palo Alto
- Software de seguridad: Deep Security de Trend Micro (obligatorio). AWS Marketplace: [Trend Micro Deep Security](#)
- Servicios de directorio aprobados: Microsoft Active Directory (AD)
- [AWS Servicios compatibles](#).
- AWS Regiones compatibles:

AMS opera en un subconjunto de todas AWS las regiones; sin embargo, solo API/CLI opera en la región «EE. UU. Este (Virginia del Norte)». Si ejecuta la API de gestión de cambios de AMS (amscm) o la API de gestión del conocimiento del servicio AMS (amsskms), en una región que no sea de EE. UU. Este), debe añadir `--region us-east-1` al comando.

- 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)
- Imágenes de máquinas de Amazon (AMIs): AMS proporciona imágenes de seguridad mejorada (AMIs) basadas en el punto de referencia CIS de nivel 1 para un subconjunto de sistemas operativos compatibles con AMS. Para encontrar sistemas operativos que tengan disponible una imagen de seguridad mejorada, consulte la Guía del usuario de seguridad de AMS. Para acceder a esta guía AWS Artifact, filtre la pestaña Informes de AWS Managed Services. Para acceder AWS Artifact, póngase en contacto con su CSDM o consulte [Introducción a AWS Artifact](#).
- Sistemas operativos compatibles:

Sistemas operativos compatibles (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (fecha prevista de finalización del soporte para AMS el 30 de junio de 2026)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux (RHEL) 9.x, 8.x
- Servidor SUSE Linux Enterprise 15 SP6
- SUSE Linux Enterprise Server para SAP 15 SP3 y versiones posteriores
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Sistemas operativos compatibles () ARM64

- Amazon Linux 2023
- Amazon Linux 2 (fecha prevista de finalización del soporte para AMS el 30 de junio de 2026)
- Sistemas operativos End of Support (EOS) compatibles:

Note

Los sistemas operativos End of Support (EOS) están fuera del período de soporte general del fabricante del sistema operativo y presentan un mayor riesgo de seguridad. Los sistemas operativos EOS se consideran configuraciones compatibles solo si los agentes que requieren AMS son compatibles con el sistema operativo y...

1. dispone de un amplio soporte con el proveedor del sistema operativo que le permite recibir actualizaciones, o

2. cualquier instancia que utilice un sistema operativo EOS sigue los [controles de seguridad](#) especificados por AMS en la Guía de usuario avanzada, o
3. usted cumple con cualquier otro control de seguridad compensatorio exigido por AMS. En caso de que AMS deje de ser compatible con un sistema operativo EOS, AMS emitirá una [recomendación fundamental](#) para actualizar el sistema operativo. Los agentes requeridos por AMS pueden incluir, entre otros: AWS Systems Manager Amazon CloudWatch, el agente Endpoint Security (EPS) y Active Directory (AD) Bridge (solo Linux).

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3 y SP4 SP5
- Servidor SUSE Linux Enterprise para SAP 15 SP2
- Servidor SUSE Linux Enterprise 12 SP5
- Servicio SUSE Linux Enterprise para SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2
- Red Hat Enterprise Linux (RHEL) :7.x
- Oracle Linux 7,5-7,9

Capacidades para sistemas operativos no compatibles en AMS

Un sistema operativo no compatible es cualquier sistema operativo que no figure en la lista.

[Configuraciones admitidas](#) AMS considera que las instancias con sistemas operativos no compatibles son «configuraciones solicitadas por el cliente» y están sujetas a las condiciones del servicio Betas y [AWS Previews](#).

El siguiente conjunto limitado de capacidades de AMS está disponible para instancias con sistemas operativos no compatibles:

Capability	Notas
Administración de incidentes	AMS proporciona una respuesta a los incidentes.
Gestión de solicitudes de servicio	AMS responde a las solicitudes de servicio.

Capability	Notas
Solicitudes de cambio (RFCs)	AMS evalúa la RFCs ejecución. Los sistemas operativo s no compatibles pueden afectar a la capacidad de ejecución. RFCs
Monitoreo	AMS supervisa y responde a las comprobaciones de estado EC2 del sistema Amazon y a las comprobaciones de estado de las instancias. Las comprobaciones de estado del sistema incluyen: pérdida de conectividad de red, pérdida de alimentación del sistema, problemas de software en el host físico y problemas de hardware en el host físico que afectan a la accesibilidad de la red. Las comprobaciones del estado de las instancias incluyen: una configuración de red o inicio incorrecta, memoria agotada, sistema de archivos dañado y núcleo incompatible.
Administración de la seguridad	AMS monitorea y responde a las EC2 GuardDuty conclusiones de Amazon.
Administración de copias de seguridad	AMS ofrece la gestión de la continuidad en AMS Advanced para EC2 utilizar AWS Backup planes y bóvedas personalizados por AMS.

Interfaces avanzadas AMS

- Consola AMS Advanced: utiliza la consola AMS Advanced para crear incidentes RFCs, informar y responder a ellos, realizar solicitudes de servicio y buscar información sobre las existentes VPCs y las pilas. Si no sabe qué hacer o si necesita ayuda con AMS o sus recursos gestionados, cree una solicitud de servicio mediante esta interfaz.
- AWS Management Console: Muchas AWS consolas pueden resultar útiles para ver la información de AMS, por ejemplo:
 - EC2 Consola de Amazon: se usa para ver la información de las instancias, incluidas las direcciones IP de los bastiones, los grupos de Amazon EC2 Auto Scaling y los balanceadores de carga.

- Cumplimiento de AWS Config las normas de zona de destino multicuenta: puede ver el estado de conformidad de sus cuentas e identificar los recursos que no las cumplen.
- AWS CloudFormation consola: se utiliza para ver la información de la pila, incluida la pila IDs (puede encontrar las pilas de Amazon RDS y la instancia de Amazon RDS IDs aquí, además de información sobre los eventos).
- Consola Amazon RDS: se usa para ver información sobre eventos, como una publicación realizada en una WordPress aplicación en un sitio de su cuenta. Tenga en cuenta que debe tener el ID de instancia de Amazon RDS.

Según el modo de su función de inicio de sesión, dispondrá de un nivel de acceso diferente a la consola AWS de administración. Para obtener más información sobre los modos, consulte [Modos AMS](#).

- API de gestión de cambios avanzada de AMS (lectura/escritura): utilice la API de gestión de cambios (API CM) para solicitar adiciones y cambios específicos en su infraestructura gestionada, incluidas las configuraciones de supervisión de recursos, registros, copias de seguridad y parches. Además, utilice esta API para solicitar acceso a los recursos, eliminarlos y crear perfiles AMIs de instancias de IAM. Puede acceder a la API CM a través de la CLI de AMS y SDKs.
- API AMS SKMS, de solo lectura: utilice esta API para enumerar los recursos gestionados y obtener la información necesaria para elaborar informes o preparar las solicitudes de cambio.
- Soporte API: utilice la Soporte API estándar para crear incidentes y solicitudes de servicio y responder a ellos mediante programación. Para obtener más información, consulte [Cómo empezar con. Soporte](#)
- AWS APIs— Solo lectura: su administrador de TI principal puede usar el AWS APIs para ver todos los recursos que se administran, ver CloudTrail los registros, la información de facturación y muchas otras funciones de lectura.

Puntos finales de VPC de AMS

Un punto de enlace de VPC le permite conectar su VPC de forma privada Servicios de AWS sin necesidad de una puerta de enlace a Internet. Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con los recursos del servicio.

Los puntos de conexión son dispositivos virtuales. Son componentes de la VPC de escalado horizontal, redundantes y de alta disponibilidad que permiten la comunicación entre las instancias de su VPC y los servicios sin que ello conlleve riesgos de disponibilidad ni imponga restricciones de ancho de banda en el tráfico de red. Para obtener más información, consulte [VPC Endpoints](#).

Existen dos tipos de puntos de enlace de la VPC: puntos de enlace de interfaz y puntos de enlace de gateway.

- Puntos de enlace de puerta de enlace: la VPC de la cuenta tiene un punto de enlace de Amazon S3 Gateway habilitado de forma predeterminada.
- Puntos finales de interfaz: las instancias de su entorno AMS pueden comunicarse con los servicios compatibles sin salir de la red de Amazon. Esto es opcional para la zona de landing zone con una sola cuenta y no está habilitada en la cuenta de forma predeterminada; envíe una solicitud de servicio a AMS Operations para habilitarla. Sin embargo, en el caso de las zonas de landing con varias cuentas, los puntos finales de la interfaz están habilitados de forma predeterminada en la cuenta de Shared Services.

Lista de puntos finales de interfaz compatibles con AMS:

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- EC2 API de Amazon
- AWS Key Management Service
- Amazon CloudWatch
- CloudWatch Eventos de Amazon
- Amazon CloudWatch Logs
- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

Espacios de nombres protegidos por AMS

La lista de espacios de nombres protegidos para AWS Managed Services (AMS). Cuando trabaje con AWS recursos, evite conflictos con AMS al no utilizar estos espacios de nombres. Para obtener más información sobre otros espacios AWS de nombres de servicios, consulte [Amazon Resource Names \(ARNs\) y AWS Service Namespaces](#).

- `ams-*` (este es el estándar de nomenclatura preferido para los nuevos recursos)

- `/ams/`*(este es el estándar de nomenclatura preferido para los recursos basados en rutas)
- `AWSManagedServices`*(este es el estándar de nomenclatura preferido para los recursos cuando CamelCase es apropiado)
- `ams*` y `AMS*` y `Ams*`
- `AWS_*` y `aws*`
- `*/aws_reserved/`*
- `CloudTrail*` y `Cloudtrail*`
- `codedeploy_service_role`
- `customer-mc-`*
- `eps` y `EPS`
- `EPSMarketplaceSubscriptionRole`
- `EPSDB*`
- `IAMPolicy*`
- `INGEST*`
- `LandingZone*`
- `Managed_Services*`
- `managementhost`
- `mc*` y `MC*` y `Mc*`
- `MMS*`
- `ms-`
- `NewAMS*`
- `Root*`
- `sentinel*` y `Sentinel*`
- `sentinel.int.`
- `StateMachine*`
- `StackSet-ams*`
- `StackSet-AWS-Landing-Zone`
- `TemplateId*`
- `UnhealthyInServiceBastion`
- `VPC_*`

Prefijos reservados AMS

Los atributos de los recursos de AMS deben cumplir ciertos patrones; por ejemplo, los nombres de los perfiles de las instancias de IAM, BackupVault los nombres, los nombres de etiquetas, etc., no deben empezar por prefijos reservados de AMS. Estos prefijos reservados son:

```
*/aws_reserved/*
ams- *
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc- *
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc *
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
```

Ventana de mantenimiento de AMS

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. Esto es para AWS Managed Services (AMS), para realizar actividades de mantenimiento de infraestructuras gestionadas, como la implementación de un nuevo AMS AMIs.

Su período de mantenimiento es el período en el que AMS aplicará los parches y usted determinará el período de mantenimiento en el momento de la incorporación. También puede aceptar el período de aplicación de parches propuesto que se proporciona en la notificación del servicio de aplicación de parches o sugerir un período diferente.

Para obtener instrucciones sobre cómo crear una ventana de mantenimiento, consulte [Ventana de mantenimiento](#).

Recursos de información de AMS

AMS proporciona varios recursos de información para ayudarlo a tener éxito.

- Guía del usuario de AMS Accelerate: le ayuda a comprender los componentes y funciones que ofrece AMS Accelerate y cómo utilizarlos. Consulte aquí la información general de AMS Accelerate y los detalles sobre la configuración predeterminada, la búsqueda de recursos y ejemplos de procedimientos. [Índice HTML](#), [PDF](#)
- Guía de usuario avanzada de AMS: le ayuda a comprender los componentes y funciones que ofrece AMS Advanced y cómo utilizarlos. Consulte aquí la información general de AMS Advanced y los detalles sobre la configuración predeterminada, la búsqueda de recursos y ejemplos de procedimientos. [Índice HTML](#), [PDF](#)
- Guía de aplicaciones avanzadas de AMS: describe los pasos para implementar aplicaciones en la infraestructura de AWS Managed Services. Consulte aquí información sobre las metodologías y consideraciones sobre la implementación y el mantenimiento de las aplicaciones. [Índice HTML](#), [PDF](#).
- Guía de incorporación avanzada de AMS: describe los pasos iniciales para crear la infraestructura básica de zonas de landing de cuentas múltiples o de una sola cuenta de AWS Managed Services

en una cuenta de AMS. Consulte aquí información básica sobre las cuentas de AMS, su validación y preguntas que le ayudarán a prepararse para incorporarse a AMS. [Índice HTML](#), [PDF](#).

- Referencia avanzada de tipos de cambios de AMS: proporciona material de referencia sobre los tipos de cambios actuales que proporciona AWS Managed Services, incluidos esquemas de tipos de cambio y ejemplos de tutoriales para cada tipo de cambio y consejos. Incluye información general sobre los tipos de cambio. Le ayuda a comprender todos los aspectos de las solicitudes de cambio (RFCs) y los tipos de cambios de AMS (). Consulte aquí los detalles sobre los tipos de cambio, incluidos los enlaces a la información relevante. [Índice HTML](#), [PDF](#).
- Referencia de la API AMS CM (gestión de cambios): describe la API CM de AWS Managed Services, que proporciona operaciones para crear y supervisar las solicitudes de cambio y proporciona información sobre los recursos que gestionan Managed Services. [Índice HTML](#).
- Guías de seguridad de AMS: describen la información de seguridad patentada de AMS.

Privado; disponible en la pestaña Informes de AMS de la consola Artifact de AWS.

- Recursos para desarrolladores de AMS: acceso a la CLI y al SDK de AMS, tanto para amscm como para amsskms. Consulte <https://console.aws.amazon.com/managedservices/>.
- YouTube Vídeos de AMS: las principales operaciones de los clientes se explican en un vídeo. Consulte los [vídeos YouTube instructivos de AWS Managed Services](#).
- Publicaciones del blog de AMS: información especializada sobre AWS Managed Services. Consulte los [blogs de AWS](#).

Conformidad con AMS

AMS se ha sometido a una auditoría para cumplir con las siguientes normas y puede utilizarse como parte de soluciones para las que debe obtener una certificación de conformidad.

AMS apoya las normas de conformidad

AMS apoya los estándares AWS de cumplimiento. Para obtener más información sobre los programas de AWS cumplimiento, consulte [AWS Cumplimiento](#).

Estos son los estándares de cumplimiento actuales respaldados por AMS.

FedRAMP: El Gobierno Federal de los Estados Unidos se dedica a prestar sus servicios al pueblo estadounidense de la manera más innovadora, segura y rentable. La computaci

ón en nube desempeña un papel clave en la forma en que el gobierno federal puede lograr eficiencias operativas e innovar bajo demanda para llevar adelante su misión en todo el país. Por eso, muchas agencias federales utilizan actualmente los servicios en la nube de AWS para procesar, almacenar y transmitir datos del gobierno federal.

Para obtener más información, consulte [FedRAMP](#).

HIPAA: [AWS ha ampliado su programa de conformidad con la Ley de Portabilidad y Responsabilidad de los Seguros de Salud \(HIPAA\) para incluir a AMS como un servicio que cumple con los requisitos de la HIPAA](#). Si tiene un acuerdo de asociación empresarial (BAA) con AWS, puede usar AMS para crear sus aplicaciones que cumplan con la HIPAA.

Consulte el [documento técnico centrado en la HIPAA](#) para obtener información sobre cómo aprovechar los AMS para el procesamiento y el almacenamiento de información de salud. Para obtener más información, consulte [Conformidad con HIPAA](#).

HITRUST: El Marco de Seguridad Común de la Health Information Trust Alliance (HITRUST CSF) aprovecha las normas y reglamentos aceptados a nivel nacional e internacional, como el GDPR, la ISO, el NIST, la PCI y la HIPAA, para crear un conjunto integral de controles básicos de seguridad y privacidad.

[Para obtener más información, consulte HITRUST CSF.](#)

La ISO 27001: ISO/IEC 27001:2013 es una norma de gestión de la seguridad que especifica las mejores prácticas de gestión de la seguridad y los controles de seguridad integrales siguiendo la guía de mejores prácticas 27002. ISO/IEC La base de esta certificación es el desarrollo y la implementación de un riguroso programa de seguridad, que incluye el desarrollo e implementación de un sistema de administración de seguridad de la información (ISMS) que define la forma en que AWS administra la seguridad de manera permanente de una manera integral y holística.

[Para obtener más información, consulte ISO/IEC 27001:2013.](#)

La norma ISO ISO/IEC 27017:2015 proporciona orientación sobre los aspectos de seguridad de la información de la computación en nube y recomienda la implementación de controles de seguridad de la información específicos para la nube que complementen las directrices de las normas 27002 y 27001. ISO/IEC ISO/IEC Este código de prácticas proporciona orientación adicional sobre la implementación de los controles de seguridad de la información específica para los proveedores de servicios en la nube.

Para obtener más información, consulte [ISO/IEC 27017:2015, Compliance.](#)

La norma ISO/IEC 27018:2019 es un código de prácticas que se centra en la protección de los datos personales en la nube. Se basa en la norma de seguridad de la ISO/IEC información 27002 y proporciona orientación sobre la implementación de los controles ISO/IEC 27002 aplicables a la información de identificación personal (PII) en la nube pública. También proporciona un conjunto de controles adicionales y la orientación correspondiente destinados a abordar los requisitos de protección de la PII en la nube pública que no se abordan en el conjunto de controles 27002 existente ISO/IEC .

Para obtener más información, consulte el artículo [ISO/IEC 27018:2019](#) Compliance.

La norma ISO 9001: la norma ISO 9001:2015 describe un enfoque orientado a los procesos para documentar y revisar la estructura, las responsabilidades y los procedimientos necesarios para lograr una gestión de calidad eficaz en una organización. Las secciones específicas de la norma contienen información sobre temas como:

- Los requisitos de un sistema de gestión de la calidad, incluida la documentación de un manual de calidad, el control de los documentos y la determinación de las interacciones entre los procesos
- Responsabilidades de la dirección
- Gestión de los recursos, incluidos los recursos humanos y el entorno de trabajo de una organización
- Desarrollo del servicio, incluidos los pasos desde el diseño hasta la entrega
- Satisfacción del cliente
- Medición, análisis y mejora del sistema de gestión de calidad mediante actividades como auditorías internas y acciones correctivas y preventivas

Para obtener más información, consulte [Cumplimiento de la norma ISO 9001:2015](#).

PCI: AMS cuenta con un certificado de conformidad con la versión 3.2 de la norma de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI), de nivel 1. Los clientes que utilizan los productos y servicios de AWS para almacenar, procesar o transmitir datos de titulares de tarjetas pueden utilizar AMS para gestionar su propia certificación de conformidad con PCI DSS.

Para obtener más información acerca de PCI DSS y sobre cómo solicitar una copia del Paquete de conformidad con PCI de AWS, consulte [PCI DSS Nivel 1](#). Lo que es más importante, debe configurar políticas de contraseñas detalladas en AMS para que sean coherentes con los estándares de la versión 3.2 de la PCI DSS. Para obtener más información sobre las políticas que se deben aplicar, consulte [Habilitar la conformidad con PCI para su directorio de AWS Microsoft AD](#).

SOC: los informes de control de sistemas y organizaciones (SOC) de AMS son informes de análisis independientes realizados por terceros que demuestran cómo AMS logra los principales controles y objetivos de conformidad. El objetivo de estos informes es ayudarlo a usted y a sus auditores a comprender los controles del AMS establecidos para respaldar las operaciones y el cumplimiento. Hay tres tipos de informes SOC del AMS:

- Informe SOC 1 de AWS: [descárguelo con AWS Artifact](#)
- SOC 2 de AWS: Informe de seguridad, disponibilidad y confidencialidad: [descárguelo con AWS Artifact](#)
- [SOC 3 de AWS: Informe de seguridad, disponibilidad y confidencialidad](#)

Para obtener más información, consulte Conformidad con el [SOC](#).

Responsabilidad compartida

La seguridad, incluida la conformidad con la PCI, es una responsabilidad [compartida](#). Es importante entender que el estado de conformidad con el AMS no se aplica automáticamente a las aplicaciones que se ejecutan en la AWS nube. Debe asegurarse de que el uso de los AWS servicios cumpla con los estándares. Para obtener más información sobre cómo AMS trabaja junto con los clientes en actividades específicas, consulte la AMS [Matriz de responsabilidad de AMS \(RACI\)](#).

Imágenes de máquinas AMS Amazon (AMIs)

AMS produce Amazon Machine Images (AMIs) actualizadas todos los meses para los sistemas operativos compatibles con AMS. Además, AMS también produce imágenes de seguridad mejorada (AMIs) basadas en el estándar de nivel 1 del CIS para un subconjunto de los [sistemas operativos compatibles con AMS](#). Para saber qué sistemas operativos tienen disponible una imagen de seguridad mejorada, consulte la Guía del usuario de AMS Security, que está disponible en la página AWS Artifact -> Reports (busque la opción Informes en el panel de navegación izquierdo) filtrada para AWS Managed Services. Para acceder a AWS Artifact, puede ponerse en contacto con su CSDM para obtener instrucciones o ir a [Introducción a AWS](#) Artifact.

Para recibir alertas cuando se AMIs publiquen nuevos AMS, puedes suscribirte a un tema de notificaciones del Amazon Simple Notification Service (Amazon SNS) denominado «AMI de AMS». Para obtener más información, consulte [Notificaciones AMI de AMS con SNS](#).

La convención de nomenclatura AMI de AMS es:customer-ams-<operating system>-<release date> - <version>. (por ejemplo,customer-ams-rhel6-2018.11-3)

Utilice únicamente los AMS AMIs que comiencen porcustomer.

AMS recomienda utilizar siempre la AMI más reciente. Puede encontrar la más reciente de AMIs las siguientes maneras:

- Busca en la consola AMS, en la AMIspágina.
- Visualización del archivo CSV AMI de AMS más reciente, disponible en su CSDM o a través de este archivo ZIP: [contenido de la AMI AMS 11.2024 y archivo CSV en](#) formato ZIP.

Para ver los archivos ZIP AMI anteriores, consulte el [historial del documento](#).

- Al ejecutar este SKMS comando AMS (se requiere el SDK de AMS SKMS):

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId,CreationTime]" --output table
```

Contenido AMI de AMS agregado a la base AWS AMIs, por sistema operativo (SO)

- Linux AMIs:
 - [AWS Herramientas CLI](#)
 - [NTP](#)
 - [Agente de Trend Micro Endpoint Protection Service](#)
 - [Implementación de código](#)
 - [PBIS/Beyond Trust AD Bridge](#)
 - [SSM Agent](#)
 - Actualización de Yum para parches críticos
 - Software de administración y scripts personalizados de AMS (que controlan el arranque, la unión a AD, la supervisión, la seguridad y el registro)
- Servidor Windows AMIs:
 - [Microsoft.NET Framework 4.5](#)
 - [PowerShell 5.1](#)
 - [AWS Herramientas para Windows PowerShell](#)
 - PowerShell Módulos AMS que controlan el arranque, la unión a AD, la supervisión, la seguridad y el registro
 - [Agente de Trend Micro Endpoint Protection Service](#)
 - [SSM Agent](#)
 - [CloudWatch Agente](#)
 - EC2Servicio de configuración (a través de Windows Server 2012 R2)
 - EC2Lanzamiento (Windows Server 2016 y Windows Server 2019)
 - EC2LaunchV2 (Windows Server 2022 y versiones posteriores)

Basado en Linux: AMIs

- Amazon Linux 2023 (última versión secundaria) (no se admite una AMI mínima)

- Amazon Linux 2 (última versión secundaria)
- Amazon Linux (2ARM64)
- Red Hat Enterprise 7 (última versión secundaria)
- Red Hat Enterprise 8 (última versión secundaria)
- Red Hat Enterprise 9 (última versión secundaria)
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu Linux 18.04
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- Amazon Linux: para obtener información general del producto, información sobre precios, información de uso e información de soporte, consulte la [AMI de Amazon Linux \(HVM/64 bits\)](#) y [Amazon Linux 2](#).

Para obtener más información, consulte [Amazon Linux 2 FAQs](#).

- RedHat Enterprise Linux (RHEL): para obtener una descripción general del producto, información sobre precios, información de uso e información de soporte, consulte [Red Hat Enterprise Linux \(RHEL\) 7 \(HVM\)](#).
- Ubuntu Linux 18.04: Para obtener una descripción general del producto, información sobre precios, información de uso e información de soporte, consulte [Ubuntu 18.04 LTS - Bionic](#).
- SUSE Linux Enterprise Server para aplicaciones SAP 15: SP6
 - Ejecute los siguientes pasos una vez por cuenta:
 1. Vaya a AWS Marketplace.
 2. Busque el producto SAP SUSE 15.
 3. Elija Continuar para suscribirse.
 4. Elija Aceptar condiciones.
 - Complete los siguientes pasos cada vez que necesite lanzar una nueva instancia de SUSE Linux Enterprise Server for SAP Applications 15 SP6:
 1. Anote el ID de AMI de la AMI de SUSE Linux Enterprise Server for SAP Applications 15 suscrita.
 2. Crear una implementación | Componentes de pila avanzados | pila | Crear tipo de cambio EC2 ct-14027q0sjyt1h RFC. *InstanceAmiId* Sustitúyala por la ID de AWS Marketplace AMI a la que te has suscrito.

Basado en Windows AMIs:

Microsoft Windows Server (2016, 2019 y 2022), basado en la versión más reciente de Windows AMIs.

Para ver ejemplos de creación AMIs, consulte [Crear AMI](#).

Desembarcar AMS AMIs:

AMS no deja AMIs de compartir nada tuyo durante la baja para evitar que tus dependencias se vean afectadas. Si quieres eliminar AMS AMIs de tu cuenta, puedes usar la `cancel-image-launch-permission` API para ocultar información específica. AMIs Por ejemplo, puedes usar el siguiente script para ocultar todos los AMS AMIs que se compartieron anteriormente con tu cuenta:

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

Debe tener la versión 2 de AWS CLI instalada para que el script se ejecute sin errores. Para ver los pasos de instalación de la CLI de AWS, consulte [Instalación o actualización de la última versión de la CLI de AWS](#). Para obtener más información sobre el `cancel-image-launch-permission` comando, consulte [cancel-image-launch-permission](#).

Seguridad mejorada AMIs

AMS proporciona imágenes de seguridad mejorada (AMIs) basadas en la referencia de nivel 1 del CIS para un subconjunto de los sistemas operativos compatibles con AMS. Para saber qué sistemas operativos tienen disponible una imagen de seguridad mejorada, consulte la Guía de seguridad para clientes de AWS Managed Services (AMS). Para acceder a esta guía, abra AWS Artifact, seleccione Informes en el panel de navegación izquierdo y, a continuación, filtre para ver AWS Managed Services. Para obtener instrucciones sobre cómo acceder AWS Artifact, póngase en contacto con su CSDM o consulte [Primeros pasos AWS Artifact](#) para obtener más información.

Cómo funciona la integración entre AD FS y AMS

La confianza unidireccional entre la red local y el dominio AMS es el medio predeterminado de acceso a las pilas y. VPCs Cuando se crean una VPC y una pila, el acceso se concede mediante

grupos de seguridad de Active Directory preconfigurados. Además, el acceso a la misma se AWS Management Console puede configurar mediante el Servicio de federación de Active Directory (AD FS) o cualquier software de federación compatible con SAML, para un inicio de sesión único (SSO) en la consola de administración. AWS

 Note

AMS puede federarse en muchos servicios de federación, como Ping, Okta, etc. No está limitado a AD FS; aquí le ofrecemos un ejemplo de una tecnología de federación disponible para usted.

La información que aparece aquí está duplicada de esta entrada de blog: [Cómo habilitar la federación para AWS usar Windows Active Directory, AD FS y SAML 2.0.](#)

1. El flujo se inicia cuando un usuario (llamémoslo Bob) visita el sitio de ejemplo de AD FS (<https://Fully.Qualified.Domain.Name/Here/adfs/ls/IdpInitiatedSignOn.aspx>) dentro de su dominio. Cuando instalas AD FS, obtienes un nuevo directorio virtual llamado adfs para tu sitio web predeterminado, que incluye esta página.
2. La página de inicio de sesión autentica a Bob frente a AD. Según el navegador que utilice Bob, es posible que se le pida su nombre de usuario y contraseña de AD.
3. El navegador de Bob recibe una afirmación de SAML en forma de respuesta de autenticación de AD FS.
4. El navegador de Bob publica la afirmación de SAML en el punto final de inicio de AWS sesión de SAML (/saml). <https://signin.aws.amazon.com> En segundo plano, el inicio de sesión utiliza la API de [AssumeRoleWithSAML](#) para solicitar credenciales de seguridad temporales y, a continuación, crea una URL de inicio de sesión para el. AWS Management Console
5. El navegador de Bob recibe la URL de inicio de sesión y se redirige a la consola.

Desde la perspectiva de Bob, el proceso se lleva a cabo de forma transparente. Comienza en un sitio web interno y termina en el AWS Management Console, sin tener que proporcionar ninguna AWS credencial.

 Note

Encontrará más información sobre cómo configurar la federación en la consola AMS en:

- Zona de destino multicuenta: [configuración de la federación con la consola AMS](#)
- Zona de destino con una sola cuenta: [configuración de la federación con la consola AMS](#)

Además, consulte [el apéndice: Regla de reclamación de AD FS y configuración de SAML](#). Para obtener información sobre el uso de AWS Microsoft AD para respaldar sus aplicaciones compatibles con Active Directory, en la AWS nube, que están sujetas a requisitos de conformidad, consulte Administrar la conformidad con [Microsoft AD](#).

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.

Implementaciones de aplicaciones AMS

La guía para desarrolladores de aplicaciones de AMS proporciona descripciones detalladas y tutoriales para las siguientes implementaciones:

- El CT de ingesta de cargas de trabajo de AMS le permite a usted y a un socio de migración a la nube de AMS trasladar fácilmente sus cargas de trabajo existentes a una VPC gestionada por AMS. Con la ingesta de carga de trabajo de AMS, puede crear una AMI de AMS enviando una RFC con la instancia migrada Deployment | Ingestion | Stack from migration partner | Create CT (ct-257p9zjk14ija). Debe tener una instancia migrada de su entorno local a una instancia realizada AWS por un socio de migración, así como una VPC y una subred de AMS de destino, en las que se incorporará la instancia.

[Para obtener más información, consulte la guía para desarrolladores de aplicaciones de AMS en Workload Ingest.](#)

- La función AWS CloudFormation de tipo de cambio de ingesta (ct-36cn2avfrj9v) le permite utilizar fácilmente una plantilla CloudFormation existente para implementar pilas personalizadas en una VPC gestionada por AMS.

[Para obtener más información, consulte la guía para desarrolladores de aplicaciones de AMS en Template Ingest. CloudFormation](#)

- Puede importar su base de datos local a una nueva base de datos a su instancia de Amazon RDS o a su bucket de Amazon S3 gestionado por AMS. Para ello, utilice los tipos de cambio Deployment | Advanced stack components | Database Migration Service (DMS), como Crear instancia de replicación (ct-27apldkhqr0ol), Crear grupo de subredes de replicación (ct-2q5azjd8p1ag5), Crear tarea de replicación (ct-1d2fml15b9eth), Crear punto final de origen

(ct-0attesnjqy2cx) o Cree el punto final de origen (S3) (ct-2oxl37nphsrjz) y cree el punto final de destino (ct-3gf8dolbo8x9p) o cree el punto final de destino (S3) (ct-05muqzievnk5).

Para obtener más información, consulte la guía para desarrolladores de aplicaciones de AMS en [Database Migration Service](#).

- Puede importar su base de datos MS SQL local a una nueva base de datos de su instancia SQL RDS administrada por AMS. Para ello, utiliza varios tipos de cambios de AMS y la API de Amazon RDS, además de AWS consolas.

Para obtener más información, consulte la guía de aplicaciones de AMS en [Importación de bases de datos \(DB\) a MS SQL RDS](#).

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.º 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 presencia Location/Telecom/Chime	AMS: CSDM y arquitecto de nube (CA) Miembros del equipo asignados por el cliente (p. ej.: equipos de Cloud/Infraestructura, 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 presencia 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: represent ante 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: represent ante 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 presentar lo 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](#).

Administración de eventos planificados en AWS Managed Services

La gestión de eventos planificados (PEM) de AWS Managed Services (AMS) es una oferta de servicios de AMS. PEM interactúa, coordina y ayuda durante los eventos y proyectos de los clientes mediante los servicios de AMS. PEM ayuda a coordinar un conjunto de actividades relacionadas RFCs que se alinean con el alcance y el cronograma acordados del evento o proyecto de PEM.

Criterios AMS PEM

Un evento planificado es un proyecto con un alcance y un plazo determinados. AMS utiliza los detalles que usted proporciona (incluidos el plan y el alcance, los resultados esperados y los cambios que se espera que realicen las operaciones de AMS) para ayudarlo de manera eficaz durante la actividad de PEM. Luego, sus arquitectos de nube (CAs) revisan y evalúan la actividad de PEM para comprobar su integridad, implementación técnica y participación en las operaciones de AMS. Tras la revisión de CA, AMS Operations revisa los planes y coordina con su gerente de prestación de servicios en la nube (CSDM) la participación del equipo de operaciones.

Tipos de PEM

Los tipos de PEM disponibles son los siguientes:

- Días de juego
 - Operational Gameday: un enfoque de juego basado en escenarios para la respuesta operativa, destinado a validar la integración de procesos, personas y sistemas.
 - Security Gameday: estrategia de respuesta a incidentes de seguridad que emplea un enfoque de juego basado en escenarios para evaluar la integración de los sistemas, los procesos y el personal.
- BYOEPS: utilice la función AMS «traiga su propia seguridad para puntos terminales» (BYOEPS) para sustituir el agente predeterminado de Trend Micro Deep Security por la solución de seguridad para puntos finales que prefiera o por una licencia personalizada de Trend Micro. Para obtener más información, consulte [AMS trae tu propio EPS](#).
- Recuperación ante desastres: en los eventos de recuperación ante desastres, AMS le ayudará durante las actividades de recuperación ante desastres planificadas. Para obtener más información, consulte [Planificación de la recuperación ante desastres](#).

- Evento de seguridad para el cliente: eventos de seguridad planificados. Por ejemplo, la actividad del usuario root y las pruebas de penetración.
- Migration Support: Soporte para la actividad planificada de incorporación y migración.

Este flujo de trabajo facilita la colaboración con AMS para coordinar los eventos planificados y las actividades de migración relacionadas con el soporte de AMS. Para una ejecución prioritaria RFCs, se recomienda utilizar la contratación de Operations on Demand (OOD). Para obtener más información, consulte [Operaciones bajo demanda](#).

El proceso AMS PEM

El proceso PEM consta de las siguientes fases:

- Inicio del PEM: trabajas con tu CSDM para definir el objetivo del evento planificado y determinar qué es lo que AMS Operations necesita. Los AMS CAs revisan los aspectos técnicos del plan PEM. CAs Trabajan con AMS Security and Operations en materia de cumplimiento, optimización de la ejecución y automatización, y en la definición de las tareas y los resultados previos a la ejecución del PEM. A continuación, su CSDM crea el ticket de PEM y proporciona a AMS la información del proyecto y los detalles técnicos. El AMS requiere un plazo de 14 días naturales para que el equipo de operaciones del AMS tenga tiempo de planificar, realizar una revisión técnica y asignar los recursos.
- Revisión de la PEM: el equipo de operaciones de AMS revisa la solicitud de PEM y trabaja con su CSDM para comprobar que la información del plan de PEM es correcta y completa.
- Aceptación del PEM: AMS revisa la información proporcionada y comunica al CSDM cuál será el nivel de apoyo durante la actividad del PEM. Si el PEM contiene información completa y su CSDM está de acuerdo con el alcance del trabajo, se aprueba el PEM.
- Preparación y ejecución: AMS se asegura de que se completen las tareas necesarias antes de que comience el PEM y facilita la comunicación interna y con los clientes. AMS se asegura de que el plan PEM funcione correctamente y proporciona informes de estado y progreso.

PEM FAQs

¿Cómo interactúo con AMS con una RFC/Service solicitud (SR) durante un evento de PEM?

- Utilice el ID de PEM compartido por su CSDM en la línea de RFC/SR asunto del formato. **PEM-ID**

- También puede crear una solicitud de servicio (SR) para analizar sus casos de uso o para responder a preguntas sobre el evento planificado. Si utilizas un SR, el PEM no tiene por qué ser válido.

¿Qué validaciones se realizan cuando se envía un RFC relacionado con el PEM?

- Verificación de que el identificador de cuenta figura en el PEM.
- Verificación de que el estado de PEM esté aprobado y activo entre las fechas de inicio y finalización indicadas.

¿Existen solicitudes de PEM SLAs o SLOs para solicitarlas?

- PEMs no están asociados a SLAs o. SLOs
- SLAs y SLOs para los elementos de trabajo relacionados con el PEM (RFC/solicitud de servicio) los define AMS. SLOs

Para obtener más información, consulte los [objetivos de nivel de servicio de AMS \(\) SLOs](#).

¿Podemos crear un PEM a través de una solicitud de servicio (SR)?

- No, la creación del PEM debe gestionarla el administrador de prestación de servicios en la nube (CSDM).

Arquitectura de redes

AWS Managed Services (AMS) ofrece dos arquitecturas de red:

- Multi-account landing zone (MALZ): proporciona servicios comunes, como acceso, seguridad de puntos finales y redes, desde cuentas compartidas para cargas de trabajo que se despliegan en cuentas de miembros independientes.
- Single-account landing zone (SALZ): proporciona cuentas autónomas en las que los servicios comunes, como el acceso, la seguridad de los puntos finales y las redes, se implementan en la misma cuenta que la carga de trabajo. Se recomienda para cargas de trabajo que requieren un alto nivel de aislamiento, ya que esto implica costes de AWS más altos.

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 (OU):

- 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 .

Entidad	Zona de aterrizaje AMS única	Varias (dos o más) zonas de aterrizaje
Gastos generales de configuración inicial (según project/migration los plazos)	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.
Configurabilidad 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 determinar 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 aplicaciones 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 aplicación 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. Administrar un gran número de cuentas puede provocar gastos generales operativos o de costes.

Entidad	Zona de aterrizaje AMS única	Varias (dos o más) zonas de aterrizaje
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.
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 interconexión de VPC.
Administración de cambios	Medio. Realizar cambios destructivos 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 administrados por AMS se prueban internamente 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.

Entidad	Zona de aterrizaje AMS única	Varias (dos o más) zonas de aterrizaje
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 cumplimiento.
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 registrará 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 AMSams-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:

[illegible]

Modelo de conmutación por error

La solución de firewalls incluye dos o tres hosts de Palo Alto (PA) (uno por zona de disponibilidad). Healthy Check Canaries sigue un programa constante para evaluar el estado de los anfitriones. Si se identifica un host como en mal estado, se notifica a AMS y el tráfico de esa AZ se traslada automáticamente a un host en buen estado en una AZ diferente mediante un cambio en la tabla de rutas. Como el flujo de trabajo de comprobación de estado se ejecuta constantemente, si el host vuelve a funcionar correctamente debido a problemas transitorios o a una corrección manual, el tráfico vuelve a la AZ correcta con el host en buen estado.

Escalado

AMS supervisa el firewall para determinar los límites de rendimiento y escalado. Cuando los límites de rendimiento superan los umbrales 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, consulte [CloudWatch 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» 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

Tipo de registro	Descripción
	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».
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 autenticación. Los usuarios pueden utilizar esta información para solucionar 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.

Tipo de registro	Descripción
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 diferentes 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>
 - DataPlaneCPUUtilizationPcto
 - DataPlanePacketBufferUtilization
 - 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 EPSTransmissionRole 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 `CustomerDefaultAssumeRole`.
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 comuniquen 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
 - Respallos 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](#).

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](#). 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, 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 AWS Directory Service e interactuar con los controladores AWS 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.

Configuración de AMS

Temas

- [Comprenda la configuración predeterminada de AMS](#)
- [Uso de las consolas AMS](#)
- [Uso de la API y la CLI de AMS](#)
- [AMS trae tu propio EPS](#)
- [Recibir notificaciones de AMS](#)
- [Configuración de DNS públicos y privados](#)
- [Gestión del tráfico de salida AMS](#)
- [Implementación de recursos de IAM en AMS Advanced](#)
- [Configuración de permisos en AMS con roles y perfiles de IAM](#)
- [Regla de notificación de AD FS y configuración de SAML](#)
- [Restringir con ACL de red](#)
- [AMS en Outposts](#)
- [Uso de etiquetas en AMS](#)
- [Programador de recursos de AWS Managed Services](#)
- [AWS Systems Manager en AMS Advanced](#)
- [Cuentas AMS externas](#)

Es posible que algunas tareas de configuración de AMS se completen en el momento de la incorporación.

Para obtener una descripción completa de las funciones y responsabilidades, incluida la AMS [AWS Servicios compatibles](#), consulte [Matriz de responsabilidad de AMS \(RACI\)](#).

Note

Para solicitar que AMS proporcione un AWS servicio adicional, presente una solicitud de servicio. Para obtener información sobre cómo realizar esta solicitud, consulte [Gestión de solicitudes de servicio](#).

Comprenda la configuración predeterminada de AMS

Su red AWS Managed Services (AMS) tiene una configuración estandarizada con valores predeterminados para la mayoría de los servicios.

En esta sección se describen los ajustes predeterminados que AMS utiliza para el acceso, la supervisión, el registro y la administración.

Para ver un ejemplo de los costes de infraestructura de una zona de aterrizaje con varias cuentas o con una sola cuenta, consulte. [Componentes básicos del entorno AMS](#)

Temas

- [Valores predeterminados de resolución de DNS \(MALZ\)](#)
- [EC2 Perfil de instancia de IAM](#)
- [Alertas del monitoreo de referencia en AMS](#)
- [Valores predeterminados de retención y rotación de registros](#)

Valores predeterminados de resolución de DNS (MALZ)

Zona de aterrizaje multicuenta de AWS Managed Services (AMS): en los entornos de AWS, la resolución del sistema de nombres de dominio (DNS) entre los resolutores de Route 53 y de DNS en una VPC se puede integrar configurando las reglas de reenvío de Resolver. Antes de poder utilizar estas reglas para reenviar consultas de DNS, es necesario configurar los puntos finales de resolución entrantes y salientes a los que se puedan reenviar estas consultas.

De forma predeterminada, las consultas de DNS dentro de la cuenta VPCs de aplicación en configuraciones de cuentas múltiples en AMS se reenvían a los reenviadores condicionales del dominio AWS Directory Service for Microsoft Active Directory (también conocido como Managed AD) presente en la cuenta de servicios compartidos. De forma opcional, AMS le permite utilizar el AmazonProvided DNS; por ejemplo, el AmazonProvided DNS al que reenviar las consultas de DNS. Esto le ayuda a utilizar puntos de enlace de VPC que, actualmente, solo admiten el DNS proporcionado por Amazon a través de Amazon Route 53. En consecuencia, las reglas de resolución también se configuran automáticamente para los puntos finales de VPC comunes que se implementan de forma predeterminada en la cuenta de servicios compartidos. Para obtener más información sobre estos puntos finales de VPC comunes, consulte. [Puntos finales de VPC de AMS](#)

Para configurar los conjuntos de opciones del Protocolo de configuración dinámica de host (DHCP) en toda la cuenta de la aplicación VPCs para utilizar el DNS proporcionado por Amazon para los

puntos de enlace de la VPC y tener reglas de Route53 Resolver que apunten a los puntos de enlace de la VPC comunes en sus cuentas de servicios compartidos (con una regla de resolución opcional para el dominio local), cree una administración | Otros | Otros | Crear solicitud de cambio (RFC) especificando la cuenta de servicios compartidos y solicitando la activación de reglas de DNS local de VPC de cuenta de aplicación y Route 53 Resolver para puntos finales de VPC.

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.
	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.

Perfil	Políticas
customer-mc-ec2-instance-profile-s3	AMSInstanceProfileBY0EPSPolicy : 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 <code>aws:iam::*:role/customer-*</code> y <code>aws:iam::*:role/customer_*</code>
Instancia para cargar eventos de registro	Permitir	Crear grupo de registros	Permite crear registros en: <code>aws:logs::*:log-group:i-*</code>
		Crear flujo de registro	Permite que los registros se transmitan a: <code>aws:logs::*:log-group:i-*</code>
CW para MMS	Permitir	DescribeAlarms, PutMetricAlarm,	Permite CloudWatch recuperar las alarmas de su cuenta.

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).

Declaración de la política	Efecto	Actions	Descripción y recurso (ARN)
		PutMetricData	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: <code>aws:logs:*:*:log-group:/mc/*</code>
Amazon EC2 Simple Systems Manager (SSM)			
Acciones de SSM	Permitir	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Permite una variedad de funciones de SSM en su cuenta.

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).

Declaración de la política	Efecto	Actions	Descripción y recurso (ARN)
Acceso a SSM en S3	Permitir	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadParts, 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. <code>aws:s3:::mc-*-*internal-*/aws/ssm*</code>

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 <code>aws:s3:::mc-*-*logs-*/encrypted/app/*</code>
Parche Data Put Object S3	Permitir	PutObject	Permite a EC2 las aplicaciones cargar los datos de los parches a sus depósitos de S3 en <code>aws:s3:::awsms-a*-patch-data-*</code>
Carga de registros propios a S3	Permitir	PutObject	Permite a EC2 las aplicaciones cargar registros personalizados en: <code>aws:s3:::mc-a*-logs-*/aws/instances/*/\${aws:userid}/*</code>

CW = CloudWatch. ARN = Nombre del recurso de Amazon. * = comodín (cualquiera).

Declaración de la política	Efecto	Actions	Descripción y recurso (ARN)
Denegar explícitamente los registros de MC Namespace S3	Denegar	GetObject* Pone*	No permite que EC2 las aplicaciones obtengan o coloquen objetos desde o hacia: <code>aws:s3:::mc-*logs-*/encrypted/mc*</code> , <code>aws:s3:::mc-*logs-*/mc/*</code> , <code>aws:s3:::mc-a*-logs-audit/*</code>
Denegar explícitamente la eliminación de S3	Denegar	* (todos)	No permite que EC2 las aplicaciones realicen ninguna acción sobre los objetos de: <code>aws:s3:::mc-a*-logs-*/*</code> , <code>aws:s3:::mc-a*-internal-*/*</code> ,
Denegar explícitamente el bucket CFN de S3	Denegar	Delete*	No permite que EC2 las aplicaciones eliminen ningún objeto de: <code>aws:s3:::cf-templates-*</code>
Denegar explícitamente List Bucket S3	Denegar	ListBucket	No le permite incluir ningún objeto cifrado, de registro de auditoría o reservado (mc) de: <code>aws:s3:::mc-*logs-*</code>

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: <code>aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-tenant-id*</code> , <code>arn:aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-activation-token*</code> , <code>aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-tenant-id*</code> , <code>aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-tenant-guid*</code>
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 <code>arn:aws:kms::*:alias/ams/eps/cloudone-migration</code>

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.

Alertas del monitoreo de referencia en AMS

Obtenga información sobre los valores predeterminados de supervisión de AMS. Para obtener más información, consulte [Supervisión y gestión de eventos en AMS](#).

La siguiente tabla muestra lo que se monitorea y los umbrales de alerta predeterminados. Puede cambiar los umbrales de alerta con una RFC de administración | Otros | Otros | Actualización (ct-0xdawir96cy7k) tras determinar los cambios que desea realizar y suscribirse al tema de Amazon SNS correspondiente. CloudWatch [Para obtener información sobre la creación de temas y la suscripción a ellos, consulte Suscribirse a un tema](#). Para obtener información general, consulte [Amazon SNS FAQs](#). Para recibir una notificación directa cuando las alarmas superen su umbral, además del proceso de alerta estándar de AMS, siga estas instrucciones sobre cómo sobrescribir las configuraciones de alarma. [Recepción de alertas generadas por AMS](#)

Amazon CloudWatch ofrece una mayor retención de las métricas. Para obtener más información, consulte [CloudWatch Límites](#).

 Note

AMS calibra su monitorización de referencia de forma periódica. Las cuentas nuevas siempre se incorporan con la supervisión de referencia más reciente y en la tabla se describe la supervisión de referencia de las cuentas recién incorporadas. AMS actualiza la supervisión básica de las cuentas existentes de forma periódica y es posible que se produzca un intervalo de tiempo antes de que se apliquen las actualizaciones. Para obtener más información, consulte [Visualización de la configuración de supervisión de una cuenta AMS](#).

Note

La alerta de EC2 instancia Non-root volume usage está DESACTIVADA de forma predeterminada. [Si necesita generar alertas basadas en esta alarma, debe habilitarla mediante el tipo de cambio de RFC ct-0erkoad6uyvvg](#)

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 Balancer (ALB)	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.
Objetivo de Application Load Balancer (ALB)	No	TargetConnectionErrorCount suma > 0 durante 1 minuto, 5 veces consecutivas.	CloudWatch alarma si el número de conexiones no se estableció correctamente entre el balanceador de cargas y las instancias registradas.
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	CloudWatch alarma.

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		> 85% durante 5 minutos, 2 veces consecutivas.	
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	AMSOupostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% durante 5 minutos, 12 veces consecutivas.	CloudWatch alarma en la familia de instancias, capacidad y disponibilidad del AWS Outposts recurso.
		AMSOupostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% durante 5 minutos, 12 veces consecutivas.	CloudWatch alarma sobre el tipo de instancia, la capacidad y la disponibilidad del AWS Outposts recurso.
		AMSOupostsConnectedStatus ConnectedStatus < 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.
		AMSOupostsCapacityException CapacityExceptions 0 durante 5 minutos, 1 vez consecutiva.	CloudWatch alarma por errores de capacidad insuficiente (por ejemplo, lanzamientos de AWS Outposts un recurso) .

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
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.	
		Uso del volumen raíz >= 95% durante 5 minutos, 6 veces consecutivas.	CloudWatch alarma.
		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-volume-s-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	

Servicio	Alerta de seguridad	Nombre de la alerta y condición de activación	Notas
		Libre de memoria*	
		MemoryFree < 5% durante 5 minutos, 6 veces consecutivas.	
	Sí	Malware EPS	CloudWatch evento.
		Se encontró malware en una instancia.	
EC2 Instancia de Amazon: Linux	No	Uso del inodo del volumen raíz	CloudWatch alarma. Se aplica solo a instancias de Linux.
		Promedio superior al 95% durante 5 minutos, 6 veces consecutivas.	
		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 .
		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 $\geq 80\%$ 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 $\geq 80\%$ 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 $\geq 50\%$ 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 $\geq 80\%$ 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.
		SurgeQueueLength > 100 durante 1 minuto, 15 veces consecutivas.	CloudWatch alarma si hay un número excesivo de solicitudes pendientes de enrutamiento.
Instancia de Elastic Load Balancing	No	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	AWS Health Dashboard	Las notificaciones se envían cuando hay cambios en el estado de los eventos AWS Health Dashboard (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 eliminando 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. DiskQueueDepth La suma es > 75 durante 1 minuto, 15 veces consecutivas.	CloudWatch alarma.

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.

AMS toma medidas proactivas (escalando el clúster) cuando se activa esta alerta.

Para obtener información sobre las medidas correctivas, consulte. [Remediación automática de alertas por parte de AMS](#)

[Vea el vídeo de Andrew para obtener más información \(7:03\)](#)

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.

Uso de las consolas AMS

Las consolas AMS de la consola AWS de gestión están disponibles para que pueda interactuar con AMS y utilizar sus recursos gestionados por AMS Advanced y AMS Accelerate. Por lo general, las consolas AMS se comportan como cualquier otra AWS consola; sin embargo, dado que AMS es una organización privada, solo las cuentas habilitadas para AMS pueden acceder a la consola. Una vez que AMS esté activado en su cuenta, podrá acceder a la consola buscando «Managed Services» en la barra de búsqueda unificada.

 Note

Según el rol de su cuenta, podrá acceder a la consola AMS Advanced o a la consola AMS Accelerate.

Cuando utilice las consolas AMS, tenga en cuenta las siguientes advertencias:

- La consola AMS es específica de cada cuenta. Por lo tanto, si tienes una cuenta «de prueba» para tu organización, no podrás ver los recursos en la cuenta «Prod» de esa organización. Del mismo modo, debe tener un rol de AMS Advanced para acceder a la consola de AMS Advanced.
- Las consolas AMS aplican una política de IAM al autenticarse que determina a qué consola puede acceder y qué puede hacer allí. El administrador puede aplicar políticas adicionales a la política de AMS predeterminada para restringir lo que puede ver y hacer en la consola.

La consola AMS Advanced cuenta con las siguientes características:

- Página de apertura: la página de apertura tiene cuadros de información y enlaces para facilitar el acceso a los incidentes RFCs, las solicitudes de servicio y los informes existentes.
- Páginas destacadas y enlaces en el panel de navegación izquierdo:
 - Panel de control: proporciona una descripción general del estado actual de su cuenta, que incluye:
 - Solicitudes de cambio: compruebe cuántas RFCs están esperando tu respuesta y ve a la página de la lista de RFC con ese filtro activo. Vea cuántas RFCs están esperando su aprobación y vaya a la página de la lista de RFC con ese filtro activo. Vea cuántos RFCs están abiertos y vaya a la página de la lista de RFC con ese filtro activo. Abra la página de la lista RFCs haciendo clic en el enlace Ver todo.
 - Incidentes: compruebe cuántos casos de incidentes están pendientes de respuesta y vaya a la página de la lista de incidentes con ese filtro activo. Vea y cuántos están abiertos y vaya a la página de lista de incidentes con ese filtro activo. Abra la página de la lista de incidentes haciendo clic en el enlace Ver todos.
 - Solicitudes de servicio: compruebe cuántas solicitudes de servicio están pendientes de respuesta y vaya a la página de lista de solicitudes de servicio con ese filtro activo. Vea y cuántas están abiertas y vaya a la página de lista de solicitudes de servicio con ese filtro activo. Abra la página de la lista de solicitudes de servicio haciendo clic en el enlace Ver todo.
 - Actualizado recientemente RFCs: fecha, enlace a los detalles del RFC y estado

- Incidentes y solicitudes de servicio creados recientemente: fecha, enlace a los detalles del caso y tipo (incidente o solicitud de servicio)
- RFCs: Abre una lista de los existentes RFCs para la cuenta
- Incidentes: abre una lista de los incidentes abiertos de la cuenta
- Solicitudes de servicio: abre una lista de las solicitudes de servicio abiertas para la cuenta
- Informes: abre la página de informes y los informes predeterminados, Daily Backup y Daily Patch y Monthly Billing
- Recursos:
 - VPCs: Abre una lista de los existentes VPCs para la cuenta
 - Pilas: abre una lista de las pilas existentes en la cuenta
 - AMIs: Abre una lista de los AMS disponibles AMIs
- Características destacadas: información sobre las últimas actualizaciones de la consola
- Recursos para desarrolladores: una página de archivos descargables, que incluye el SDK de administración de cambios avanzada de AMS y más
- Documentación: Página de inicio de la documentación de AWS Managed Services

Uso de la API y la CLI de AMS

La API de AWS Managed Services (AMS) es similar a la APIs de otros AWS servicios. Puede obtener información sobre la API de AMS en la [referencia de la API de AMS](#).

Puntos finales HTTP de la API AMS para llamadas REST

Además de los diversos SDKs, AMS proporciona una CLI; también puede invocar llamadas a la API REST en el punto final de AMS.

Hay dos AMS APIs (el punto final de ambos reside en us-east-1):

- Administración de cambios: utilice esta API para solicitar el acceso a su infraestructura o realizar cambios en ella, incluida la creación y actualización RFCs, el despliegue de nuevas instancias, la actualización y eliminación de instancias, la obtención de información y la CTs creación. AMIs El punto final HTTP es:

`https://amscm.us-east-1.amazonaws.com`

- SKMS: utilice esta API para obtener información sobre su infraestructura, incluidas las pilas VPCs, las subredes y. AMLs El punto final HTTP es:

`https://amsskms.us-east-1.amazonaws.com`

Instalación o actualización de la CLI de AMS

La CLI de AMS es una forma sencilla de interactuar con la API de AMS y se utiliza en los ejemplos de esta sección. Para conocer las convenciones de uso de la AWS CLI y la CLI de AMS, consulte [Uso de la interfaz de línea de AWS comandos](#).

Para obtener información sobre la instalación de SAML, consulte [Regla de notificación de AD FS y configuración de SAML](#).

Para instalar o actualizar la CLI de AMS, siga estas instrucciones:

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`

Uso de la API AMS en CLI, Ruby, Python y Java

La siguiente es una lista de fragmentos de código para la `ListChangeTypeClassificationSummaries` operación de la API de AMS, en todos los idiomas disponibles.

Para Python, Ruby y Java SDKs, consulta [Herramientas para Amazon Web Services](#) y desplázate hacia abajo hasta la SDKs sección. Cada instalador del SDK contiene un archivo README con fragmentos de código adicionales.

Ejemplo de API a CLI de AMS

Una vez instalada la CLI de AMS (requiere la AWS CLI; consulte [Instalación o actualización de la CLI de AMS](#)), puede ejecutar cualquier operación de la API de AMS reformando primero la llamada especificando qué API de AMS `aws amscm oaws amsskms`, a continuación, asignando la acción con guiones en lugar de mayúsculas y minúsculas. Por último, proporcione credenciales, como SAML.

Para obtener más información, consulte [Uso de la interfaz de línea de AWS comandos](#).

Ejemplo:

- API: `'ChangeTypeClassificationSummaries[].[Category,Subcategory,Item,Operation,ChangeTypeId]'`
- CLI: `amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[*].[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

Note

Si se autentica con SAML, `aws --profile saml` añádalo al principio del comando. Por ejemplo:

```
aws --profile saml amscm list-change-type-classification-  
summaries --query "ChangeTypeClassificationSummaries[*].  
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

Ejemplo de API AMS para Python

Para utilizar la API de AMS con Python, instale la CLI de AMS e instale boto3. Siga estos pasos:

1. Instale la CLI de AMS. Consulte [Instalación o actualización de la CLI de AMS](#).
2. Instala boto3, el AWS SDK para Python. Para obtener más información, consulta esta entrada del blog [Ahora disponible: AWS SDK para Python \(Boto3\)](#).

```
import boto3
```

3. Obtenga el cliente AMS Change Management:

```
cm = boto3.client('amscm')
```

4. Obtenga el AMS CTs:

```
cts = cm.list_change_type_classification_summaries()

print(cts)
```

Ejemplos de Python

A continuación, se muestran algunos ejemplos del uso de Python en AMS. Para crear EC2 instancias, and/or utilice Lambda.

Ejemplo de Python para crear un EC2

En este ejemplo se muestra cómo se puede utilizar la RESTFul API amscm desde el código de Python para archivar y realizar procesos de RFC.

1. Instale la CLI de AMS en algún lugar al que tenga acceso; necesitará los archivos que proporciona.
2. Llama a las bibliotecas de Python y crea la EC2 instancia:

```
import boto3
import json
import time

# Create the amscm client
cm = boto3.client('amscm')

# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
```

```
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)

# Extract the RFC ID from the response
NewRfcID = cts['RfcId']

# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
    if RFC_Status_Code == "PendingApproval":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "InProgress":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "Failure":
        print(RFC_Status_Code)
        break
    else:
        print(RFC_Status_Code)

RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

Ejemplo de Python con Lambda

En este ejemplo, se muestra cómo agrupar los modelos AMS con el código para poder usarlos con Lambda, o EC2 en lugares en los que no se va a instalar o no se puede instalar. `amsccli`

Note

AMS no proporciona un SDK de Python importable específico para AMS. El `amsccli` script de instalación instala los modelos de datos del servicio AMS en la ruta normal de la CLI. Para el uso de CLI y el uso de Python del sistema, está bien, ya que ambos `amsccli` `boto3` leen sus modelos de servicio desde las mismas ubicaciones predeterminadas (`~/ .aws/models`). Sin embargo, cuando desea utilizar los servicios de AMS a través de `boto3` en Lambda (o en cualquier otro entorno de ejecución no local), se interrumpe porque ya no tiene los modelos de datos. El siguiente es un método para solucionar este problema empaquetando los modelos de datos con la función.

Hay pasos sencillos que puede seguir para ejecutar su código Python integrado en AMS en Lambda o en otro entorno de ejecución como EC2 Fargate, etc. El siguiente flujo de trabajo muestra los pasos necesarios para las funciones Lambda integradas en AMS.

Al añadir los modelos de datos al paquete de implementación del código y actualizar la ruta de búsqueda del SDK, puede simular una experiencia de SDK.

Important

Este ejemplo y todos los comandos que no son de Python que se muestran se probaron en un ordenador Mac.

Ejemplo de flujo de trabajo:

1. Instale la `amsccli`. Esto crea una carpeta `~/ .aws/models` en su ordenador (Mac).
2. Copie los modelos a un directorio local: `cp ~/ .aws/models ./models`.
3. Incluya los modelos en el paquete de implementación de su código.
4. Actualice el código de la función para añadir los nuevos modelos a la ruta del SDK. ¡Ten en cuenta que este código debe ejecutarse antes de importar `boto3` o `botocore`!

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

Como los modelos de ejemplo están en un directorio llamado `models`, los agregamos a `_PATH`. `./models AWS_DATA` Si el directorio tuviera un nombre `/ams/boto3models`, añadiríamos el siguiente código:

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

El código debería encontrar correctamente los modelos AMS. Como ejemplo más específico sobre el empaquetado, este es el flujo de trabajo específico de Lambda.

Ejemplo de flujo de trabajo Lambda de AMS:

En estos pasos se aplica el ejemplo genérico anterior a la creación de una función de AWS Lambda.

1. Instale el `amscli`. Esto crea una carpeta `~/ .aws/models` en su ordenador (Mac).
2. Copie los modelos a un directorio local:

```
cp ~/.aws/models ./models
```

3. Añada los modelos al archivo zip de despliegue de su función:

```
zip -r9 function.zip ./models
```

 Important

Actualiza el código de tu función para añadir los nuevos modelos a la ruta del SDK. ¡Ten en cuenta que este código debe ejecutarse antes de importar boto3 o botocore!

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

 Note

Como los modelos de ejemplo están en un directorio llamado `models`, los agregamos a `_PATH`. `./models AWS_DATA` Si el directorio tuviera un nombre `/ams/boto3models`, añadiríamos el siguiente código:

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Ahora, despliega tu función:

1. Añade el código de su función al archivo zip de despliegue (si aún no lo ha hecho):

```
zip -g function.zip lambda-amscm-test.py
```

2. Cree o actualice su función con el archivo zip que creó (consola o CLI):

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://
function.zip --region us-east-1
```

Su Python Lambda integrado en AMS debería funcionar ahora.

 Note

Su función debe tener permisos de IAM `amscm` o se producirá un error de permisos.

Ejemplo de código de función Lambda para probar `amscm` (contenido de `.py`): `lambda-amscm-test`

```
import json

# Force lambda to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore

def lambda_handler(event, context):
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
        cts = cm.list_change_type_categories()
        print(cts)
    except botocore.exceptions.UnknownServiceError:
        print("amscm not found")

    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

Resultados de la prueba (éxito):

Respuesta de la función:

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}
```

Request ID:

"1cea13c0-ed46-43b1-b102-a8ea28529c27"

Registros de funciones:

```
START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: $LATEST
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',
  'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-
bcc2-10cf0aa19ece', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid':
  'e27276a0-e081-408d-bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1',
  'content-length': '89', 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

Ejemplo de API de AMS a Ruby

Para usar la API de AMS con Ruby, instale el SDK de AWS Ruby y la CLI de AMS. Siga estos pasos:

1. Instale la CLI de AMS. Consulte [Instalación o actualización de la CLI de AMS](#).
2. Instale el SDK de AWS Ruby. Consulte [Herramientas para Amazon Web Services](#).
3. Configura Ruby con estos comandos:

```
require 'aws-sdk'

config = {

  region: 'us-east-1',

  credentials: Aws::Credentials.new('ACCESS_KEY', 'SECRET_KEY')}
```

4. Obtenga el AMS CTs:

```
ams_cm = Aws::amscm::Client.new(config)

cts = ams_cm.list_change_type_classification_summaries

print(cts)
```

Ejemplo de API de AMS para Java

Para utilizar la API de AMS con Java, instale el SDK de AWS Java y la CLI de AMS. Siga estos pasos:

1. Instale la CLI de AMS. Consulte [Instalación o actualización de la CLI de AMS](#).
2. Instale el SDK de AWS Java. Consulte [Herramientas para Amazon Web Services](#).

3. Configure Java con estos comandos:

```
import com.amazonaws.auth.BasicAWSCredentials;

import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesReque

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResul
```

```
public static void getChangeTypeClassificationSummaries() {
```

4. Establezca las credenciales. Le recomendamos que no lo codifique de forma rígida.

```
final BasicAWSCredentials awsCredsCm =

    new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. Cree el cliente AMS Change Management:

```
final AWSManagedServicesCMClient cmClient =

    new AWSManagedServicesCMClient(awsCredsCm);
```

6. Obtenga el AMS CTs:

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();

final ListChangeTypeClassificationSummariesResult listCtsResult =

cmClient.listChangeTypeClassificationSummaries(listCtsRequest);

System.out.println("List of CTs");

listCtsResult.getChangeTypeClassificationSummaries().stream()

.map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" +
x.getItem() + "/" + x.getOperation())

.forEach(System.out::println);
```

}

AMS trae tu propio EPS

Utilice la función «traiga su propia seguridad de punto final» (BYOEPS) de AMS para sustituir el agente predeterminado de Trend Micro Deep Security por su propia solución de seguridad de punto final o licencia de Trend Micro. Si ya dispone de licencias rentables para productos distintos de Trend Micro Deep Security, o de un equipo que le proporciona su EPS, o si quiere utilizar una herramienta de EPS específica, utilice BYOEPS en sus instancias.

El BYOEPS funciona a nivel de cuenta. Las instancias de la cuenta utilizan BYOEPS o el EPS predeterminado administrado por AMS:

- multi-account landing zone (MALZ): Usted designa las cuentas de aplicación que utilizan BYOEPS o EPS gestionado.
- single-account landing zone (SALZ): tus cuentas AMS utilizan BYOEPS o EPS gestionado.

BYOEPS reduce el coste de su AWS factura para Trend Micro Deep Security. El EPS sigue incurriendo en costes porque el EPS gestionado por AMS sigue siendo necesario para proteger las EC2 instancias creadas y mantenidas por AMS que se requieren para la gestión del acceso (bastiones y hosts de administración). Para calcular el impacto total en los costos, debe tener en cuenta el costo de las licencias de su nueva herramienta y el costo de administrar el EPS en los niveles de servicio que necesite.

El uso del BYOEPS cambia las funciones y responsabilidades de AMS en materia de gestión de la seguridad:

- R significa parte responsable que hace el trabajo para lograr la tarea.
- C significa consultada; parte cuya opinión se solicita, por lo general en calidad de expertos en la materia; y con la que existe comunicación bilateral.
- I significa informado; una parte que recibe información sobre el progreso, a menudo solo una vez finalizada la tarea o el producto final.

Administración de la seguridad	Cliente	AWS Managed Services
Mantener licencias válidas de Managed EPS para EC2 las instancias de AMS Shared Services	R	C
Configure el EPS gestionado para EC2 instancias de AMS Shared Services	I	R
Actualice el EPS gestionado para EC2 las instancias de AMS Shared Services	I	R
Supervisión del malware en EC2 instancias de AMS Shared Services	I	R
Mantenimiento y actualización de las firmas de virus para EC2 las instancias de AMS Shared Services	I	R
Corregir las instancias infectadas con malware en las EC2 instancias de AMS Shared Services	C	R

Al utilizar BYOEPS, pierde uno de los controles de seguridad que ofrece AMS. Aún cuenta con la gestión de la seguridad proporcionada a través de herramientas como Amazon GuardDuty, Amazon Macie y controles de procesos, como las revisiones de las configuraciones de IAM. El uso del BYOEPS no afecta a las certificaciones y atestaciones de conformidad con la AMS. Sin embargo, muchos marcos y certificaciones de seguridad tienen requisitos de protección contra el malware y los códigos maliciosos. Para ayudar a mantener tu cuenta segura y en conformidad, evalúa los controles planificados para asegurarte de que cumplen los requisitos de seguridad de las certificaciones de conformidad de tu carga de trabajo.

Activa el BYOEPS en tu cuenta

El proceso para activar el BYOEPS consta de tres etapas y utiliza varias RFCs. Revisa la siguiente información para obtener información sobre las tres etapas necesarias para activar el BYOEPS. Luego, coordina con tu CSDM la activación del BYOEPS en tu cuenta.

Temas

- [Etapa 1: Requisitos previos](#)
- [Etapa 2: habilita el BYOEPS en tu cuenta](#)
- [Etapa 3: migración de instancias](#)

Etapa 1: Requisitos previos

- El perfil de EC2 instancia de Amazon predeterminado es `customer-mc-ec2-instance-profile`. Si utilizas un perfil de EC2 instancia de Amazon diferente además del perfil predeterminado, permite la `ssm:GetParameter` acción del `/ams/end-point-security` recurso en tu perfil de EC2 instancia.

Si no puedes actualizar los perfiles de EC2 instancia, envía una RFC que especifique los perfiles de instancia que necesitas actualizar.

- Comprende el alcance de este cambio.

Las implementaciones mediante un tipo de cambio automatizado (CT) de AMS le permiten especificar la AMI utilizada en la creación.

Para utilizar BYOEPS con cuentas que utilizan EPS gestionado por AMS, debe trabajar con AMS para desinstalar los agentes de Trend Micro de esas EC2 instancias y actualizar el código de AMS (por ejemplo, los scripts de arranque) de esas instancias. Es posible que estas acciones requieran un reinicio, por lo que se recomienda realizarlas como parte de un período de mantenimiento. Póngase en contacto con su CSDM para identificar un período de mantenimiento para realizar esta actividad y crear un plan de migración. Para el plan de migración, tenga en cuenta las siguientes preguntas:

1. ¿Cuántas instancias necesita migrar? Divida la cantidad total de instancias en lotes incrementales más pequeños.
2. ¿Cómo dividirá las instancias en lotes? Por ejemplo, puede dividir por grupos de recursos y crear una lista para compartirla con el equipo de operaciones de AMS.

3. ¿Cuánto tiempo tardará cada lote? ¿Cuánto tiempo total se necesita? Tenga en cuenta que es posible que desee instalar sus herramientas de EPS preferidas en el mismo período de mantenimiento. ¿Cuánto tiempo llevará esto?
- Su CSDM comparte el plan de migración con el equipo de operaciones de AMS. Si su flota de instancias supera las 50, colabore con su CSDM para crear un evento planificado mediante el proceso de gestión de eventos planificados (PEM). Para obtener más información, consulte [Administración de eventos planificados en AWS Managed Services](#)
- AMS Operations se coordina con su CSDM y le aconseja cómo presentarlo de acuerdo con sus plazos de mantenimiento, RFCs en función del número de instancias de su cuenta.
- Actualice las automatizaciones o los procesos de lanzamiento de EC2 instancias mediante un sistema personalizado o AMS AMIs para utilizar el AMS AMIs publicado después de diciembre de 2020.

Etapa 2: habilita el BYOEPS en tu cuenta

Cuando utilizas el BYOEPS en tu cuenta, las responsabilidades de AMS en materia de gestión de la seguridad cambian. Consulte a su equipo de seguridad y plataforma en la nube antes de activar el BYOEPS.

Para solicitar el BYOEPS para tu cuenta, envía un RFC (Gestión | Otros | Otros | Otros | Actualización) de «MOO» al ct-0xdawir96cy7k, con la siguiente información:

```
Please enable BYOEPS for this account/these accounts
Account IDs: IDs for the accounts for BYOEPS.
```

AMS implementa las actualizaciones del almacén de parámetros en la cuenta y actualiza el perfil de la [instancia de Amazon EC2 IAM](#).

Note

- Las cuentas con nuevos lanzamientos de instancias que utilicen la versión más reciente de AMS AMIs pueden omitir la instalación del agente de Trend Micro. AMIs las versiones anteriores a diciembre de 2020 no admiten la función BYOEPS. Actualice las automatizaciones antiguas AMIs para que utilicen el AMS más reciente con compatibilidad AMIs con la función BYOEPS.

- Para ver el manejo de EC2 instancias existente, consulta la Etapa 3: Migraciones de instancias

Etapa 3: migración de instancias

Usa una de las siguientes opciones para migrar tus instancias, según tu caso de uso. Si no está seguro de qué opción elegir, póngase en contacto con su CA o CSDM.

Cuentas con EC2 instancias que utilizan EPS gestionado por AMS

Durante el período de mantenimiento, de acuerdo con la planificación de la fase 1, se llevan a cabo las siguientes acciones en cada instancia que debe incorporarse al BYOEPS:

- Realizado por AMS: actualice el código de AMS (scripts de arranque, módulos, etc.) a las versiones más recientes. Esto es necesario porque los scripts de arranque de AMS antiguos no admiten la función BYOEPS y se debe volver a instalar el agente de Trend Micro en cada arranque. Además, desinstale el agente de Trend Micro.
- Realizado por usted: instale y configure su herramienta EPS preferida.

Important

Trend Micro Agent ofrece protección contra el malware. Asegúrese de instalar un repuesto adecuado para proteger sus instancias.

Para realizar estos cambios, envíelos RFCs con el tipo de cambio ct-2iz9nvw8zlhst, [Trend Micro DSM | Elimine Trend Micro](#) EPS Agent (es necesario revisar), en lotes.

EC2 Cuentas sin instancias que utilizan EPS gestionado por AMS

Las cuentas con nuevos lanzamientos de instancias que utilicen la versión más reciente de AMS AMIs pueden omitir la instalación del agente de Trend Micro. AMIs las versiones anteriores a diciembre de 2020 no admiten la función BYOEPS. Actualice las automatizaciones antiguas AMIs para que utilicen el AMS más reciente con compatibilidad AMIs con la función BYOEPS.

Añada su agente a las instancias EC2

Puede utilizar AMS Patterns para desplegar agentes de herramientas como CrowdStrike Qualys. Envíe una solicitud de servicio para obtener asistencia.

Recibir notificaciones de AMS

Las comunicaciones entre usted y AMS se producen por varios motivos:

- Un RFC creado por AMS que requiere tu aprobación
- Un caso de AMS creado para investigar una RFC que usted creó y que falló
- Eventos que se crean al monitorear las alertas
- Notificaciones del servicio de parches que le informan de la próxima aplicación de parches
- Solicitudes de servicio e informes de incidentes
- Informes mensuales de CRM
- Anuncios ocasionales importantes de AWS (su CSDM se pone en contacto con usted si es necesaria alguna acción por su parte)

Todas estas notificaciones se envían a la información de contacto predeterminada (el correo electrónico de la cuenta raíz) que proporcionó a AMS cuando se incorporó. Como es difícil mantener actualizados los correos individuales, te recomendamos que utilices un correo de grupo que puedas actualizar por tu parte. Las operaciones de AMS también reciben todas las notificaciones que se le envían y las analizan antes de responder.

El servicio de notificaciones de AMS ofrece dos formas adicionales de configurar los contactos para las notificaciones:

- Etiquete sus recursos con etiquetas de contacto (la etiqueta Valor clave es la información de contacto) y proporcione la etiqueta con el nombre de la clave a su CSDM. Las alarmas de esos recursos se enviarán a los contactos indicados en el valor clave, además del contacto de la cuenta creado en el momento de la incorporación. Esto es especialmente útil para los propietarios de aplicaciones. Para obtener más información, consulte [Notificación de alertas basada en etiquetas](#).
- (Obligatorio al momento de la incorporación) Envíe a su CSDM listas de contactos con nombres para las notificaciones que no estén basadas en recursos. Por ejemplo, puede tener una lista llamada «SecurityContacts» y otra llamada OperationsContacts «», etc. AMS agrega la lista al servicio de notificaciones y las alarmas que se aplican al contexto de esa lista se envían a esos contactos. Esto es especialmente útil para cuestiones organizativas.

Esta función avanzada de enrutamiento de alertas está activa para la mayoría de las CloudWatch alarmas esenciales, como el fallo de una EC2 instancia de Amazon, la utilización de la capacidad de

volumen de Amazon Elastic Block Store (Amazon EBS): uso de raíz, uso de Amazon NonRoot EBS, uso elevado de memoria, uso elevado de intercambio y uso elevado de CPU para Amazon. EC2

Además, cuando presenta una solicitud de servicio o un informe de incidente, tiene la opción de añadir «correos electrónicos CC» (muy recomendable) y esas direcciones de correo electrónico reciben notificaciones sobre la solicitud de servicio o el incidente.

Important

Si bien las direcciones de correo electrónico CC que aparecen en las solicitudes de servicio y los informes de incidentes reciben notificaciones de comunicaciones por correo electrónico, otras notificaciones, como las notificaciones de parches, aparecen en su lista de solicitudes de servicio (también se envía un correo electrónico al contacto predeterminado), sin que se le notifique explícitamente que tiene una comunicación pendiente de su atención. Por este motivo, recomendamos encarecidamente añadir un correo electrónico CC siempre que sea posible y configurar el correo electrónico de contacto predeterminado como un grupo al que pertenezcan todos los usuarios de AMS.

Además, puedes solicitar notificaciones especiales para las nuevas cuentas de AMS AMIs, las que cambien de estado o las que cambien en la configuración de tu cuenta de AMS. Estos servicios de notificación opcionales se describen a continuación.

Notificaciones AMI de AMS con SNS

AMS proporciona un servicio de notificación de AMI. Puede utilizarla para suscribirse a un tema del Amazon Simple Notification Service (SNS) que le notifique cuando se publiquen actualizaciones de la AMI de AMS. Puede elegir recibir notificaciones únicamente para los AMS AMIs que utilice o puede suscribirse para recibir notificaciones de actualización para todos los AMS. AMIs Para obtener más información sobre temas de SNS, consulte [¿Qué es Amazon Simple Notification Service?](#)

Siempre que AMIs se publican, enviamos notificaciones a los suscriptores del tema correspondiente; en esta sección se describe cómo suscribirse a las notificaciones AMI de AMS.

Mensaje de ejemplo

```
{
  "Type" : "Notification",
```

```

"MessageId" : "example messageId",
"TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
"Subject" : "New AMS AMIs are Now Available",
"Message" : "{\"v1\": {\"Message\": \"A new version of the AMS Amazon Machine Images has
been released. You are now able to launch new EC2 stacks from these AMIs.
Please use this time to update any dependencies such as CloudFormation or Autoscaling
groups. Release Notes Windows - Contains latest Windows Patches:
Microsoft Windows Server 2008 R2 Datacenter - (KB2819745, KB3018238, KB4507004,
KB4507437) Microsoft Windows Server 2016 Datacenter Security Enhancedn - (KB4509091,
KB4507459)
Microsoft Windows Server 2016 Datacenter - (KB4509091, KB4507459) Microsoft Windows
Server 2012 R2 Security Enhancedn - (KB3191564, KB3003057, KB3013172, KB3185319,
KB4504418,
KB4506996, KB4507463) Microsoft Windows Server 2012 R2 Standardn - (KB3003057,
KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Linux - Contains latest Linux
patches -
All AMIs now force domainjoin-cli leave before domainjoin-cli join for better
stability in the domain join process.\"\", \"images\":
{\"images\": {\"image_name\": \"customer-ams-windows2019-2021.08-1\", \"image_id\":
\"ami-05dfa45396fddaa5e\"}}, \"region\": \"us-east-1\"}}\",
\"Timestamp\" : \"2021-09-03T19:05:57.882Z\",
\"SignatureVersion\" : \"1\",
\"Signature\" : \"example sig\",
\"SigningCertURL\" : \"example url\",
\"UnsubscribeURL\" : \"example url\"
}

```

Posibles temas de AMI de AMS a los que suscribirse:

- **TODOS:** `Usocustomer-ams-all-amis`. La suscripción a este tema le notifica cuando se actualiza alguno de AMIs los AMS.
- **AMS AWS Linux AMIs:** para Amazon Linux, utilice `customer-ams-amazon1` y `customer-ams-amazon1-security-enhanced`. Para Amazon Linux 2, utilice `customer-ams-amazon2` y `customer-ams-amazon2-security-enhanced`.
- **AMS SUSE Linux AMIs:** se utiliza `paracustomer-ams-sles12`. `customer-ams-sles15`
- **AWS AMS RedHat AMIs:** `Usocustomer-ams-rhel8`, `customer-ams-rhel8-security-enhanced`, `customer-ams-rhel7`, `customer-ams-rhel7-security-enhanced`.
- **AWS AMS CentOS AMIs:** Utilice `customer-ams-centos7`, `customer-ams-centos7-security-enhanced`.
- **AMS Ubuntu AMIs:** `Usocustomer-ams-ubuntu18`.

- AMS AWS Windows AMIs: Utilice `customer-ams-windows2019customer-ams-windows2019-security-enhanced,customer-ams-windows2016,customer-ams-windows2016-security-enhanced,customer-ams-windows2012,customer-ams-windows2012r2,customer-ams-windows2012r2-security-enhanced,customer-ams-windows2022`.

Para suscribirse a las nuevas notificaciones de AMI de AMS mediante la consola Amazon SNS:

1. Abra [Panel](#) en la consola de Amazon SNS.
2. En la esquina superior derecha, cambia a la región de AWS a la AMIs que te estás suscribiendo.
3. En el panel de navegación izquierdo, elija Suscripciones y, a continuación, elija Crear suscripción.
4. Proporcione la información siguiente:
 - a. Tema ARN: `arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}` donde REGION es la región de AWS seleccionada (donde se creó la notificación de SNS) y AMS_AMI_NAME es la AMI sobre la que desea recibir notificaciones. Ejemplos:
 - Para suscribirse a las notificaciones del nuevo AMS Amazon Linux AMIs en la región us-east-1 de AWS, utilice este tema ARN = `arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`
 - Para suscribirse a las notificaciones del nuevo AMS Window Server 2016 AMIs en la región us-west-2 de AWS, utilice este tema ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
 - b. En Protocolo, elija Correo electrónico.
 - c. En Punto de conexión, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones. Recomendamos una lista de distribución en lugar del correo electrónico de una persona.
5. Seleccione Crear suscripción.
6. Cuando reciba un correo electrónico de confirmación con el asunto «Notificación de AWS: confirmación de suscripción», abra el correo electrónico y elija Confirmar suscripción para completar la suscripción.

 Note

No está limitado al correo electrónico para el Protocolo. Para obtener información sobre otros protocolos aceptables y cómo usarlos, consulte [suscribirse](#).

Para cancelar la suscripción a las nuevas notificaciones de AMI de AMS mediante la consola AWS SNS:

1. Abra [Panel](#) en la consola de Amazon SNS.
2. En la barra de navegación, cambie a la región de AWS que prefiera. Debe utilizar la región de AWS en la que desee recibir las notificaciones correspondientes AMIs.
3. En el panel de navegación, elija Suscripciones, seleccione la suscripción y, a continuación, elija Acciones -> Eliminar suscripciones.
4. Cuando se le pida confirmación, seleccione Eliminar.

Para suscribirse a las nuevas notificaciones de AMI de AMS mediante Deployment | Ingestion | Stack from CloudFormation Template | Create (ct-36cn2avfrj9v):

1. Para suscribirse AmazonLinuxSubscription, crear y guardar un archivo JSON de parámetros de ejecución; en este ejemplo se le asigna el nombre .json: CreateSubscribeAmiParams

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "AmazonLinuxSubscription": {
      "Type": "AWS::SNS::Subscription",
      "Properties": {
        "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
        "Protocol": "email",
        "Endpoint": "username@yourdomain.com"
      }
    }
  }
}
```

2. Cree y guarde el archivo JSON de parámetros de RFC con el siguiente contenido; en este ejemplo se le llama CreateSubscribeAmiRfc archivo.json:

```
{
  "ChangeTypeId": "ct-36cn2avfrrj9v",
  "ChangeTypeVersion": "1.0",
  "Title": "cfn-ingest-subscribe-ami"
}
```

3. Cree el RFC especificando el CreateSubscribeAmiRfc archivo y el archivo: CreateSubscribeAmiParams

```
aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json --
execution-parameters file://CreateSubscribeAmiParams.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 ver ejemplos de creación AMIs, consulte [Crear AMI](#).

Para obtener información sobre el consumo AMIs mediante programación, consulte [EC2 stack: creating](#).

Notificaciones de servicio

AMS envía solicitudes de servicio salientes o notificaciones de servicio cuando necesitas actuar o tener conocimiento de algo que pueda afectar a tu cuenta o tus recursos, como:

- Impacto en la infraestructura: AMS envía una notificación de servicio cuando hay un servicio de AWS subyacente que afecta a su infraestructura y usted necesita tomar medidas antes de una fecha determinada, o puede que se produzca una interrupción.
- EC2 Problemas de hardware: AMS envía notificaciones de servicio cuando hay problemas de EC2 hardware que le obligan a reiniciar una EC2 instancia antes de una fecha determinada o le informa de que AMS reiniciará la instancia por usted. Este es un aviso importante porque el reinicio puede provocar una interrupción y debes responder con una fecha aceptable o crear un RFC con el nombre ct-09qbhy7kvtxqw para reiniciar la instancia tú mismo. Una notificación de servicio como esta se cierra automáticamente en cinco días si no respondes.

Notificaciones de cambio de estado de RFC

AMS ofrece notificaciones de los cambios de estado de los RFC por correo electrónico y CloudWatch eventos:

- Correos electrónicos a través de la consola AMS: hay una opción en la segunda página del asistente de creación de RFC, en la que puede añadir hasta cinco direcciones de correo electrónico para recibir notificaciones cuando cambie el estado de la RFC.
- CloudWatch Eventos: puede configurar diferentes reglas y objetivos para que CloudWatch Events reciba notificaciones cada vez que cambie el estado de la RFC.

Notificaciones por correo electrónico

Puede añadir direcciones de correo electrónico para recibir los cambios de estado de un RFC en un RFC que cree en la consola AMS o mediante la API/CLI de AMS.

En la consola AMS, utilice la opción de notificaciones por correo electrónico, que se encuentra en la segunda página del asistente de creación de RFC:

En la API/CLI de AMS, añada una línea como esta a la sección de parámetros de RFC de su RFC (no añada la línea a la sección de parámetros de ejecución):

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"
```

El comportamiento de las notificaciones varía según el tipo de programación de la RFC:

- Está programado RFCs recibir notificaciones por correo electrónico las siguientes fechas: enviadas, programadas, completadas InProgress, rechazadas, canceladas, rechazadas automáticamente o canceladas automáticamente.
- RFCs Reciba lo antes posible una notificación por correo electrónico sobre: enviado, completado InProgress, rechazado AutoRejected, cancelado o cancelado automáticamente.

Note

- Las notificaciones por correo electrónico se envían desde esta dirección: `no-reply@managedservices.amazonaws.com`

- Los caracteres especiales y URLs el título de su RFC están redactados en los correos electrónicos que enviamos. Se trata de una medida de seguridad.

CloudWatch Notificaciones de eventos

AMS ofrece notificaciones automáticas para los cambios de estado de la RFC a través CloudWatch de eventos. Para recibir estas notificaciones:

1. Crea un tema y una suscripción a los que se enviarán las notificaciones. Puedes darle al tema el nombre que desees; para obtener información sobre cómo hacerlo, consulta [Tema y suscripción de SNS: Creación](#).
2. Envíe un RFC a la dirección | Otros | Otros | Cree el tipo de cambio e incluya el tema del SNS y la suscripción en la solicitud de avisos de cambio de estado del RFC.

Al enviar la solicitud de RFC de Administración | Otros | Otros para esta función, puede especificar los cambios de estado de la RFC sobre los que desea recibir notificaciones y los tipos de cambios, además de configurar otros filtros. Por ejemplo, es posible que desee solicitar que se le notifique únicamente cuando los tipos de cambio de Admin Access sean EventType = RfcSubmitted y EventType =. RfcUpdated

Esta es una plantilla de notificaciones de CloudWatch eventos que puede recibir (con todos los valores posibles):

```
{
  "source ": "aws.managedservices",
  "detail-type": "AMS RFC State Change",
  "detail": {
    "ActionState": "null | AwsActionPending | AwsOperatorAssigned | CustomerActionPending | NotApplicable | NoActionPending",
    "ActualExecutionTimeRange": {
      "StartTime": "null | Actual Start Time",
      "EndTime": "null | Actual End Time"
    },
    "AutomationStatus": "Automated | Manual",
    "AwsAccountId": "AWS Account ID",
    "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending | Rejected | Approved",
    "ChangeTypeId": "Change_Type_ID",
```

```

    "ChangeTypeVersion": "Change_Type_Version",
    "CreatedTime": "Created_Time",
    "CustomerApprovalStatus": "null | SubmissionPending | NotRequired |
ApprovalPending | Rejected | Approved",
    "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected |
RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted |
RfcUpdated",
    "LastModifiedTime": "Last_Updated_Time",
    "LastSubmittedTime": "null | Last_Submitted_Time",
    "RequestedExecutionTimeRange": {
        "StartTime": "null | Expected_Start_Time",
        "EndTime": "null | Expected_End_Time"
    },
    "RfcId": "RFC_ID",
    "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled |
ExecutionLock | InProgress | Success | Failure",
    "Title": "Title"
}
}

```

Los cambios de estado del RFC admitidos (EventType), tal como aparecen en la notificación de CloudWatch eventos real, son:

- RfcActionStateUpdated (sin opción de consola AMS): la RFC en uno de los estados, que se describe más adelante, cambió.
- RfcApproved (sin opción de consola AMS): el RFC ha superado la validación del operador del and/or AMS del sistema y se ha aprobado su finalización.
- RfcAutoRejected (Rechazado automáticamente): el RFC no pasó la validación del sistema o del operador del AMS y se rechazó.
- RfcCanceled (Cancelado o cancelado automáticamente): el remitente o un operador de AMS cancelaron la RFC.
- RfcCompleted (Completado): se han completado los parámetros de ejecución de la RFC, incluidos los siguientes: UserData
- RfcCreated (sin opción de consola AMS): el RFC se creó correctamente (el JSON y los parámetros enviados eran válidos).
- RfcInProgress (InProgress): La ejecución del RFC aún está en curso.
- RfcRejected (Rechazada): Se ha rechazado la validación del sistema o del operador del AMS que ha fallado con la RFC.

- **RfcSubmitted (Enviado):** el RFC se ha enviado y se encuentra en proceso de validación del sistema.
- **RfcUpdated (sin opción de consola AMS):** un operador de AMS actualizó manualmente el RFC.

Además, puedes enviar notificaciones de CloudWatch eventos (CWE) a cualquiera de los destinos compatibles y crear tus propios sistemas a partir de estas notificaciones automáticas:

- EC2 Instancias de Amazon
- AWS Lambda funciones
- Flujos de Amazon Kinesis Data Streams
- Flujos de entrega en Amazon Data Firehose
- Registrar grupos en Amazon CloudWatch Logs
- Tareas de Amazon ECS
- Systems Manager Run Command
- Automatización de Systems Manager
- AWS Batch trabajos
- Máquinas de estado de Step Functions
- Tuberías en CodePipeline
- CodeBuild proyectos
- Plantillas de evaluación de Amazon Inspector
- Temas de Amazon SNS
- Colas de Amazon SQS
- Objetivos integrados: llamada a la EC2 CreateSnapshot API, llamada a la EC2 RebootInstances API, llamada a la EC2 StopInstances API, llamada a la EC2 TerminateInstances API.
- El bus de eventos predeterminado de otra cuenta de AWS

 Note

Enviamos una notificación de CloudWatch eventos en caso de cambios de estado en el RFC, haciendo todo lo posible.

Configuración de DNS públicos y privados

Durante la incorporación, AMS configura un servicio de DNS privado para las comunicaciones entre sus recursos gestionados y AMS.

Puede usar AMS Route 53 para administrar los nombres DNS internos de los recursos de su aplicación (servidores web, servidores de aplicaciones, bases de datos, etc.) sin exponer esta información a la Internet pública. Esto añade un nivel de seguridad adicional y también permite realizar la conmutación por error de un recurso principal a uno secundario (lo que suele denominarse «inversión») asignando el nombre DNS a una dirección IP diferente.

Después de crear recursos de DNS privados mediante Deployment | Advanced stack components | DNS (privado) | Create (ct-0c38gftq56zj6) o Deployment | Advanced stack components | DNS (público) | Create (ct-0vzsr2nyraedl), puede utilizar Management | Advanced stack components | DNS (privado) | Update (ct-1d55pi44ff21u) y Management | Advanced stack components | DNS (público) | Actualizar (ct-1hzofpphabs3i) CTs para configurar conjuntos de registros adicionales o actualizar los existentes. En el caso de las cuentas de zona de aterrizaje multicuenta (MALZ), los recursos de DNS creados en la cuenta de la aplicación se VPCs pueden compartir con la cuenta de servicios compartidos VPC para mantener el DNS centralizado mediante AMS AD.

MALZ

El siguiente gráfico ilustra una posible configuración de DNS para la zona de destino multicuenta AMS. Muestra una configuración de DNS híbrida entre AMS y una red de clientes típica. Un registro de nombres canónico (CNAME) del servidor DNS de la red del cliente lo reenvía al DNS de AMS AD de la cuenta de servicios compartidos, con un reenvío condicional en el que el CNAME del FQDN de AMS se reenvía al registro A.

SALZ

El siguiente gráfico ilustra una posible configuración de DNS para una sola cuenta landing zone (SALZ). Muestra una configuración de DNS híbrida entre AMS y una red de cliente típica. Un CNAME del servidor DNS de la red del cliente lo reenvía al DNS de AMS AD con un reenvío condicional en el que el CNAME del FQDN de AMS se reenvía al registro A.

SALZ Route53 DNS

El siguiente gráfico ilustra una posible configuración de DNS para una sola cuenta landing zone (SALZ). Muestra una configuración de DNS híbrida entre AMS y una red de cliente típica. Un

CNAME del servidor DNS de la red del cliente lo reenvía al DNS de AMS AD con un reenvío condicional en el que el CNAME del FQDN de AMS se reenvía al registro A. Esto también aprovecha Route53 para el tráfico de red saliente, de modo que cualquier aplicación de la cuenta pueda tener una resolución de DNS en la cuenta con la mayor disponibilidad.

Rutas de resolución habilitadas para Route53:

- Instancia que intenta resolver el nombre MAD de AMS --> VPC +2 (Route53/ AmazonProvided DNS) --> Se evaluaron los reenviadores condicionales --> La regla del reenviador condicional MAD de Route53 coincidió -> Resolver de salida de Route53 -> DNS de AD administrado
- Instancia que intenta resolver el nombre local del cliente --> VPC +2 (Route53/ AmazonProvided DNS) --> Se evaluaron los reenviadores condicionales --> La regla del reenviador condicional local de Route53 coincidió -> Resolver de salida de Route53 -> DNS local del cliente
- Instancia que intenta resolver el nombre de Internet --> VPC +2 (Route53/ AmazonProvided DNS) --> Reenviadores condicionales evaluados --> No hay reenviador coincidente --> Servicio DNS de Internet

Para obtener más información, consulte [Uso de DNS con su VPC](#) y [Trabajo con zonas alojadas privadas](#).

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.

Implementación de recursos de IAM en AMS Advanced

AMS despliega los recursos de IAM en su aplicación de zona de aterrizaje multicuenta (MALZ) y en sus cuentas de zona de aterrizaje de cuenta única (SALZ) de dos maneras:

- **Aprovisionamiento automatizado de IAM:** esta función de AMS le permite enviar, crear, actualizar o eliminar tipos de cambios para el aprovisionamiento de funciones o políticas de IAM, sin necesidad de que el operador los revise y, con IAM y AMS, las comprobaciones de validación se ejecutan automáticamente.

Esta capacidad debe estar habilitada de forma explícita con la opción Administración | Cuenta gestionada | Aprovisionamiento automatizado de IAM con permisos de lectura y escritura | [Habilitar \(es necesario revisar\) el tipo de cambio \(ct-1706xvbk6j9hf\)](#). Para obtener más información, consulte [Aprovisionamiento automatizado de IAM \(AMS\)](#). Una vez activado el aprovisionamiento automatizado de IAM por AMS, tendrá acceso a los tipos de cambios de creación, actualización y eliminación para gestionar sus recursos de IAM.

- **Revise el tipo de cambio de IAM requerido:** Este tipo de cambio, Deployment | Advanced stack components | Identity and Access Management (IAM) | [Crear entidad o política \(es necesaria una revisión\) \(ct-3dpd8mdd9jn1r\)](#), [requiere una revisión](#) por parte del operador de AMS, que a veces puede tardar unos días en completarse si se necesitan aclaraciones.

Note

Sea cual sea el método que se utilice, se aprovisiona un rol de IAM a la cuenta o cuentas correspondientes y, una vez aprovisionado el rol, debe incorporarlo a su solución de federación.

Aprovisionamiento automatizado de IAM (AMS)

AWS Managed Services (AMS) admite la validación y el aprovisionamiento automatizados de los recursos de IAM, incluidas las funciones y las políticas, mediante las solicitudes de cambio avanzadas (RFCs) y los nuevos tipos de cambio () de AMS. CTs Anteriormente, estas solicitudes se sometían a un proceso semiautomatizado que, en ocasiones, provocaba largos tiempos de espera. Ahora, puede utilizar el aprovisionamiento automatizado de IAM por AMS para aprovisionar los recursos de IAM y obtener los resultados con mucha más rapidez.

Cómo funciona el aprovisionamiento automatizado de IAM en AMS

El aprovisionamiento automatizado de IAM se basa en comprobaciones automatizadas de IAM en tiempo de ejecución para validar los cambios en los recursos de IAM. Estas comprobaciones automatizadas, que se realizan cuando se ejecutan los tipos de cambios de creación, actualización

o eliminación, evitan que los recursos de IAM que son demasiado permisivos o tienen patrones inseguros se desplieguen en su cuenta. Esto le permite ajustar el nivel de rigor de las revisiones de IAM a la experiencia de su equipo. Recomendamos que los equipos que son nuevos en los servicios en la nube y necesitan comprobar manualmente todos los cambios en los recursos de IAM utilicen el tipo de cambio existente que requiere revisión: Implementación | Componentes de pila avanzados | Identity and Access Management (IAM) | [Crear entidad o política \(requiere revisión\)](#), (ct-3dpd8mdd9jn1r). Los equipos con AWS experiencia y control de sus entornos pueden utilizar el aprovisionamiento automatizado de IAM para acelerar sus despliegues. Puede utilizar esta función para realizar la validación mediante comprobaciones automatizadas en tiempo de ejecución o para realizar la validación y el aprovisionamiento de los recursos de IAM una vez que la validación se haya realizado correctamente.

Important

AWS Managed Services ha implementado de forma proactiva una lista de [comprobaciones del tiempo de ejecución](#) de la validación que impiden la creación de recursos o políticas de IAM con determinados permisos y condiciones. Para obtener una descripción de estos privilegios y condiciones, consulte [Implementación de recursos de IAM en AMS Advanced](#). Los tipos de cambio automatizados [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1difq](#) y [ct-17cj84y7632o6](#) [permiten a los usuarios que dominan la administración de los recursos de IAM aprovisionar](#) funciones y políticas de IAM que permiten realizar acciones más allá de los privilegios de solo lectura.

Además, puede usar las funciones creadas mediante los tipos de cambio automatizados [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1diafq](#) y [ct-17cj84y7632o6](#) para crear los nuevos recursos. Sin embargo, los recursos no pueden seguir el estándar de nomenclatura de AMS y no forman parte de la pila de AMS estándar. AMS proporciona el apoyo operativo y de seguridad de esos recursos específicos haciendo todo lo posible.

Si bien tanto los procesos manuales como los automatizados tienen como objetivo mantener nuestros estándares de seguridad, es importante tener en cuenta que existen diferencias en los controles entre ambos. El aprovisionamiento automatizado permite una mayor flexibilidad a la hora de crear y actualizar funciones y políticas; por lo tanto, no son lo mismo. Se recomienda que su organización revise detenidamente las [comprobaciones del tiempo de ejecución](#) de las validaciones que se indican en la Guía del usuario de AMS para asegurarse de que se ajustan a las expectativas y los requisitos de la organización.

Flujo de validación

Flujo de validación y aprovisionamiento

Note

Esta función es adecuada para los equipos que tienen experiencia con AWS los recursos de IAM y no la recomendamos para los equipos que son nuevos en ellos. AWS El proceso de validación automática está diseñado para atrapar la mayoría de los errores y es útil para que los equipos revisen rápidamente los cambios en la IAM, cuando entienden los permisos que necesitan. Para utilizar los nuevos tipos de cambios de forma segura y eficaz, te recomendamos que conozcas bien la AWS IAM y las [comprobaciones en tiempo de ejecución](#) que ofrecen los tipos de cambio para determinar si son adecuados para tu equipo.

Incorporación al aprovisionamiento automatizado de IAM en AMS

[Para utilizar los nuevos tipos de cambio, active primero el aprovisionamiento automatizado de IAM por AMS enviando una RFC con el siguiente tipo de cambio: Administración | Cuenta gestionada | Aprovisionamiento automatizado de IAM por AMS con permisos de lectura y escritura | Habilitar \(es necesario revisar\) \(ct-1706xvbk6j9hf\)](#). AWS requiere que su organización pase por un proceso de gestión de riesgos de seguridad del cliente (CSRM) para garantizar que el uso de estos tipos de cambios esté alineado con las políticas de su organización. El equipo de AWS operaciones trabaja con usted para obtener la aprobación explícita de su contacto del equipo de seguridad en forma de aceptación del riesgo como parte de la revisión requerida. Para obtener más información, consulte el proceso de [gestión de riesgos para clientes \(CSRM\) de la RFC](#).

Una vez finalizada la solicitud de confirmación para activar la función de aprovisionamiento automatizado de IAM con permisos de lectura-escritura, AMS habilita el aprovisionamiento automatizado de IAM por AMS para cambiar los tipos de cambio en la cuenta utilizada para enviar la RFC de activación. Para confirmar que una cuenta tiene activado el aprovisionamiento automatizado de IAM por AMS, compruebe la función en la consola de IAM. `AWSTManagedServicesIAMProvisionAdminRole`

Como parte de la incorporación, AMS aprovisiona IAM Access Analyzer en la misma región de AWS de la cuenta para aprovechar su capacidad de vista previa del acceso. IAM Access Analyzer ayuda a identificar los recursos de su organización y las cuentas que se comparten con una entidad externa,

valida las políticas de IAM comparándolas con la gramática de las políticas y las mejores prácticas, y genera políticas de IAM en función de la actividad de acceso de sus registros. AWS CloudTrail [Para obtener más información, consulte Uso. AWS Identity and Access Management Access Analyzer](#)

Una vez incorporado, `AWSTrustedArns` se implementa en las cuentas habilitadas. Si decide utilizar este rol a través de la federación SAML, debe incorporar el rol a su solución de federación.

Como parte de la incorporación, puede solicitar la actualización de la política `IAMProvisionAdminRole` de confianza de `AWSTrustedArns` para conceder otro ARN de rol de IAM con el que pueda asumir este rol. `AWS Security Token Service`

Uso del aprovisionamiento automatizado de IAM de AMS en AMS

Puede crear RFCs con los siguientes tipos de cambios en el aprovisionamiento automatizado de IAM de AMS.

Note

- Solo se admite el aprovisionamiento de funciones y políticas.

Al actualizar las funciones, la actualización CT sustituye la lista existente de nombres de recursos de Amazon para políticas gestionadas y el documento de política «asumir una función», por la lista proporcionada de políticas gestionadas ARNs y el documento de política «asumir funciones». ARNs En una actualización parcial, por ejemplo, no se permite agregar o eliminar un ARN de la lista existente de políticas administradas ARNs, ni agregar o eliminar declaraciones de políticas individuales al documento de política de «asumir funciones». Del mismo modo, al actualizar las políticas, la actualización CT reemplaza el documento de política existente y no permite agregar o eliminar una declaración de política individual en el documento de política existente.

- Cuando se selecciona la opción «validar únicamente», las comprobaciones en tiempo de ejecución se realizan sin aprovisionar ninguna entidad o política de IAM. Independientemente de los resultados, el estado de la RFC es «correcto». El estado «correcto» indica que la validación se realizó correctamente con respecto a la entidad o política de IAM proporcionada.

- Implementación | Advanced Stack Components | Identity and Access Management (IAM) | [Crear entidad o política \(permisos de lectura-escritura\) \(ct-1n9gfnog5x7fl\)](#): una nueva entidad o política de IAM se valida y aprovisiona automáticamente.
- Administración | Advanced Stack Components | Identity and Access Management (IAM) | [Actualizar entidad o política \(permisos de lectura-escritura\) \(ct-1e0xmuy1diafq\)](#): una entidad o política de IAM existente se actualiza y valida automáticamente.
- Administración | Advanced Stack Components | Identity and Access Management (IAM) | [Eliminar entidad o política \(permisos de lectura-escritura\) \(ct-17cj84y7632o6\)](#): se elimina una entidad o política de IAM existente que se aprovisiona mediante el tipo de cambio de política o entidad de creación automática.

Solo puede llamar a las tres anteriores mediante una función de IAM dedicada: `CTs AWSManagedServicesIAMProvisionAdminRole` Esta función solo está disponible en las cuentas que se han incorporado a la función mediante los permisos de lectura/escritura de Administración | Cuenta gestionada | AMS Automated IAM Provisioning | [Habilitar \(es necesario revisar\) \(ct-1706xvvk6j9hf\)](#).

Important

Los tipos de cambios de creación, actualización y eliminación siempre están visibles en su cuenta, pero no están activados de forma predeterminada. Si intenta enviar una RFC mediante uno de estos tipos de cambios sin activar primero la función de aprovisionamiento automatizado de IAM por parte de AMS, aparecerá un mensaje de error que indica que no está autorizado.

Limitaciones:

- La función Create CT podría permitirle crear un rol o una política de IAM con permiso para crear recursos. AWS Sin embargo, AMS no administra los AWS recursos creados por estas funciones y políticas. Se recomienda ceñirse al control de la organización para limitar la creación de dichos roles o políticas.
- La actualización CT no puede modificar las funciones y políticas de IAM creadas con CFN Ingest, Direct Change Mode, Developer Mode o, en algunos casos, mediante el AMS Advanced existente, manual o automatizado. CTs

- El comando Delete CT no puede eliminar las funciones o políticas existentes que no se hayan creado con el AMS Automated IAM Provisioning Create CT.
- La función de aprovisionamiento automatizado de IAM de AMS con permisos de lectura y escritura no es compatible con las funciones del modo de cambio directo. Esto significa que no puede aprovisionar ni actualizar las funciones y políticas de IAM con permisos de lectura y escritura mediante estas funciones.
- El aprovisionamiento automatizado de IAM por AMS con permisos de lectura y escritura Los tipos de cambios de creación, actualización y eliminación no son compatibles con el Connector. ServiceNow

El tiempo de ejecución comprueba el aprovisionamiento automatizado de IAM en AMS

El aprovisionamiento automatizado de IAM aprovecha las comprobaciones y validaciones de la política de límites de AWS Identity and Access Management Access Analyzer AMS y realiza comprobaciones y validaciones adicionales en función de la misma. AMS definió las comprobaciones y validaciones adicionales en función de las mejores prácticas de IAM, la experiencia de gestionar la carga de trabajo de los clientes en la nube y la experiencia colectiva de evaluación manual de AMS IAM.

Puede ver los resultados de las comprobaciones de las políticas en tiempo de ejecución en el resultado de la solicitud de cambio (RFC). Los resultados incluyen el identificador del recurso, la ubicación dentro de la and/or política de roles que generó los hallazgos y un mensaje en el que se describe la comprobación que la entidad o el recurso de IAM no pudo superar. Estos hallazgos le ayudan a crear políticas que sean funcionales y se ajusten a las mejores prácticas de seguridad.

Note

El aprovisionamiento automatizado de IAM intenta ser específico en cuanto a la ubicación dentro de la definición de la entidad o política que no pasa la prueba. Según el tipo, la ubicación puede incluir el nombre del recurso, el ARN o el índice dentro de una matriz. Por ejemplo, una declaración que le ayude a ajustar la entidad o la política para obtener un resultado exitoso.

Para disfrutar de una experiencia de aprovisionamiento automatizado de IAM por parte de AMS sin problemas, se recomienda utilizar la opción «solo validar» para ejecutar las comprobaciones de validación hasta que no se detecten resultados de las comprobaciones de validación que figuran

en los resultados de la RFC. Cuando las comprobaciones de validación no arrojen resultados, seleccione Crear copia desde la consola AMS para crear rápidamente una copia de la RFC existente. Cuando esté listo para aprovisionar, en la sección Parámetros, cambie el valor Validar solo de Sí a No y, a continuación, continúe.

Estas son las comprobaciones en tiempo de ejecución que AMS Automated IAM Provisioning realiza para garantizar la seguridad de sus recursos de IAM:

 Note

Para aprovisionar políticas de IAM que contengan acciones denegadas por estos tipos de cambios automatizados, debe seguir el proceso de gestión de riesgos de seguridad para los clientes (CSRM) de la RFC. Utilice el siguiente tipo de cambio: Implementación | Componentes de pila avanzados | Identity and Access Management (IAM) | Crear entidad o política (es necesario revisar) (ct-3dpd8mdd9jn1r).

- [Verificación y validación de políticas de IAM Access Analyzer: consulte también la referencia de verificación de políticas de Access Analyzer y la validación de políticas de IAM Access Analyzer.](#)
- Comprobaciones de la política de límites de permisos de AMS: acciones en un conjunto de servicios que se deniegan de forma predeterminada. Para obtener más información, consulte Comprobación [automática de los límites de los permisos de aprovisionamiento de IAM](#).
- Comprobaciones de la política de límites de permisos definidas por el cliente: acciones restringidas adicionales en un conjunto de servicios que se deniegan. Para obtener más información, consulte Comprobación [automática de los límites de los permisos de aprovisionamiento de IAM](#).
- Comprobaciones personalizadas definidas por AMS: comprobaciones que identifican diversas políticas o patrones de acceso inseguros y excesivamente permisivos dentro de una entidad o política de IAM solicitada, y deniegan la solicitud si se encuentra alguna. [Para obtener más información, consulte AWS Elementos de la política de JSON: Principal.](#)

Resultado	Descripción
Se puede acceder al rol desde una cuenta externa que se encuentra fuera de su zona de confianza.	Este hallazgo se refiere a un elemento principal incluido en la política de confianza de roles que se encuentra fuera de su zona de confianza . Una zona de confianza se define como

Resultado	Descripción
	la cuenta en la que se crea el rol o la AWS organización a la que pertenece la cuenta. Una entidad que no pertenece a la cuenta ni a la misma AWS organización es una entidad externa. Para resolver este problema, revisa el identificador de la cuenta en el principal ARNs y asegúrate de que te pertenece y de que se trata de una cuenta integrada en AMS.
Puede acceder al rol una entidad externa propiedad de una cuenta <i>External_Account_ID</i> que no sea propiedad de la cuenta propiedad del cliente de AMS. <i>Account_ID</i>	Esta conclusión se genera si la política de confianza de roles incluye un ARN principal que tiene un identificador de cuenta que no es de tu propiedad y una cuenta incorporada de AMS. Para resolver este problema, elimina dicho principal de la política de confianza del rol.
El ID de usuario canónico no es un principio admitido en la política de confianza de IAM.	La política de confianza de IAM no admite IDs los principios canónicos. Para resolver el problema, elimine dicho principio de la política de confianza del rol.
Se puede acceder al rol mediante una identidad web externa que se encuentre fuera de su zona de confianza.	Este hallazgo se genera si la política de confianza de roles permite un proveedor de identidad web (IdP) externo distinto del IdP de SAML. Para resolver este problema, revise la política de confianza de roles y elimine las sentencias que permiten la operación. <code>sts:AssumeRoleWithWebIdentity</code>
Se puede acceder a la función a través de la federación de SAML; sin embargo, el proveedor de identidad (IdP) de SAML proporcionado no existe.	Este hallazgo se genera si la política de confianza de roles contiene un IdP de SAML que no existe en su cuenta. Para resolverlo, asegúrate de que todos los IDP de SAML listados existen en tu cuenta.

Resultado	Descripción
La política contiene acciones privilegiadas equivalentes al acceso de un administrador o de un usuario avanzado. Considere la posibilidad de reducir el alcance del permiso a un servicio, acción o recurso específicos. Si se utilizan elementos de política avanzados como <code>NotAction</code> o <code>NotResource</code> no se utilizan, asegúrese de que no concedan más acceso del previsto, especialmente en las instrucciones <code>Allow</code> .	Cuando se establecen permisos AWS Identity and Access Management con políticas de IAM, se recomienda conceder únicamente los permisos necesarios para realizar una tarea. Para ello, defina las acciones que se pueden llevar a cabo en recursos específicos en condiciones específicas, lo que también se conoce como permisos con privilegios mínimos. Esta conclusión se genera cuando la automatización detecta que la política concede amplios permisos y no se ajusta al principio del privilegio mínimo. Para resolver el problema, revise y reduzca los permisos.
La declaración contiene acciones privilegiadas para <code>Service_Name</code> . Considere excluir estas acciones con una declaración de rechazo. Consulte la referencia sobre la política de límites en la documentación de la AMS para obtener una lista de acciones privilegiadas.	AMS identificó determinadas acciones relacionadas con un servicio determinado como riesgosas y que el equipo de seguridad del cliente debía volver a estudiarlas y aceptarlas. Esta conclusión se genera cuando la automatización detecta la política determinada que concede dichos permisos. Para resolver este problema, deniega estas acciones en tu política. Para obtener una lista de acciones, consulte la política de límites de la AMS. Para obtener más información sobre la política de límites de AMS, consulte Verificación automática de límites de permisos de aprovisionamiento de IAM por AMS .

Resultado	Descripción
La declaración otorga acceso a los tipos de cambio de RFC privilegiados: ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq y ct-17cj84y7632o6 para el servicio. <i>Service_Name</i> Considere la posibilidad de establecer el alcance de los permisos para tipos de cambio específicos o excluya estos tipos de cambio con una sentencia de denegación.	Esta conclusión se genera si la política concede permisos para realizar acciones relacionadas con la RFC mediante los tipos de cambio del aprovisionamiento automatizado de IAM (). CTs CTs Están sujetos a la aceptación de riesgos y solo se deben utilizar para las funciones incorporadas. Por lo tanto, no puedes concederles permiso. CTs Para resolver este problema, deniegue las acciones de RFC al utilizarlas CTs.
La declaración contiene acciones privilegiadas que no se limitan a sus recursos de servicio. <i>Service_Name</i> Considere la posibilidad de limitar las acciones a recursos específicos o excluir los recursos con prefijos de espacio de nombres AMS. Si se utilizan caracteres comodín, asegúrese de que restrinjan el ámbito a sus recursos.	Esta conclusión se genera si la política concede acciones privilegiadas que no se limitan a los recursos del servicio en cuestión. Los comodines suelen crear políticas demasiado permisivas que incluyen un amplio conjunto de recursos o acciones en el ámbito de aplicación del permiso. Para resolver este problema, reduce el alcance de los permisos de los recursos de tu propiedad o excluye los recursos que se encuentran en el espacio de nombres AMS. Para obtener una lista de los prefijos de los espacios de nombres de AMS, consulte la política de límites en la documentación de AMS. Tenga en cuenta que no todos los prefijos se aplican a todos los servicios . Para obtener más información sobre la política de límites de AMS, consulte Verificación automática de límites de permisos de aprovisionamiento de IAM por AMS.

Resultado	Descripción
El identificador de cuenta o el nombre de recurso de Amazon (ARN) no son válidos.	Este hallazgo se genera si algún ARN o identificador de cuenta especificado en la política o la política de confianza de roles no es válido. Para revisar los recursos de un ARN de recurso válido para los servicios, consulte la Referencia de autorización de servicios . Asegúrese de que el ID de la cuenta sea un número de 12 dígitos y de que la cuenta esté activa en AWS.
El uso del comodín (*) como identificador de cuenta en el ARN está restringido.	Este resultado se genera si se especifica un comodín (*) en el campo de ID de cuenta de un ARN. Un comodín en el campo del identificador de una cuenta coincide con cualquier cuenta y podría conceder permisos involuntarios a los recursos. Para resolver este problema, sustituye el comodín por un identificador de cuenta específico.
La cuenta de recursos especificada no pertenece a la misma cuenta <i>Account_ID</i> propietaria del cliente de AMS.	Este hallazgo se genera si un identificador de cuenta especificado en el ARN de un recurso no le pertenece y AMS no lo administra. Para resolver este problema, asegúrese de que todos los recursos (tal como se especifica en su ARN en la política) pertenezcan a sus cuentas administradas por AMS.
El nombre de la función se encuentra en el espacio de nombres restringido de AMS.	Este resultado se genera si intenta crear un rol con un nombre que comience con un prefijo reservado de AMS. Para resolver este problema, utilice un nombre para el rol que sea específico para su caso de uso. Para obtener una lista de los prefijos reservados de AMS, consulte Prefijos reservados de AMS .

Resultado	Descripción
El nombre de la política está en el espacio de nombres restringido de AMS.	Este resultado se genera si intenta crear una política con un nombre que comience con un prefijo reservado de AMS. Para resolver este problema, usa un nombre para la política que sea específico para tu caso de uso. Para obtener una lista de los prefijos reservados de AMS, consulte Prefijos reservados de AMS .
El ID de recurso del ARN se encuentra en el espacio de nombres restringido de AMS.	Este resultado se genera si se intenta crear una política que conceda permisos a los recursos con nombre asignado que se encuentran en el espacio de nombres AMS. Para resolver este problema, asegúrese de limitar los permisos a sus recursos o denegar los permisos a los recursos que se encuentran en el espacio de nombres AMS. Para obtener más información sobre los espacios de nombres de AMS, consulte Espacios de nombres restringidos de AMS.
Caso de variable de política no válido. Actualice la variable a <i>Variable_Names</i> .	Este resultado se genera si se intenta crear una política que contenga una variable de política global de IAM en el caso incorrecto. Para resolver este problema, utilice las mayúsculas y minúsculas correctas para las variables globales de su política. Para obtener una lista de variables globales, consulta las claves de contexto de las condiciones AWS globales . Para obtener más información sobre las variables de política, consulte Elementos de la política de IAM: variables y etiquetas

Resultado	Descripción
La declaración contiene acciones privilegiadas que no están sujetas a las claves de KMS. Considere la posibilidad de limitar estos permisos a claves específicas o excluir las claves propiedad de AMS.	Esta conclusión se genera si la política contiene permisos que no se limitan a claves de KMS específicas de su propiedad. Para resolver este problema, limita el permiso a claves específicas o excluye las claves que son propiedad de AMS. Las claves propiedad de AMS tienen conjuntos de alias específicos. Para obtener una lista de los alias de clave propiedad de AMS, consulte Verificación automática de límites de permisos de aprovisionamiento de IAM por AMS .
La declaración contiene acciones privilegiadas que no se limitan a los alias de las claves de KMS. Considere la posibilidad de limitar estos permisos a sus claves o alias, o excluya los alias de clave propiedad de AMS.	Esta conclusión se genera si la política contiene permisos que no están limitados a un alias de claves de KMS específico de su propiedad. Para resolver este problema, limita el permiso a claves específicas o excluye las claves que son propiedad de AMS. Las claves propiedad de AMS tienen conjuntos de alias específicos. Para obtener una lista de los alias de clave propiedad de AMS, consulte Verificación automática de límites de permisos de aprovisionamiento de IAM por AMS .

Resultado	Descripción
La declaración contiene acciones privilegiadas que no tienen un alcance adecuado para sus claves de KMS mediante el. <code>kms:ResourceAliases condition</code> Considere la posibilidad de utilizar nombres de alias específicos junto con el operador de conjunto adecuado para la clave de condición. Si se utilizan caracteres comodín en los nombres de los alias, asegúrese de restringir el ámbito a un conjunto limitado de claves de KMS.	Este resultado se genera si estás limitando los permisos de tus claves de KMS mediante condiciones y no limitándolos <code>kms:ResourceAliases</code> a los alias de tus claves de KMS. O bien, si la clave de <code>kms:ResourceAliases</code> condición tiene un valor que también incluye los alias de las claves de KMS propiedad de AMS. Para resolver este problema, actualiza la condición para limitar los permisos únicamente a los alias de tus claves de KMS o excluir los alias de las claves de KMS que son propiedad de AMS. Para obtener una lista de los alias de clave propiedad de AMS, consulte. Verificación automática de límites de permisos de aprovisionamiento de IAM por AMS
El rol debe tener adjunto <code>customer_deny_policy</code>. Incluya el ARN de la política en la lista de políticas administradas. ARNs	Este resultado se genera si el rol que está creando no tiene el rol <code>customer_deny_policy</code> adjunto. Para resolver este problema, inclúyalo <code>customer_deny_policy</code> en la ARNs lista de políticas administradas.
La política AWS gestionada es demasiado permisiva o concede permisos restringidos por la política de límites de AMS.	Este resultado se genera si el <code>ManagedPolicyArns</code> valor de la función contiene alguna política gestionada por AMS que proporcione acceso total o de administrador al servicio correspondiente. Para resolver este problema, revise el uso de la política AWS administrada y utilice una política que otorgue permisos para reducir el alcance o defina su propia política que siga el principio del privilegio mínimo.

Resultado	Descripción
La política gestionada por el cliente se encuentra en un espacio de nombres de AMS restringido.	Esta conclusión se genera si se asocia a la función alguna política gestionada por el cliente con un nombre como prefijo en el AWS espacio de nombres. Para resolver este problema, elimine la política de la ManagedPolicyArns lista para el rol.
El customer_deny_policy no se puede separar del rol. Incluya el ARN de la política en la lista de políticas administradas. ARNs	Este resultado se genera si customer_deny_policy se separa del rol durante una actualización. Para resolver este problema, añada el customer_deny_policy ManagedPolicyArns campo del rol e inténtelo de nuevo.
Las políticas gestionadas por el cliente se proporcionaron fuera del servicio AMS Change Management o sin validación previa.	Esta conclusión se genera si una o más políticas gestionadas por el cliente existentes ARNs están asociadas a un rol y las políticas no se aprovisionan a través del servicio de gestión de cambios de AMS (mediante una RFC). Por ejemplo, el modo de desarrollador o el modo de cambio directo permiten a los clientes aprovisionar políticas de IAM sin una RFC. Para resolver este problema, elimine la política gestionada por el cliente ARNs de la ManagedPolicyArns lista correspondiente al rol.
El número de políticas administradas proporcionadas ARNs supera la cuota de política adjunta por rol.	Este resultado se genera si el número total de políticas administradas asociadas al rol supera la cuota de política por rol. Para obtener más información sobre las cuotas de IAM, consulte las cuotas de IAM y AWS STS, los requisitos de nombres y los límites de caracteres . Utilice esta información para reducir la cantidad de políticas que asocia al rol.

Resultado	Descripción
El tamaño de la política de confianza ({trust_policy}) supera la cuota de tamaño de la política de rol asumido de {size}.	Este resultado se genera si el tamaño del documento de política que asume el rol supera la cuota de tamaño de la política. Para obtener más información sobre las cuotas de IAM, consulte las cuotas de IAM y AWS STS, los requisitos de nombres y los límites de caracteres .
La declaración contiene todas las acciones mutativas de Amazon S3. Considere limitar estos permisos únicamente a las acciones obligatorias. Si se utilizan caracteres comodín, asegúrese de que abarquen un conjunto limitado de acciones mutativas.	Esta conclusión se genera si la política en cuestión concede todos los permisos mutativos de Amazon Simple Storage Service, independientemente de uno o más recursos. Para resolver este problema, incluye solo las acciones mutativas de Amazon S3 obligatorias contra tus buckets.
La declaración contiene acciones privilegiadas que no están permitidas en ningún bucket de Amazon S3. Considere la posibilidad de añadir una declaración en la que se nieguen estas acciones.	Esta conclusión se genera si la política concede acciones privilegiadas en cualquier categoría. Para ver una lista de las acciones privilegiadas, consulta Verificación automática de límites de permisos de aprovisionamiento de IAM por AMS . Para resolver este hallazgo, eliminar o denegar estas acciones en tu política.
La declaración contiene acciones privilegiadas que no están dentro del ámbito de sus buckets en Amazon S3. Considere la posibilidad de incluir sus buckets o excluirlos con prefijos de espacio de nombres AMS. Si se utilizan caracteres comodín, asegúrate de que coincidan con los grupos de tus espacios de nombres.	Este hallazgo se genera si la política concede a Amazon S3 acciones que no se limitan únicamente a sus buckets. Esto suele ocurrir si se utilizan caracteres comodín al especificar los recursos del bucket. Para resolver este problema, especifique los nombres de los buckets o los ARNs que sean de su propiedad o excluya los buckets que tienen prefijos de espacio de nombres AMS.

Resultado	Descripción
La declaración contiene acciones privilegiadas que no están dentro del ámbito de sus buckets en Amazon S3. Considere la posibilidad de evitar el uso de caracteres comodín (*) que abarquen todos los segmentos de la cuenta.	Este hallazgo se genera si la política concede a Amazon S3 acciones que no están dentro del ámbito de su bucket. Esto suele ocurrir si se utilizan caracteres comodín al especificar los recursos del bucket. Para resolver este problema, especifique los nombres de los buckets o los ARNs que sean de su propiedad o excluya los buckets que tienen prefijos de espacio de nombres AMS.
La declaración contiene un comodín de recursos que se aplica a todos los buckets de Amazon S3, incluidos los buckets inexistentes y los buckets que no son de su propiedad. Considere la posibilidad de establecer el alcance de los permisos mediante una condición y una clave de condición. <code>s3:ResourceAccount</code>	Esta conclusión se genera si la política concede permisos a los grupos especificados mediante caracteres comodín. El uso de comodines suele incluir grupos inexistentes o no propietarios. Para resolver este problema, usa la condición y la clave de <code>aws:ResourceAccount</code> condición para limitar el permiso únicamente a los grupos de la cuenta corriente. Para obtener más información, consulte Limitar el acceso a los buckets de Amazon S3 propiedad de AWS cuentas específicas.
La declaración contiene un elemento de <code>NotResource</code> política, que puede abarcar un gran número de grupos, incluidos los que no existen y los que no son de su propiedad. Considere la posibilidad de establecer el alcance de los permisos mediante una condición y una clave de condición. <code>s3:ResourceAccount</code>	Esta conclusión se genera si la política utiliza el elemento de <code>NotResources</code> política para especificar los recursos del bucket. El uso del <code>NotResource</code> elemento puede abarcar una gran cantidad de grupos, incluidos los que no existen o que no son propietarios. Para resolver este problema, usa las condiciones y la clave de <code>aws:ResourceAccount</code> condición para limitar el permiso a los grupos únicamente dentro de la cuenta corriente.

Resultado	Descripción
La declaración contiene una acción de Amazon S3 en relación con grupos <i>Bucket_Name</i> que no existen, que no son propiedad de la cuenta <i>Account_ID</i> o el nombre contiene un comodín que puede estar limitado a un gran número de grupos, incluidos los que no existen y los que no son de su propiedad. Considere la posibilidad de establecer el alcance de los permisos mediante una condición y la clave de condición <code>s3:ResourceAccount</code>	Esta conclusión se genera si la política concede permiso a grupos que no existen, que no son de tu propiedad o que tienen caracteres comodín en los nombres de los grupos que cubren un gran número de grupos y el acceso no está limitado únicamente a la cuenta corriente. Para resolver este problema, usa la condición y la clave de <code>aws:ResourceAccount</code> condición para limitar el permiso únicamente a los grupos de la cuenta corriente.
La declaración contiene una acción de Amazon S3 en relación con grupos <i>Bucket_Name</i> que no existen o que no son propiedad de la cuenta <i>Account_ID</i> , o el nombre contiene un comodín que puede estar limitado a un gran número de grupos, incluidos los que no existen y los que no son de su propiedad. El acceso no está restringido al uso <code>s3:ResourceAccount</code> de una cuenta de recursos específica en la condición de que no le pertenezca.	Esta conclusión se genera si la política concede permiso a grupos que no existen, que no son de tu propiedad o que tienen caracteres comodín en los nombres de los grupos que cubren un gran número de grupos y el acceso está limitado únicamente a una cuenta específica. Sin embargo, la cuenta especificada en la clave de <code>aws:ResourceAccount</code> condición no le pertenece y está gestionada por AMS. Para resolver este problema, actualice la clave de <code>aws:ResourceAccount</code> condición y establezca el identificador de cuenta adecuado que sea de su propiedad y que esté gestionado por AMS.

Resultado	Descripción
La declaración contiene acciones privilegiadas que no están dentro del ámbito de tus instancias para Amazon EC2. Considere la posibilidad de limitar las acciones a una instancia específica a ARNs o excluir las instancias que tengan una clave de etiqueta con un valor en los prefijos de los espacios de nombres de AMS. Si se utilizan caracteres comodín, asegúrate de que coincidan con los espacios de nombres de tu propiedad.	Esta conclusión se genera si la política concede acciones privilegiadas contra las EC2 instancias de Amazon que son propiedad de AMS. Las instancias de AMS se etiquetan con la clave de la etiqueta de nombre con los valores del espacio de nombres de AMS. Para resolver este problema, especifique sus recursos o excluya las instancias de AMS con una condición que tenga la <code>aws:ResourceTag/Name</code> clave que excluya los valores del espacio de nombres de AMS mediante el operador <code>StringNotLike</code>
La declaración contiene acciones privilegiadas que no están relacionadas con los recursos del almacén de parámetros. AWS Systems Manager Considere la posibilidad ARNs de especificar sus parámetros o excluirlos con prefijos de espacio de nombres AMS. Si se utilizan caracteres comodín, asegúrese de que solo afecten a sus parámetros.	Este resultado se genera si la política concede permisos a parámetros que no son de su propiedad. Esto suele ocurrir cuando se utilizan caracteres comodín o cuando los parámetros con prefijos de espacio de nombres AMS aparecen en la sección de recursos de una declaración de política. Para resolver este problema, especifique los parámetros que estén dentro de su espacio de nombres o excluya los parámetros de AMS con una sentencia de rechazo.
La declaración contiene acciones privilegiadas contra los recursos de. AWS Systems Manager Considere la posibilidad de limitar los permisos a las acciones de solo lectura o a las acciones contra sus recursos.	Este hallazgo se genera si la política concede permisos distintos del almacén de parámetros o las acciones de solo lectura contra los recursos de Systems Manager. Para resolver este problema, reduzca los permisos para las acciones de solo lectura o para el almacén de parámetros únicamente.

Resultado	Descripción
La declaración contiene acciones privilegiadas que no se limitan a {message}, ya <i>Service_Name</i> que son tuyas. Considere la posibilidad de limitar estos permisos a tipos de recursos específicos, según proceda, o excluya los recursos propiedad de AMS. Si se utilizan comodines, asegúrese de que <i>Resources</i> coincidan.	Esta conclusión se genera si la política permite acciones privilegiadas que no se conceden con cargo a tus recursos, especialmente en el caso de los recursos con nombre asignado. Para resolver este problema, revisa tu lista de recursos y comprueba si solo se refieren a los recursos que se encuentran en tu espacio de nombres. Como alternativa, excluya los recursos que se encuentran en el espacio de nombres AMS.
La declaración contiene acciones de etiquetado de {<i>Service_Name</i> } que no se limitan a valores específicos para la clave de etiqueta de nombre. Considere la posibilidad de establecer el alcance de estas acciones configurando la clave de <code>aws:RequestTag/Name</code> condición con valores en su espacio de nombres o restrinja estas acciones configurando la clave de <code>aws:RequestTag/Name</code> condición con el <code>StringNotLike</code> operador con valores en los prefijos del espacio de nombres AMS.	Esta conclusión se genera si la política concede el permiso de etiquetado para un servicio determinado y el permiso no se limita a claves/valores de etiqueta específicos. Para determinar qué clave o valor se puede usar para etiquetar acciones, por ejemplo, al solicitar la realización de las acciones, usa la condición <code>.aws:RequestTag/tag key</code> Por lo tanto, para resolver esto, usa esta clave de condición para restringir la clave o los valores en tu espacio de nombres. O bien, deniegue la clave de <code>Name etiqueta (aws:RequestTag/Name)</code> con valores en el espacio de nombres AMS.
Error interno al validar la política de confianza de roles de IAM.	Este hallazgo se genera cuando CT Automation detecta un error al validar la política de confianza de los roles de IAM a través del servicio IAM Access Analyzer. Para resolver este problema, vuelva a enviar la RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.

Resultado	Descripción
Error interno al validar la política gestionada por el cliente.	Este hallazgo se genera cuando CT Automatio n detecta un error al validar la política gestionada por el cliente a través del servicio IAM Access Analyzer. Para resolver este problema, vuelva a enviar el RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.
No se encuentra el analizador de acceso en. <i>Región de AWS</i> No se pudo realizar la comprobación previa del acceso a la política de confianza de roles.	Este hallazgo se genera cuando el recurso IAM Access Analyzer no se encuentra en el. Región de AWS Póngase en contacto con AMS Operations para solucionar problemas y crear el recurso IAM Access Analyzer en la región de AWS.
Política de confianza no válida para el rol <i>Role_Name</i>	Este hallazgo se genera cuando el rol de IAM proporcionado contiene una política de confianza no válida. Para resolverlo, revise la política de confianza para comprobar que es válida.
IAM Access Analyzer ha detectado un error interno. No se pudo crear la vista previa de acceso para el rol <i>Role_Name</i>	Este hallazgo se genera cuando la automatiz ación detecta un error al crear una vista previa del acceso para un rol mediante el analizador de acceso de IAM. Para resolver este problema, vuelva a enviar la RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.

Resultado	Descripción
No se pudo crear una vista previa de acceso a la política de confianza del rol <i>Role_Name</i>	Este hallazgo se genera cuando la automatización detecta un error al crear una vista previa de acceso para un rol mediante el analizador de acceso de IAM. Para resolver este problema, vuelva a enviar la RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.
Error interno al validar el IDP de SAML listado.	Este hallazgo se genera cuando la automatización detecta un error al validar el SAML proporcionado que IdPs figura en la política de confianza del rol. Para resolver este problema, vuelve a enviar la RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.
Error interno al validar los permisos. AWS Key Management Service	Este hallazgo se genera cuando la automatización detecta un error al validar los permisos AWS KMS clave de la política proporcionada. Para resolver este problema, vuelva a enviar la RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.
Error interno al validar la política gestionada de la lista. ARNs	Este hallazgo se genera cuando la automatización detecta un error al validar la política gestionada de la lista. ARNs Para resolver este problema, vuelva a enviar el RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.

Resultado	Descripción
Error interno al validar el adjunto predeterminado <code>customer_deny_policy</code> .	Este hallazgo se genera cuando la automatización detecta un error al validar que <code>customer_deny_policy</code> está asociado al rol. Para resolver este problema, vuelva a enviar la RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.
Error interno al validar los avisos de política gestionada para el rol <i>Role_Name</i>	Este hallazgo se genera cuando la automatización detecta un error al validar la política gestionada ARNs para el rol. Para resolver este problema, vuelva a enviar la RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.
Error interno al validar con arreglo a la política de límites <i>Policy_name</i> definida por el cliente <code>AWSManagedServicesIAMProvisionCustomerBoundaryPolicy</code>	Este hallazgo se genera cuando la automatización detecta un error al validar la política que contiene la lista de rechazados personalizada. Para resolver este problema, vuelve a enviar la RFC. Si el error persiste, póngase en contacto con AMS Operations para solucionar el error.
La política de límites definida por el cliente <code>AWSManagedServicesIAMProvisionCustomerBoundaryPolicy</code> existe en la cuenta. Sin embargo, la política contiene declaraciones de autorización que otorgan permisos. La política solo debe contener declaraciones de rechazo.	Esta conclusión se genera cuando la política que contiene su lista de denegaciones personalizada incluye una declaración que concede el permiso. Aunque la lista de denegación personalizada existe en tu cuenta como una política gestionada por IAM, no se puede utilizar para la gestión de permisos. La política solo debe contener declaraciones de denegación que indiquen que usted desea que AMS Automated IAM Provisioning valide y deniegue las acciones de sus políticas de IAM creadas por AMS Automated IAM Provisioning.

Resultado	Descripción
La declaración contiene las acciones privilegiadas para las que ha definido su organización. Service_Name Considere la posibilidad de excluir estas acciones con una declaración de rechazo. Consulta la política indicada en tu cuenta para consultar la lista de acciones restringidas.	Este resultado se genera cuando la automatización detecta cualquier acción en tu política que hayas definido en la lista de denegaciones personalizada. Para resolver el problema, revisa tu declaración de política y elimina cualquier acción que esté definida en tu lista de denegación personalizada o añade una declaración de denegación que deniegue dichas acciones.
El rol debe estar POLICY_ARN asociado. Incluye el ARN de la política en la lista de políticas administradas. ARNs	Este resultado se genera si el rol que está creando no tiene el rol POLICY_ARN adjunto. Para resolver este problema, POLICY_ARN inclúyelo en el ManagedPolicyArns campo del rol y vuelve a intentarlo.
No se POLICY_ARN puede separar del rol. Incluye el ARN de la política en la lista de políticas administradas. ARNs	Este resultado se genera si POLICY_ARN se separa del rol durante una actualización. Para resolver este problema, añade el POLICY_ARN ManagedPolicyArns campo del rol e inténtelo de nuevo.

Verificación automática de límites de permisos de aprovisionamiento de IAM por AMS

Las verificaciones de límites de permisos de AMS le ayudan a cumplir con la política de límites de permisos predeterminada proporcionada por AMS. Esta política es una lista de acciones denegadas por el aprovisionamiento automatizado de IAM por parte de AMS. Las políticas de aprovisionamiento que contienen estas acciones restringidas requieren una aceptación adicional y explícita del riesgo. Descargue la política aquí: [boundary-policy.zip](#).

Utilice las comprobaciones de la política de límites de permisos definidas por el cliente para personalizar las acciones de denegación más allá de los valores predeterminados de la política de límites de permisos de AMS. Si se incorpora al aprovisionamiento automatizado de IAM por AMS mediante el siguiente tipo de cambio: Administración | Cuenta gestionada | Aprovisionamiento automatizado de IAM por AMS con permisos de lectura y escritura | [Activado \(es necesario](#)

[revisar](#)) (ct-1706xvvk6j9hf), puede incluir una lista de acciones de denegación personalizadas que especifiquen acciones restringidas adicionales.

Puede actualizar la lista de acciones de denegación mediante el tipo de cambio: Administración | Cuenta gestionada | Aprovisionamiento automatizado de IAM con permisos de lectura y escritura | [Actualizar lista de denegaciones personalizada](#) (ct-2r9xvd3sdsic0). Debe utilizar `AWSTypesManagedServicesIAMProvisionAdminRole` la función de IAM dedicada para ejecutar este tipo de cambio.

Note

- Debe proporcionar una lista completa de las acciones de denegación para cada actualización. La lista anterior se sustituye por la nueva.
- La lista de acciones de denegación debe contener únicamente las acciones que se van a denegar. No se admiten las acciones de permiso.
- La lista de acciones de denegación se encuentra en la cuenta con el nombre `AWSTypesManagedServicesIAMProvisionCustomerBoundaryPolicy` de una política gestionada por IAM. La política no debe estar asociada a ningún rol.
- El término límite de permisos utilizado para designar las acciones denegadas en el aprovisionamiento automatizado de IAM por parte de AMS tiene un significado contextual diferente al del límite de permisos de IAM. El límite de permisos de IAM establece el permiso máximo que una política puede conceder en tiempo de ejecución a una entidad de IAM. Para obtener más información sobre el límite de permisos de IAM, consulte los [tipos de políticas](#) en la Guía del AWS Identity and Access Management usuario. El límite de permisos del aprovisionamiento automatizado de IAM por parte de AMS impide aprovisionar una política de IAM que contenga un conjunto determinado de permisos, por ejemplo, una lista de acciones denegadas.

Solución de problemas y errores del aprovisionamiento automatizado de IAM de AMS

Existen tres formas en las que puede tener problemas al utilizar el aprovisionamiento automatizado de IAM por parte de AMS:

- Errores de RFC: pueden producirse por diversos motivos; por ejemplo, una entrada incorrecta. Para obtener más información, consulte [Solución de problemas de errores de RFC en AMS](#).

- Errores de SSM: pueden producirse por diversos motivos; por ejemplo, un formato deficiente. Para obtener más información, consulte [Solución de problemas de automatización de Systems Manager](#).
- Hallazgos de las comprobaciones de validación: se producen cuando una de las muchas comprobaciones de validación que ejecuta Automated IAM Provisioning encuentra un problema. Para obtener una lista de las comprobaciones de validación y las acciones recomendadas para solucionarlas, consulte. [El tiempo de ejecución comprueba el aprovisionamiento automatizado de IAM en AMS](#)

Configuración de permisos en AMS con roles y perfiles de IAM

AMS utiliza AWS Identity and Access Management (IAM) para administrar los usuarios, las credenciales de seguridad, como las claves de acceso, y los permisos que controlan a qué AWS recursos pueden acceder los usuarios y las aplicaciones. AMS proporciona un rol de usuario de IAM predeterminado y un perfil de EC2 instancia de Amazon predeterminado (que incluye una declaración que permite al recurso acceder al rol de usuario de IAM predeterminado).

Solicitar un nuevo perfil de instancia o rol de usuario de IAM

AMS usa una función de IAM para establecer los permisos de usuario a través del servicio de federación y un perfil de instancia de IAM como contenedor para esa función de IAM.

Puede solicitar un rol de IAM personalizado con el tipo de cambio Deployment | Advanced stack components | Identity and Access Management (IAM) | Crear entidad o política (es necesario revisar) (ct-3dpd8mdd9jn1r) o un perfil de instancia de IAM con Management | Applications | Perfil de instancia de IAM | Crear administración | Aplicaciones | Perfil de instancia de IAM | Crear (es necesario revisar) tipo de cambio (ct-0t-0ixp4ch2tiu04). Consulte las descripciones de cada uno en esta sección.

Note

AMS tiene una política de IAM `customer_deny_policy` que bloquea los espacios de nombres y las acciones peligrosas. Esta política está asociada a todos los roles de cliente de AMS de forma predeterminada y rara vez supone un problema para los usuarios. Sus solicitudes de usuarios y roles de IAM no incluyen esta política, pero incluirla automáticamente `customer_deny_policy` en las solicitudes de roles de IAM ayuda a AMS a implementar nuevos perfiles de instancias de IAM con mayor rapidez. Puede

solicitar la exclusión de la política. `customer_deny_policy` Sin embargo, esta solicitud se someterá a una revisión de seguridad exhaustiva y es probable que se rechace por motivos de seguridad.

Restrinja los permisos con las declaraciones de política de funciones de IAM

AMS usa una función de IAM para establecer los permisos de usuario a través del servicio de federación.

Zona de destino de una sola cuenta AMS: consulte [SALZ: roles de usuario de IAM predeterminados](#).

Zona de destino multicuenta AMS: consulte [MALZ](#): roles de usuario de IAM predeterminados.

Un rol de IAM es una entidad de IAM que define un conjunto de permisos para realizar solicitudes de servicio. AWS Las funciones de IAM no están asociadas a un usuario o grupo específico. En cambio, las entidades de confianza asumen funciones, como los usuarios, las aplicaciones o los AWS servicios de IAM, como Amazon EC2. Para obtener más información, consulte [Roles de IAM](#).

Puede definir la política que desee para un usuario que asuma el rol de usuario de AMS IAM mediante la operación de API del AWS Security Token Service (STS), [AssumeRole](#) introduciendo una política de IAM más restrictiva en el `Policy` campo de solicitud.

A continuación, se incluyen ejemplos de declaraciones de política que puede utilizar para restringir el acceso a CT.

Con los grupos de Active Directory (AD) configurados y la operación de la API del AWS Security Token Service (STS) [AssumeRole](#), puede establecer permisos para determinados usuarios o grupos, incluida la restricción del acceso a determinados tipos de cambios (CTs). Puede utilizar las declaraciones de política que se muestran a continuación para restringir el acceso a CT de varias maneras.

Declaración de cambio de tipo de AMS en el perfil de instancia de IAM predeterminado que permite el acceso a todas las llamadas a la API de AMS (`amscm` y `amsskms`) y a todos los tipos de cambios:

```
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
```

```

    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
}

```

1. Declaración que permite el acceso y todas las acciones solo a dos de las especificadas CTs, donde «Acción» se refiere a las operaciones de la API de AMS (una amscm o variasamsskms) y «Recurso» representa el tipo de cambio y el número de versión existentes: IDs

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "amscm:*",
      "Resource": [
        "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
        "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
      ]
    }
  ]
}

```

2. Se especificó una declaración que permitía el acceso a CreateRfc UpdateRfc, y SubmitRfc solo a dos de ellas CTs:
3. Declaración para permitir el acceso a CreateRfc UpdateRfc, y SubmitRfc en todos los disponibles CTs:
4. Declaración en la que se deniega el acceso a todas las acciones en las zonas restringidas de Connecticut y se permite en otras CTs:

Restrinja los permisos con los perfiles de instancia de Amazon EC2 IAM

Un perfil de instancia de IAM es un contenedor para un rol de IAM que puedes usar para pasar la información del rol a una EC2 instancia de Amazon cuando se inicia la instancia.

Actualmente, `customer-mc-ec2-instance-profile` existe un perfil de instancia predeterminado de AWS Managed Services (AMS) que concede permisos a las aplicaciones que se ejecutan en la instancia, no a los usuarios que inician sesión en ella. Es posible que desee modificar el perfil de instancia predeterminado o crear uno nuevo si quiere conceder a una instancia acceso a algo sin conceder también el acceso a otras instancias. Puede solicitar un nuevo perfil de instancia de IAM con la opción Gestión | Aplicaciones | Perfil de instancia de IAM | Crear tipo de cambio (ct-0ixp4ch2tiu04). Al enviar la RFC, puede crear su propio perfil de instancia e incluirlo como tal, o simplemente informar a AMS (utilizando el mismo `InstanceProfileDescription` campo) de los cambios que desea realizar. Como se trata de un CT manual, AMS debe aprobar el cambio y se pondrá en contacto contigo al respecto.

Si no estás familiarizado con las políticas de Amazon IAM, consulta [Descripción general de las políticas de IAM](#) para obtener información importante. También hay una buena entrada de blog, [Demystifying EC2 Amazon Resource-Level Permissions](#). [Tenga en cuenta que, actualmente, AMS no admite el control de acceso basado en recursos, pero sí admite controles a nivel de recursos mediante políticas de funciones de IAM \(para obtener una explicación de la diferencia, consulte Servicios que funcionan con IAM\).AWS](#)

Zona de destino con una sola cuenta (AMS):

Para ver una tabla de permisos que concede el perfil de instancia de IAM de AMS predeterminado, vaya a Perfil de instancia de [EC2 IAM](#).

Regla de notificación de AD FS y configuración de SAML

ActiveDirectory Regla de notificación de Federation Services (AD FS) y configuración de SAML para AWS Managed Services (AMS)

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 el blog [Habilitar la federación hasta AWS con Windows Active Directory, AD FS y SAML 2.0](#)

- 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 Distribuibles -> CLI -> Windows o Managed Cloud Distribuibles -> 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 (ignóralo 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 install beautifulsoup4
```

9. Copie el script a home/ec2-user

Establezca los permisos necesarios

Ejecute el script: samlapi.py

Restringir con ACL de red

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 destino multicuenta gestionada por AMS, para que AMS pueda gestionar y supervisar la infraestructura de forma eficaz, el uso de NACLs esta se limita a los siguientes ámbitos:

- NACLs no se admiten en las cuentas principales de Landing Zone con múltiples cuentas, es decir, la cuenta de administración, las redes, los servicios compartidos, el registro y la seguridad.

- NACLs están admitidas en las cuentas de la aplicación Landing Zone con varias cuentas, siempre y cuando solo se utilicen como una lista «denegada» y tengan la opción «Permitir todo» para permitir las operaciones de supervisión y gestión de AMS.

En entornos de múltiples cuentas a gran escala, también puede aprovechar funciones como los firewalls de salida centralizados para controlar el tráfico saliente o las tablas de enrutamiento de AWS Transit Gateway en la zona de aterrizaje multicuenta de AMS para segregar el tráfico de red entre ellos. VPCs

AMS en Outposts

[AWS Outposts](#) es una solución de hardware gestionada que extiende las zonas de aterrizaje gestionadas por AMS a los centros de datos de los clientes. Con el soporte de AMS AWS Outposts, los clientes que buscan la experiencia en la nube, el ahorro de costes y la plataforma estandarizada que ofrece AMS ya no se limitan a alojar recursos en su interior Regiones de AWS. Con AMS AWS Outposts, los clientes con necesidades locales ahora pueden modernizarse y, al mismo tiempo AWS, disfrutar de los servicios de parches, copias de seguridad, aprovisionamiento, gestión de incidentes, continuidad empresarial y optimización de costes que ofrece AMS.

Una AWS Outposts vez activado en tu cuenta de AMS MultiAccount Landing Zone o Single-Account Landing Zone, podrás seguir los procesos de gestión de cambios de AMS existentes para aprovisionar y gestionar los recursos. AWS La infraestructura alojada en AMS se puede administrar especificando su subred específica. AWS Outposts Los ciclos de vida se pueden gestionar directamente en la AWS Outposts consola mediante la función de autoaprovisionamiento de servicios. AWS Outposts

Para obtener información sobre el rol, consulte. [AWS Outposts](#)

AWS Outposts administración de la instalación y las operaciones

El AWS Outposts proceso de incorporación a AMS On consta de:

1. Planificación de Outposts
2. Validación de pedidos
3. Incorporación de Outposts a AMS
4. Administración del ciclo de vida

AWS Outposts planificación

Durante la AWS Outposts planificación, identificas a AMS en función de los casos de AWS Outposts uso e interactúas con las principales partes interesadas, incluidos tu equipo de cuentas de AMS y sus AWS Outposts representantes, para alinear la estrategia de capacidad.

1. Una vez identificados los casos de uso que requieren la utilización de AMS, póngase en AWS Outposts contacto con su equipo de cuentas de AMS para analizar la planificación de la capacidad.
2. Una vez determinados sus requisitos de AWS Outposts capacidad, su equipo de cuentas de AMS contacta con el equipo de AWS Outposts servicio para analizar el plan de AWS Outposts incorporación, las funciones y las responsabilidades. Durante este tiempo, se le asignará un punto de contacto AWS Outposts único (SPOC). El AWS Outposts SPOC ayuda a finalizar AWS Outposts los requisitos de tamaño.

AWS Outposts validación de pedidos

Durante la validación del pedido, usted crea un AWS Outposts sitio y solicita la capacidad requerida directamente en la AWS Outposts consola o a través del representante de su AWS Outposts cuenta.

Una vez que usted, el equipo de cuentas de AMS y el AWS Outposts equipo, estén alineados, pueden solicitar el rol de servicio AWS Outposts autoaprovisionado utilizando el identificador de tipo de cambio `ct-3qe6io8t6jtny`, para crear su sitio y realizar pedidos directamente en la consola. AWS Outposts AWS Outposts

Como alternativa, puede utilizar el SPOC para crear sitios y pedidos de Outpost. AWS Outposts Tu AWS Outposts SPOC seguirá proporcionándote actualizaciones de estado a ti y al equipo de cuentas de AMS durante la validación y la instalación del sitio y los pedidos. AWS Outposts

AWS Outposts Incorporación a AMS

Una vez que tu AWS Outposts unidad esté activada en tu VPC gestionada por AMS, puedes solicitar que se creen monitores para rastrear la disponibilidad, la capacidad, las excepciones y la conectividad de red de tu hardware de Outposts. Al seguir los pasos de implementación de monitoreo que se describen a continuación, AMS monitorea activamente su AWS Outposts hardware.

1. Una vez instalado AWS Outposts y activado, puede solicitar una supervisión AWS Outposts específica enviando la siguiente plantilla junto con una RFC utilizando el tipo de cambio

Management | Other | Other | Create (ct-1e1xtak34nx76). Las operaciones de AMS garantizan que las herramientas internas de AMS rastreen la subred. AWS Outposts

- AWS Outposts ID
- CIDR de subred
- AWS Outposts Alarmas recomendadas:
 - InstanceFamilyCapacityAvailabilityAlert
 - InstanceTypeCapacityAvailabilityAlert
 - EBSVolumeTypeCapacityAvailabilityAlert
 - CapacityExceptionsAlert
 - Direct Connect ConnectionAlert
- Para cada una de las alertas anteriores, especifique los siguientes parámetros:
 - Estadística (se recomienda «Promedio»). Otras opciones incluyen suma, máximo, mínimo, recuento de muestras y p90)
 - Período (se recomienda «5 minutos»). Otras opciones incluyen 10 y 30 segundos, 1, 5 y 15 minutos, 1 y 6 horas y 1 día)
 - Tipo de umbral (se recomienda «Estático»). La opción «Anomalía» también es una opción.)
 - Condición («Siempre que el recuento de llamadas sea mayor que», «igual a» o «menor que» también son opciones).
 - El valor de condición (« 25% ») está configurado de forma predeterminada. Se permite otro número entero positivo.)
 - Tema de notificación (los temas de operaciones de AMS se asignan automáticamente). Sin embargo, también se puede añadir cualquier otro tema o tema personalizado).

2. Soporte de monitoreo y operaciones

- Las operaciones de AMS monitorean AWS Outposts las métricas para detectar desconexiones de la red o fallas en los componentes. Las operaciones de AMS proporcionan servicios de primera respuesta en caso de AWS Outposts problemas y, si es necesario, pasan a ofrecer asistencia o EC2 asistencia Premium.
- Las operaciones de AMS están disponibles para abordar problemas relacionados con su AWS Outposts unidad.

3. Cuando se produce un error en las comprobaciones del estado de la EC2 instancia o del sistema, las operaciones de AMS siguen los procesos existentes para volver a poner la instancia en funcionamiento. Si el reinicio falla o la AWS Outposts capacidad es insuficiente, un miembro del equipo de operaciones de AMS se lo notificará directamente para determinar los pasos a seguir.

AWS Outposts gestión del ciclo de vida

Una vez que se AWS Outposts haya incorporado a su cuenta de AMS, se le notificará si se produce alguna excepción de disponibilidad, capacidad o red. Puede retirar el servicio AWS Outposts directamente a través de la AWS Outposts consola o del SPOC. AWS Outposts

Puede administrarlo AWS Outposts directamente en la AWS Outposts consola mediante el rol de servicio de aprovisionamiento de AWS Outposts autoservicio o el modo de desarrollador. También puede realizar la solicitud AWS Outposts a través de su CSDM, o punto de contacto AWS Outposts único (SPOC).

AWS Outposts Se puede lograr una alta disponibilidad mediante la implementación de dos o más. AWS Outposts La configuración de dos o más AWS Outposts habilita la opción de zona de disponibilidad múltiple para las instancias de Amazon Relational Database Service.

Aprovisionamiento de recursos gestionados por AMS en AWS Outposts

El aprovisionamiento de AWS recursos alojados AWS Outposts (por ejemplo, Amazon EC2, Amazon EMR, Amazon EKS, Amazon ECS, Amazon EBS y Amazon S3) en cuentas AMS (cuentas de zona de destino de una sola cuenta, zona de destino de múltiples cuentas y Accelerate) está sujeto a los mismos niveles de soporte de AMS que los recursos de. Regiones de AWS Puede utilizar la gestión de cambios de AMS, los servicios de aprovisionamiento de autoservicio o el modo desarrollador para crear y modificar los recursos creados en ellos. AWS Outposts

Actualmente, todos los tipos de instancias (M5/M5d, C5/C5d, R5/R5d, i3en, G4dn), Amazon Elastic Block Store, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, Amazon EMR, Amazon Relational Database Service, Application Load Balancers y el proxy App Mesh Envoy están disponibles directamente en. DBs AWS Outposts Estos recursos son aptos para recibir el mismo soporte de operaciones de AMS que los recursos de las regiones existentes.

Limitaciones de AMS en AWS Outposts

- El soporte operativo AWS Outposts de los recursos alojados depende de una conectividad de red coherente. AWS Outposts La desconexión de la red impide que las operaciones de AMS puedan solucionar cualquier incidente o problema que se produzca en la unidad desconectada. AWS Outposts Para obtener información sobre el AMS sobre las contingencias de nivel de AWS Outposts servicio, consulte los [acuerdos de nivel AWS de servicio](#) actualizados (). SLAs
- Amazon Relational Database Service:

- El tipo de cambio de creación de RDS (ct-2z60dyvto9g6c), de forma predeterminada, habilita Multi-AZ y requiere un grupo de subredes de base de datos. Los grupos de subredes de base de datos requieren dos subredes en dos zonas de disponibilidad (AZ) independientes. Si solo tiene una AWS Outposts, la creación de un grupo de subredes de base de datos es un problema, ya que solo AWS Outposts se asignan a una única AZ. Para evitar esta limitación, siga estas instrucciones:
 1. Solicite un grupo de subredes de base de datos mediante una RFC con un CT de Management | Other | Other y especifique la subred en el AWS Outposts
 2. Cree una plantilla CFN personalizada para implementar RDS y especifique el AWS Outposts grupo de subredes creado en el paso anterior. [Para obtener más información sobre cómo hacerlo, consulte Recursos personalizados.](#)
 3. Solicita que AMS despliegue la plantilla CFN que contiene la instancia de RDS de destino mediante el AMS CFN ingest CT (ct-36cn2avfrj9v).
 4. Tenga en cuenta que, actualmente, RDS for AWS Outposts no proporciona métricas ni registros debido a una limitación del servicio RDS.
- Ingesta de carga de trabajo (WIGs): Linux WIGs solo funciona si la WIGs EC2 instancia previa no está en una subred.AWS Outposts El motivo es que Linux WIGs crea un WIGs nodo en la subred de la primera EC2 instancia mediante m4.large, de forma predeterminada. Como AWS Outposts no tiene ese tipo de instancia, WIGs no puede lanzar su nodo de trabajo. La solución consiste en crear la EC2 instancia inicial en una que no sea una AWS Outposts subred y, a continuación, crear la instancia de destino en ella. AWS Outposts Además, actualmente solo se admiten los tipos de EC2 instancias basados en Nitro, como C5, C5d, M5, M5d, R5, R5d, G4 e I3en. AWS Outposts
- Amazon Elastic Block Store (EBS): Crear EBS Volume CT (ct-16xg8qguovg2w) no funciona, ya que los volúmenes se crean en lugar de porque AWS Outposts no proporcionamos el número de recurso de Amazon (ARN) AWS como parámetro de entrada al CT. AWS Outposts
- Conectividad de red: la conectividad de red es responsabilidad del equipo. AWS Outposts
- Brownfield y toma de control de cuentas: las cuentas AWS Outposts activadas en cuentas ajenas a AMS no pueden transferirse a AMS, debido a la naturaleza de la AWS Outposts facturación y a los requisitos de soporte empresarial.

AWS Outposts AMS sobre el cumplimiento

AMS sobre la certificación AWS Outposts de conformidad

AWS Outposts El plano de control ha sido certificado como apto para la HIPAA y cumple con las normas PCI e ISO. Sin embargo, no se ha certificado la presencia de AMS en el plano de AWS Outposts control. AWS Outposts Por este motivo, se recomienda a los clientes que soliciten el certificado de conformidad AMS en materia de medio ambiente. AWS Outposts

Para controlar la creación de recursos en la unidad de Outpost, se recomienda a los clientes que segreguen el acceso de los desarrolladores a Outpost para evitar que los desarrolladores accedan en exceso a las cuentas gestionadas por AMS estándar.

Cargas de trabajo gestionadas por AMS que requieren el cumplimiento de FedRAMP

En primer lugar, las cuentas de administración de AMS deben evaluarse primero para comprobar su conformidad con la normativa, ya que los datos del plano de control se transferirían AWS Outposts a las cuentas de administración de AMS.

Si se requiere la certificación de FedRAMP y la estructura de cuentas AMS es compatible, se recomienda utilizar un proveedor de centros de datos que ya tenga la certificación requerida y sea propietario de todo el dispositivo Service Link (o que ya cifre los datos de salida).

Por último, puedes implementar una protección de datos adicional si trabajas con tu equipo de cuentas para implementar un SCP que restrinja los datos a los recursos de la región AWS Outposts e impida su creación en la cuenta que aloja el Outpost.

Impacto en el cumplimiento actual de las cuentas AMS

AWS Outposts No es necesario volver a comprobar la conformidad de una cuenta, siempre y cuando no se consuman datos regulados y la cuenta esté separada de forma lógica. Las cuentas de administración de AMS pueden administrar cuentas reguladas y no reguladas siempre que los flujos de datos cruzados entre cuentas authentication/authorization y de entrada/salida estén separados. VPCs Por lo tanto, aunque tanto la cuenta de Outpost que no cumple las normas como las cuentas de aplicación existentes que cumplen con las normas pertenecen a la misma organización (incluidos los servicios compartidos, las redes, los registros, los servicios AMS maestros y de seguridad), la cuenta de la aplicación de conformidad sigue manteniendo la conformidad, ya que los datos están separados de forma lógica.

AMS está activada AWS Outposts FAQs

¿En qué casos de uso se puede solicitar el soporte de AMS AWS Outposts?

Las empresas que necesitan un modelo operativo en la nube probado AWS Outposts pueden utilizar AMS on, ya que tienen cargas de trabajo que requieren baja latencia (por ejemplo, la gestión de robots de fábrica y la migración de mainframes), computación periférica (por ejemplo, estaciones de trabajo remotas y optimización de datos periféricos) y grandes cargas de transferencia de datos.

¿Por qué debo utilizar esta característica?

AMS supervisa el AWS Outposts hardware y es la primera respuesta ante cualquier problema de hardware. AWS Outposts Además, las siguientes funciones son compatibles con todos los recursos gestionados alojados en AWS Outposts:

- Registro, monitoreo, banderas y administración de eventos
- Gestión de la continuidad
- Gestión de la seguridad y el acceso
- Administración de parches
- Administración de cambios
- Administración de aprovisionamiento automatizada y de autoservicio
- Administración de incidentes y problemas
- Informes (la creación de informes para el AWS Outposts hardware no se admitirá inicialmente con el AMS activado) AWS Outposts
- Gestión de solicitudes de servicio
- Modo de desarrollador
- Enterprise Support

¿Cómo utilizo esta característica?

AWS Outposts planificación: Durante la AWS Outposts planificación, identificará los casos de AWS Outposts uso de AMS y colaborará con las principales partes interesadas, incluidos el equipo de cuentas de AMS y AWS Outposts sus representantes, para alinear la estrategia de capacidad.

Validación del pedido: durante la validación del pedido, usted crea un AWS Outposts sitio y solicita la capacidad necesaria directamente en la AWS Outposts consola o a través del representante de su AWS Outposts cuenta.

AWS Outposts Incorporación a AMS: una vez que su AWS Outposts unidad esté activada en su VPC gestionada por AMS, puede solicitar su incorporación a AWS Outposts su cuenta de AMS enviando una solicitud de cambio (RFC) utilizando la plantilla de la Guía del usuario de AMS (). [AWS Outposts](#) A continuación, AMS Operations crea una subred y monitorea tu Outpost mediante las entradas incluidas en la RFC.

Gestión del ciclo de vida: una vez que se AWS Outposts haya incorporado a su cuenta de AMS, se le notificará cualquier excepción de disponibilidad, capacidad o red. Puede retirar el servicio AWS Outposts directamente a través de la AWS Outposts consola o de su punto de contacto AWS Outposts único (SPOC).

¿Cuáles son las limitaciones del AMS? AWS Outposts

Los casos de uso de la residencia de datos (p. ej., las leyes de localización de datos específicas de cada país, etc.) aún no se han validado para AMS On AWS Outposts.

AWS Outposts las cuentas activadas en cuentas que no son de AMS no se pueden transferir a AMS, debido a la naturaleza de la AWS Outposts facturación y a los requisitos de Enterprise Support.

AWS Outposts El plano de control ha sido certificado como apto para la HIPAA y cumple con las normas PCI e ISO. Sin embargo, no se ha certificado la presencia de AMS en el plano de AWS Outposts control. AWS Outposts Por este motivo, se recomienda a los clientes que soliciten el certificado de conformidad AMS en materia de medio ambiente. AWS Outposts

¿Puedo excluirme de esta función?

El aprovisionamiento AWS Outposts en su entorno AMS es opcional. Una vez implementado en su cuenta AMS, se AWS Outposts puede desaproveccionar a través de la AWS Outposts consola en cualquier momento, si ya no es necesario.

¿Cómo se facturará AMS On AWS Outposts ?

El aumento de los AWS Outposts cargos por parte de AMS se aplicará en el nivel B del Grupo.

¿Cómo se adaptará el acuerdo de nivel de servicio de AMS para adaptarlo? AWS Outposts

La gestión de incidentes dependerá de la AWS Outposts disponibilidad. AWS Outposts la disponibilidad está sujeta a la disponibilidad de la red del cliente, que es responsabilidad del cliente. AWS Outposts la disponibilidad también está sujeta al tiempo de actividad del AWS Outposts hardware, que depende de los acuerdos de nivel AWS Outposts de servicio.

Véase también [AWS Outposts FAQs](#).

Uso de etiquetas en AMS

Temas

- [Etiquetado automático de infraestructuras AMS](#)
- [Etiquetas recomendadas por AMS](#)
- [Etiquete las notas de actualización masiva](#)

Proporcionar etiquetas puede ser de gran valor. Para obtener información detallada, consulta [Cómo etiquetar tus EC2 recursos de Amazon](#).

RFCs que crean instancias, como un bucket de Amazon S3 o un AWS Elastic Load Balancer (ELB), suelen proporcionar un esquema que le permite añadir hasta siete etiquetas (pares clave/valor); puede añadir más etiquetas a su depósito de S3 enviando un formulario Management | Advanced stack components | Amazon S3 storage | Update CT. Amazon EC2, Amazon EFS, Amazon 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

Al utilizar la consola AMS, debe habilitar la vista 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 nombran el recurso que se está creando. Algunos esquemas ofrecen un parámetro para nombrar el recurso que está creando y otros no. Por ejemplo, el esquema CT de la EC2 pila Create Amazon no ofrece un parámetro para nombrar la EC2 instancia de Amazon. Para ello, debes crear una etiqueta con la clave «Nombre» y el valor que quieres que tenga el nombre. Si no creas una etiqueta de este tipo, tu EC2 instancia de Amazon se mostrará en la EC2 consola de Amazon sin ningún atributo de nombre.

¿Existen restricciones de etiquetas? Sí:

- Las etiquetas distinguen entre mayúsculas y minúsculas.
- La longitud máxima de la clave es de 128 caracteres Unicode.
- La longitud máxima del valor es de 256 caracteres Unicode.

- El número máximo de etiquetas por recurso es 50.
- El prefijo reservado es `aws :`.
- A los nombres y los valores de etiquetas generados por AWS se les asigna automáticamente el prefijo `aws :`, que usted no puede asignar. Los nombres de las etiquetas definidas por el usuario poseen el prefijo `user :` en el informe de asignación de costos.
- Utilice cada clave solo una vez para cada recurso. Si intentas usar la misma clave dos veces en el mismo recurso, se rechazará tu solicitud.
- Los caracteres permitidos son letras Unicode, espacios en blanco, números y los siguientes caracteres especiales: `+ - =. _:/`

¿Qué tipos de AWS recursos admiten etiquetas? Consulte [Ahora organice sus AWS recursos utilizando hasta 50 etiquetas por recurso](#).

Etiquetado automático de infraestructuras AMS

AMS puede etiquetar todos los recursos creados por AMS con fines de administración, en sus cuentas de zona de aterrizaje multicuenta (MALZ) y zona de aterrizaje de cuenta única (SALZ) mediante una solicitud de cambio (RFC) con el tipo de cambio `Deployment | Advanced stack components | Tag | Create` (es necesario revisar) (`ct-0176f0n99vcps`). Esto puede ayudarle a identificar los recursos creados por AMS con fines de gestión.

AMS puede identificar automáticamente los recursos creados por AMS en función de los estándares de nomenclatura y comprobar si el recurso tiene las siguientes claves y valores de etiqueta: `"AppName«," AppId «," AMSResource` y `"»EnvironmentType`. Si la clave de etiqueta no existe o el valor está vacío, AMS puede crear esas claves de etiqueta automáticamente con el valor de etiqueta `"»`. `AMSInfrastructure`

Puede personalizar las etiquetas que desee en los recursos creados por AMS en función de los estándares de etiquetado de su organización. Puede incluir sus propias claves y valores de etiqueta al enviar la solicitud a AMS. [Siga estos estándares de nomenclatura AWS de etiquetas: Mejores prácticas de etiquetado](#)

Note

En el caso de las cuentas MALZ, el etiquetado personalizado de la infraestructura de AMS solo se admite en las cuentas de aplicaciones. Actualmente, no se admite el etiquetado personalizado en las cuentas principales.

Si el nombre de la clave de etiqueta que proporciona en su RFC ya existe en el recurso, el valor de la etiqueta se reemplaza por el nuevo valor de etiqueta que proporcionó en la RFC. La longitud total de los pares clave-valor de la etiqueta no debe superar los 256 caracteres.

Incluya la siguiente información en su RFC junto con el tipo de cambio Deployment | Advanced stack components | Tag | Create (es necesario revisar) (ct-0176f0n99vcps) para etiquetar los recursos creados por AMS.

1. Lista de cuentas de zona de aterrizaje multicuenta o de zona de aterrizaje de cuenta única en las que le gustaría etiquetar los recursos creados por AMS con fines de administración.
2. Nombre de la clave de etiqueta y valor de etiqueta obligatorios (si es necesario). De forma predeterminada, AMS puede etiquetar con el nombre de la clave de etiqueta como "» y el valor de la etiqueta como EnvironmentType "». AMSInfrastructure [Si necesita un nombre de clave de etiqueta y un valor de etiqueta personalizados, siga los estándares de nomenclatura de etiquetas: prácticas recomendadas de etiquetado AWS](#)

Actualmente, el etiquetado de la infraestructura de AMS admite estos recursos:

```
API Gateway
Amazon CloudFront
Amazon DynamoDB
Amazon EBS
Amazon EC2
Amazon OpenSearch Service
Amazon Quantum Ledger Database (QLDB)
Amazon Redshift
Amazon RDS
Amazon S3 (specific buckets only*)
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
Amazon VPC AWS Certificate Manager AWS CloudFormation AWS CloudTrail AWS CodeBuild
AWS CodePipeline AWS Elastic Beanstalk AWS Lambda AWS Secrets Manager AWS Service
Catalog AWS Systems Manager AWS WAF Regional
Elastic Load Balancing
```

* «arn:aws:s3: ::awsms-a*-patch-data-*», «arn:aws:s3: ::ams-a*-log-management-*»,
«arn:aws:s3: ::cf-templates-*», «arn:aws:s3: ::mc-a*», «arn:aws:s3: ::ams-a*-backup-reports-*»,

«arn:aws:s3: :ams-a*- -*», «arn:aws:s3: ::ams-a*- -*», «arn:aws:s3: ::ams-a*- -*», «arn:aws:s3: ::ams-a*-release-assets-*», «arn:aws:s3::: -*», «arn:aws:s3::: *» patch-data-customer-reports patch-data-raw patch-data-reporting ams-cfn-drift-remediation ams-reporting-data-a

Etiquetas recomendadas por AMS

AMS recomienda las siguientes etiquetas en los recursos compatibles. Las etiquetas con estrellas (*) son muy recomendables.

Note

Puede utilizar etiquetas para programar la aplicación de parches. Para obtener más información, consulte [AMS Advanced Patch Orchestrator: un modelo de parches basado en etiquetas](#).

Prefijos reservados AMS

Los atributos de los recursos de AMS deben cumplir ciertos patrones; por ejemplo, los nombres de los perfiles de las instancias de IAM, BackupVault los nombres, los nombres de etiquetas, etc., no deben empezar por prefijos reservados de AMS. Estos prefijos reservados son:

```
*/aws_reserved/*
ams- *
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
```

Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion

Etiquetas recomendadas por AMS

Clave de etiqueta	Valores admitidos	Notas
AppName* AppId*	Sin restricciones.	Identifique las aplicaciones que residirán en el recurso o que requerirán acceso a él. Esto facilita el seguimiento y las comunicaciones entre AMS y usted.
EnvironmentType *		
OwnerTeamEmail *	Dirección de correo electrónico de la lista de distribución	Identifique la dirección de correo electrónico de la lista de distribución del equipo responsable del recurso. El correo electrónico no debe ser personal; debe ser anónimo, como una lista de distribución.

Clave de etiqueta	Valores admitidos	Notas
ComplianceFramework	Sin restricciones	Identifique qué controles y políticas deben aplicarse al recurso.
CostCenter		Identifique el centro de costos o la unidad de negocios asociada a un recurso (por lo general, para la asignación y el seguimiento de los costos).
Customer		Lo utilizan los clientes de AMS que tienen recursos de varios clientes (subclientes de AMS). Para agrupar los recursos del entorno gestionado en función del cliente específico al que prestan servicio. Identifique a un cliente específico en un grupo concreto de recursos o servicios.
DataClassification		Identifique el nivel de confidencialidad de datos específico que admite un recurso. Identifique qué controles y políticas deben aplicarse al recurso.
HoursOfOperation		Identifique la fecha o la hora en que se debe iniciar, detener, eliminar o rotar un recurso.
OwnerTeam		Identifique el equipo responsable del recurso. Facilita la comunicación con el equipo responsable del recurso.

Clave de etiqueta	Valores admitidos	Notas
Patch Group	Dispone de dos opciones para hacerlo: - Puede enviar una solicitud de servicio con la información que se describe en AMS Advanced Patch Orchestrator: un modelo de parches basado en etiquetas, y AMS crea una etiqueta a partir de los recursos que especifique y, con la información que proporcione, una Patch Group etiqueta para usted. - Si ya ha creado una Patch Group etiqueta en sus recursos, los valores admitidos no tienen restricciones.	Qué recursos incluir en un período de mantenimiento de parches automatizado.
ProjectId	Sin restricciones	Identifique los proyectos que respalda el recurso.

Clave de etiqueta	Valores admitidos	Notas
SupportPriority	Uno de los seis acrónimos posibles para confidencialidad, integridad o disponibilidad; la prioridad es el orden de los acrónimos. Por ejemplo, I.C.A. significaría que el orden es Integridad, Confidencialidad y Disponibilidad. Otros valores aceptables son C.I.A., C.A.I., I.A.C., A.C.I. y A.I.C.	Identifique qué tipo de soporte debe ser prioritario: confidencialidad, integridad o disponibilidad.

Etiquete las notas de actualización masiva

Estas notas se utilizan con los tutoriales de ejemplo de tipo de cambio [Tag | Bulk Update y Tag | Bulk Update \(es necesario revisar\)](#).

Notas sobre las etiquetas de actualización masiva:

- Servicios compatibles:
 - Para [Tag | Actualización masiva \(es necesaria una revisión\)](#): Todas.
 - Para [etiqueta | Actualización masiva](#):
 - Auto Scaling
 - Amazon EC2
 - Elastic Load Balancing
 - Amazon RDS
 - Buckets de Amazon S3
- Para generar el archivo de valores separados por comas (CSV), inicie sesión en Resource Groups > Tag Editor en la AWS consola, busque los recursos que desee etiquetar y expórtelos a un archivo CSV. Para obtener más información, consulte [Exportar resultados a CSV](#).

NOTA: Recomendamos utilizar una URL prefirmada de S3 para proporcionar la ubicación del objeto CSV.

- Debe haber columnas con los encabezados Servicio, Tipo e Identificador. Estas columnas son obligatorias.
- Cambie el nombre del identificador de la columna a ID.
- Los valores de las columnas Service, Type e Identifier (cambiados a ID) son los que proporciona el editor de etiquetas en Resource Groups.
- Si un recurso que se va a etiquetar no está disponible en el editor de etiquetas, utilice el nombre del recurso de Amazon (ARN) del recurso como identificador de columna (cambiado a ID) y deje los campos Servicio y Tipo en blanco.
- Los encabezados de las columnas de las etiquetas que se van a añadir o modificar deben tener el formato Etiqueta: *TagKey*
- Los encabezados de las columnas de las etiquetas que se van a eliminar deben tener el formato Untag: *TagKey*
- Cada fila es para etiquetar o desetiquetar un recurso.
- Si se va a añadir una etiqueta a un recurso, especifique el valor de la etiqueta en la *TagKey* columna Etiqueta: correspondiente.
- Si se va a eliminar una etiqueta de un recurso, especifique True en la *TagKey* columna Untag: correspondiente.
- Si una etiqueta: *TagKey* o Desetiquetar: no *TagKey* se aplica a un recurso, añada un guión (-) a la columna correspondiente o manténgala en blanco.

NOTA: La opción Untag anula la etiqueta. Esto se debe a que, a diferencia de la etiqueta, Untag debe añadirse manualmente al archivo CSV, por lo que suponemos que la intención era eliminar, no modificar, la etiqueta.

- Se ignoran las columnas adicionales que no se ajusten a los criterios.

Important

La exportación del editor de etiquetas rellena una matriz de todas las etiquetas de todos los recursos; las etiquetas que faltan se rellenan con el valor «no etiquetadas». Al reutilizar este CSV de exportación como entrada a la RFC, se crean todas las etiquetas que antes faltaban, con el valor literal de «no etiquetadas».

 Note

Para obtener información sobre cómo exportar etiquetas a un archivo CSV, consulte [Buscar recursos para etiquetar -> Exportar resultados a CSV](#).

Programador de recursos de AWS Managed Services

Utilice el programador de recursos de AWS Managed Services (AMS) para programar el inicio y la parada automáticos de AutoScaling los grupos, las EC2 instancias de Amazon y las instancias de RDS de su cuenta. Esto ayuda a reducir los costos de infraestructura cuando los recursos no están destinados a funcionar las 24 horas del día, los 7 días de la semana. La solución se basa en [Instance Scheduler AWS](#), pero contiene funciones y personalizaciones adicionales específicas para las necesidades de AMS.

 Note

De forma predeterminada, el programador de recursos de AMS no interactúa con los recursos que no forman parte de una pila. AWS CloudFormation El recurso debe formar parte de una pila que comience por «stack-», «sc-» o «SC-». Para programar los recursos que no forman parte de una CloudFormation pila, puede actualizar el parámetro de pila del Programador de recursos `ScheduleNonStackResources` a `Yes`.

El programador de recursos de AMS utiliza períodos y programas:

- Los períodos definen las horas en las que se ejecuta el Programador de recursos, como la hora de inicio, la hora de finalización y los días del mes.
- Los programas contienen los períodos definidos, junto con configuraciones adicionales, como el período de mantenimiento del SSM, la zona horaria, la configuración de hibernación, etc., y especifican cuándo deben ejecutarse los recursos, según las reglas de período configuradas.

Puede configurar estos períodos y programas mediante los tipos de cambios automatizados del Programador de recursos de AMS (). CTs

[Para obtener más información sobre los ajustes disponibles para el programador de recursos de AMS, consulte la documentación correspondiente del programador de AWS instancias en Componentes de la solución. Para obtener una vista de la arquitectura de la solución, consulte la documentación correspondiente del programador de AWS instancias en \[Architecture overview.html\]\(#\).](#)

Implementación del programador de recursos AMS

Para implementar el programador de recursos de AMS, utilice el tipo de cambio automático (CT): Despliegue | Programador de recursos de AMS | Solución | Implementación (ct-0ywnhc8e5k9z5) para generar una RFC que, a continuación, despliegue la solución en su cuenta. Una vez ejecutada la RFC, se aprovisiona automáticamente en su cuenta una pila que contiene los recursos del programador de recursos de AMS con CloudFormation la configuración predeterminada. [Para obtener más información sobre los tipos de cambios del Programador de recursos, consulte el Programador de recursos de AMS.](#)

Note

Para saber si AMS Resource Scheduler ya está implementado en su cuenta, consulte la consola AWS Lambda de esa cuenta y busque AMSResource la función Scheduler.

Una vez aprovisionado el programador de recursos de AMS en su cuenta, le recomendamos que revise la configuración predeterminada y, si es necesario, que personalice las configuraciones, como la clave de etiqueta, la zona horaria, los servicios programados, etc., en función de sus preferencias. Para obtener más información sobre las personalizaciones recomendadas, consulte a continuación. [Personalización del programador de recursos AMS](#)

Para realizar las configuraciones personalizadas o simplemente confirmar la configuración del Resource Scheduler,

Personalización del programador de recursos AMS

[Le recomendamos que personalice las siguientes propiedades del programador de recursos de AMS mediante los tipos de cambio actualizados del programador de recursos de AMS; consulte el programador de recursos de AMS.](#)

- Nombre de etiqueta: el nombre de la etiqueta que el Programador de recursos utilizará para asociar los cronogramas de instancias a los recursos. El valor predeterminado es Schedule.

- **Servicios programados:** lista de servicios separados por comas que Resource Scheduler puede administrar. El valor predeterminado es «ec2, rds, autoscaling». Los valores válidos son «ec2», «rds» y «autoscaling»
- **Zona horaria predeterminada:** especifique la zona horaria predeterminada que utilizará el programador de recursos. El valor predeterminado es UTC.
- **Utilice CMK:** una lista separada por comas de la clave gestionada por el cliente (CMK) de Amazon KMS a la ARNs que se le pueden conceder permisos a Resource Scheduler.
- **Uso LicenseManager:** se pueden conceder permisos para ese programador de recursos a una lista separada por comas de ARNs los administradores de AWS licencias.

Note

AMS puede, de vez en cuando, publicar funciones y correcciones para mantener el Programador de recursos de AMS actualizado en su cuenta. Cuando esto ocurre, se conservan todas las personalizaciones que realice en el programador de recursos de AMS.

Uso del programador de recursos AMS

Para configurar el programador de recursos de AMS una vez implementada la solución, utilice el programador de recursos automatizado CTs para crear, eliminar, actualizar y describir (obtener detalles sobre) los períodos del programador de recursos de AMS (las horas en que se ejecuta el programador de recursos) y los programas (los períodos configurados y otras opciones). [Para ver un ejemplo del uso de los tipos de cambio del programador de recursos de AMS, consulte el programador de recursos de AMS.](#)

Para seleccionar los recursos que gestionará el programador de recursos de AMS, tras la creación del despliegue y el programa, utilice la etiqueta AMS Create CTs para etiquetar los grupos de Auto Scaling, las pilas de Amazon RDS y EC2 los recursos de Amazon con la clave de etiqueta que proporcionó durante la implementación y el programa definido como valor de etiqueta. Una vez etiquetados los recursos, se programa su inicio o finalización según el cronograma definido por el programador de recursos.

El uso del programador de recursos de AMS no conlleva ningún coste adicional. Sin embargo, la solución utiliza varios Servicios de AWS y se le cobrará por estos recursos a medida que se utilicen. Para obtener más información, consulte [Descripción general de la arquitectura](#).

Para excluirse del programador de recursos de AMS:

- Para excluirse o deshabilitarse temporalmente: envíe una RFC mediante el tipo de cambio automatizado Management | AMS Resource Scheduler | State | Disable (ct-14v49adibs4db)
- Para su eliminación definitiva, envíe un RFC de administración | Otros | Otros | Actualice (es necesario revisar) (ct-0xdawir96cy7k) solicitando su eliminación del sistema automatizado de versiones de Resource Scheduler

Estimador de costos de AMS Resource Scheduler

Para hacer un seguimiento del ahorro de costes, el programador de recursos de AMS incluye un componente que calcula cada hora el ahorro de costes estimado para los recursos de Amazon EC2 y RDS gestionados por el programador. Estos datos de ahorro de costes se publican luego como una CloudWatch métrica (AMS/ResourceScheduler) para ayudarle a realizar un seguimiento de los mismos. El estimador de ahorros de costos solo estima los ahorros en las horas de funcionamiento de una instancia. No tiene en cuenta ningún otro coste, como los costes de transferencia de datos asociados a un recurso.

El estimador de ahorro de costes está activado con Resource Scheduler. Funciona cada hora y recupera datos de costos y uso de. AWS Cost Explorer A partir de esos datos, calcula el costo promedio por hora para cada tipo de instancia y, a continuación, proyecta el costo de un día completo si se ejecutó sin programarse. El ahorro de costos es la diferencia entre el costo proyectado y el costo real informado por Cost Explorer para un día determinado.

Por ejemplo, si la instancia A está configurada con el Programador de recursos para que se ejecute de 9 a. m. a 5 p. m., son ocho horas de un día determinado. Cost Explorer informa que el costo es de 1 dólar y el uso de 8. Por lo tanto, el costo promedio por hora es de 0,125 USD. Si la instancia no estaba programada con Resource Scheduler, se ejecutaría 24 horas ese día. En ese caso, el costo habría sido de $24 \times 0,125 = 3\$$. Resource Scheduler le ayudó a ahorrar 2 dólares en costos.

Para que el estimador de ahorros de costos recupere el costo y el uso solo de los recursos administrados por Resource Scheduler desde Cost Explorer, la clave de etiqueta que el Programador de recursos utiliza para destinar los recursos debe activarse como etiqueta de asignación de costos en el panel de facturación. Si la cuenta pertenece a una organización, la clave de etiqueta debe estar activada en la cuenta de administración de la organización. Para obtener información sobre cómo hacerlo, consulte [Activación de etiquetas de asignación de costes definidas por el usuario y etiquetas de asignación](#) de [costes definidas por el usuario](#)

Una vez que la clave de etiqueta se activa como etiqueta de asignación de costos, la AWS facturación comienza a hacer un seguimiento del costo y el uso de los recursos administrados por el programador de recursos y, una vez disponibles los datos, la calculadora de ahorros de costos comienza a calcular los ahorros de costos y a publicar los datos en el espacio de nombres de las métricas en. `AMS/ResourceScheduler` CloudWatch

Consejos para la estimación de costos

Cost Savings Estimator no acepta descuentos como instancias reservadas, planes de ahorro, etc., para su cálculo. El estimador toma los costos de uso de Cost Explorer y calcula el costo promedio por hora de los recursos. Para obtener más información, consulte Cómo [entender sus conjuntos de datos de AWS costos](#): una hoja de referencia

Para que el estimador de ahorros de costos recupere el costo y el uso solo de los recursos administrados por Resource Scheduler desde Cost Explorer, la clave de etiqueta que el Programador de recursos utiliza para destinar los recursos debe activarse como etiqueta de asignación de costos en el panel de facturación. Si la cuenta pertenece a una organización, la clave de etiqueta debe estar activada en la cuenta de administración de la organización. Para obtener información sobre cómo hacerlo, consulte [Etiquetas de asignación de costes definidas por el usuario](#). Si la etiqueta de asignación de costes no está activada, el estimador no podrá calcular los ahorros ni publicar la métrica, aunque esté habilitada.

Mejores prácticas de AMS Resource Scheduler

Programación de Amazon EC2 Instances

- El comportamiento de cierre de instancias debe estar configurado en `stop` y no `terminate`. Está preestablecido `stop` para las instancias que se crean con el tipo de cambio automatizado `AMS Amazon EC2 Create (ct-14027q0sjyt1h)` y se puede configurar para las instancias de EC2 Amazon creadas con la ingestión, estableciendo la propiedad en. `AWS CloudFormation InstanceInitiatedShutdownBehavior stop` Si el comportamiento de cierre de las instancias está establecido `terminate`, finalizarán cuando el programador de recursos las detenga y el programador no pueda volver a iniciarlas.
- AMS Resource Scheduler no procesa individualmente las EC2 instancias de Amazon que forman parte de un grupo de Auto Scaling, aunque estén etiquetadas.
- Si el volumen raíz de la instancia de destino está cifrado con una clave maestra de cliente (CMK) de KMS, es necesario añadir un `kms:CreateGrant` permiso adicional a la función de IAM del programador de recursos para que el programador pueda iniciar dichas instancias. Este permiso

no se añade a la función de forma predeterminada para mejorar la seguridad. Si necesita este permiso, envíe una RFC al tipo de cambio Management | AMS Resource Scheduler | Solution | Update y especifique una lista ARNs del KMS separada por comas. CMKs

Programación de grupos de Auto Scaling

- El programador de recursos de AMS inicia o detiene el escalado automático de los grupos de Auto Scaling, no de las instancias individuales del grupo. Es decir, el planificador restaura el tamaño del grupo de Auto Scaling (inicio) o establece el tamaño en 0 (parada).
- Etiquete el AutoScaling grupo con la etiqueta especificada y no las instancias del grupo.
- Durante la parada, el programador de recursos AMS almacena los valores de capacidad mínima, deseada y máxima del grupo Auto Scaling y establece la capacidad mínima y deseada en 0. Durante el inicio, el planificador restaura el tamaño del grupo de Auto Scaling tal como estaba durante la parada. Por lo tanto, las instancias de grupo de Auto Scaling deben usar una configuración de capacidad adecuada para que la finalización y el relanzamiento de las instancias no afecten a ninguna aplicación que se ejecute en el grupo Auto Scaling.
- Si se modifica el grupo de Auto Scaling (la capacidad mínima o máxima) durante un período de ejecución, el planificador almacena el nuevo tamaño del grupo de Auto Scaling y lo usa para restaurar el grupo al final de una programación de paradas.

Programación de instancias de Amazon RDS

- El programador puede tomar una instantánea antes de detener las instancias de RDS (no se aplica al clúster de base de datos Aurora). Esta función está activada de forma predeterminada con el parámetro de AWS CloudFormation plantilla Crear instantánea de instancia de RDS establecido en true. La instantánea se conserva hasta la próxima vez que se detenga la instancia de Amazon RDS y se cree una nueva instantánea.

El programador puede ser una instancia de start/stop Amazon RDS que forme parte de un clúster o una base de datos Aurora de Amazon RDS o que se encuentre en una configuración de zona de disponibilidad múltiple (Multi-AZ). Sin embargo, compruebe las limitaciones de Amazon RDS cuando el programador no pueda detener la instancia de Amazon RDS, especialmente las instancias Multi-AZ. Para programar el inicio o la parada del Clúster de Aurora, utilice el parámetro de plantilla Programar cúmulos de Aurora (el valor predeterminado es true). El clúster Aurora (no las instancias individuales del clúster) debe etiquetarse con la clave de etiqueta definida durante la configuración inicial y el nombre del programa como valor de etiqueta para programar ese clúster.

Cada instancia de Amazon RDS tiene un período de mantenimiento semanal durante el cual se aplican los cambios en el sistema. Durante el período de mantenimiento, Amazon RDS iniciará automáticamente las instancias que hayan estado detenidas durante más de siete días para aplicar el mantenimiento. Tenga en cuenta que Amazon RDS no detendrá la instancia una vez que se complete el evento de mantenimiento.

El programador permite especificar si se debe añadir el período de mantenimiento preferido de una instancia de Amazon RDS como período de ejecución a su programación. La solución iniciará la instancia al principio del período de mantenimiento y la detendrá al final del período de mantenimiento si ningún otro período de ejecución especifica que la instancia debe ejecutarse y si el evento de mantenimiento se ha completado.

Si el evento de mantenimiento no se completa al final del período de mantenimiento, la instancia se ejecutará hasta el intervalo de programación posterior a la finalización del evento de mantenimiento.

Note

El programador no valida que un recurso se haya iniciado o detenido. Realiza la llamada a la API y sigue adelante. Si la llamada a la API falla, registra el error para su investigación.

AWS Systems Manager en AMS Advanced

Un AWS Systems Manager documento (documento SSM) define las acciones que Systems Manager realiza en sus AWS recursos. Systems Manager incluye más de una docena de documentos preconfigurados que puede utilizar especificando parámetros en tiempo de ejecución. Los documentos utilizan la notación de JavaScript objetos (JSON) o YAML e incluyen los pasos y parámetros que especifique.

AWS Managed Services (AMS) es un editor de confianza para documentos SSM. Los documentos SSM propiedad de AMS se comparten únicamente con las cuentas AMS integradas, siempre comienzan con un prefijo reservado (AWSManagedServicios-*) y aparecen en la consola de Systems Manager, como propiedad de. AWS El proceso AMS para el desarrollo y la publicación de documentos SSM sigue las AWS mejores prácticas y requiere múltiples revisiones por pares a lo largo del ciclo de vida del documento. Para obtener más información sobre las prácticas

AWS recomendadas para compartir documentos SSM, consulte [Prácticas recomendadas para documentos SSM compartidos](#).

Documentos AMS Advanced SSM disponibles

Los documentos SSM de AMS Advanced están disponibles exclusivamente para los clientes de AMS Advanced y se utilizan para automatizar el flujo de trabajo operativo para gestionar su cuenta.

Para ver los documentos SSM avanzados de AMS disponibles en: AWS Management Console

1. [Abra la consola de Systems Manager en la consola.AWS Systems Manager](#)
2. Seleccione Compartido conmigo.
3. En la barra de búsqueda, filtra por prefijo de nombre de documento, luego por igual y establece el valor en AWSManagedServicios-.

Para obtener instrucciones de AWS CLI, consulte [Uso de documentos SSM compartidos](#).

Versiones de documentos AMS Advanced SSM

Los documentos SSM admiten el control de versiones. Los documentos SSM de AMS Advanced no se pueden modificar desde la cuenta del cliente ni se pueden volver a compartir. AMS Advanced los gestiona y mantiene de forma centralizada para gestionar la cuenta.

Los números de versión se incrementan con cada actualización de un documento específico Región de AWS. A medida que haya nuevas regiones disponibles, el mismo contenido del documento en dos regiones puede tener números de versión diferentes; esto es normal y no significa que su comportamiento vaya a ser diferente. Si desea comparar dos documentos SSM avanzados de AMS, le recomendamos comparar sus hashes con la CLI AWS :

```
aws ssm describe-document \  
--name AWSManagedServices-DOCUMENTNAME \  
--output text --query "Document.Hash"
```

Dos documentos SSM son idénticos si sus hashes coinciden.

Precios de Systems Manager en AMS

El acceso a los documentos SSM avanzado de AMS no conlleva ningún coste. El costo del tiempo de ejecución varía según el tipo de documento SSM, sus pasos y la duración del tiempo de ejecución. Para obtener más información, consulta los [AWS Systems Manager precios](#).

Cuentas AMS externas

AMS ofrece asistencia para la salida del embarque para cuentas de zona de aterrizaje de cuenta única y de zona de aterrizaje multicuenta.

AMS no deja de compartir ninguna información suya durante AMIs la desconexión para evitar que sus dependencias se vean afectadas. Si quieres eliminar AMS AMIs de tu cuenta, puedes usar la `cancel-image-launch-permission` API para ocultar información específica. AMIs Por ejemplo, puedes usar el siguiente script para ocultar todos los AMS AMIs que se compartieron anteriormente con tu cuenta:

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
    aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

Debe tener la versión 2 de AWS CLI instalada para que el script se ejecute sin errores. Para ver los pasos de instalación de la CLI de AWS, consulte [Instalación o actualización de la última versión de la CLI de AWS](#). Para obtener más información sobre el `cancel-image-launch-permission` comando, consulte [cancel-image-launch-permission](#).

Note

La fecha de finalización del servicio es el último día del mes natural siguiente al final del período de preaviso de rescisión requerido de 30 días. Si el final del período de notificación de rescisión requerido cae después del día 20 del mes calendario, la fecha de terminación 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.

Temas

- [Olvídese de las cuentas de zona de aterrizaje de cuenta única de AMS](#)
- [Olvídese de las cuentas multicuenta de AMS en las zonas de landing zone](#)

Olvídese de las cuentas de zona de aterrizaje de cuenta única de AMS

AMS ofrece asistencia para dejar de embarcar dentro de los 30 días anteriores a la finalización de AMS.

Debe solicitar la asistencia para salir del embarque al menos 7 días antes de que se le pueda prestar dicha asistencia. La asistencia a la hora de embarcar se puede ofrecer de dos formas:

- Transferencia del control: AMS le devuelve el control de la cuenta junto con las credenciales de acceso a todas las aplicaciones gestionadas por AMS, o
- Cancelación de recursos por cierre de cuenta: AMS elimina todos los datos de su entorno gestionado por AMS y desaproviona todos los recursos activos de la cuenta. Al enviar la solicitud de exclusión, los clientes pueden solicitar que AMS:
 - Elimine o conserve los objetos de datos (incluidos los registros) que están almacenados en los buckets de Amazon S3
 - Eliminar o conservar los buckets de Amazon S3
 - Elimine o conserve los puntos de AWS Backup restauración

Important

Cualquier otra solicitud específica (sujeta a plausibilidad) debe comunicarse a AMS antes de que se inicie la desvinculación.

Requisitos previos opcionales (si es necesario):

Note

Antes de la solicitud de exclusión, los clientes pueden solicitar la asistencia de AMS para transferir sus datos en el formato existente utilizando AWS Snowball Edge o cualquier otro medio con el que se pueda interactuar AWS .

Además de las copias de seguridad de los datos, se pueden proporcionar los siguientes datos de los clientes como parte de la asistencia a la hora de embarcar:

- Datos almacenados en los servicios de almacenamiento, incluidos los registros
- Esquemas de tipos de cambio específicos para cada cliente
- CloudFormation plantillas para esquemas de tipos de cambio

Si las actividades de exclusión no se completan tras la finalización de AMS, cedemos el control de la (s) cuenta (s) para que puedas completar cualquier actividad pendiente.

Función	¿Qué se ha eliminado	Impact	Acciones necesarias
Supervisión, registro, alertas	Se ha eliminado la monitorización de AMS Se canceló la suscripción al MMS (Sistema de monitoreo administrado) Se eliminaron el etiquetador de recursos y el administrador de alarmas CloudWatch Las alertas de referenci	AMS ya no tiene acceso ni visibilidad de sus recursos y su entorno.	Usted es el propietario de las contingencias relacionadas con los servicios retirados o cancelados.

Función	¿Qué se ha eliminado	Impact	Acciones necesarias
	a permanecen en los recursos existentes GuardDuty y Macie: La propiedad recae en ti		
Administración de copias de seguridad	Se ha eliminado la automatización de AMS Backup, aunque el AWS Backup servicio sigue disponible para su uso. Los almacenes y datos de Backup se conservan a menos que se solicite su eliminación.	AMS ya no supervisa los trabajos de copia de seguridad ni realiza acciones de restauración durante los incidentes. Las alarmas y alertas están desactivadas. Al eliminar la función de copia de seguridad de IAM y las claves de KMS, las copias de seguridad de AMS quedan inoperativas.	Los planes de backup de AMS deben reconfigurarse. Le devolverá toda la propiedad de la supervisión y la remediación.
Automatizaciones AMS para la gestión de servicios	Los manuales de automatización de AWS SSM seleccionados por AMS, las funciones Amazon Simple Notification Service (SNS) y AWS Lambda ya no están disponibles.	No hay acceso de AMS a sus cuentas. Toda la automatización está deshabilitada.	Si es necesario, es necesario volver a crear toda la automatización, incluidas las funciones SSM, SNS y Lambda.

Función	¿Qué se ha eliminado	Impact	Acciones necesarias
Conformidad	La visibilidad y el monitoreo de AMS para todas GuardDuty y AWS Config las reglas eliminadas, aunque estas reglas permanecen en las cuentas.	AMS ya no gestiona todo el monitoreo, los informes GuardDuty y AWS Config las correcciones de Amazon y Rules.	Usted asumirá la supervisión y la corrección de todas las herramientas de seguridad y cumplimiento.
Agentes en instancia	Se elimina el acceso al programador de recursos, al etiquetado de recursos o a la configuración de instancias automatizada para instalar los agentes necesarios en EC2 las instancias.	CloudWatch y los agentes SSM de las instancias se mantienen en su lugar con las configuraciones existentes; sin embargo, AMS ya no ayuda con estas configuraciones.	Usted administra el etiquetado y las configuraciones de los agentes SSM CloudWatch y locales.
Infraestructura de parches e informes	AMS ya no gestiona las actividades previas y posteriores a la aplicación de los parches, y se ha eliminado el acceso y la visibilidad de estos servicios.	AMS ya no crea una instantánea de la instancia antes de aplicar el parche, ya no instala ni supervisa la instalación del parche y ya no le notifica el resultado. Los informes y los paquetes de S3 de «auditoría» se guardan en sus cuentas si así lo solicita. AMS ya no genera informes de métricas de servicio.	Conservas las líneas base y las instantáneas de los parches creadas en el pasado. Además, se mantiene la configuración de los períodos de mantenimiento de los parches, pero AMS ya no los instala ni corrige. Todos los informes sobre las métricas operativas de la infraestructura son ahora su responsabilidad.

Función	¿Qué se ha eliminado	Impact	Acciones necesarias
Administración de procesos	Todas las cuentas están excluidas de la gestión de servicios proporcionada para los incidentes, incluida la gestión de las solicitudes de servicio, los problemas y los cambios.	AMS ya gestiona todas las interrupciones del servicio que anteriormente solucionaba mediante incidentes y solicitudes de servicio, y los cambios en el entorno, así como las investigaciones sobre las causas fundamentales.	Usted recupera la plena propiedad de toda la gestión de procesos.

Olvídese de las cuentas multicuenta de AMS en las zonas de landing zone

Hay dos tipos de AWS cuentas que puedes eliminar de la zona de aterrizaje multicuenta de AMS Advanced:

- Cuentas de aplicaciones
- Cuentas principales

Para eliminar todas las cuentas de tu landing zone multicuenta de AMS, debes cerrar todas las cuentas de la Aplicación antes de cerrar las cuentas principales.

Para asumir y seguir gestionando las cargas de trabajo en las cuentas principales o de aplicación externas, asegúrate de revisar esta documentación con tu equipo de cuentas de AMS. En esta documentación se describen los cambios que AMS realiza durante el proceso externo.

Tareas que deben completarse para continuar con el funcionamiento de las cuentas externas

Las siguientes tareas son necesarias para seguir gestionando las cuentas que has excluido de la zona de aterrizaje multicuenta de AMS:

- Activa el modo de desarrollador: para obtener más permisos para tus cuentas, activa el modo de desarrollador antes de cerrar las cuentas de la aplicación de AMS. Al activar el modo de desarrollador, puede realizar con mayor facilidad los cambios necesarios para prepararse para la desconexión. No intentes eliminar ni modificar los recursos de la infraestructura de AMS. Si eliminas los recursos de infraestructura de AMS, es posible que AMS no pueda cerrar tu cuenta correctamente. Para obtener información sobre cómo activar el modo de desarrollador, consulte [Introducción al modo AMS Advanced Developer](#).

Si no puedes realizar los cambios necesarios para prepararte para la desconexión después de activar el modo de desarrollador, ponte en contacto con el equipo de tu cuenta de AMS para analizar tus requisitos.

- Elige un método alternativo para acceder a la EC2 pila: una vez que desconectes las cuentas de la aplicación de AMS, no podrás utilizarlas RFCs para acceder a los recursos de la pila. Revisa [y Cambios en la contratación](#), a continuación, elige un método de acceso alternativo para conservar el acceso a tus pilas. Para obtener más información, consulte [Alternativas de acceso](#).

Extraiga las cuentas de la aplicación AMS

Para eliminar las cuentas de la Aplicación de tu entorno de landing zone con varias cuentas, sigue los siguientes pasos para cada cuenta:

1. Compruebe que no haya ninguna cuenta abierta RFCs . Para obtener más información, consulte [Crear, clonar, actualizar, buscar y cancelar RFCs](#).
2. Compruebe que puede acceder a la dirección de correo electrónico del usuario principal o raíz de la cuenta.
3. Desde la cuenta de la aplicación, envíe un RFC con la cuenta de la aplicación | [Confirme el tipo de cambio de la cuenta de la solicitud \(ct-2wlfo2jxj2rkj\)](#). En la RFC, especifique la cuenta de la aplicación que desea eliminar.
4. Desde la cuenta de administración, envíe una RFC con el tipo de cambio de cuenta de [administración | Cuenta de aplicación externa \(ct-0vdiy51oyrhbm\)](#). En la RFC, especifique la cuenta de la aplicación que desea eliminar. Además, indica si deseas eliminar o conservar la pasarela de tránsito adjunta a la landing zone.
5. Para asegurarse de que se interrumpe la facturación de AMS, notifique a su CSDM que ha cancelado la cuenta.

Tras la desconexión de la cuenta de la Aplicación, se produce lo siguiente:

- Todos los componentes están disociados de los servicios de AMS, pero los recursos que haya creado permanecen en la cuenta. Puede optar por conservar o cerrar la cuenta externa de AMS.
- Las cuentas principales y el resto de las cuentas de la Aplicación funcionan normalmente después de cerrar una cuenta de la Aplicación.
- La facturación de AMS se detiene, pero no se detiene hasta que cierres la AWS cuenta. Para obtener más información, consulta [Lo que debes saber antes de cerrar tu cuenta](#).
- Si una cuenta está cerrada, estará visible en su organización en el suspended estado durante 90 días. Transcurridos 90 días, la cuenta cerrada se elimina de forma permanente y deja de estar visible en su organización.
- Una vez cerrada la cuenta, puedes seguir iniciando sesión y presentar una solicitud de asistencia a un contacto Soporte durante 90 días.
- Transcurridos 90 días, cualquier contenido que permanezca en la cuenta se eliminará permanentemente y los AWS servicios restantes se cancelarán.

Preguntas frecuentes sobre la desvinculación de cuentas de aplicaciones

P: ¿Puedo usar mis funciones de IAM federadas para seguir accediendo a una cuenta de aplicación que he retirado de mi landing zone multicuenta de AMS?

Sí. Los [roles predeterminados AWS Identity and Access Management \(IAM\) creados por AMS](#) permanecen disponibles en la cuenta después de la desconexión de AMS. Sin embargo, estas funciones y políticas están diseñadas para usarse con la administración de acceso a AMS. Para proporcionar el acceso necesario a sus usuarios, es posible que necesite implementar sus propios recursos de IAM.

P: ¿Cómo obtengo acceso completo a una cuenta de aplicación que he retirado de mi landing zone multicuenta de AMS?

Las cuentas de aplicaciones externas se trasladan a la unidad organizativa (OU) obsoleta de la estructura de cuentas. AWS Organizations Esta medida elimina las restricciones de acceso de SCP que anteriormente bloqueaban el acceso de los usuarios root. Para obtener información sobre cómo restablecer las credenciales de un usuario root, consulte [Restablecer una contraseña de usuario root perdida u olvidada](#).

P: ¿Qué cambios se realizan durante la desactivación de la cuenta de la Aplicación?

Para obtener información sobre las acciones que AMS toma cuando el servicio cierra cuentas, consulte. [Cambios en la contratación](#)

P: ¿Puedo cancelar la suscripción de una cuenta de la aplicación sin separarla de la pasarela de transporte?

Sí. Utilice el tipo [de cambio de cuenta de administración | Cuenta de aplicación externa](#) (ct-0vdiy51oyrhbm) para enviar la RFC y especifique el parámetro como. DeleteTransitGatewayAttachment False

P: ¿Cuánto tiempo se tarda en cerrar una cuenta de aplicación?

Si utiliza la cuenta de [administración | Cuenta de aplicación externa](#) (ct-0vdiy51oyrhbm), cambie de tipo y complete el proceso en 1 hora. RFCs

P: ¿Es obligatorio cerrar la cuenta externa?

No. El cierre de la cuenta tras la salida de AMS no es obligatorio. Durante el proceso de desvinculación, AMS elimina el acceso y la administración de tu AWS cuenta, pero tu cuenta y los recursos de la cuenta permanecen. Es importante tener en cuenta que, tras la salida de AMS, tú eres el único responsable de gestionar y mantener tu AWS cuenta y tus recursos. AMS no se hace responsable de ningún problema, incidente o interrupción del servicio que pueda producirse en tu cuenta una vez finalizado el proceso de exclusión. Para obtener más información, consulta [¿Cómo cierro mi cuenta? AWS](#).

P: Si presento una solicitud de cierre de cuenta, ¿se eliminan inmediatamente todos los recursos existentes?

No. El cierre de la cuenta no cancela sus recursos. Los recursos de la cuenta se cancelan automáticamente 90 días después de la solicitud de cierre. La facturación de AMS se detiene, pero la facturación de AWS recursos no se detiene hasta que se cierra la cuenta. Para obtener más información, consulta [Lo que debes saber antes de cerrar tu cuenta](#).

P: ¿Puedo programar la desactivación de una cuenta de la Aplicación?

Sí. Puede programarla RFCs para que se ejecute a una hora específica. Sin embargo, debe completar la RFC sobre la [cuenta de la solicitud | Confirme la desconexión](#) antes de poder programar la cuenta de [administración | La RFC sobre la cuenta de solicitud externa](#). [Para obtener más información, consulte Programación de RFC](#).

Cuenta de aplicación que abandona RACI

- R: Parte responsable. La parte responsable de completar la tarea de la lista.
- R: Parte responsable. La parte que aprueba la tarea completada.

- C: Parte consultada. Parte cuya opinión se solicita, por lo general como experta en la materia, y con la que existe una comunicación bilateral.
- I: Parte informada. Una parte a la que se informa sobre el progreso, a menudo solo al finalizar la tarea o el producto final.

Actividad	Cliente	AWS Managed Services (AMS)
Requisitos previos		
Verifica el acceso a la dirección de correo electrónico raíz de cada ID de AWS cuenta que se vaya a eliminar	R	C
Revisa la documentación de AMS sobre las medidas recomendadas para los clientes y prepara las cuentas para la desvinculación de AMS	R	C
Si es necesario, envía una RFC para habilitar el modo Desarrollador a fin de preparar las cuentas para la desvinculación de AMS	R	I
Si es necesario, elige un método alternativo para acceder a la EC2 pila.	R	I
Desembarque		
Envíe RFCs para confirmar y solicitar la desvinculación de las cuentas de la Aplicación	R	I
Extraiga los componentes de AMS de las cuentas de la aplicación	I	R
Notifique a AMS CSDM de las cuentas externas para detener la facturación de AMS	R	I
Tras la salida del embarque		
Restablezca la contraseña de la cuenta de usuario root y verifique el acceso root en las cuentas externas	R	C

Actividad	Cliente	AWS Managed Services (AMS)
Cierre la cuenta o siga las instrucciones de AMS sobre las medidas recomendadas para los clientes que figuran en la documentación de desvinculación de AMS para seguir gestionando las cuentas	R	C

Extraiga las cuentas principales

Para eliminar las cuentas principales de Landing Zone con varias cuentas, sigue estos pasos:

1. Compruebe que todas las cuentas de la aplicación en la landing zone hayan sido retiradas de AMS.
2. Compruebe que no tiene ninguna cuenta abierta RFCs . Para obtener más información, consulte [Crear, clonar, actualizar, buscar y cancelar RFCs](#).
3. Compruebe que puede acceder a la dirección de correo electrónico del usuario principal o raíz de todas las cuentas principales. Para obtener más información, consulte [Cuentas multicuenta de Landing Zone](#).
4. Compruebe que puede acceder al número de teléfono del usuario principal o raíz de la cuenta de administración. Utilice la función `AWSSManagedServicesBillingRole` de IAM para actualizar el número de teléfono. Para obtener más información, consulta [¿Cómo actualizo el número de teléfono asociado a mi AWS cuenta?](#) .
5. Inicia sesión en tu cuenta de gestión de landing zone de AMS y envía una solicitud de servicio de AMS. En la solicitud de servicio, especifica si deseas abandonar toda tu landing zone.

Tras la desconexión de las cuentas principales, ocurre lo siguiente:

- Todos los componentes están desasociados de los servicios de AMS, pero algunos AWS recursos permanecen en la cuenta. Puede optar por conservar o cerrar las cuentas principales externas de AMS.
- La facturación de AMS se detiene, pero no se detiene hasta que cierres la AWS cuenta. Para obtener más información, consulta [Lo que debes saber antes de cerrar tu cuenta](#).

- Si una cuenta está cerrada, estará visible en su organización en el suspended estado durante 90 días. Transcurridos 90 días, la cuenta de miembro cerrada se elimina de forma permanente y deja de estar visible en su organización.
- Una vez cerrada la cuenta, podrás seguir iniciando sesión y presentar una solicitud de asistencia o un contacto Soporte durante 90 días.
- Una vez cerrada la cuenta durante 90 días, cualquier contenido que permanezca en la cuenta se eliminará permanentemente y los AWS servicios restantes se cancelarán.

Preguntas frecuentes sobre la desvinculación de la cuenta principal

P: ¿Puedo usar mis funciones de IAM federadas para seguir accediendo a las cuentas principales no autorizadas?

Sí. Los [roles predeterminados AWS Identity and Access Management \(IAM\) creados por AMS](#) permanecen disponibles en la cuenta externa. Sin embargo, estas funciones y políticas están diseñadas para usarse con la administración de acceso a AMS. Para proporcionar el acceso necesario a sus usuarios, es posible que necesite implementar sus propios recursos de IAM.

P: ¿Cómo obtengo acceso total a la cuenta MALZ de administración, servicios compartidos, redes u otra cuenta [MALZ que no sea de aplicación después de salir de la landing zone multicuenta](#) de AMS?

Tras la desconexión, siga las instrucciones de [Restablecer una contraseña de usuario raíz perdida u olvidada para utilizar las credenciales de usuario](#) principal (raíz) para acceder a las cuentas principales distintas de la cuenta de administración. A diferencia de otros tipos de cuentas, la cuenta de administración conserva un dispositivo de autenticación multifactor (MFA) inaccesible que está asociado al usuario raíz para evitar su uso. Para recuperar el acceso root, debe seguir el proceso de [recuperación del dispositivo MFA perdido](#).

P: ¿Qué cambios se realizan durante la desconexión de la cuenta principal?

Para obtener información sobre las acciones que AMS toma cuando el servicio cierra cuentas, consulte. [Cambios en la contratación](#)

P: ¿Cuánto tiempo se tarda en cerrar la cuenta principal?

El proceso de cierre de la cuenta principal suele tardar hasta 30 días en completarse. Sin embargo, para asegurarte de que todos los pasos necesarios se hayan completado correctamente, debes iniciar la solicitud de exclusión al menos 7 días antes de que comience la exclusión. Para facilitar la transición, planifique con antelación y envíe su solicitud de exclusión con antelación.

P: ¿Cómo puedo gestionar los componentes compartidos tras la desvinculación de AMS?

El Active Directory gestionado por AMS y otros componentes de la infraestructura de servicios compartidos están diseñados para que los operadores de AMS puedan acceder a ellos. Es posible que deba actualizar los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2), la política de control de AWS Organizations servicios (SCP) o realizar otros cambios para conservar el acceso total a estos componentes.

P: ¿Puedo cerrar las cuentas principales no registradas?

De forma predeterminada, las cuentas de aplicación dependen en varias ocasiones de las cuentas principales de MALZ, por ejemplo, la AWS Organizations membresía, la conectividad a la red de las pasarelas de tránsito y la resolución de DNS a través de AMS Managed Active Directory. Una vez resueltas estas dependencias, puedes dar de baja y cerrar la cuenta Core que ya no está conectada. Para obtener más información, consulte [Cuentas multicuenta de Landing Zone](#).

Cuenta principal que abandona RACI

- R: Parte responsable. La parte responsable de completar la tarea de la lista.
- R: Parte responsable. La parte que aprueba la tarea completada.
- C: Parte consultada. Parte cuya opinión se solicita, por lo general como experta en la materia, y con la que existe una comunicación bilateral.
- I: Parte informada. Una parte a la que se informa sobre el progreso, a menudo solo al finalizar la tarea o el producto final.

Actividad	Cliente	AWS Managed Services (AMS)
Requisitos previos		
Compruebe el acceso a la dirección de correo electrónico raíz de cada ID de cuenta de AWS que se vaya a eliminar	R	C

Actividad	Cliente	AWS Managed Services (AMS)
Verifique el acceso al número de teléfono del usuario raíz de la cuenta de administración y actualícelo	R	C
Revisa la documentación de AMS sobre las medidas recomendadas para los clientes y prepara las cuentas para dejar de usar AMS	R	C
Desembarque		
Presentar una solicitud de servicio para solicitar el desembarque de la zona de aterrizaje	R	I
Extraiga los componentes de AMS de las cuentas principales	I	R
Tras la salida del embarque		
Restablezca la contraseña de la cuenta de usuario root y verifique el acceso root en las cuentas externas	R	C
Cierre las cuentas o siga las instrucciones de AMS sobre las medidas recomendadas para los clientes que figuran en la documentación de desvinculación de AMS para seguir gestionando las cuentas	R	C

Cambios en la contratación

En la siguiente tabla se describen las medidas que AMS toma para la desconexión de zonas de landing zone con varias cuentas, los posibles impactos y las acciones recomendadas.

Componere	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomendada para el cliente
Administración de accesos	Cuentas de aplicaciones	Tras la desconexión, ya no se puede enviar el acceso a las pilas con un acceso limitado en el tiempo RFCs para just-in-time acceder a las pilas a través de los EC2 hosts bastiones de AMS AMS ya no administra los componentes relacionados con el acceso en ninguna pila de EC2 recursos existente (agente abierto de PBIS, scripts de unión de dominios)	No puede usar los bastiones de AMS a través de RFS para acceder a las instancias EC2 EC2 las instancias lanzadas desde un servidor no proporcionado por AMS AMLs no están unidas al dominio de Active Directory administrado Si no se eliminan, los scripts de inicio de AMS en las pilas de recursos existentes pueden producir errores debido a la falta de dependencias de AMS e impedir que se vuelvan a unir a un dominio diferente	Utilice métodos alternativos para acceder a la EC2 instancia (consulte) Alternativas de acceso Elimine los scripts de lanzamiento de AMS de las pilas de EC2 recursos existentes (consulte Deshabilite los scripts de EC2 inicio de AMS)
Administración de acceso	Cuentas principales	Si migraste de PBIS Open a PBIS Enterprise (AD Bridge), AMS ya no renovará las licencias tras	Si se permite que la licencia de PBIS Enterprise caduque, las credenciales de	Si migró a PBIS Enterprise (AD Bridge), decida si desea mantener las

Componer e	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomendada para el cliente
(continuación)		la desvinculación de la cuenta principal	Active Directory no son válidas para las pilas de instancias existentes basadas en Linux EC2	licencias o retirarlas (consulte) PBIS Open/Enterprise (AD Bridge)
Registro, supervisión y administración Incident/Event	Cuentas principales y de aplicaciones	Alertas del monitoreo de referencia en AMS Se eliminan los componentes de AMS que se van a implementar CloudWatch Las alarmas de Amazon desplegadas actualmente permanecen, pero ya no crean incidentes de AMS AWS Config Se eliminan las autorizaciones de agregación de AMS y de la cuenta de seguridad MALZ Core AWS Config las reglas permanecen implementadas y Amazon GuardDuty permanece habilitada, pero ya no crea incidentes de AMS	Los recursos recién creados no tienen activadas las alarmas ni la supervisión de referencia de AMS Las métricas de infraestructura, las alarmas y los eventos de seguridad ya no generan incidentes de AMS AWS Config ya no está agregado en una cuenta central	Defina, capture y analice las métricas de las operaciones para ver los eventos de carga de trabajo y tomar las medidas adecuadas. Implemente cualquier flujo de trabajo de alertas necesario para seguir aplicando la supervisión operativa y las alarmas necesarias en los nuevos recursos y para recibir alertas de AWS Config seguridad de Amazon GuardDuty.

Componen e	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomenda da para el cliente
Administra ción de la continuid ad (Backup and Restore)	Cuentas de aplicacio nes	AMS ya no supervisa los trabajos de copia de seguridad ni realiza solicitudes de copia de seguridad y restauración Las bóvedas de respaldo predeterminadas de AMS, la clave de cifrado de copias de seguridad y la función de copia de seguridad permanecen	Es posible que no se noten los errores en la operación de Backup	Supervise y revise las configuraciones del plan de respaldo

Componer e	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomendada para el cliente
Administración de parches	Cuentas principales y de aplicaciones	AMS ya no supervisa las operaciones de aplicación de parches para garantizar su correcta ejecución ni realiza los parches de forma manual AMS ya no actualiza los componentes de la infraestructura del AMS Se conservan las líneas base de los parches proporcionados por AMS Los manuales de automatización de AWS Systems Manager parches proporcionados por AMS no se comparten y ya no están disponibles para su uso	Es posible que no se noten los errores en la operación de parcheo Las configuraciones de parches existentes que dependen de los manuales de ejecución de Systems Manager Automation proporcionados por AMS deben reconfigurarse para que continúen sin interrupciones.	Revise y reconfigure las configuraciones de los parches según sea necesario

Componer e	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomendada para el cliente
Administración de red	Cuentas de aplicaciones	Si se especifica, se elimina el archivo adjunto a la pasarela de tránsito de la cuenta de la aplicación externa	La cuenta de aplicación externa ya no puede usar una pasarela de tránsito para acceder a servicios compartidos, como las cuentas de Active Directory administradas u otras cuentas de aplicaciones	Especifique si desea DeleteTransitGatewayAttachment False conservar la conectividad de la pasarela de tránsito

Componer e	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomendada para el cliente
Administración de la seguridad	Cuentas de aplicaciones	La cuenta está separada de la consola central de Trend Micro DSM. Además, los agentes de puntos finales ya no envían alertas a través del proceso de incidentes de AMS Los agentes de Trend Micro permanecen instalados, pero AMS ya no los gestiona ni actualiza AMS ya no mantiene ni actualiza las personalizaciones de AMI que implementan el agente de Trend Micro.	EC2 es posible que las detecciones de malware en los puntos finales de la instancia no se noten El microagente de Trend no se implementa en EC2 las instancias que se lanzan desde un dispositivo que no esté provisto por AMS AMIs	Considere las opciones para mantener o interrumpir Trend Micro (consulte Trend Micro Deep Security)

Componer e	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomendada para el cliente
Gestión de la seguridad (continuación)	Cuentas principales	La infraestructura DSM de Trend Micro permanece en las cuentas de Shared Services, pero AMS ya no la mantiene ni actualiza Trend Micro DSM ya no reenvía alertas a través del proceso de incidentes de AMS	EC2 por ejemplo, las detecciones de malware en terminales pueden pasar desapercibidas EC2 la protección de los puntos finales de una instancia podría verse afectada si no se mantiene la infraestructura (actualizaciones de definiciones, licencias, etc.)	Decida si desea continuar o interrumpir Trend Micro (consulte Trend Micro Deep Security)

Componer e	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomendada para el cliente
Administración de cambios	Cuentas principales y de aplicaciones	Se han eliminado la consola RFC y la API de AMS Las políticas de control de servicios personalizadas de AMS (SCPs) que contienen restricciones de acceso a nivel de cuenta se eliminan al cerrar la cuenta de la aplicación y se eliminan durante la desconexión de la cuenta principal	Debe usar una AWS API nativa para crear nuevos recursos, cambiar los recursos existentes o actualizar las pilas existentes AWS CloudFormation Las restricciones de acceso ya no se imponen a nivel de cuenta a través de los AMS proporcionados SCPs	Asegúrese de que los roles de usuario proporcionen un acceso suficiente para usar los servicios AWS Cree SCPs para proporcionar restricciones de permisos a nivel de cuenta

Componen e	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomenda da para el cliente
Imágenes y automatiz aciones del sistema operativo AMS para la gestión de servicios	Cuentas principal es y de aplicacio nes	AMS ya no admite las personalizaciones y los scripts de lanzamiento incluidos en los AMS proporcionados EC2 AMIs Los AMS proporcionados EC2 AMIs permanecen disponibles en sus cuentas externas Los manuales de automatización de Systems Manager proporcionados por AMS no se comparten y ya no están disponibles para su uso.	Tras la desconexión, AMS AMIs lanzó la señal AWS CloudFormation send cfn-signal FAILURE porque no dependía de los componentes de AMS Los procesos operativos que dependen de los manuales de automatización de Systems Manager proporcionados por AMS pueden fallar	Revise y actualice cualquier proceso operativo o de construcción que dependa de los manuales proporcionados por AMS AMIs o de los manuales de automatización de Systems Manager
Infraestr uctura de servicios compartid os	Cuentas principal es	Se ha eliminado el acceso a AMS y AMS ya no administra los componentes compartidos, incluido el Active Directory gestionado por AMS AWS Transit Gateway, y AWS Organizations	Pérdida de la administración de la infraestructura compartida	Restablezca el acceso de administrador al Active Directory gestionado por AMS y asuma la gestión de los componentes de los servicios compartidos

Componen e	Account type (Tipo de cuenta)	Medidas adoptadas para desembarcar	Posibles impactos	Acción recomenda da para el cliente
Informes	Cuentas principales y de aplicaciones	AMS ya no recopila detalles a nivel de cuentas o recursos para generar informes agregados	Pérdida de informaci ón sobre las métricas operativa s y empresariales (cobertura de copias de seguridad y parches, gestión de cambios y actividad de incidentes)	Sustituya todos los informes de datos agregados necesarios en todas las cuentas por su propia solución
Equipo de cuentas y servicio de asistenci a de AMS	Cuentas principales y de aplicación	El equipo de cuentas de AMS (CSDM, CA) y el servicio de operaciones de AMS ya no admiten las cuentas externas	Pérdida de soporte operativo con experiencia en la arquitectura de zona de aterrizaj e multicuenta diseñada por AMS y componentes relacionados	Asegúrese de que haya suficiente personal y esté familiarizado con la estructura y los recursos de la cuenta para respaldar las operaciones en el entorno

Alternativas de acceso

Los siguientes son métodos alternativos para conservar el acceso a tu EC2 pila después de cerrar las cuentas de AMS:

- Utilice el administrador de sesiones para acceder a EC2 las instancias con permisos elevados sin necesidad de bastiones ni acceso a la red entrante. Para obtener más información, consulte [AWS Systems Manager Session Manager](#).

- Vuelva a unir EC2 las instancias a un dominio de Active Directory diferente con las nuevas credenciales de dominio. Si las usa AWS Directory Service, consulte [Unir una EC2 instancia a su AWS Managed Microsoft AD directorio](#).
- Usa cuentas de usuario locales que hayas creado mediante uno de los otros métodos de acceso o mediante [AWS Systems Manager Run Command](#).

Deshabilite los scripts de EC2 inicio de AMS

Sistemas operativos Linux

Usa el administrador de paquetes de tu distribución para desinstalar el `ams-modules` paquete. Por ejemplo, para el uso de Amazon Linux 2 `yum remove ams-modules`.

Sistemas operativos Windows

Para deshabilitar los scripts de EC2 inicio en Windows, siga estos pasos:

1. Windows Server 2008/2012/2012r2/2016/2019:

Desactive o elimine la tarea programada de inicio de Managed Services del Programador de tareas. Para ver una lista de las tareas programadas, ejecute el `Get-ScheduledTask - TaskName '*Ec2*'` comando.

Windows Server 2022:

Elimine la [tarea EC2 Launch v2](#). Esta tarea se ejecuta por postReady etapas `Initialize-AMSBoot` en `C:\AmazonProgramData\EC2 Launch\config\agent-config.yml` de la instancia. El siguiente es un fragmento de un ejemplo: `agent-config.yml`

```
{
  "task": "executeScript",
  "inputs": [
    {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
    }
  ]
}
```

2. (Opcional) Elimine el siguiente contenido del archivo:


```
C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*  
C:\Windows\System32\WindowsPowerShell\v1.0\Modules  
\AWSManagedServices.Build.Utilities\*
```

PBIS Open/Enterprise (AD Bridge)

Para determinar si utilizas la edición PBIS Open o PBIS Enterprise (AD Bridge), ejecuta el siguiente comando en una instancia gestionada por Linux EC2 :

```
yum info | grep pbis
```

El siguiente es un ejemplo de resultado que muestra PBIS Enterprise (AD Bridge):

```
Name      : pbis-enterprise  
From repo  : pbise  
Name      : pbis-enterprise-devel  
Repo      : pbise  
Description : The pbis-enterprise-devel package includes the development
```

PBIS abierto

PBIS Open es un producto obsoleto que BeyondTrust ya no es compatible. Para obtener más información, consulte la documentación de [BeyondTrust pbis-open](#).

AD Bridge (PBIS Enterprise)

Puede elegir una de las opciones siguientes:

- Renueve las licencias y continúe operando AD Bridge. Póngase en contacto con nosotros BeyondTrust para hablar sobre las licencias y el soporte.
- Suspenda el uso de AD Bridge. Ejecute el siguiente comando de Shell para eliminar el paquete PBIS-Enterprise de las instancias administradas de Linux. Para obtener más información, consulta la BeyondTrust documentación [Dejar un dominio y desinstalar el agente AD Bridge](#).

```
$ sudo /opt/pbis/bin/uninstall.sh purge
```

Deje el dominio de Active Directory administrado por AMS sin eliminar el agente PBIS

Tiene la opción de abandonar el Active Directory administrado por AMS sin eliminar el agente de PBIS. Utilice una de las siguientes soluciones, según el sistema operativo:

Linux operating systems

Usa el PBIS del AD administrado por AMS para ejecutar el siguiente comando de shell para desunir una instancia de Linux. EC2 Para obtener más información, consulta la documentación de [BeyondTrust pbis-open](#) o [BeyondTrust AD Bridge](#), según la versión que utilices.

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

Es posible que veas un mensaje de error similar al siguiente:

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]
Cannot resolve network address for KDC in requested realm
```

Si se produce este error, ejecuta los siguientes comandos para eliminar el registro del proveedor de AD y reiniciar lwsmd los servicios:

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin]'
```

Usa el resultado del ID de directorio que recibiste del comando anterior (por ejemplo, **A123EXAMPLE.AMAZONAWS.COM**) para ejecutar los siguientes comandos:

```
$ /opt/pbis/bin/regshell delete_tree \
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\
\DIRECTORIID]'
```

```
$ /etc/pbis/redhat/lwsmd restart
```

```
$ /opt/pbis/bin/lwsm restart lwreg
```

Windows operating systems

```
# Collect hostname and domain name using:

Test-ComputerSecureChannel -verbose
```

```
# Disjoin computer from the domain:  
  
netdom remove hostname /domain:domain name /force
```

Note

Asegúrese de deshabilitar o eliminar la tarea programada de inicio de Managed Services como se menciona en [Deshabilite los scripts de EC2 inicio de AMS](#).

Trend Micro Deep Security

Utilice una de las siguientes opciones para continuar o interrumpir el uso de Trend Micro Deep Security:

Continuar con el uso

- (Si se va a desconectar todo el MALZ) Tras la desconexión de la cuenta principal, vuelva a conectar las cuentas de aplicaciones desconectadas al Trend Micro Deep Security Manager (DSM) existente y mantenga las licencias en la cuenta de servicios compartida. [Para obtener más información, consulte Añadir cuentas en la AWS nube y Comprobar la información de su licencia.](#)
 1. Inicie sesión en la cuenta de servicios compartidos y vaya a la consola de Secrets Manager.
 2. Recupere las credenciales de administrador de la consola DSM que están almacenadas en la `/ams/eps/` ruta.
 3. [Inicie sesión en la consola de DSM en https://dsm.sentinel.int](https://dsm.sentinel.int).
 4. Seleccione Usar función multicuenta y, a continuación, introduzca `arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role`. Reemplace ACCOUNTID por el ID de cuenta de la aplicación externa.
 5. Elija Siguiente.
 6. Espere unos minutos a que DSM procese la detección de la cuenta y demuestre que la sincronización se ha realizado correctamente.
- Vuelva a conectar las cuentas de aplicaciones externas a una nueva instalación de Trend Micro DSM. [Para obtener más información, consulte Activar y proteger agentes y Activar el agente.](#)
- Vuelva a conectar las cuentas de aplicaciones externas a Trend Micro Cloud One. Para obtener más información, consulte [Migración de Deep Security a Workload Security](#) y [Migración desde un DSM local](#).

Suspenda su uso

- Desinstale los agentes de Trend Micro Deep Security de las cuentas de aplicaciones externas. Para obtener más información, consulte [Desinstalar Deep Security](#).

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 AMS](#) y 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 subcontractarla 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 provisionados de autoservicio (SSP)	El cliente es responsable de los recursos provisionados 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 provisionados de autoservicio (SSP)	El cliente es responsable de los recursos provisionados 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	Aprovisio namiento de autoservi cio	Modo de desarroll ador	Gestionad o 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 provisionados de autoservicio (SSP)	El cliente es responsable de los recursos provisionados 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 provisionados de autoservicio (SSP)	El cliente es responsable de los recursos provisionados 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	Aprovisio namiento de autoservi cio	Modo de desarroll ador	Gestionad o por el cliente
Gestión del aprovisio namiento	Prescriptivo y estandari zado para las opciones de aprovisio namiento que se ofrecen en AMS	Flexibili dad para utilizar directame nte la API de servicios de AWS para AWS Service Catalog siguiendo los estándares prescript ivos de AMS	Flexibili dad para utilizar directame nte la API de servicios de AWS siguiendo los estándares prescript ivos de AMS	Flexibilidad para utilizar directame nte el servicio de AWS APIs para los servicios de SSP	Flexibilidad para utilizar directame nte la API de servicios de AWS para el aprovisio namiento	

Cuestiones de decisión	Modo CM estándar/ OOD *	AWS Service Catalog	Modo de cambio directo	Aprovisio namiento de autoservi cio	Modo de desarroll ador	Gestionad o 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	Aprovisio namiento de autoservi cio	Modo de desarroll ador	Gestionad o por el cliente
Refactori zación de aplicacio nes	Es necesaria una refactorización de la luz				Es necesaria una refactori zación 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 operativa s de las aplicaciones del cliente		De 6 a 18 meses, según las competenc ias del cliente en materia de infraestr uctura y operaciones de aplicacio nes
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 contenerizada 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 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 [CreateRfc](#) sección 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-rtc` 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 [AssumeRoleWithWebIdentity](#) AWS 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 sam1 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=sam1` (en Windows, sería en Linux `export AWS_DEFAULT_PROFILE=sam1`). 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 `AWSManagedServicesAdminRole` utilizar la que `AWSManagedServicesChangeManagementRole` 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.

`RfcActionStateDefiniciones` (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 **ActionState** cambia 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 **ActionState** automáticamente a **AwsActionPending** 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 **ActionState** automáticamente cambia a **AwsActionPending**, 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 **ActionState** a **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, **ActionState** se establece automáticamente en **AwsActionPending**.
- Cuando se crea un RFC, **ActionState** se establece automáticamente en **NoActionPending**.
- Cuando se envía un RFC, **ActionState** se establece automáticamente en **AwsActionPending**.

- Cuando una RFC es rechazada, cancelada o completada con un estado de éxito o error, `ActionState` 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

enCustomerActionPending, 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	Rechazados: RFCs se rechazan normalmente porque no se validan; por ejemplo, se especifica a un recurso inutilizable, es decir, una subred
PendingApproval /Enviado: El RFC se ha enviado y el sistema está determinando si requiere aprobación y obteniendo esa aprobación, si es necesaria	Cancelados: RFCs se cancelan normalmente porque no pasan la validación antes de que haya transcurrido la hora de inicio configurada
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	Fallo: el RFC ha fallado; consulte el StatusReason 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	una alerta de avería y se comunicará con usted según sea necesario
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 correctamente	

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 a `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 `InProgress` o `Failure`, 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 AWS 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-3king0u4l33zf)

Estos son los recursos que admite el tipo de cambio de remediación de desviaciones (ct-3king0u4l33zf). 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 \(ct-3king0u4l33zf\)](#)

⚠ 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 DryRun opción 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 solicite una hora de inicio que sea, como mínimo, 24 horas después de la fecha en que planea 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 aRequestedStartTime, la RFC se considera programada y RequestedEndTime se rellena con el ExecutionDurationInMinutes valor.
- solo aRequestedEndTime, 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 (elijá 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: [ApproveRfc](#) marca 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: [RejectRfc](#) marca 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 [UpdateRestrictedExecutionTimes](#) API 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 [ListRestrictedExecutionTimes](#) API. Ejemplo:

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

Si quieres enviar una RFC durante un tiempo de ejecución restringido específico, añade la `RestrictedExecutionTimesOverrideId` con el valor de `OverrideRestrictedTimeRanges` y 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 RFCs para 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-123h45t6uz7j1 |
| Management| Load balancer (ELB) stack | Update | ct-01tm873rseb9  |
+-----+-----+-----+-----+
```

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

2. Busque la versión más reciente del CT:

`ChangeTypeIdChangeTypeVersion`: El identificador de tipo de cambio para este tutorial es `ct-123h45t6uz7j1` (crear ELB). Para encontrar la última versión, ejecute este comando:

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=ct-123h45t6uz7j1
```

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-123h45t6uz7j1" --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.

`TimeoutInMinutes` En 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-sdhopv000000000000",
  "Name":             "MyElbInstance",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "ELBSubnetIds":    ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold": 4,
```

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

- 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
```

- 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"  
}
```

- 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 desees 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 `AwsOperatorAssigned` indicar que un operador está consultando la RFC en ese momento, es `AwsActionPending` decir, que un operador de AMS debe realizar algo antes de que la ejecución de la RFC pueda continuar o `CustomerActionPending` que 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 [ListRfcSummaries](#) operación 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 yValues.

Filtrado RFC

Atributo	Valores válidos	Condicion es válidas	Condición predeterm inada	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 exactamen te 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 exactamen te 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, «20170101T000000Z»)	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, «20170101T000000Z»)	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, «20170101T000000Z»)	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, «20170101T000000Z»)	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, «20170101T000000Z»)	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-123h45t6uz7j1|
|Management| Monitoring & Notification    |SQS   |Update |ct-123h45t6uz7j1|
+-----+-----+-----+-----+-----+-----+

```

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 RFCs de 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 RFCs lista 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 (.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 (`ams cmyamsskms`) 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`

Suscríbese al correo electrónico diario del RFC

Puedes suscribirte a un correo electrónico diario en el que se resume 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 PendingApproval estado 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 aprovisiona 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 (elijan ASAP en la consola y deje en blanco la hora de inicio y finalización en la API/CLI), ya que CTs requieren que un operador de AMS examine la RFC y, posiblemente, se comuniquen 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, consulte 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

Actualmente API/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, `AwsApprovalId` y `CustomerApprovalId` que 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, consulte [Automatizado 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
<code>AwsApprovalId: Required</code>	El sistema de cambio de tipos AMS,	No hay que hacer nada más. Esta condición es típica de los sistemas automatizados CTs.
<code>AwsApprovalId: NotRequiredIfSubmitter</code>	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.
<code>CustomerApprovalId: NotRequired</code>	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 ApproveRfc operación.
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-sft6rv000000000000",
      "type": "string",

```

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

```

    "enum": ["stm-sft6rv000000000000"]
  },
  "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 rellena 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/pr edeterminada	Notas
ChangeTypeId	Cualquier cadena que represente a ChangeTypeId (por ejemplo: ct-abc123xyz7890)	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/pr edeterminada	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 AWS CloudFormation consola. Puedes identificar tu pila comparándola con el nombre que tiene en la consola AMS. La AWS 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, consulte [Comprenda 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 en AWS CloudFormation en plantillas. Como cliente, tiene acceso de solo lectura a todos los servicios de AWS CloudFormation, incluidos los que puede identificar rápidamente la AWS CloudFormation pila que representa su pila en función de la descripción de la pila mediante la AWS CloudFormation consola. Es probable que la pila fallida se encuentre en un estado de `DELETE_COMPLETE`. Una vez que haya identificado la AWS 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 AWS 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 AWS 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 `elcustomer-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-3mvvt2zkyvej` 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 ejemplo `Create/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`
 - `AWSManagedServicesUpdateDenyActionsOnAMSInfra` Política

- 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 (consulte [Funciones 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 AMS, distintas de las enumeradas anteriormente, deben tener prefijos iguales o iguales a mayúsculas y minúsculas. AMS* MC* upper/lower/mix	Sí. Se interrumpe para CloudFormation la API EFS OpenSearch, CloudWatch Logs, SQS, SSM y Tagging, ya que estos servicios no admiten la <code>aws:TagsKey</code> 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 Appld el entorno y, pero no los recursos que son propiedad de AMS. AppName No se puede lograr con los permisos de IAM.	El etiquetado incorrecto de los recursos de AMS puede afectar negativamente a las operaciones de generación de informes, alertas y parches de sus recursos, por parte de AMS.	El acceso debe estar restringido para realizar cambios en los requisitos de etiquetado predeterminados de AMS para cualquier persona que 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 <code>aws:TagsKey</code> 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 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 aprovisio nado de autoservi cio (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 correspondiente.
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 confidenciales y puede estar expuesto a cuentas no deseadas.	AMIs Compartelos 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 organización, ya que no es posible verificar que	Los registros pueden contener datos confidenciales y pueden estar expuestos a cuentas no deseadas.	Comparta los registros únicamente 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 organización.		de la cuenta antes de compartirlas fuera de su organización. 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
AWS 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 AWS 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 [AWS 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 AWS 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 `AWSTrajectoryServicesDevelopmentRole` 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: `AWSTrajectoryServicesDevelopmentRole`
- 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 en [Requisitos 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 gestionarlos.

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 CloudTrail 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 AWS Directory Service las siguientes acciones. La política de límites de permisos del modo Desarrollador deniega todas las demás acciones de Directory Service: • <code>ds:AuthorizeApplication</code> • <code>ds:CreateAlias</code> • <code>ds:CreateIdentityPoolDirectory</code> • <code>ds>DeleteDirectory</code> • <code>ds:DescribeDirectories</code> • <code>ds:GetAuthorizedApplicationDetails</code> • <code>ds:ListAuthorizedApplications</code> • <code>ds:UnauthorizeApplication</code> En las cuentas de landing zone de una sola cuenta, la política de límites deniega explícitamente el acceso al directorio gestionado por AMS Advanced utilizado por AMS Advanced para mantener el acceso a las cuentas habilitadas para el modo dev.

Servicio	Notas
Amazon Elastic Compute Cloud	No puedo acceder a Amazon EC2 APIs que contenga la cadena: DhcpOptions Gateway,Subnet,VPC, yVPN. No puedo acceder ni modificar EC2 los recursos de Amazon que tengan una etiqueta con el prefijoAMS,, 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 navegación 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
AWS Resource Groups	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. DecodeAuthorizationMessage
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 prefijoams, 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: • <code>lakeformation:DescribeResource</code> • <code>lakeformation:GetDataLakeSettings</code> • <code>lakeformation:DeregisterResource</code> • <code>lakeformation:RegisterResource</code> • <code>lakeformation:UpdateResource</code> • <code>lakeformation:PutDataLakeSettings</code>
Amazon Elastic Inference	Solo puedes llamar a la acción de la API de Elastic Inference. <code>elastic-inference:Connect</code> Este permiso está incluido en el <code>customer_sagemaker_admin_policy</code> que se adjunta a <code>customer_sagemaker_admin_role</code> 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 AWS 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, AWS Management Console 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_alex_console_role` siguiente función de IAM a su cuenta:. También `customer_alex_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_alex_gateway_installer_user` y `customer_alex_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-3d8mdd9jn1r)`.

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 autenticuen 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 provisionado el rol, incorpore el rol a su solución de federación e inicie sesión y, a continuación, acceda a AWS Glue 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 provisionado 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 deseada 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 AWS Management Console AWS CLI o APIs crear imágenes personalizadas en su AWS cuenta. Cuando utilice el AWS Management Console, 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 autoaprovechado | 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

AWS Management Console 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-10xx2g2d7hc90). 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-Admin y 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 tráfico 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 autoaprovechado | 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. Aprovechione 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-36cn2avfrj9v), 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 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 autoaprovechado | 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 autoaprovisionado 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 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, consulte [Utilice 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, consulte [Utilice 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, consulte [Utilice 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, consulte [Utilice 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 AMS](#) [Utilice AMS SSP para](#)

[aprovisionar AWS CodeDeploy en su cuenta AMS](#), y [Utilice 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: GenerateDataKey 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-Premises. 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 provisionado 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-Ro1e` la siguiente función de IAM en su cuenta: Una vez provisionado 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 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 provisionado 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-0fpjlx808sh2 (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 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 autoaprovechado | 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 autoaprovechado | 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 autoaprovechado | 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:GenerateDataKey` 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-Premises. 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 autoaprovechado | 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 provisionado 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 AWS Management Console 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](#) . 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 AWS Management Console. 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 autoaprovechado | 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 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 AWS 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. Respóndenlos 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 `AMS Secrets Manager Shared Policy`, 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 en su cuenta AMS

Utilice el modo de aprovisionamiento de autoservicio (SSP) de AMS para acceder directamente a AWS Security Hub las funciones de su cuenta gestionada por AMS. AWS Security Hub 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](#).

Preguntas frecuentes sobre Security Hub en AWS Managed Services

P: ¿Cómo solicito acceso a AWS Security Hub 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

No hay requisitos previos ni dependencias para su uso AWS Security Hub 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 provisionados 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 automatización que haya 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 ResourceProperty —	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 provisionados 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/Export capabilities 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-117rmp64d5mbv: 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 catalog 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 aprovisiona 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](#).

Búsqueda de los datos que necesita (SKMS), AMS

Para encontrar los datos que necesita al utilizar sus cuentas de AWS Managed Services (AMS), recurre al sistema de gestión del conocimiento del servicio AMS (SKMS). ADAMS.

SKMS son las siglas de Service Knowledge Management System y se refiere a toda la información relacionada con el servicio AWS Managed Services (AMS) para un cliente. AMS tiene una API de SKMS para buscar datos.

Temas

- [¿Qué es la gestión del conocimiento de los servicios?](#)
- [Búsqueda de VPC IDs en AMS](#)
- [Búsqueda de subred IDs en AMS](#)
- [Encuentra AMI IDs, AMS](#)
- [Buscar grupo de seguridad \(SG\) IDs, AMS](#)
- [Encuentre entidades de IAM en AMS](#)
- [Encuentra una pila IDs en AMS](#)
- [Busque direcciones IP IDs o de instancia en AMS](#)
- [Encuentra nombres de recursos de Amazon \(ARNs\) en AMS](#)
- [Encuentre recursos por ARN en AMS](#)
- [Encuentra la configuración de la cuenta AMS](#)

¿Qué es la gestión del conocimiento de los servicios?

La gestión del conocimiento del servicio es el almacenamiento de toda la información de su cuenta AMS. La información sobre lo siguiente se obtiene del sistema de gestión del conocimiento del servicio AMS (SKMS), a través de la API AMS SKMS o de la consola AMS:

- VPCs
- Subredes administradas
- Apila y apila componentes, incluidas las EC2 instancias de Amazon y otros recursos
- Imágenes de máquinas de Amazon (AMIs)

Puede utilizar la información del SKMS para comprender la infraestructura que se gestiona y como información para la gestión de cambios y las solicitudes de servicio destinadas a crear, cambiar o eliminar la infraestructura.

 Note

Se graban todas las llamadas a la API AMS SKMS. AWS CloudTrail

Acceda al SKMS a través de la API AMS SKMS, que proporciona operaciones para descubrir información sobre un entorno (VPCs y subredes) y los recursos de la aplicación (pilas, instancias de EC2 Amazon e imágenes de instancias AMLs o) que se pueden implementar allí.

VPCs y las imágenes de las instancias se configuran en una cuenta, con los permisos de acceso necesarios, durante la incorporación. Una vez establecidas, puedes utilizar el sistema de gestión de cambios para rellenarlas VPCs con pilas en funcionamiento.

Búsqueda de VPC IDs en AMS

Una nube privada virtual (VPC) tiene una o más subredes. En AMS, su VPC está en un Región de AWS y tiene subredes públicas y privadas.

Véase también [Búsqueda de subred IDs en AMS](#).

Algunas CTs requieren la. VpcId Para encontrar un ID de VPC, puede usar la consola AMS o la API/ CLI.

Consola AMS:

En el panel de navegación, seleccione VPCs y la VPC correspondiente. Se abre la página de detalles de la VPC seleccionada con información que incluye el ID de la VPC.

API ListVpcSummaries o CLI de AMS SKMS:

 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.

1. En los ejemplos siguientes, el primer comando solicita una lista de resúmenes de todos los miembros de VPCs la cuenta. El segundo comando solicita la lista de VPCs, con un filtro de consulta para mostrar solo las que VPCs se crearon en 2016, y muestra los `CreatedTime` valores `VpcId`, y `Name`.

Note

Puede obtener la CLI de AMS SKMS a través de la página de recursos para desarrolladores de la consola AMS.

```
aws amsskms list-vpc-summaries --output table
```

```
-----
|                               |
|               ListVPCSummaries               |
|-----+-----+
|                               |
|               VPCSummaries                   |
|+-----+-----+
| CreatedTime | 2016-01-15T18:50:11Z |
| VpcId       | vpc-01234567890abcdef |
| LastModifiedTime | 2016-01-15T18:50:11Z |
| Name        | 952444781316-initial-vpc |
|+-----+-----+
|                               |
```

Visibility	
+-----+-----+	
Id	PrivateAndPublic
Name	PrivateAndPublic
+-----+-----+	

2. Esta vez con una consulta:

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?
starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output
table
```

ListVPCSummaries		
+-----+-----+-----+		
2016-01-15T18:50:11Z	vpc-01234567890abcdef	952444781316-initial-VPC
+-----+-----+-----+		

Búsqueda de subred IDs en AMS

Varios recursos requieren que especifique una subred, o una lista de subredes, en el momento de la configuración. Para buscar subredes, puede usar la consola AMS o el AMS SKMS API/CLI. Note that the AMS SKMS API/CLI es privado y debe estar instalado antes de poder usarlo.

Consola AMS:

1. En el panel de navegación, seleccione VPCs y la VPC correspondiente. Se abre la página de detalles de la VPC seleccionada con una tabla de subredes. Haga clic en un ID de subred para abrir la página de detalles y buscar el ID.

API ListSubnetSummaries o CLI de AMS SKMS:

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 encontrar las subredes de su VPC, puede realizar una búsqueda con `list-subnet-summaries` el comando que se muestra.

 Note

Si busca subredes que no estén en una cuenta AMS, puede intentarlo. `aws ec2 describe-subnets --region us-west-2`

1. La operación SKMS API/CLI `ListSubnetSummaries` :

Una lista sencilla:

```
aws amsskms list-subnet-summaries
```

Salida a una tabla:

```
aws amsskms list-subnet-summaries --output table
```

2. La `ListSubnetSummaries` operación de la API SKMS tiene parámetros para limitar los resultados en función de la visibilidad. Además, puede [filtrar](#) los resultados en función del nombre. Si usa la CLI, también puede usar la `--query` opción para restringir el resultado o buscar en una parte de un valor. Por ejemplo, para buscar todas las subredes de una VPC concreta, puede utilizar este comando:

```
aws amsskms list-subnet-summaries --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

Que devuelve algo como esto:

```
-----
|                               ListSubnetSummaries                               |
+-----+-----+-----+-----+
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
+-----+-----+-----+-----+
```

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](#).

3. Si tiene varias VPCs, incluya un filtro de VPC en el comando y, a continuación, ejecute el comando para cada VPC. Por ejemplo:

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxx --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

4. En AWS, utilice [describe-subnets](#).

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](#).

Nombres de subredes

Las subredes AMS se crean automáticamente después de recopilar sus datos y añadirlos al sistema. AMS utiliza una fórmula para crear los nombres de las subredes: A **ACCOUNT_ID** - **SUBNET-TYPE**. **AZ-IDENTIFIER** El tipo de subred sería dmzshared-services, o. customer-application. Si tiene más de una subred de aplicaciones de cliente, se puede agregar un identificador opcional al nombre de la subred, después del ID de cuenta, para indicar que la subred es una subred «adicional» o «reservada».

Encuentra AMI IDs, AMS

Una imagen de máquina de Amazon, o AMI, es una plantilla para EC2 instancias de Amazon, creada a partir de una EC2 instancia de Amazon. AWS proporciona actualizaciones AMIs (con parches, por ejemplo) todos los meses; sin embargo, AWS Managed Services (AMS) exige AMIs que se hayan modificado para su uso en AMS. Cada mes, AMS lanza nuevas versiones AMIs que podrá utilizar poco después del martes de parches.

Amazon Machine Images (AMIs) son plantillas de configuración de instancias que se utilizan para crear EC2 instancias en AWS. AMS exige que AMIs se utilice esa especificación para los recursos administrados por AMS. Los tipos de cambio para crear EC2 instancias y grupos de EC2 Auto Scaling requieren que especifique una AMI para que AMS la utilice como base para las instancias que crea el tipo de cambio. AMS recomienda que seleccione siempre la AMI más reciente que esté disponible para usted.

Para obtener más información AWS AMIs, consulte [Diseño de AWS AMI](#).

Al crear una EC2 pila de Amazon o un grupo de Amazon EC2 Auto Scaling para su cuenta de AMS, debe especificar una AMI de Amild. Está limitado a AMIs empezar por «cliente-» y le recomendamos que elija siempre la AMI más reciente.

Para encontrar la AMI más reciente de su cuenta, puede realizar una búsqueda con un comando de CLI de AMS SKMS o utilizar la página de detalles de la consola de AMS para ver la VPC correspondiente:

- Utilice la consola AMS: AMIs las disponibles aparecen en la página AMI de la consola AMS. Seleccione uno AMIs de los nombres que comiencen por «customer-».
- Utilice la API/CLI ListAmis operación AMS SKMS.

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 aws-cli-command --region=us-east-1`

Este es un ejemplo de CLI con una query opción que restringe los resultados al cliente AMIs:

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --output table
```

En este ejemplo, se usa la `filter` opción con la query opción de buscar Windows AMIs que comiencen por «cliente»:

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows --output table
```

- 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](#).

Buscar grupo de seguridad (SG) IDs, AMS

La EC2 creación y la OpenSearch creación de dominios de Amazon CTs requieren un ID de grupo de seguridad. Esto aparecerá en el formulario `sg-02ce123456e7893c7`. Su cuenta tiene al menos dos grupos de seguridad predeterminados; consulte [Grupos de seguridad](#). Además, es posible que tenga grupos de seguridad que haya creado para fines específicos. Para descubrir sus grupos de seguridad:

- Consola de AWS: utilice la consola EC2 o la consola de VPC para ver todos los grupos de seguridad de la VPC seleccionada.
- API/CLI (al iniciar sesión en su cuenta AMS):

Enumere sus grupos de seguridad:

```
aws ec2 describe-security-groups
```

Encuentre entidades de IAM en AMS

Su cuenta tiene funciones y políticas de IAM predeterminadas; consulte [Función de usuario de IAM en AMS](#) los perfiles de instancia de IAM predeterminados; consulte [EC2 Perfil de instancia de IAM](#) las políticas predeterminadas. Para descubrir sus funciones y políticas de IAM:

- Consola: utilice la consola de IAM para ver todas las políticas y funciones de IAM de su cuenta.
- API/CLI (al iniciar sesión en su cuenta AMS):

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`

Haz una lista de tus funciones:

```
aws --profile saml iam list-roles
```

Enumere sus políticas:

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

Encuentra una pila IDs en AMS

Para encontrar un Stack ID, puedes usar la EC2 consola Amazon, la consola AMS o la API/CLI AMS SKMS.

Consola AMS:

- En el panel de navegación, seleccione y RFCs, a continuación, haga clic en el RFC que creó la pila. Utilice la opción de filtro de la parte superior para reducir la lista. Se abre la página de detalles del RFC e incluye el resultado de la ejecución con el ID de pila.
- Como alternativa, puede seleccionar Pilas en el panel de navegación para abrir la página de lista de pilas y, a continuación, recorrer la lista de pilas hasta encontrar la pila que le interese. Este método es más útil si conoces el tema de la pila que estás buscando.

EC2 Consola Amazon:

En el panel de navegación, seleccione Instances o Load Balancers o Auto Scaling Groups.

API ListStackSummaries o CLI de AMS SKMS:

 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 ver una lista de las pilas de la cuenta corriente, ejecute la ListStackSummaries operación de la API SKMS (CLI: `list-stack-summaries`). Para obtener información completa sobre una instancia de pila en particular StackId, ejecute. GetStack

- En los ejemplos siguientes, el primer comando solicita una lista de resúmenes de todas las instancias de pila de la cuenta. El segundo comando solicita la lista de instancias de pila, con un filtro de consulta para mostrar solo las de una plantilla de pila específica, y muestra los valores VpcId, Name y StackId.

```
aws amsskms list-stack-summaries --output table
```

```
-----
|                               ListStackSummaries                               |
|                               StackSummaries                                |
+-----+-----+-----+-----+
| VpcId | StackId | StackTemplateId | Name |
+-----+-----+-----+-----+
| vpc-0123abcd | stack-1fb7fe2212345678 | stm-sdhopvbb123456789 | Test ELB |
| vpc-0123abcd | stack-8323cc0e12345678 | stm-s2b72beb123456789 | S3 store |
| vpc-0123abcd | stack-2309fa0712345678 | stm-sdhopvbb123456789 | ELB      |
| vpc-0123abcd | stack-5e61a70512345678 | stm-sdpabqbb123456789 | PatchSim |
| vpc-0123abcd | stack-bd0e080d12345678 | stm-s2b72beb123456789 | CLI demo |
+-----+-----+-----+-----+
```

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](#).

Note

Para obtener información sobre el uso de la instancia IDs para el acceso, consulte también [Acceso a las instancias mediante bastiones](#).

Busque direcciones IP IDs o de instancia en AMS

- Para solicitar acceso a una instancia, iniciar sesión en una instancia o crear una AMI, debe tener el ID de la instancia. En el caso de una EC2 instancia (ya sea una instancia independiente o una parte de una pila) o de 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-s6xvs0000000000000",
"CreatedTime": "1486584508416",
"Name": "Amazon"
}
```

Encuentra nombres de recursos de Amazon (ARNs) en AMS

Un nombre de recurso de Amazon (ARN) es una cadena que identifica de forma exclusiva un AWS recurso, como EC2 instancias, buckets de S3, cuentas, funciones de Lambda, etc. AWS requiere un ARN cuando se quiere especificar un recurso de forma inequívoca en todos los ámbitos, por ejemplo AWS, en las políticas de IAM, las etiquetas de Amazon Relational Database Service (Amazon RDS) y las llamadas a la API. ARNs se crean a partir de identificadores que especifican el servicio, la región, la cuenta y otra información. Existen tres formatos de ARN:

```
arn:aws:service:region:account-id:resource-id
arn:aws:service:region:account-id:resource-type/resource-id
arn:aws:service:region:account-id:resource-type:resource-id
```

Note

El formato exacto de un ARN depende del tipo de servicio y recurso. [Para obtener más información ARNs, consulte Nombres de recursos de Amazon \(ARNs\) y Espacios de nombres de AWS servicios y formatos ARN.](#)

Para ver ejemplos de formato ARN por recurso, consulte la tabla de [tipos de recursos de referencia de autorización de AWS](#) servicio.

Encontrar el ARN de un objeto de AWS puede resultar difícil. Estas son tres formas de intentarlo:

- Consola de servicios de AWS: vaya a la consola de servicios de AWS correspondiente, localice el recurso y busque el ARN en los detalles del recurso.
- AWS API/CLI (primero debe instalar la CLI de AWS): busque el servicio correspondiente en la [AWS CLI Command Reference](#) y, a continuación, según el servicio de AWS, busque la operación correspondiente describe, por ejemplo `get`, o, etc. Por ejemplo, para todos los roles, políticas y usuarios de IAM, puede obtener el ARN en el resultado de la CLI con:

```
aws iam get-role --role-name EMR_DefaultRole
```

- Cree el ARN en función del formato correspondiente: busque el formato ARN del recurso consultando la página [Acciones, recursos y claves de condición de los servicios de AWS, busque el servicio correspondiente y](#), a continuación, la acción correspondiente, y profundice en el formato ARN del recurso. Una vez que tenga el formato, sustituya las variables por la configuración correspondiente.

Puede crear el ARN usted mismo siguiendo el formato apropiado (los formatos cambian según el tipo de servicio y recurso) y rellenando la información. Estos son algunos ejemplos de ARN:

- Un Cuenta de AWS ARN tiene la siguiente sintaxis:

```
arn:aws:iam::ACCOUNT-ID:root
```

- Un ARN de S3 tiene una jerarquía plana de depósitos y objetos asociados:

```
arn:aws:s3:::ams-bucket
```

- Un EC2 ARN tiene subtipos de recursos, como imagen, grupos de seguridad, instancia, etc. Este ejemplo incluye el ID de la instancia al final:

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Un ARN de Lambda tiene el nombre de la función para la parte del identificador del recurso y es posible que deba incluir el número de versión al final, como se muestra en este ejemplo:

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```

El AWS Key Management Service servicio proporciona la siguiente información: [Búsqueda del ID de clave y el ARN de clave](#).

[Para encontrar el ARN de una tabla de DynamoDB, utilice la CLI de tablas de descripción de DynamoDB](#).

Para obtener información ajena a la búsqueda AWS ARNs, consulte [AWS ARN Explained: Amazon Resource Name Guide](#).

Encuentre recursos por ARN en AMS

Los nombres de recursos de Amazon (ARNs) identifican AWS los recursos de forma exclusiva. [Para obtener información sobre ARNs los formatos de ARN, consulte Nombres de recursos de Amazon \(ARNs\) y Espacios de nombres de AWS servicios y formatos de ARN](#).

Note

Para obtener detalles sobre un recurso a partir de su ARN, debe tener acceso a la cuenta que creó el recurso.

No existe una ruta directa AWS para buscar todos los detalles de los recursos en el ARN del recurso, ya que los servicios tienen varios tipos de recursos con información relacionada diferente. Si tiene el ARN de un recurso, puede determinar:

- El AWS servicio relacionado (el tercer segmento de ARN) le indica qué consola de AWS debe buscar para encontrar el recurso
- El ID del recurso (el sexto o séptimo segmento del ARN) confirma que ha encontrado el recurso correcto

O bien, puede buscar los comandos de AWS CLI disponibles para ese servicio en la [Referencia de comandos de AWS CLI](#) para obtener información sobre cómo obtener detalles sobre el recurso.

Por ejemplo, a partir del siguiente ARN, puede determinar si el servicio es `lambda`, la cuenta es `123456789012`, el tipo de recurso es `function` y el nombre de la función es `TestFunction`.

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

A partir de ahí, puede revisar la [documentación de la AWS CLI del servicio Lambda](#) para saber cómo se pueden recuperar más detalles con varios comandos, como `get-function` y `get-function-configuration`.

Por ejemplo, puede usar los siguientes comandos para obtener más información sobre una función Lambda si tiene su nombre o ARN:

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

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 Backup](#) servicio 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](#).

Gestión de acceso en AMS

Aprenda cómo acceder a los recursos mediante SSH, o protocolo de escritorio remoto (RDP), y cómo usar los bastiones.

El sistema de administración de acceso de AWS Managed Services (AMS) se configura durante la incorporación. Solo los usuarios con el rol de usuario de IAM de AMS, federados a través de AMS, pueden acceder a los recursos de AMS de la cuenta.

Además de la confianza federada, que se describe a continuación, los grupos de seguridad de AMS son un elemento importante en el acceso a las aplicaciones públicas y privadas. Para obtener información sobre los grupos de seguridad de AMS y cómo cambiarlos, consulte [Grupos de seguridad](#).

Temas

- [¿Qué es la gestión de acceso?](#)
- [Cómo y cuándo usar la cuenta de usuario root en AMS](#)
- [Consola AMS Advanced y EC2 acceso a Amazon](#)
- [Acceso a la consola AWS de administración y a la consola AMS](#)
- [Acceso a las instancias mediante bastiones](#)

¿Qué es la gestión de acceso?

La administración del acceso es la forma en que AMS protege sus recursos al permitir solo el acceso autorizado y autenticado. AMS utiliza un perfil de instancia y un rol de usuario de IAM predeterminados, así como una autenticación multifactorial, grupos de seguridad, nombres de bastiones compatibles con el DNS, etc., para mantener sus recursos protegidos.

AMS se centra en tres tipos de acceso que requieren administración:

- **Acceso a la consola:** al aprovechar la federación, los usuarios de Active Directory de la cuenta pueden acceder a la consola mediante el inicio de sesión único (SSO). Si ha configurado la autenticación multifactor para estas cuentas, puede seguir necesitando MFA para acceder a la consola.
- **Acceso a las instancias con RDP o SSH:** al aprovechar la confianza de Active Directory, los usuarios del Active Directory existente de la cuenta pueden solicitar acceso a una instancia

y, después, autenticarse correctamente en un bastión y en la instancia con sus credenciales corporativas existentes. Si tienes configurada la autenticación multifactor para esas cuentas, puedes seguir requiriendo la MFA para solicitar el acceso a una instancia. AMS utiliza una solución de MFA propia para restringir el acceso de los ingenieros de AMS a las instancias.

- Acceso a las aplicaciones: varía según el caso de uso.

Temas

- [Por qué y cuándo AMS accede a tu cuenta](#)

Por qué y cuándo AMS accede a tu cuenta

AWS Managed Services (AMS) administra la infraestructura de AWS y, en ocasiones, por motivos específicos, los operadores y administradores de AMS acceden a su cuenta. Estos eventos de acceso se documentan en sus registros AWS CloudTrail (CloudTrail).

En los siguientes temas se explica por qué, cuándo y cómo AMS accede a su cuenta.

Activadores de acceso a la cuenta de cliente de AMS

La actividad de acceso a la cuenta de los clientes de AMS depende de factores desencadenantes. Los factores desencadenantes actuales son los AWS tickets creados en nuestro sistema de gestión de problemas en respuesta a las alarmas y eventos de Amazon CloudWatch (CloudWatch), y los informes de incidentes o las solicitudes de servicio que envíes. Se pueden realizar varias llamadas de servicio y actividades a nivel de anfitrión para cada acceso.

La justificación del acceso, los activadores y el iniciador del disparador se muestran en la siguiente tabla.

Activadores de acceso

Acceso	Initiator	Desencadenador
Aplicación de parches	AMS	Problema con el parche
Implementaciones de infraestructura	AMS	Problema de despliegue
Investigación de problemas internos	AMS	Problema problemático (un problema que se ha identificado como sistémico)

Acceso	Initiator	Desencadenador
Investigación y solución de alertas	AMS	Elementos de trabajo operativos (SSM OpsItems) de AWS Systems Manager
Ejecución manual de RFC	Usted	Problema con la solicitud de cambio (RFC). (Los sistemas no automatizados RFCs pueden requerir el acceso de AMS a sus recursos)
Investigación y solución de incidentes	Usted	Caso de soporte entrante (una solicitud de servicio o incidente que envíes)
Cumplimiento de una solicitud de servicio entrante	Usted	

Funciones de IAM para el acceso a la cuenta de los clientes de AMS

Cuando se activa, AMS accede a las cuentas de los clientes mediante funciones AWS Identity and Access Management (IAM). Como ocurre con toda la actividad de su cuenta, se registran los roles y su uso. CloudTrail



Important

No modifique ni elimine estas funciones.

Funciones de IAM para el acceso de AMS a las cuentas de los clientes

Nombre de función	Tipo de cuenta (SALZ, MALZ Management, MALZ Application, etc.)	Descripción
ams-service-admin	SALZ, MALZ	AMS Service automatiza el acceso y los despliegues de infraestructura automatizados,

Nombre de función	Tipo de cuenta (SALZ, MALZ Management, MALZ Applicati on, etc.)	Descripción
		por ejemplo, Patch, Backup o Automated Remediation.
ams-application-infra-read-solo	SALZ, aplicación MALZ, aplicación MALZ Tools-apl icación	Acceso de solo lectura por parte del operador
ams-application-infra-operations		Acceso del operador para incidents/service las solicitudes
ams-application-infra-admin		Acceso de administrador de AD
ams-primary-read-only	Administración de MALZ	Acceso de solo lectura por parte del operador
ams-primary-operations		Acceso del operador para incidents/service las solicitudes
ams-primary-admin		Acceso de administrador de AD
ams-logging-read-only	Registro de MALZ	Acceso de solo lectura por parte del operador
ams-logging-operations		Acceso del operador para incidents/service las solicitudes
ams-logging-admin		Acceso de administrador de AD
ams-networking-read-only	MALZ Networkin g	Acceso de solo lectura por parte del operador
ams-networking-operations		Acceso del operador para incidents/service las solicitudes
ams-networking-admin		Acceso de administrador de AD

Nombre de función	Tipo de cuenta (SALZ, MALZ Management, MALZ Applicati on, etc.)	Descripción
ams-shared-services-read-solo	Servicios compartidos MALZ	Acceso de solo lectura por parte del operador
ams-shared-services-operations		Acceso del operador para incidents/service las solicitudes
ams-shared-services-admin		Acceso de administrador de AD
ams-security-read-only	Seguridad MALZ	Acceso de solo lectura por parte del operador
ams-security-operations		Acceso del operador para incidents/service las solicitudes
ams-security-admin		Acceso de administrador de AD
ams-access-security-analyst	SALZ, aplicación MALZ, aplicación MALZ Tools-Aplicación, MALZ Core	Acceso a AMS Security
ams-access-security-analyst-de solo lectura		AMS Security, acceso de solo lectura
Sentinel_ _Role_ 0 AdminUser MBhE PXHaz RQadu PVc CDc	SALSA	[BreakGlassRole] Se utiliza para introducir Glass en las cuentas de los clientes
PowerUserSentinel_ _Role_ S0 0 wZuPu ROOI IazDb RI9	SAL, MALTA	Acceso de usuarios avanzados a las cuentas de los clientes para la ejecución de RFC
Sentinel_ _Role_PD4 L6RW9RD0InLKD5 ReadOnlyUser JOo		ReadOnly acceso a las cuentas de los clientes para la ejecución de la RFC

Nombre de función	Tipo de cuenta (SALZ, MALZ Management, MALZ Applicati on, etc.)	Descripción
ams_admin_role		Acceso de administrador a las cuentas de los clientes para ejecutar el RFC
AWSManagedServices_Provisioning_CustomerStacksRole		Se utiliza para lanzar y actualizar las pilas de CFN en nombre de los clientes a través de Ingest CloudFormation
customer_ssm_automation_role		Las ejecuciones de CT transfieren el rol a SSM Automation para la ejecución del runbook
ams_ssm_automation_role	SALZ, aplicación MALZ, código MALZ	Los servicios de AMS transfirieron la función a SSM Automation para la ejecución del manual
ams_ssm_iam_deployment_role	Aplicación MALZ	Función utilizada por el catálogo de IAM
ams_ssm_shared_services_intermediary_role	Servicios compartidos MALZ	Función utilizada por la aplicación ams_ssm_automation_role para ejecutar documentos SSM específicos en la cuenta de Shared Services
AmsOpsCenterRole		Se utiliza para crear y actualizar cuentas OpsItems de clientes
AMSOpsItemAutoExecutionRole	SAL, MALA	Se utiliza para obtener documentos SSM, describir etiquetas de recursos OpsItems, actualizar e iniciar la automatización
customer-mc-ec	Perfil de 2 instancias	Perfil de EC2 instancia de cliente predeterminado (rol)

¿Solicita acceso a la instancia

Para acceder a un recurso, primero debe enviar una solicitud de cambio (RFC) para ese acceso. Hay dos tipos de acceso que puede solicitar: de administrador (permisos de lectura/escritura) y de solo lectura (acceso de usuario estándar). De forma predeterminada, el acceso dura ocho horas. Esta información es obligatoria:

- ID de pila, o conjunto de pilas IDs, de la instancia o instancias a las que quieres acceder.
- El nombre de dominio completo de su dominio de confianza en AMS.
- El nombre de usuario de Active Directory de la persona que quiere acceder.
- El ID de la VPC en la que se encuentran las pilas a las que desea acceder.

Una vez que se te haya concedido el acceso, puedes actualizar la solicitud según sea necesario.

Para ver ejemplos de cómo solicitar acceso, consulta [Stack Admin Access | Grant](#) o [Stack Read-only Access | Grant](#).

Cómo y cuándo usar la cuenta de usuario root en AMS

El [usuario raíz](#) es el superusuario de su AWS cuenta. AMS monitorea el uso de root. Le recomendamos que utilice root solo para las pocas tareas que lo requieran, por ejemplo: cambiar la configuración de la cuenta, activar el acceso AWS Identity and Access Management (IAM) a la facturación y la gestión de costes, cambiar la contraseña raíz y habilitar la autenticación multifactor (MFA). Consulte [las tareas que requieren credenciales de usuario raíz](#) en la Guía del AWS Identity and Access Management usuario.

Note

La MFA se habilita durante la incorporación de AMS Advanced para impedir específicamente el acceso de los usuarios root. El acceso root en las cuentas gestionadas por AMS es diferente al de otras AWS cuentas y es fundamental para la seguridad de todo el entorno gestionado por AMS. La MFA configurada es una MFA virtual y se realiza mediante un dispositivo propiedad de AMS. Una vez que el MFA virtual se configura con la ayuda de AMS, el token virtual se elimina inmediatamente. Esto garantiza que ni usted ni AMS conserven la capacidad de iniciar sesión en la cuenta como usuario root. El inicio de sesión root solo se puede volver a habilitar en caso de solicitudes especiales (se explica a continuación) y AMS espera que dichos accesos solo se utilicen cuando sea absolutamente

necesario. Para obtener información sobre la MFA, consulte [Proteger una cuenta nueva con autenticación multifactor](#).

El acceso root siempre desencadena una respuesta del equipo de seguridad y operaciones de AMS. AMS supervisa las llamadas a la API para detectar el acceso root y, si se detecta dicho acceso, se activan alarmas.

La solicitud de acceso raíz es ligeramente diferente entre los distintos tipos de cuentas de AMS.

Acceso root con la zona de landing de cuenta única AMS Advanced:

Si tienes una landing zone con una sola cuenta, ponte en contacto con tu administrador de entrega de servicios en la nube (CSDM) y con los arquitectos de la nube (CAs) para que les informen sobre el trabajo de acceso raíz que necesitas. Lo mejor es avisar con veinticuatro horas de antelación a la actividad propuesta.

Acceso root con la zona de aterrizaje multicuenta AMS Advanced:

Para las cuentas multicuenta de aplicaciones, servicios compartidos, seguridad o redes de landing zone, utilice el tipo de cambio Management | Other | Other (ct-1e1xtak34nx76). Incluya la fecha, la hora y el propósito del uso de las credenciales del usuario raíz y programe la RFC para asegurarse de avisar con veinticuatro horas de antelación a la actividad propuesta. Usa tu cuenta de Landing Zone Management multicuenta para enviar la RFC.

Además, póngase en contacto con su CSDM y con CAs veinticuatro horas de antelación para informarle sobre el trabajo de acceso root que necesita.

Respuesta de seguridad y operaciones de AMS al uso de root:

AMS recibe una alarma cuando se utiliza la cuenta de usuario raíz. Si el uso de las credenciales raíz no está programado, se ponen en contacto con el equipo de seguridad de AMS y con el equipo de su cuenta para comprobar si se trata de una actividad esperada. Si no es una actividad prevista, AMS trabaja con su equipo de seguridad para investigar el problema.

Consola AMS Advanced y EC2 acceso a Amazon

Acceder a la consola AMS Advanced.

Acceder a tus EC2 instancias de Amazon.

Envíe la solicitud de acceso:

Iniciar sesión en sus EC2 instancias de AMS Amazon:

Acceso a la consola AWS de administración y a la consola AMS

Durante la incorporación, se le proporciona un inicio de sesión en la consola de AWS administración (con privilegios limitados: puede escribir en la consola AMS y en algunos campos de la página de información del cliente). Para acceder a la consola AMS, seleccione el enlace Managed Services en la consola AWS de administración. Las credenciales de acceso federado o compartidas (nombre de usuario/contraseña) se preparan según lo acordado con el equipo de administración de TI. Para seguir creando cuentas o grupos, envíe una solicitud de servicio a AMS.

Para obtener información sobre cómo acceder a la consola AWS de administración, consulte [Trabajar con la consola AWS de administración](#).

Para obtener algunos consejos sobre el uso de la consola AMS, consulte [Uso de la consola AMS](#).

Acceso temporal a la consola AMS

Si aún no ha configurado un proveedor de identidad (por ejemplo, SAML) para autenticarse en AMS, puede obtener acceso temporal a la consola AMS. Póngase en contacto con su CSDM para que envíe en su nombre una solicitud de cambio de implementación | Advanced stack components | Identity and Access Management (IAM) | Cree una solicitud de cambio de entidad o política (ct-3dpg8mdd9jn1r) con los siguientes valores:

- **UserName:** un nombre para la entidad de usuario de IAM que está creando
- **AccessType:** «Acceso a la consola»
- **UserPermissions:** «Acceso temporal a la consola AMS para **USERNAME** (la persona a la que quieres tener acceso temporal)»
- **Notificaciones por correo electrónico:** tu dirección de correo electrónico, para que puedas aprobar la solicitud cuando AMS te lo pida

 Note

Este RFC para el acceso temporal a la consola AMS requiere una revisión de seguridad y la aceptación tanto del equipo de seguridad interno como de AMS Global Security.

Una vez que se haya completado esta solicitud y puedas iniciar sesión, tendrás que aprobar la RFC que se creó, realizar un seguimiento de la aprobación y permitir que el equipo de AMS cierre el trabajo. Para aprobar la RFC, búscala en la página de lista de la RFC (junto a ella aparecerá una marca de pendiente de aprobación), selecciónela para abrir la página de detalles de la RFC correspondiente a esa RFC y, a continuación, elija Aprobar. Tenga en cuenta que no podrá utilizar AMS hasta que se apruebe la RFC.

Cuando la RFC se complete correctamente, las operaciones de AMS le proporcionarán el nuevo usuario de IAM y una contraseña. A continuación, siga estos pasos:

1. Ve a la consola AWS de administración e inicia sesión con las credenciales proporcionadas. Se te pedirá que crees una contraseña nueva. Al iniciar sesión, también debe configurar la autenticación multifactor (MFA); para obtener más información sobre cómo hacerlo, [consulte Uso de la autenticación multifactor \(MFA\)](#) en AWS.
2. En la consola AWS de administración, cambie a la función de IAM proporcionada ().
`customer_CustomerCode_readonly_user_role`
3. Abra la consola AMS Managed Services.

 Note

El acceso temporal se establece de forma predeterminada en sesenta días; sin embargo, puede solicitar una prórroga de treinta días poniéndose en contacto con su CSDM.

Acceso a las instancias mediante bastiones

Todo el acceso a los recursos de las cuentas administradas por AMS, tanto para los clientes como para los operadores de AMS, está restringido mediante el uso de hosts Bastion. Mantenemos bastiones RDP para Linux y Windows para el acceso a las cuentas AMS Advanced de zonas de aterrizaje multicuenta (MALZ) y zonas de aterrizaje de cuentas únicas (SALZ).

Solo se puede acceder a tus bastiones a través de tu conexión privada (VPN o DX). AWS Direct Connect Además de utilizar firewalls para evitar el tráfico entrante, los bastiones se reabastecen periódicamente (con las credenciales existentes) según un horario fijo.

 Note

Para obtener información sobre cómo mover archivos a una EC2 instancia, consulta [Transferencia de archivos: Windows local o MAC PC a Linux Amazon EC2](#).

MALZ

Para acceder a las instancias de su cuenta, inicie sesión en una instancia de bastión con sus credenciales de Active Directory (AD). Amazon usa bastiones ubicados en la red perimetral VPC (cuenta de red), y usted usa los bastiones de sus clientes, ubicados en la subred de Bastiones de clientes de la cuenta de servicios compartidos.

Cuando su entorno AMS esté incorporado inicialmente, dispondrá de dos bastiones de SSH y dos de RDP, según su elección.

SALZ

Para acceder a las instancias de su cuenta, inicie sesión en una instancia de bastión con sus credenciales de Active Directory (AD). AMS usa bastiones ubicados en las subredes de la red perimetral y usted usa bastiones ubicados en sus subredes privadas.

Cuando su cuenta está incorporada inicialmente, tiene dos bastiones de RDP y dos de SSH de forma predeterminada.

 Note

Como parte de la zona de aterrizaje de una sola cuenta, AMS proporciona bastiones RDP (Windows) y SSH (Linux) para acceder a tus pilas; sin embargo, puedes elegir si quieres solo bastiones RDP o solo bastiones SSH. Para solicitar que solo se mantengan los bastiones de RDP o de SSH, envíe una solicitud de servicio.

Para acceder a una instancia, necesita:

- Acceso concedido a la pila. Para obtener acceso a una pila, consulta [Stack Admin Access | Grant](#) o [Stack Read-Only Access | Grant](#).

- El ID de pila al que quieres acceder para poder acceder a la instancia. Para encontrar un ID de pila, consulta [Encuentra una pila IDs en AMS](#).
- La IP de la instancia a la que quieres acceder. Para buscar la IP de una instancia, consulte [Busque direcciones IP IDs o de instancia en AMS](#).
- El nombre del bastión compatible con DNS o la IP del bastión. A continuación se describe cómo utilizar nombres de bastiones compatibles con DNS y cómo encontrar una IP de bastión.

Nombres de bastiones compatibles con DNS

AWS Managed Services (AMS) utiliza nombres de bastión 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 AMI de bastión nueva, 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 RDP (Windows), utilice registros DNS como estos:
`rdp-Username.Your_Domain.com`

Por ejemplo, si el nombre de usuario es `alex`, `test` o `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 AMI de bastión nueva, 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).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).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`

Ahorro de costes en los bastiones de las zonas de landing zone con una sola cuenta (SALZ)

AMS proporciona dos bastiones SSH y dos bastiones RDP en la configuración predeterminada para que pueda conectarse a sus EC2 instancias de Amazon, y también despliega dos bastiones DMZ en la configuración predeterminada para las operaciones de servicio. Los bastiones utilizan EC2 instancias Amazon de un metro de tamaño predeterminado. Tiene la opción de cambiar las EC2 instancias de Amazon utilizadas para los bastiones a t3.small y ahorrar costes.

Si utiliza instancias bajo demanda, instancias puntuales o un plan de ahorro, debería considerar esta función y ahorrar costes. Si usa instancias reservadas, considere si el uso de instancias t3.small podría reducir sus costos. Para cambiar el tipo de instancia, envíe una RFC a Management | Advanced stack components | EC2 instance stack | Resize (ct-15mazjj88xc69) CT desde su cuenta de AMS.

Ponte en contacto con tu administrador de prestación de servicios en la nube (CSDM) si tienes más preguntas o para comprobar si puedes aprovechar esta función.

Uso de direcciones IP de bastión

Los clientes de AMS pueden usar bastiones SSH y RDP, ya sea 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.

Ejemplos de acceso a instancias en AMS

Estos ejemplos muestran cómo iniciar sesión en una instancia de su cuenta de AMS mediante un bastión después de que se le haya concedido el acceso mediante una RFC. Para obtener información sobre cómo obtener la concesión del acceso, consulte. [¿Solicita acceso a la instancia](#)

Note

Para obtener información sobre cómo mover archivos a una EC2 instancia, consulta [Transferencia de archivos: Windows local o MAC PC a Linux Amazon EC2](#).

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. [Uso de direcciones IP de bastión](#)

Note

Una EC2 instancia de Amazon creada a través de un grupo de Amazon EC2 Auto Scaling tendrá una dirección IP que entrará y saldrá y tendrá que usar la EC2 consola de Amazon para encontrar esa dirección IP.

- Nombre de usuario (por ejemplo `DOMAIN_FQDN\USERNAME`) y contraseña: credenciales de la cuenta. `USERNAME` Debe ser su nombre de usuario de Active Directory.

Tenga en cuenta que se puede utilizar un nombre de usuario con el formato `username@customerdomain.com`, pero esto puede causar problemas con la configuración de PBIS.

- Dirección IP de la pila: para encontrarla, consulta el resultado de la ejecución del RFC que has enviado para lanzar la pila o busca la dirección IP de la EC2 instancia de Amazon en la EC2 consola de Amazon. Para una sola EC2 instancia de Amazon, también puedes usar el comando `AMS SKMS ListStackSummaries` para buscar el ID de la pila y, `GetStack` a continuación, buscar la dirección IP de la pila. Para ver la referencia de la API AMS SKMS, consulte la pestaña Informes de AWS Artifact Console.

Acceda a la dirección IP del bastión, ya sea SSH o RDP, según corresponda, e inicie sesión mediante uno de los siguientes procedimientos.

 Note

Los bastiones RDP solo permiten dos conexiones simultáneas. Por lo tanto, en el mejor de los casos, solo 4 administradores pueden conectarse a Windows Stacks al mismo tiempo. Si necesita más conexiones para RDP, consulte las [opciones de AMS Bastion durante la migración o la incorporación de aplicaciones en la guía de incorporación de AMS](#).

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_instances` 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).AMSAccountNumber.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).AMSAccountNumber.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_instances` 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 Windows Remote Desktop Connection para conectarse a una instancia de Windows desde un ordenador Windows.

MALZ

Para obtener más información sobre los nombres amigables de los bastiones, consulte [Nombres 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. Abra 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, consulte [Nombres 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).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. Abra 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).AMSAccountNumber.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
```

Control de acceso basado en equipos o roles en una cuenta AMS

Escenario: dos equipos de aplicaciones, A y B, utilizan una sola cuenta AMS para sus aplicaciones «AA» y «BB», respectivamente. El equipo A solo quiere acceder a los recursos de la aplicación «AA» y el equipo B solo quiere acceder a los recursos de la aplicación «BB». ¿Cómo configuro eso?

Utilice las herramientas de su ITSM para implementar controles de acceso basados en equipos (TBAC). Por ejemplo, puede utilizar la aplicación AMS ServiceNow Connector para la integración con AMS. APIs Póngase en contacto con su CSDM para obtener orientación de alto nivel sobre esta implementación.

Configuración automatizada de instancias en AMS

Advanced

El servicio de configuración automática de instancias AMS Advanced se ejecuta a diario y analiza y actualiza automáticamente el SSM y CloudWatch los agentes y los archivos de configuración de las EC2 instancias gestionadas. Las actualizaciones se aplican, según sea necesario, a:

- SSM y agentes CloudWatch
- CloudWatch archivos de configuración

Estas actualizaciones permiten a AMS acceder a las EC2 instancias administradas por AMS y configurarlas para que emitan los [registros](#) y las métricas adecuados.

Temas

- [Requisitos previos para la configuración automatizada de instancias](#)
- [Instalación automática de SSM Agent](#)
- [Cambios automatizados](#)

Requisitos previos para la configuración automatizada de instancias

Los clientes de AMS Advanced que implementan instancias con Change Management deben cumplir los siguientes requisitos previos:

- El agente SSM está instalado y en un estado administrado.
- La instancia está etiquetada como instancia gestionada. (La `aws:cloudformation:stack-name` etiqueta tiene un valor que comienza por `stack-osc-`.)

Si el agente SSM aún no está instalado en la instancia, puede instalarlo mediante la función de instalación automática del agente SSM de AMS. Para obtener más información, consulte [Instalación automática de SSM Agent](#).

O bien, puede instalar el agente SSM manualmente. Para obtener más información, consulte los siguientes temas:

- Linux: [instale manualmente el agente SSM en EC2 instancias para Linux - AWS Systems Manager](#)
- Windows: [instale manualmente el agente SSM en EC2 las instancias de Windows Server - AWS Systems Manager](#)

Para obtener más información sobre el agente SSM, consulte la documentación de AWS [Cómo trabajar con el agente SSM](#).

Instalación automática de SSM Agent

Para que AMS administre sus instancias de Amazon Elastic Compute Cloud (Amazon EC2), debe instalar AWS Systems Manager SSM Agent en cada instancia. Si tus instancias no tienen instalado el Agente SSM, puedes usar la función de instalación automática del Agente SSM de AMS.

Note

- Esta función solo está disponible para EC2 instancias que no estén en un grupo de Auto Scaling y que ejecuten sistemas operativos Linux compatibles con AMS.
- La función de instalación automática del agente AMS SSM está deshabilitada de forma predeterminada. Para habilitarla, póngase en contacto con su CA o CSDM.

Requisitos previos para el uso del agente SSM

- Asegúrese de que el perfil de instancia asociado a las instancias de destino tenga una de las siguientes políticas (o permisos equivalentes a los permitidos que figuran en ellas):
 - Amazon SSMManged EC2 InstanceDefaultPolicy
 - Amazon SSMManged InstanceCore
- Asegúrese de que no haya una política de control de servicios en el AWS Organizations nivel que deniegue explícitamente los permisos enumerados en las políticas anteriores.

Para obtener más información, consulte [Configuración de permisos de instancia requeridos para Systems Manager](#).

- Para bloquear el tráfico saliente, asegúrese de que los siguientes puntos finales de la interfaz estén habilitados en la VPC en la que residen las instancias de destino (sustituya «región» en la URL según corresponda):

- `ssm.<region>.amazonaws.com`
- `ssmmessages.<region>.amazonaws.com`
- `mensajes ec2.<region>.amazonaws.com`

Para obtener más información, consulte [Mejorar la seguridad de las EC2 instancias mediante puntos de enlace de VPC para Systems Manager](#).

Para obtener consejos generales sobre cómo habilitar o solucionar problemas de la disponibilidad de los nodos gestionados, consulte la [Solución 2: Compruebe que se haya especificado un perfil de instancia de IAM para la instancia \(solo EC2 instancias\)](#).

Note

AMS detiene e inicia cada instancia como parte del proceso de instalación automática. Cuando se detiene una instancia, se pierden los datos almacenados en los volúmenes del almacén de instancias y los datos almacenados en la RAM. Para obtener más información, consulta [Qué ocurre cuando detienes una instancia](#).

Solicita la instalación automática del agente SSM en tus instancias

Si sus cuentas están integradas en AMS Accelerate Patch Add-On, configure una ventana de mantenimiento de parches (MW) para las instancias. Se necesita un agente SSM que funcione para completar el proceso de revisión. Si falta el agente SSM en una instancia, AMS intentará instalarlo automáticamente durante el período de mantenimiento del parche.

Note

AMS detiene e inicia cada instancia como parte del proceso de instalación automática. Cuando se detiene una instancia, se pierden los datos almacenados en los volúmenes del almacén de instancias y los datos almacenados en la RAM. Para obtener más información, consulta [Qué ocurre cuando detienes una instancia](#).

Cómo funciona la instalación automática de SSM Agent

AMS usa los datos EC2 del usuario para ejecutar el script de instalación en sus instancias. Para añadir el script de datos de usuario y ejecutarlo en las instancias, AMS debe detener e iniciar cada instancia.

Si la instancia ya tiene un script de datos de usuario existente, AMS completa los siguientes pasos durante el proceso de instalación automática:

1. Crea una copia de seguridad del script de datos de usuario existente.
2. Sustituye el script de datos de usuario existente por el script de instalación del agente SSM.
3. Reinicia la instancia para instalar el agente SSM.
4. Detiene la instancia y restaura el script original.
5. Reinicia la instancia con el script original.

Cambios automatizados

El servicio de configuración automática de instancias AMS Advanced realiza los cambios necesarios en sus EC2 instancias.

Qué cambios:

- [Actualice automáticamente el código en las instancias de Linux](#)
- [Actualice automáticamente PBIS en instancias de Linux](#)
- [Actualice automáticamente la versión mínima de SSM y CloudWatch de los agentes](#)
- [CloudWatch archivos de configuración, detalles de actualización](#)
- [Registros configurados automáticamente](#)

Actualice automáticamente el código en las instancias de Linux

AMS actualiza automáticamente el código de la instancia en las instancias de Linux. Esto ayuda a mejorar por completo la estabilidad operativa y la seguridad de los componentes y el entorno de AMS.

Preguntas frecuentes:

¿Qué incluye el código de instancia (OIC) en Linux?

El OIC incluye el paquete `ams-toolkit` junto con algunos archivos de configuración y tareas cron. Los AMS requieren estos archivos y paquetes para su integración (Active Directory y otras dependencias). CloudFormation Preconfiguramos estos archivos en los archivos proporcionados por AMS AMIs o los instalamos en su instancia durante la ingestión de la carga de trabajo.

¿Cuándo actualizará AMS el OIC?

AMS actualiza el OIC cuando lanzamos una nueva versión con correcciones de errores u otras mejoras. El flujo de trabajo para comprobar la versión y la actualización de la OIC se ejecuta a diario.

Actualice automáticamente PBIS en instancias de Linux

AMS usa el módulo Power Broker Identity Service (PBIS) para unir instancias de Linux a Active Directory administrado por AMS.

AMS actualiza automáticamente el PBIS en las instancias de Linux.

Preguntas frecuentes:

¿Cuándo actualizará AMS el PBIS?

AMS activa la actualización de PBIS al reiniciar el sistema. Si hay una nueva versión de PBIS disponible, AMS intentará instalarla durante el siguiente reinicio de la instancia.

¿Se puede desactivar la actualización de PBIS?

Puede desactivar la actualización de PBIS a nivel de instancia o cuenta:

- Nivel de cuenta: cree un parámetro en el almacén de parámetros del SSM: Nombre: `/ams/skip-pbis-update`, Valor: `true` (en cualquier caso).

Note

El perfil de la instancia debe tener permisos para leer los parámetros del SSM. Si falta el indicador, el comportamiento predeterminado es ejecutar la actualización.

- Nivel de instancia:

- Basado en etiquetas: agrega la siguiente etiqueta a la instancia: `Clave:skip_pbis_update`, `Valor: true` (en cualquier caso).
- Config file: añade la siguiente marca al `/opt/aws/ams/etc/ams.conf.d/state.ini` archivo: `skip_pbis_update = true`.

Note

La etiqueta tiene una prioridad más alta que el parámetro SSM. Puede desactivar la actualización del PBIS a nivel de cuenta a través del parámetro, pero puede activarla para una instancia única (o varias) añadiendo una `etiquetaKey:skip_pbis_update.Value:false`

Para configurar cualquiera de las opciones descritas, siga el proceso de administración de cambios estándar de su entorno AMS.

Actualice automáticamente la versión mínima de SSM y CloudWatch de los agentes

La versión mínima de AMS Advanced (del SSM o de CloudWatch los agentes) es la versión que ha sido probada por el equipo de servicio de AMS y aprobada previamente para su sistema operativo. Intentamos ser proactivos y utilizar la última versión estable y compatible, por lo que el número de versión cambia con el tiempo. Para encontrar la versión mínima actual, envíe una solicitud de servicio a AMS.

- Administración de agentes SSM

El agente Amazon SSM es responsable de ejecutar los comandos remotos en la instancia. La automatización de la configuración de la instancia garantiza que el agente SSM ejecute la versión mínima.

- Administración de agentes de Cloudwatch

El CloudWatch agente de Amazon es responsable de emitir los registros y las métricas del sistema operativo. La configuración automatizada de instancias realiza lo siguiente:

- Si es necesario, deshabilita el agente de CloudWatch registro antiguo y migra la configuración al nuevo agente unificado CloudWatch

- Si la instancia ejecuta el agente de CloudWatch registro heredado, la configuración automática de la instancia deshabilita el servicio de agente de CloudWatch registro antiguo y migra su configuración al agente unificado. CloudWatch
- Personaliza la CloudWatch configuración para emitir los registros y las métricas adecuados.

Archivos y directorios afectados:

- Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configuraciones\
- Linux
 - /opt/aws/amazon-cloudwatch-agent/etc/
 - /-cloudwatch-agent.d/ opt/aws/amazon-cloudwatch-agent/etc/amazon
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

CloudWatch archivos de configuración, detalles de actualización

Leemos CloudWatch las configuraciones personalizadas (solo en JSON) de los siguientes CloudWatch directorios (consulte [los directorios recomendados](#)) y las combinamos con la CloudWatch configuración AMS estándar:

- CloudWatch Archivos
 - En la instancia:
 - Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configuraciones\
 - %ProgramFiles%\ ModulesWindowsPowerShell\ AWSManaged Services.Logging.Utilities\ Files\ Config.json
 - Linux
 - opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon/-cloudwatch-agent.json
 - En Amazon S3:
 - Windows:
 - [https://ams-configuration-artifacts-*REGION_NAME*.s3.*REGION_NAME*.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json](https://ams-configuration-artifacts-<i>REGION_NAME</i>.s3.<i>REGION_NAME</i>.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json)
 - Linux:

- https://s3.amazonaws.com/ams-configuration-artifacts/REGION_NAME/REGION_NAME/configurations/cloudwatch/latest/linux-cloudwatch-config.json

Registros configurados automáticamente

Configuramos la instancia para que escriba los siguientes registros.

- Windows:
 - AmazonSSMAgentLog
 - AmazonCloudWatchAgentLog
 - AmazonSSErrorsLog
 - AmazonCloudFormationLog
 - ApplicationEventLog
 - EC2ConfigServiceEventLog
 - MicrosoftWindowsAppLockerEXEAndDLLEventRegistro
 - MicrosoftWindowsAppLockerMSIAndScriptEventLog
 - MicrosoftWindowsGroupPolicyOperationalEventLog
 - SecurityEventLog
 - SystemEventLog
- Linux:
 - /var/log/amazon/ssm/amazon-ssm-agent.log
 - /var/log/amazon/ssm/errors.log
 - /var/log/audit/audit
 - /var/log/cloud-init.log
 - /var/log/cron
 - /var/log/dpkg.log
 - /var/log/maillog
 - /var/log/messages
 - /var/log/secure
 - /var/log/spooler
 - /var/log/syslog

- `/.log var/log/yum`
- `/.log var/log/zypper`

Supervisión y gestión de eventos en AMS

Temas

- [¿Qué es la monitorización?](#)
- [¿Qué monitorea el sistema de monitoreo AMS?](#)
- [Cómo funciona la supervisión](#)
- [Visualización de la configuración de supervisión de una cuenta AMS](#)
- [Cambiar la configuración de supervisión de una cuenta AMS](#)
- [Notificaciones de incidentes compatibles con las aplicaciones en AMS](#)
- [OpsCenter Utilizándolo en AMS](#)
- [Notificaciones de alerta de AMS](#)
- [Creación de CloudWatch alarmas adicionales en AMS](#)
- [Creación de CloudWatch métricas y alarmas personalizadas en AMS](#)
- [Uso de CloudWatch Application Insights para .Net y SQL Server en AMS](#)
- [Uso de Amazon EventBridge Managed Rules en AMS](#)
- [Remediador de confianza en AMS](#)

El sistema de supervisión AWS Managed Services (AMS) supervisa los recursos de AMS para detectar errores, degradación del rendimiento y problemas de seguridad. El sistema de monitoreo AMS se basa en servicios de AWS como Amazon CloudWatch (CloudWatch), Amazon GuardDuty, Amazon Macie y AWS Health. Además del sistema de monitoreo, AMS también lo implementa TrendMicro DeepSecurity para protegerse contra el malware en las instancias de Amazon Elastic Compute Cloud (Amazon EC2). Para obtener información sobre los valores predeterminados de seguridad de puntos finales (EPS), consulte [Seguridad de terminales \(EPS\)](#).

La supervisión de AMS ofrece las siguientes ventajas:

- Una base de monitoreo para que tenga un nivel de protección predeterminado incluso si no configura ningún otro monitoreo para sus cuentas administradas. Para obtener información, consulte [Alertas del monitoreo de referencia en AMS](#).
- Alertas de investigación para determinar la acción adecuada. Por ejemplo, si GuardDuty encuentra actividad que indica intentos de fuerza bruta contra una EC2 instancia de Amazon, AMS analiza los registros de flujo de la VPC para comprender el origen y el contexto de la actividad.

- Corregir las alertas, siempre que sea posible, para evitar o reducir el impacto en sus aplicaciones. Por ejemplo, si utilizas una EC2 instancia de Amazon independiente y no pasa la comprobación del estado del sistema, AMS intentará recuperar la instancia deteniéndola y reiniciándola. Para obtener más información, consulte [Remediación automática de alertas por parte de AMS](#).
- Transparencia en el uso de alertas activas y previamente resueltas. OpsCenter Por ejemplo, si tiene un uso elevado e inesperado de la CPU en una EC2 instancia de Amazon, puede solicitar acceso a la consola de AWS Systems Manager (incluye el acceso a la OpsCenter consola) y verla OpsItem directamente en la OpsCenter consola.

¿Qué es la monitorización?

El sistema de monitoreo AMS monitorea sus AWS recursos para detectar fallas, degradación del rendimiento y problemas de seguridad. Como cuenta gestionada, AMS configura e implementa las alarmas para AWS los recursos aplicables, las monitorea y realiza las correcciones necesarias cuando es necesario.

El sistema de monitoreo AMS genera alertas en función de la configuración de monitoreo de su cuenta. La configuración de supervisión de una cuenta hace referencia a todos los parámetros de recursos de la cuenta que crean una alerta; para obtener información sobre los parámetros de los recursos, consulte [Alertas del monitoreo de referencia en AMS](#). La configuración de supervisión de una cuenta incluye las definiciones de CloudWatch alarma y las reglas de CloudWatch eventos que generan la alerta (alarma o evento).

La configuración de supervisión básica es el conjunto de definiciones de alarma ([Alertas del monitoreo de referencia en AMS](#)) seleccionadas por AMS para supervisar los recursos de la cuenta gestionada. La configuración de supervisión de una cuenta puede diferir de la configuración básica debido a los cambios que usted solicite.

Una notificación de fallos inminentes, continuos, decrecientes o potenciales, de una degradación del rendimiento o de problemas de seguridad generados por la supervisión básica configurada en una cuenta se denomina alerta. Algunos ejemplos de alertas son una CloudWatch alarma de Amazon, un CloudWatch evento de Amazon, un evento o un servicio de Finding de AWS GuardDuty, como Amazon, y un evento o alerta de Trend Micro Deep Security.

Las alertas de los servicios de AWS relacionados con la seguridad, como Amazon GuardDuty, Amazon Macie o Trend Micro Deep Security, se denominan alertas de seguridad para diferenciarlas de otros tipos de alertas.

La supervisión de AMS ofrece las siguientes ventajas:

- La capacidad de personalizar las alarmas de recursos de referencia para que se ajusten a sus necesidades.
- Solución automática de las alertas, siempre que sea posible, para evitar o reducir el impacto en sus aplicaciones. Por ejemplo, si utilizas una EC2 instancia de Amazon independiente y no pasa la comprobación de estado del sistema, AMS intentará recuperar la instancia deteniéndola y reiniciándola. Para obtener más información, consulte [Remediación automática de alertas por parte de AMS](#).
- Transparencia en el uso de alertas activas y previamente resueltas. OpsCenter Por ejemplo, si tienes un uso elevado e inesperado de la CPU en una EC2 instancia de Amazon, puedes solicitar acceso a la AWS Systems Manager consola (que incluye el acceso a la OpsCenter consola) y verla OpsItem directamente en la OpsCenter consola.
- Investigando las alertas para determinar las acciones adecuadas.
- Las alertas se generan en función de la configuración de su cuenta y de AWS los servicios compatibles. La configuración de supervisión de una cuenta hace referencia a todos los parámetros de recursos de la cuenta que crean una alerta. La configuración de supervisión de una cuenta incluye las definiciones de CloudWatch alarma y EventBridge (anteriormente CloudWatch denominadas eventos) que generan la alerta (alarma o evento). Para obtener más información sobre los parámetros de los recursos, consulte [Alertas del monitoreo de referencia en AMS](#).
- Notificación de fallos inminentes, continuos, inminentes o potenciales, de una degradación del rendimiento o de problemas de seguridad generados por la supervisión básica configurada en una cuenta (conocida como alerta). Entre los ejemplos de alertas se incluyen una CloudWatch alarma, un evento o un hallazgo de un servicio de AWS, como GuardDuty o AWS Health.

¿Qué monitorea el sistema de monitoreo AMS?

De acuerdo con el modelo de responsabilidad de servicios compartidos de AWS Managed Services (AMS), el sistema de monitoreo AMS supervisa la infraestructura de AWS. Para obtener información detallada sobre la supervisión de referencia en AMS, incluidos los recursos de AWS monitorizados y el tipo de alertas de cada recurso, consulte [Alertas del monitoreo de referencia en AMS](#). En el caso de EC2 las instancias de Amazon, AMS supervisa el sistema operativo y proporciona una supervisión básica basada en las métricas del sistema operativo, como el uso de la CPU y el uso del volumen raíz.

Recomendamos complementar la supervisión de AMS con una supervisión adicional mediante los servicios de AWS adaptados a su aplicación. [Para obtener orientación sobre la supervisión de la disponibilidad, consulte la sección «Supervisión y alarmas» de este documento técnico: el pilar de la fiabilidad.](#) Puede configurar su propio monitoreo para que se adapte a sus necesidades operativas; cómo hacerlo se explica en [Creación de CloudWatch alarmas adicionales en AMS](#) y [Creación de CloudWatch métricas y alarmas personalizadas en AMS](#)

Supervisión proactiva de la confianza de Active Directory en AMS en la zona de destino con una sola cuenta

AMS single-account landing zone (SALZ) supervisa el estado de las relaciones de confianza unidireccionales entre el Active Directory gestionado (AD) de su cuenta gestionada por AMS y el dominio de su empresa. La confianza unidireccional con Managed AD es fundamental para las solicitudes de acceso y las solicitudes de inicio de sesión de instancias. Con esta nueva supervisión, AMS ahora responde de forma proactiva a los problemas relacionados con la confianza y reduce el tiempo medio necesario para detectar los incidentes relacionados con el acceso.

Esta función se habilita automáticamente en sus cuentas de AWS Managed Services (AMS).

El impacto en los costos es pequeño. La función utiliza cuatro CloudWatch métricas de AWS y dos CloudWatch alarmas de AWS para una confianza.

Cómo funciona la supervisión

Consulte los siguientes gráficos sobre la arquitectura de supervisión en AWS Managed Services (AMS).

El siguiente diagrama proporciona una descripción general de alto nivel del flujo de trabajo de monitoreo de zonas de aterrizaje con múltiples cuentas de AMS y zonas de aterrizaje con una sola cuenta de AMS.

- **Generación:** en el momento de la incorporación de la cuenta, AMS configura la supervisión de referencia (una combinación de alarmas CloudWatch (CW) y reglas de eventos de CW) para todos los recursos creados en una cuenta gestionada. La configuración de supervisión básica genera una alerta cuando se activa una alarma de CW o se genera un evento de CW.
- **Agregación:**

- Zona de destino con varias cuentas: las alertas las generan los recursos de las cuentas de la aplicación y de la unidad organizativa principal y las envían al sistema de monitoreo AMS dirigiéndolas a través de la cuenta de seguridad.
- Zona de destino con una sola cuenta: todas las alertas generadas por tus recursos se envían al sistema de supervisión de AMS, dirigiéndolas a un tema de SNS de la cuenta.
- También puede configurar la forma en que AMS agrupa EC2 las alertas. AMS agrupa todas las alertas relacionadas con la misma EC2 instancia en un solo incidente o crea un incidente por alerta, según sus preferencias. Puede cambiar esta configuración en cualquier momento trabajando con su administrador de prestación de servicios en la nube o con un arquitecto de nube. Esto funciona de la misma manera tanto si utiliza una zona de destino con varias cuentas como con una zona de destino con una sola cuenta.
- Procesamiento: AMS analiza las alertas y las procesa en función de su potencial de impacto. Las alertas se procesan como se describe a continuación.
- Alertas con un impacto conocido en los clientes: conducen a la creación de un nuevo informe de incidentes y AMS sigue el proceso de gestión de incidentes; para obtener información sobre la gestión de incidentes, consulte [Respuesta a incidentes de AMS](#).

Ejemplo de alerta: una EC2 instancia de Amazon no pasa una comprobación de estado del sistema, AMS intenta recuperar la instancia deteniéndola y reiniciándola.

- Alertas con un impacto incierto en los clientes: en el caso de este tipo de alertas, AMS envía un informe del incidente y, en muchos casos, te pide que compruebes el impacto antes de que AMS tome medidas. Sin embargo, si se aprueban las comprobaciones relacionadas con la infraestructura, AMS no le enviará ningún informe del incidente.

Por ejemplo: una alerta de un uso superior al 85% de la CPU durante más de 10 minutos en una EC2 instancia de Amazon no se puede clasificar inmediatamente como incidente, ya que este comportamiento podría esperarse en función del uso. En este ejemplo, AMS Automation realiza comprobaciones relacionadas con la infraestructura del recurso. Si se aprueban esas comprobaciones, AMS no envía ninguna notificación de alerta, incluso si el uso de la CPU supera el 99%. Si Automation detecta que las comprobaciones relacionadas con la infraestructura están fallando en el recurso, AMS envía una notificación de alerta y comprueba si es necesaria una mitigación. Las notificaciones de alerta se analizan en detalle en esta sección. AMS ofrece opciones de mitigación en la notificación. Cuando respondes a la notificación confirmando que la alerta es un incidente, AMS crea un nuevo informe de incidente y comienza el proceso de gestión de incidentes de AMS. Las notificaciones de servicio que reciben una

respuesta que indica que «no afecta al cliente» o que no reciben respuesta alguna durante tres días se marcan como resueltas y la alerta correspondiente se marca como resuelta.

- Alertas sin impacto en el cliente: si, tras una evaluación, AMS determina que la alerta no afecta al cliente, se cierra.

Por ejemplo, AWS Health notifica que una EC2 instancia necesita ser reemplazada, pero esa instancia ha sido cancelada desde entonces.

EC2 notificaciones agrupadas por instancias

Puede configurar la supervisión de AMS para agrupar las alertas de la misma EC2 instancia en un solo incidente. Su administrador de prestación de servicios en la nube o su arquitecto de nube pueden configurarlo por usted. Hay cuatro parámetros que puede configurar para cada cuenta administrada por AMS.

1. Alcance: elija entre toda la cuenta o basado en etiquetas.

- Para especificar una configuración que se aplique a todas las EC2 instancias de esa cuenta, selecciona scope = account-wide.
- Para especificar una configuración que se aplique solo a EC2 las instancias de esa cuenta con una etiqueta específica, elige scope = tag-based.

2. Regla de agrupación: elija entre clásica o instancia.

- Para configurar la agrupación a nivel de instancia para todos los recursos de tu cuenta, elige ámbito = toda la cuenta y regla de agrupación = instancia.
- Para configurar recursos específicos de tu cuenta para que usen la agrupación a nivel de instancia, etiqueta esas instancias y, a continuación, elige ámbito = basado en etiquetas y regla de agrupación = nivel de instancia.
- Para no usar la agrupación de instancias para las alertas de tu cuenta, elige la regla de agrupación = clásica.

3. Opción de participación: elige entre ninguna, solo informar o predeterminada.

- Para que AMS no cree incidentes ni ejecute automatizaciones para las alarmas desde esos recursos mientras la configuración esté activa, no elija ninguna.
- Para que AMS no cree incidentes ni ejecute automatizaciones para las alarmas desde esos recursos mientras la configuración esté activa, ni ejecute la reparación automática de los documentos de Systems Manager, sino que incluya registros de estos eventos en los informes, elija solo informar. Esto puede resultar útil si desea reducir el volumen de casos de asistencia

ante incidentes con los que interactúa y si algunos incidentes procedentes de algunos recursos no requieren atención inmediata, por ejemplo, los que se producen en una cuenta que no es de producción.

- Para que AMS procese sus alertas, ejecute automatizaciones y cree casos de incidentes cuando sea necesario, elija la opción predeterminada.
4. Resolver después: elija entre 24 horas, 48 horas o 72 horas. Por último, configure cuándo se cierran automáticamente los casos de incidentes. Si el tiempo transcurrido desde la correspondencia del último caso alcanza el valor de resolución posterior configurado, el incidente se cierra.

Notificación de alerta

Como parte del procesamiento de alertas, en función del análisis de impacto, AWS Managed Services (AMS) crea un incidente e inicia el proceso de administración de incidentes para su corrección, cuando se puede determinar el impacto. Si no se puede determinar el impacto, AMS envía una notificación de alerta a la dirección de correo electrónico asociada a su cuenta mediante una notificación de servicio. En algunos casos, esta notificación de alerta no se envía. Por ejemplo, si las comprobaciones relacionadas con la infraestructura superan una alerta de uso elevado de la CPU, no se te enviará ninguna notificación de alerta. Para obtener más información, consulte el diagrama sobre la arquitectura de supervisión de AMS para ver el proceso de gestión de alertas en.

[Cómo funciona la supervisión](#)

Notificación de alertas basada en etiquetas

Usa etiquetas para enviar notificaciones de alerta para tus recursos a diferentes direcciones de correo electrónico. Se recomienda utilizar notificaciones de alerta basadas en etiquetas, ya que las notificaciones que se envían a una sola dirección de correo electrónico pueden causar confusión cuando varios equipos de desarrolladores utilizan la misma cuenta. Las notificaciones de alertas basadas en etiquetas no se ven afectadas por la [EC2 notificaciones agrupadas por instancias](#) configuración que elijas.

Con las notificaciones de alerta basadas en etiquetas, puedes:

- Enviar alertas a una dirección de correo electrónico específica: etiqüete los recursos que tengan alertas que deban enviarse a una dirección de correo electrónico específica con `OwnerTeamEmail,value = EMAIL_ADDRESS`.

- Enviar alertas a varias direcciones de correo electrónico: para usar varias direcciones de correo electrónico, especifique una lista de valores separados por comas. Por ejemplo, `key = OwnerTeamEmail, value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, . . .`. El número total de caracteres del campo de valor no puede superar los 260.
- Use una clave de etiqueta personalizada: para usar una clave de etiqueta personalizada, proporcione el nombre de la clave de etiqueta personalizada a su CSDM en un correo electrónico en el que dé su consentimiento explícito para activar las notificaciones automáticas para la comunicación basada en etiquetas. Se recomienda utilizar la misma estrategia de etiquetado para las etiquetas de contacto en todas las instancias y recursos.

Note

El valor clave *OwnerTeamEmail* no tiene por qué estar en camel Case. Sin embargo, las etiquetas distinguen entre mayúsculas y minúsculas y se recomienda utilizar el formato recomendado.

La dirección de correo electrónico debe especificarse en su totalidad, con el signo «at» (@) para separar la parte local del dominio. Ejemplos de direcciones de correo electrónico no válidas: *Team.AppATabc.xyz* o *john.doe*. Para obtener información general sobre tu estrategia de etiquetado, consulta los recursos de [etiquetado AWS](#). No añadas información de identificación personal (PII) en tus etiquetas. Usa listas de distribución o alias siempre que sea posible.

La notificación de alertas basada en etiquetas es compatible con los recursos de los siguientes servicios de Amazon: Elastic Block Store (EBS) EC2, Elastic Load Balancing (ELB), Application Load Balancer (ALB), Network Load Balancer, Relational Database Service (RDS), Elastic File System (EFS) y VPN. OpenSearch FSx Site-to-Site

Visualización de la configuración de supervisión de una cuenta AMS

Hay dos partes clave de la configuración de monitoreo de una cuenta que puede ver:

- CloudWatch Alarmas: para ver todas las alarmas CW de la cuenta, ve a la CloudWatch consola y selecciona los distintos servicios que te interesen.
- CloudWatch Eventos:

- Zona de destino multicuenta: CloudWatch los eventos monitoreados en la cuenta se pueden encontrar filtrando todas las reglas de eventos de CW con la cadena "ams -".
- Zona de destino para una sola cuenta: CloudWatch los eventos monitorizados en la cuenta se pueden encontrar filtrando todas las reglas de eventos de CW con la cadena. "mc -"

Cambiar la configuración de supervisión de una cuenta AMS

Puede cambiar la configuración de supervisión básica para EC2 los recursos de Amazon. Para ver las alertas que se pueden configurar, consulte [Alertas del monitoreo de referencia en AMS](#). Puede cambiar la definición de la alarma, el destino de la alarma o desactivar la notificación de alarma en los monitores de referencia para que las alertas cumplan con los requisitos operativos de su aplicación. Puede solicitar alguno o todos los cambios mencionados anteriormente enviando un CT de Gestión | Otros | Otros | Actualización (ct-0xdawir96cy7k) con la siguiente información.

- Instancia IDs [opcional, si no se menciona, todas las instancias de la cuenta están incluidas en el ámbito de aplicación]
- CloudWatch nombre de la métrica, por ejemplo, uso de CPU/swap free/ IOwait
- Destino: ID de correo electrónico o número de teléfono para un tema de SMS o SNS

Para obtener más información sobre el tipo de cambios que puede solicitar en la configuración de supervisión básica, consulte la [CloudWatch documentación de Amazon](#).

Notificaciones de incidentes compatibles con las aplicaciones en AMS

Utilice las notificaciones de incidentes automatizadas compatibles con las aplicaciones para personalizar su experiencia de comunicación en los casos de asistencia que AMS cree en su nombre. Al utilizar esta función, AMS recupera las preferencias de carga de trabajo personalizadas [AWS Service Catalog AppRegistry](#) para enriquecer las comunicaciones sobre incidentes de AMS con metadatos sobre sus aplicaciones y personalizar la gravedad de los casos de soporte creados por AMS en su nombre. Para utilizar esta función, primero debe aprovisionarla AWS Service Catalog AppRegistry en su cuenta de AMS.

Para obtener más información sobre los valores predeterminados de monitoreo de AMS, consulte [Supervisión y gestión de eventos en AMS](#).

AppRegistry Aprovechone en su cuenta AMS y cree aplicaciones

El AppRegistry servicio está disponible en el modo de autoaprovisionamiento (SSP) para su cuenta AMS. Para obtener instrucciones sobre cómo solicitar acceso, consulte [Cómo utilizar el SSP de AMS para aprovisionar AWS Service Catalog AppRegistry en su cuenta de AMS](#).

Tras el aprovisionamiento AppRegistry, utilice uno de los siguientes métodos para crear aplicaciones:

1. AWS consola: para obtener más información sobre cómo crear una aplicación AppRegistry a través de la consola de AWS, consulte [Creación de aplicaciones](#) en la Guía AWS Service Catalog AppRegistry del administrador.
2. CloudFormation: Puede definir su AppRegistry aplicación del mismo modo que define cualquier otro recurso. Para obtener más información, consulte la [referencia de tipos de recursos de AWS Service Catalog AppRegistry](#) en la Guía del usuario de AWS CloudFormation .

Cree etiquetas para permitir el enriquecimiento de mayúsculas y minúsculas

Debe etiquetar sus aplicaciones para que AMS pueda acceder a los metadatos de las aplicaciones. En la siguiente tabla se muestra la etiqueta necesaria.

Clave de etiqueta	Valor de etiqueta
gestionado por AMS	true

Personalice la gravedad de los casos de soporte de AMS para sus aplicaciones

Puede personalizar la gravedad de los casos de soporte creados por AMS especificando el grado de importancia de su solicitud para su organización. Esta configuración se controla mediante un grupo de atributos asociado a la aplicación en AppRegistry. El nombre del grupo de atributos debe coincidir con el siguiente patrón:

```
AMS.<ApplicationName>.CommunicationOptions
```


En el patrón anterior, `ApplicationName` debe coincidir con el nombre utilizado `AppRegistry` al crear la aplicación.

Contenido de ejemplo:

```
{
  "SchemaVersion": "1.0",
  "Criticality": "low"
}
```

SchemaVersion

Esto determina la versión del esquema que está utilizando y el subconjunto de funciones disponibles para su uso.

Versión del esquema	Característica
1.0	Gravedad de los casos de soporte personalizada en función del valor de criticidad

Criticidad

La importancia de esta solicitud determina la gravedad de los casos de soporte creados por los sistemas automatizados de AMS.

Valores válidos:

```
low|normal|high|urgent|critical
```

Para obtener más información sobre los niveles de gravedad, consulte [SeverityLevel](#) referencia de la AWS Support API.

Obligatorio: sí

Revisa los permisos necesarios

Para utilizar esta función, AMS necesita tener acceso a los siguientes permisos: AWS Identity and Access Management

- objetivo: `ListRoleTags`

- objetivo: ListUserTags
- API de etiquetado de grupos de recursos: GetResources
- catálogo de servicios: registro de aplicaciones: GetApplication
- catálogo de servicios - registro de aplicaciones: ListAssociatedAttributeGroups
- catálogo de servicios - registro de aplicaciones: GetAttributeGroup

Important

Asegúrese de que no haya una política de IAM o una política de control de servicios (SCP) que deniegue las acciones anteriores.

El rol realiza las llamadas a la `ams-access-admin` API. El siguiente es un ejemplo de lo que puede ver:

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

OpsCenter Utilizándolo en AMS

El equipo de operaciones de AWS Managed Services (AMS) lo utiliza [AWS Systems Manager OpsCenter](#) para diagnosticar y corregir muchas alertas relacionadas con sus recursos.

Su uso OpsCenter reduce el tiempo medio de resolución (MTTR) y, al mismo tiempo, proporciona una visión transparente de las colas operativas de los equipos de operaciones de AMS.

Gracias a OpsCenter ello, AMS le proporciona una visión transparente de los elementos de trabajo operativos, también conocidos como [OpsItems](#) «en los que trabajan activamente los equipos de AMS», además de soluciones automatizadas.

Para obtener más información sobre OpsCenter y OpsItems, consulte [AWS Systems Manager OpsCenter](#). Para obtener información sobre cómo obtener acceso a la consola AWS de administración, consulte [Trabajar con la consola de administración de AWS](#). Desde la consola de administración de AWS, puede ir a la consola de AWS Systems Manager y OpsCenter, para obtener más información, consulte [AWS Systems Manager Session Manager](#). OpsCenter también proporciona una API que puede utilizar; para obtener más información, consulte [Más información OpsCenter](#).

OpsCenter es una función con un precio aproximado de 1000€ OpsItems que cuesta menos de 10\$. Para obtener información, consulte [Precios de AWS Systems Manager](#).

Notificaciones de alerta de AMS

Como parte del procesamiento de alertas, en función del análisis de impacto, AWS Managed Services (AMS) crea un incidente e inicia el proceso de administración de incidentes para su corrección, cuando se puede determinar el impacto. En caso de que no se pueda determinar el impacto, AMS envía una notificación de alerta a la dirección de correo electrónico asociada a su cuenta mediante una notificación de servicio; consulte el diagrama sobre la arquitectura de supervisión de AMS para ver el proceso de gestión de alertas en el diagrama. [Cómo funciona la supervisión](#)

Recepción de alertas generadas por AMS

AWS Managed Services (AMS) le permite recibir notificaciones de alerta de EC2 los recursos de Amazon directamente para reducir los retrasos en la comunicación. Para recibir las EC2 alertas de Amazon directamente, suscriba su destinatario (correo electrónico preferido) al tema Direct-Customer-Alerts de Amazon SNS utilizando el tipo de cambio Gestión | Supervisión y notificación | SNS | Suscríbete (ct-3rc19u1k017wu).

Note

No todas las alertas de referencia se envían al tema Direct-Customer-Alerts de forma predeterminada. Para ver todas las alertas generadas por el sistema de monitoreo AMS, suscríbase al tema Amazon SNS para el sistema de monitoreo AMS. En la solicitud, pregunte por el «tema de supervisión de AMS», especifique un canal de suscripción para recibir las alertas (Lambda, Amazon SQS, HTTP/S, correo electrónico o SMS) y especifique los puntos de enlace (por ejemplo, las direcciones de correo electrónico, si elige el protocolo de correo electrónico) que recibirán las alertas.

El tema de supervisión de AMS recibe alertas que utilizan los servicios compartidos de AMS, por lo que puede ser ruidoso.

Para obtener más información, consulta la sección [Suscríbete](#) en la referencia de la API de suscripción de Amazon Simple Notification Service.

Para obtener una lista de las alertas de referencia que proporciona AMS, consulte [Alertas del monitoreo de referencia en AMS](#).

Notificaciones de alertas basadas en etiquetas en AMS

Usa etiquetas para enviar notificaciones de alerta para tus recursos a diferentes direcciones de correo electrónico. Se recomienda utilizar notificaciones de alerta basadas en etiquetas, ya que las notificaciones que se envían a una sola dirección de correo electrónico pueden causar confusión cuando varios equipos de desarrolladores utilizan la misma cuenta.

Important

Las notificaciones de alertas basadas en etiquetas solo funcionan para las notificaciones relacionadas con Amazon EC2, Amazon EBS, Elastic Load Balancing, Network Load Balancer, Application Load Balancer, Amazon RDS, Amazon Redshift y. OpenSearch. No añada información de identificación personal (PII) en sus etiquetas.

Envía alertas a una dirección de correo electrónico específica

Etiquete los recursos que tienen alertas que deben enviarse a una dirección de correo electrónico específica con `key = OwnerTeamEmail,value = EMAIL_ADDRESS`.

Envíe alertas a varias direcciones de correo electrónico

Para usar varias direcciones de correo electrónico, especifique una lista de valores separados por comas. Por ejemplo, `key = OwnerTeamEmail,value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`. El número total de caracteres del campo de valor no puede superar los 260.

Utilice una clave de etiqueta personalizada

Para usar una clave de etiqueta personalizada, proporciona el nombre de la clave de etiqueta personalizada a tu CSDM en un correo electrónico con el consentimiento para activar la notificación automática para la comunicación basada en etiquetas. Se recomienda utilizar la misma estrategia de etiquetado para las etiquetas de contacto en todas las instancias y recursos.

La dirección de correo electrónico debe especificarse en su totalidad, con el signo «at» (@) para separar la parte local del dominio. Ejemplos de direcciones de correo electrónico no válidas: `Team.AppATabc.xyz` o `john.doe`. Para obtener información general sobre su estrategia de

etiquetado, consulte [Uso de etiquetas](#). Para etiquetar un recurso existente, envíe una RFC con el tipo de cambio Deployment | Advanced stack components | Tag | Create (auto) (ct-3cx7we852p3af).

Note

No es necesario que el valor clave esté en mayúsculas y minúsculas. *OwnerTeamEmail* Sin embargo, las etiquetas distinguen entre mayúsculas y minúsculas y se recomienda utilizar el formato recomendado.

Remediación automática de alertas por parte de AMS

Tras la verificación, AWS Managed Services (AMS) corrige automáticamente determinadas alertas según las condiciones y los procesos específicos que se describen en esta sección.

Nombre de la alerta	Descripción	Umbrales	Acción
Canal seguro roto	La alarma de canal seguro roto se activa en las EC2 instancias de Windows cuando la instancia pierde la conexión con el controlador de dominio de AD.	El umbral ha superado el valor definido 10 veces en los últimos 15 minutos.	La corrección automática de AMS valida que la instancia esté en línea en SSM, que el nombre de host no esté duplicado y que el objeto informático de AD esté alineado con la pila. CloudFormation La corrección repara la conexión de canal seguro para restablecer el acceso a la instancia.
Comprobación de estado no superada	Posibles fallos de hardware o un estado de fallo de la instancia.	El sistema ha detectado un estado de error al menos una vez en los últimos 15 minutos.	La corrección automática de AMS valida primero si se puede acceder a la instancia. Si no se puede acceder a la instancia, se detiene y se reinicia. La parada y el inicio

Nombre de la alerta	Descripción	Umbrales	Acción
			permiten que la instancia migre a un nuevo hardware subyacente. Para obtener más información, consulte la siguiente sección, «Automatización de la corrección de errores de comprobación de EC2 estado».
AMSLinuxDiskUsage	Se activa cuando se está agotando el espacio de disco utilizado en 1 punto de montaje (espacio designado en un volumen) de la EC2 instancia.	El umbral supera el valor definido 6 veces en los últimos 30 minutos.	La corrección automática de AMS elimina primero los archivos temporales. Si esto no libera suficiente espacio en disco, amplía el volumen para evitar tiempos de inactividad si el volumen se llena.
AMSWindowsDiskUsage	Cuando se esté agotando el uso de 1 punto de montaje (espacio designado en un volumen) en el disco de la EC2 instancia.	El umbral supera el valor definido 6 veces durante los últimos 30 minutos.	La corrección automática de AMS elimina primero los archivos temporales. Si esto no libera suficiente espacio en disco, amplía el volumen para evitar tiempos de inactividad si el volumen se llena.

Nombre de la alerta	Descripción	Umbrales	Acción
RDS-EVENT-0089	La instancia de base de datos ha consumido más del 90 % del almacenamiento asignado.	El almacenamiento está asignado en más del 90%.	La corrección automática de AMS valida primero que la base de datos esté en un estado modificable y disponible o que esté lleno de almacenamiento. A continuación, intenta aumentar el almacenamiento asignado, las IOPS y el rendimiento del almacenamiento mediante un conjunto de cambios. CloudFormation Si ya se ha detectado una desviación de la pila, recurre a la API de RDS para evitar el tiempo de inactividad. Puede inhabilitar esta función añadiendo la siguiente etiqueta a la instancia de base de datos de RDS: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Nombre de la alerta	Descripción	Umbrales	Acción
RDS-EVENT-0007	Se agotó el almacenamiento asignado a la instancia de base de datos. Para resolverlo, asigne almacenamiento adicional.	El almacenamiento está asignado al 100%.	La corrección automática de AMS valida primero que la base de datos esté en un estado modificable y disponible o que esté lleno de almacenamiento. A continuación, intenta aumentar el almacenamiento asignado, las IOPS y el rendimiento del almacenamiento mediante un conjunto de cambios. CloudFormation Si ya se ha detectado una desviación de la pila, recurre a la API de RDS para evitar el tiempo de inactividad. Puede inhabilitar esta función añadiendo la siguiente etiqueta a la instancia de base de datos de RDS: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Nombre de la alerta	Descripción	Umbrales	Acción
RDS-EVENT-0224	El almacenamiento asignado solicitado alcanza o supera el umbral de almacenamiento máximo configurado.	Se ha agotado el umbral de almacenamiento máximo de la instancia de base de datos o es superior o igual al almacenamiento asignado solicitado.	La corrección automática de AMS valida primero que la cantidad de almacenamiento de RDS solicitada supere el umbral máximo de almacenamiento. Si se confirma, AMS intenta aumentar el umbral máximo de almacenamiento en un 30% con un CloudFormation conjunto de cambios o directamente a la API de RDS si no se aprovisionan los recursos. CloudFormation Puede inhabilitar esta función añadiendo la siguiente etiqueta a la instancia de base de datos de RDS: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Nombre de la alerta	Descripción	Umbrales	Acción
Capacidad de almacenamiento de RDS	Queda menos de 1 GB en el almacenamiento asignado a la instancia de base de datos.	El almacenamiento está asignado en un 99%.	La corrección automática de AMS valida primero que la base de datos esté en un estado modificable y disponible o que esté lleno de almacenamiento. A continuación, intenta aumentar el almacenamiento asignado, las IOPS y el rendimiento del almacenamiento mediante un conjunto de cambios. CloudFormation Si ya se ha detectado una desviación de la pila, recurre a la API de RDS para evitar el tiempo de inactividad. Puede inhabilitar esta función añadiendo la siguiente etiqueta a la instancia de base de datos de RDS: "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Amazon EC2 Broken Secure Channel: nota sobre la automatización de la remediación

Antes de que la corrección automática de AWS Managed Services (AMS) corrija los problemas de Amazon EC2 Windows Broken Secure Channel, la automatización lleva a cabo las siguientes comprobaciones previas y crea un informe de incidentes para una investigación más exhaustiva:

- Valida que el estado SSM de la EC2 instancia de Amazon sea «Online».
- Valida si la EC2 instancia de Amazon forma parte de un grupo de Auto Scaling y si todas las instancias del grupo Auto Scaling tienen el mismo nombre de host.
- Comprueba si la EC2 instancia de Amazon forma parte de la CloudFormation pila que se utilizó para aprovisionarla. Si la instancia se ha eliminado de la CloudFormation pila, la automatización verifica si la unidad organizativa (OU) de Active Directory asociada sigue haciendo referencia a la pila.

Una vez superadas las validaciones anteriores, la automatización procede a corregir el canal Broken Secure.

Pasos de remediación:

- La corrección automática intenta reparar el canal seguro entre la EC2 instancia y el dominio de AD, restaurando el acceso a la instancia.
- Tras la corrección, la automatización comprueba que se ha establecido el canal seguro. Si no lo consigue, AMS crea un incidente y pone en marcha las operaciones de AMS para que lo investiguen.

EC2 error en la comprobación de estado: notas sobre la automatización de la remediación

Cómo funciona la corrección automática de AMS con problemas de error en la comprobación de EC2 estado:

- Si no se puede acceder a tu EC2 instancia de Amazon, debes detenerla y volver a iniciarla para poder migrarla a un nuevo hardware y recuperarla.
- Si la raíz del problema está en el sistema operativo (falta de dispositivos en fstab, el núcleo está dañado, etc.), la automatización no podrá recuperar la instancia.
- Si la instancia pertenece a un grupo de Auto Scaling, la automatización no realiza ninguna acción: la acción de AutoScalingGroup escalado reemplaza a la instancia.

- Si la instancia tiene habilitada la recuperación EC2 automática, la corrección no se lleva a cabo.

EC2 automatización de la corrección del uso del volumen

Cómo funciona la corrección automática de AWS Managed Services (AMS) con los problemas de uso EC2 del volumen:

- La automatización primero valida si la expansión del volumen es necesaria y si se puede realizar. Si la expansión se considera adecuada, la automatización puede aumentar la capacidad de volumen. Este proceso automatizado equilibra la necesidad de crecimiento con una expansión limitada y controlada.
- Antes de ampliar un volumen, la automatización realiza tareas de limpieza (Windows: Disk Cleaner, Linux: Logrotate y eliminación del registro del agente Simple Service Manager) en la instancia para intentar liberar espacio.

Note

Las tareas de limpieza no se ejecutan en las instancias de la familia EC2 «T» porque dependen de los créditos de la CPU para seguir funcionando.

- En Linux, la automatización solo admite la ampliación de los sistemas de archivos tipo EXT2 A EXT4 y XFS. EXT3
- En Windows, la automatización solo es compatible con el Sistema de archivos de nueva tecnología (NTFS) y el Sistema de archivos resiliente (ReFS).
- La automatización no amplía los volúmenes que forman parte del Logical Volume Manager (LVM) o de una matriz RAID.
- La automatización no amplía los volúmenes del almacén de instancias.
- La automatización no actúa si el volumen afectado ya es superior a 2 TiB.
- La expansión mediante la automatización está limitada a un máximo de tres veces por semana y cinco veces en total durante la vida útil del sistema.
- La automatización no amplía el volumen si la expansión anterior se produjo en las últimas seis horas.

Cuando estas reglas impiden que la automatización tome medidas, AMS se pondrá en contacto con usted mediante una solicitud de servicio saliente para determinar las siguientes acciones a tomar.

Automatización de la corrección de eventos de bajo almacenamiento en Amazon RDS

Cómo funciona la corrección automática de AWS Managed Services (AMS) con los problemas de eventos de bajo almacenamiento de Amazon RDS:

- Antes de intentar ampliar el almacenamiento de la instancia de Amazon RDS, la automatización realiza varias comprobaciones para garantizar que la instancia de Amazon RDS se encuentra en un estado modificable y disponible, o con almacenamiento lleno.
- Cuando se detecta CloudFormation una desviación de pila, la corrección se realiza a través de la API de Amazon RDS.
- La acción correctiva no se ejecuta en los siguientes escenarios:
 - El estado de la instancia de Amazon RDS no es «disponible» ni «lleno de almacenamiento».
 - El almacenamiento de instancias de Amazon RDS no se puede modificar actualmente (por ejemplo, si el almacenamiento se ha modificado en las últimas seis horas).
 - La instancia de Amazon RDS tiene activado el almacenamiento con autoscalamiento.
 - La instancia de Amazon RDS no es un recurso dentro de una CloudFormation pila.
- La corrección se limita a una expansión cada seis horas y a no más de tres expansiones en un período continuo de catorce días.
- Cuando se producen estas situaciones, AMS se pone en contacto con usted para informarle sobre un incidente saliente para determinar las siguientes medidas.

Creación de CloudWatch alarmas adicionales en AMS

Puede crear nuevas CloudWatch alarmas mediante el cambio de tipo de implementación | Monitorización y notificación de AWS Managed Services (AMS) CloudWatch | | Crear alarmas.

Important

AMS no supervisa CloudWatch las alarmas que usted crea.

Uso de CloudWatch métricas y alarmas personalizadas para las EC2 instancias de Amazon (solo funciona para implementaciones mutables que no dependen de las actualizaciones AMIs implementadas en los grupos de Auto Scaling):

1. Cree su script de monitoreo de aplicaciones y una métrica personalizada. Para obtener más información y acceder a scripts de ejemplo, consulte [Supervisión de métricas de memoria y disco para instancias de Amazon EC2 Linux](#). Los scripts CloudWatch de monitoreo de Amazon para EC2 instancias de Amazon de Linux muestran cómo producir y consumir métricas CloudWatch personalizadas de Amazon. Estos scripts Perl de muestra contienen un ejemplo totalmente funcional que informa sobre métricas de memoria, intercambio y utilización del espacio en disco de una instancia de Linux.
2. Cargue su script de monitoreo. Para cargar el script de monitoreo a su grupo de Auto Scaling o configuración de EC2 instancias de Amazon, puede usarlo UserData al configurar su grupo de Auto Scaling o EC2 instancia de Amazon o, si su aplicación se implementó con CodeDeploy, puede modificar la configuración con Deployment | Applications | CodeDeploy application | Deploy CT (ct-2edc3sd1sqmrb).
3. Publique su métrica personalizada en CloudWatch (la primera vez que publique un punto de datos para una nueva métrica personalizada, se crea), consulte [Publicar métricas personalizadas](#).
4. Cree la CloudWatch alarma; consulte [Crear una CloudWatch alarma para una instancia](#).

 Important

Los datos de monitoreo deben enviarse a esta ruta [infra/INSTANCE_ID/YOUR_CUSTOM_METRIC]

Para modificar o eliminar una CloudWatch alarma, envía una RFC al tipo de cambio Management | Other | Other | Create (ct-1e1xtak34nx76) con los parámetros necesarios para completar la acción, tal y como se describe en la referencia de la API de Amazon. CloudWatch [PutMetricAlarm](#)

Puede utilizar la transmisión de eventos. CloudWatch AMS está integrado CloudWatch y puede solicitar que cualquier llamada a la API de AWS active un CloudWatch evento.

Para ello, envíe un documento de administración | Otros | Otros | Actualización CT (ct-0xdawir96cy7k) con las llamadas a la API que le interesen. Un operador de AMS hablará con usted para recopilar los requisitos. Para obtener más información, consulta la [CloudWatch documentación de Amazon](#).

Para acceder a la transmisión del CloudWatch evento, envíe un documento de administración | Otros | Otros | Actualice CT (ct-0xdawir96cy7k) para añadir a una persona al tema de notificaciones de SNS. Un operador de AMS hablará con usted para recopilar los requisitos.

Creación de CloudWatch métricas y alarmas personalizadas en AMS

Puedes almacenar las métricas de tu empresa y de tus aplicaciones en Amazon CloudWatch. Puede ver gráficos y configurar alarmas en función de estas métricas, del mismo modo que puede ver las métricas que CloudWatch ya se almacenan para sus recursos de AWS Managed Services (AMS). Para obtener más información CloudWatch, consulte [Amazon CloudWatch Concepts](#).

Amazon SNS permite a las aplicaciones enviar mensajes urgentes a varios suscriptores mediante un mecanismo de «inserción» contra el tema del AMS Managed Monitoring System o MMS, Amazon SNS (SNS) en el que se publican las alarmas; en este caso, MMS y sus colas de SQS. Puede utilizarlas CloudWatch para crear métricas personalizadas y, a través de un tema de SNS, hacer que AMS le avise adecuadamente. Para ello, siga estos pasos.

Note

Este proceso no funciona para despliegues inmutables que se basan en despliegues actualizados en grupos de Auto Scaling, sino que es adecuado para AMIs despliegues de aplicaciones mutables (no ASG).

Configurar una métrica personalizada dentro de las limitaciones de AMS Advanced es una tarea compleja. Para ver un ejemplo CloudWatch, consulte [Ejemplo: contar las apariciones de un término](#).

1. Cree el script de monitoreo de aplicaciones y una métrica personalizada (como el ejemplo del recuento de ocurrencias). Para obtener más información y acceder a scripts de ejemplo, consulte [Supervisión de métricas de memoria y disco para instancias de Amazon EC2 Linux](#).
2. Cargue su script de monitoreo. Para cargar el script de monitoreo a su grupo de Auto Scaling o configuración de EC2 instancias de Amazon, puede usarlo UserDataal configurar su grupo de Auto Scaling o EC2 instancia de Amazon o, si su aplicación se implementó con CodeDeploy, puede modificar la configuración con Deployment | Applications | CodeDeploy application | Deploy CT (ct-2edc3sd1sqmrb).
3. Publique su métrica personalizada en CloudWatch (se crea la primera vez que publica un punto de datos para una nueva métrica personalizada), consulte [Publicar métricas personalizadas](#).

4. Para integrar la métrica de sus clientes en su sistema de supervisión de aplicaciones, solicite a AMS que cree un tema de SNS para la métrica enviando una RFC con el tipo de cambio Implementación | Supervisión y notificación | SNS | Crear (ct-3dfnglm4ombbs).
5. Cree la CloudWatch alarma, consulte [Creación de CloudWatch alarmas en Amazon](#).

 Important

Los datos de monitoreo deben enviarse a esta ruta
[infra/*INSTANCE_ID/YOUR_CUSTOM_METRIC*].

Uso de CloudWatch Application Insights para .Net y SQL Server en AMS

Puede utilizar Amazon CloudWatch Application Insights para configurar los monitores de los recursos de sus aplicaciones de AWS Managed Services (AMS) a fin de analizar continuamente los datos en busca de señales de problemas en sus aplicaciones y reducir el tiempo medio de reparación (MTTR) a la hora de solucionar problemas con las aplicaciones. Para obtener más información sobre CloudWatch Application Insights, consulte [CloudWatch Application Insights para .NET y SQL Server](#).

 Important

AMS no supervisa los problemas desde CloudWatch Application Insights porque se trata del código de aplicación que usted controla.

Para usar CloudWatch Application Insights, envíe una RFC con el tipo de cambio Deployment | Advanced stack components | Identity and Access Management (IAM) | Cree una entidad o política (es necesario revisar) (ct-3dpd8mdd9jn1r) con una solicitud para crear un rol de IAM que le dé permiso para configurar Application Insights. CloudWatch Hay dos opciones para recibir los problemas identificados: a través de un tema de SNS o con un objetivo en las reglas de un evento. CloudWatch En el RFC, especifique lo que desee. Si planea usar reglas de CloudWatch eventos, especifique también la definición de la regla en la RFC. Una vez que haya configurado CloudWatch Application Insights, recibirá notificaciones sobre posibles problemas, incluida información que apunta a una posible causa raíz.

Para obtener información sobre cómo puede asumir el cargo, consulte la guía de incorporación de AMS: [federe su Active Directory con los roles de IAM de AMS](#).

Uso de Amazon EventBridge Managed Rules en AMS

AMS Advanced utiliza Amazon EventBridge Managed Rules. Una regla gestionada es un tipo de regla único que está directamente vinculada a AMS. Estas reglas coinciden con los eventos entrantes y los envían a los destinos para su procesamiento. Las reglas administradas están predefinidas por AMS e incluyen los patrones de eventos que el servicio requiere para administrar las cuentas de los clientes y, a menos que se defina lo contrario, solo el servicio propietario puede utilizar estas reglas administradas.

Las reglas gestionadas por AMS están vinculadas al principio del `events.managedservices.amazonaws.com` servicio. Estas reglas administradas se administran a través de la función [AWSServiceRoleForManagedServices_Eventsvinculada al servicio](#). Para eliminar estas reglas, se requiere una confirmación especial por parte del cliente. Para obtener más información, consulte [Eliminar reglas administradas para AMS](#).

Para obtener más información sobre las reglas, consulta [Reglas](#) en la Guía del EventBridge usuario de Amazon.

Amazon EventBridge Managed Rules implementadas por AMS

Reglas EventBridge gestionadas por Amazon

Nombre de la regla	Descripción	Definición
AMSAdvancedCoreRule	Esta regla reenvía Amazon CloudWatch Alarms a AMS Monitoring. Las CloudWatch alarmas del	<pre>{ { "source": ["aws.cloudwatch"], "detail-type": ["CloudWatch Alarm State Change"], } }</pre>

Nombre de la regla	Descripción	Definición
	monitor de CloudWatch eventos de Amazon.	

Creación de reglas gestionadas para AMS

No necesitas crear manualmente Amazon EventBridge Managed Rules. Cuando te incorporas a AMS en la consola de AWS administración AWS CLI, la o la AWS API, AMS las crea automáticamente.

Edición de reglas gestionadas para AMS

AMS no permite editar las reglas gestionadas. AMS predefine el nombre y el patrón de eventos de cada regla gestionada.

Eliminar reglas administradas para AMS

No es necesario eliminar manualmente las reglas gestionadas. Cuando te desconectas de AMS en la consola AWS de administración, en la AWS CLI AWS API o en la consola, AMS limpia los recursos y elimina automáticamente todas las reglas gestionadas que son propiedad de AMS.

En caso de que AMS no elimine las reglas gestionadas durante la desconexión, también puedes utilizar la EventBridge consola de Amazon, la AWS CLI o la AWS API para eliminar manualmente las reglas gestionadas. Para ello, primero debes abandonar AMS y forzar la eliminación de las reglas gestionadas.

Remediador de confianza en AMS

Trusted Remediator es una solución de AWS Managed Services que automatiza la corrección y las [AWS Trusted Advisor](#) recomendaciones. [AWS Compute Optimizer](#) Trusted Remediator crea recomendaciones cuando Trusted Advisor y Compute Optimizer indica oportunidades para reducir costos, mejorar la disponibilidad del sistema, optimizar el rendimiento o cerrar sus brechas de seguridad. Cuentas de AWS Con Trusted Remediator, puede abordar estas recomendaciones de seguridad, rendimiento, optimización de costos, tolerancia a fallas y límites de servicio de una

manera segura y estandarizada que utiliza las mejores prácticas establecidas. Trusted Remediator le permite configurar una solución de remediación y se ejecuta automáticamente según un cronograma que usted cree, lo que simplifica el proceso de remediación. Este enfoque simplificado aborda los problemas de manera coherente y eficiente y sin intervención manual.

Ventajas clave de Trusted Remediator

Los principales beneficios de Trusted Remediator son los siguientes:

- Mejora de la seguridad, el rendimiento y la optimización de los costes: Trusted Remediator le ayuda a mejorar la seguridad general de sus cuentas, a optimizar la utilización de los recursos y a reducir los costes operativos.
- Instalación y configuración de autoservicio: puede configurar Trusted Remediator para que se ajuste a sus requisitos y preferencias.
- Trusted Advisor Comprobaciones automatizadas y AWS Compute Optimizer recomendaciones de corrección: tras la configuración, Trusted Remediator ejecuta automáticamente las acciones de corrección de las comprobaciones seleccionadas. Esta automatización elimina la necesidad de intervención manual.
- Implementación de las mejores prácticas: las acciones de remediación se basan en las mejores prácticas establecidas, por lo que los problemas se abordan de manera estandarizada y eficaz.
- Ejecución programada: puede elegir el programa de remediación que se adapte a sus day-to-day flujos de trabajo operativos.

Trusted Remediator le permite abordar de forma proactiva los problemas identificados en sus AWS entornos, lo que le ayuda a cumplir con las mejores prácticas y a mantener una infraestructura de nube segura, rentable y de alto rendimiento.

Cómo funciona Trusted Remediator

A continuación se muestra un ejemplo del flujo de trabajo de Trusted Remediator:

Trusted Remediator evalúa las recomendaciones de Compute Optimizer para Cuentas de AWS usted Trusted Advisor y las crea. AWS Systems Manager [OpsItems](#) OpsCenter A continuación, puede utilizar los documentos de automatización de Trusted Remediator para corregir los problemas de forma automática o manual. OpsItems A continuación se detallan los detalles de cada tipo de remediación:

- Corrección automatizada: Trusted Remediator ejecuta el documento de automatización y supervisa la ejecución. Una vez finalizado el documento de automatización, Trusted Remediator resuelve el problema.
- Corrección manual: Trusted Remediator crea el archivo OpsItem para que usted lo revise. Tras la revisión, puede crear un RFC automatizado, [Trusted Remediator | Finding | Remediate](#), cambiar el tipo para corregir el recurso. Para obtener información sobre los pasos de corrección manual, consulte [Ejecute las correcciones manuales en Trusted Remediator](#)

Los registros de corrección se almacenan en un bucket de Amazon S3. Puede usar los datos del depósito de S3 para crear QuickSight paneles personalizados para la elaboración de informes. AMS también proporciona informes a pedido para Trusted Remediator. Para recibir estos informes, póngase en contacto con su CSDM.

Términos clave de Trusted Remediator

Los siguientes son términos que es útil conocer cuando se utiliza Trusted Remediator en AMS:

- AWS Trusted Advisor y AWS Compute Optimizer: servicios de optimización de la nube proporcionados por AWS. Trusted Advisor y Compute Optimizer inspeccionan su AWS entorno y proporcionan recomendaciones basadas en las mejores prácticas en las seis categorías siguientes:
 - Optimización de costos
 - Rendimiento
 - Seguridad
 - Tolerancia a errores
 - Excelencia operativa
 - Límites de los servicios

Para obtener más información, consulte [AWS Trusted Advisor](#) y [AWS Compute Optimizer](#).

- Trusted Remediator: una solución de corrección de AMS para [Trusted Advisor](#) realizar comprobaciones y recomendaciones. [AWS Compute Optimizer](#) Trusted Remediator le ayuda a corregir de forma segura las Trusted Advisor comprobaciones y las recomendaciones de Compute Optimizer con las mejores prácticas conocidas para mejorar la seguridad, el rendimiento y reducir los costes. Trusted Remediator es fácil de instalar y configurar. La configuración se realiza una vez y Trusted Remediator ejecuta las correcciones según la programación que prefiera (diaria o semanalmente).

- **AWS Systems Manager Documento SSM:** archivo JSON o YAML que define las acciones que se AWS Systems Manager realizan en sus recursos. AWS El documento SSM sirve como especificación declarativa para automatizar las tareas operativas en varios AWS recursos e instancias.
- **AWS Systems Manager OpsCenter OpsItem:** un recurso de administración de problemas operativos en la nube que le ayuda a rastrear y resolver los problemas operativos en su AWS entorno. OpsItems proporcionan una visión y un sistema de gestión centralizados para los datos operativos y los problemas en todos Servicios de AWS los recursos. Cada uno OpsItem representa un problema operativo, como un posible riesgo de seguridad, un problema de rendimiento o un incidente operativo.
- **Configuración:** una configuración es un conjunto de atributos almacenados en [AWS AppConfig, una capacidad de AWS Systems Manager](#). La aplicación Trusted Remediator AWS AppConfig ayuda a configurar las correcciones a nivel de cuenta.
- **Modo de ejecución:** el modo de ejecución es un atributo de configuración que determina cómo ejecutar la corrección para cada Trusted Advisor resultado de la comprobación. Se admiten cuatro modos de ejecución: automatizado, manual, condicional e inactivo.
- **Anulación de recursos:** esta función utiliza etiquetas de recursos para anular la configuración de recursos específicos.
- **Registro de elementos de remediación:** un archivo de registro en el depósito de registros de S3 sobre remediaciones de Trusted Remediator. El registro de elementos de corrección se crea cuando se crean las correcciones. OpsItems Este archivo de registro contiene la corrección de la ejecución manual OpsItems y la corrección de la ejecución automática. OpsItems Utilice este archivo de registro para realizar un seguimiento de todos los elementos de corrección.
- **Registro de ejecución de correcciones automatizado:** un archivo de registro en el depósito de registros de S3 sobre correcciones de Trusted Remediator. El registro de ejecución de correcciones automatizadas se crea cuando se completa la ejecución automatizada de un documento SSM. Este registro contiene los detalles de la ejecución de SSM para la corrección automática de las ejecuciones. OpsItems Utilice este archivo de registro para realizar un seguimiento de las correcciones automatizadas.

Comience con Trusted Remediator en AMS

Trusted Remediator está disponible en AMS sin coste adicional. Trusted Remediator admite configuraciones de cuenta única y de cuentas múltiples.

Incorporado a Trusted Remediator

Para incorporar sus cuentas de AMS a Trusted Remediator, envíe un correo electrónico a sus arquitectos de nube o gerentes de prestación de servicios en la nube (CSDMs). En el mensaje, incluya la siguiente información:

- Cuentas de AWS: El número de identificación de la cuenta de doce dígitos. Todas las cuentas que desee incorporar a Trusted Remediator deben pertenecer al mismo cliente de AMS Advanced.
- Cuenta de administrador delegado: la cuenta que se usa para Trusted Advisor comprobar la configuración de Compute Optimizer para cuentas únicas o múltiples.
- Cuentas de miembro: son las cuentas vinculadas a la cuenta de administrador delegado. Estas cuentas heredan las configuraciones de la cuenta de administrador delegado. Puede tener una cuenta de miembro o varias cuentas de miembro.

Note

Las cuentas de los miembros heredan las configuraciones de la cuenta de administrador delegado. Si necesita configuraciones diferentes para cuentas específicas, incorpore varias cuentas de administrador delegado con las configuraciones que prefiera. Planifique la estructura de la cuenta y las configuraciones con sus arquitectos de nube antes de incorporarla.

- Región de AWS: El Región de AWS lugar donde se encuentran sus recursos. Para ver una lista Regiones de AWS, consulta [Servicios de AWS por región](#).
- Calendario y hora de remediación: su programa de remediación preferido (diario o semanal). Trusted Remediator recopila las Trusted Advisor comprobaciones e inicia la reparación a la hora programada. Por ejemplo, puede configurar el programa de remediación para la 1:00 a.m. del domingo de cada semana, hora estándar del este de Australia.
- Correo electrónico de notificación: Trusted Remediator utiliza el correo electrónico de notificación para notificarle diariamente si hay soluciones. El asunto del correo electrónico de notificación es «Resumen de las correcciones de Trusted Remediator» y el contenido proporciona información sobre las correcciones de Trusted Remediator ejecutadas en las últimas 24 horas.

Note

Revise sus aplicaciones y recursos después de cada corrección programada. Para obtener asistencia adicional, póngase en contacto con AMS.

Tras enviar la solicitud de incorporación con los detalles necesarios a su CA o CSDM, AMS incorpora sus cuentas a Trusted Remediator. Trusted Remediator utiliza AWS AppConfig, una capacidad de AWS Systems Manager, para definir la configuración de las comprobaciones. Trusted Advisor Estas configuraciones son un conjunto de atributos que se almacenan en AWS AppConfig. Para evitar cargos no autorizados a sus recursos, todas las Trusted Advisor comprobaciones admitidas se configuran como inactivas cuando las cuentas se incorporan a Trusted Remediator. Estas configuraciones le ayudan a corregir automáticamente Trusted Advisor comprobaciones específicas o a evaluar y corregir manualmente las comprobaciones restantes. Las configuraciones son altamente personalizables, lo que le permite aplicar configuraciones para cada Trusted Advisor comprobación. Para obtener más información, consulte [Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator](#).

Configure Trusted Remediator en su Cuentas de AWS

Cuando se complete la incorporación, su CA o CSDM se lo notificará y las configuraciones predeterminadas se crearán en su administrador delegado. Cuenta de AWS La configuración se almacena en la aplicación Trusted AWS AppConfig Remediator. Puede utilizar RFC [Management | Trusted Remediator | Remediation configuration | Update](#) para solicitar actualizaciones de configuración. Para obtener más información, consulte [Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator](#).

Para ver las configuraciones predeterminadas de Trusted Remediator, siga estos pasos:

1. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>

Note

Asegúrese de estar en la cuenta de administrador delegado.

2. Elija Administración de aplicaciones, AppConfig.
3. Seleccione Trusted Remediator de la lista de aplicaciones.

A continuación, se muestra un ejemplo de la AWS AppConfig consola que muestra las configuraciones de Trusted Remediator:

Elija las comprobaciones y recomendaciones que desee corregir

De forma predeterminada, el modo de ejecución de correcciones está inactivo para todas las Trusted Advisor comprobaciones y recomendaciones de Compute Optimizer de tu configuración. Esto evita la corrección no autorizada y protege los recursos. AMS proporciona documentos de automatización de SSM seleccionados para la corrección de los Trusted Advisor cheques.

Para seleccionar las comprobaciones que desea corregir con Trusted Remediator, complete los siguientes pasos:

1. Revise la lista de [recomendaciones compatibles Trusted Advisor y de Compute Optimizer o el nombre de los documentos de automatización de SSM asociados](#) para decidir qué comprobaciones y recomendaciones desea corregir con Trusted Remediator.
2. Envía una solicitud [de administración | Trusted Remediator | Configuración de remediación | Actualización para actualizar la configuración](#) de las comprobaciones seleccionadas. Trusted Advisor Para obtener instrucciones sobre cómo seleccionar las comprobaciones, consulte [Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator](#)

Realice un seguimiento de sus correcciones en Trusted Remediator

Tras actualizar la configuración a nivel de cuenta, Trusted Remediator crea una para cada corrección. OpsItems Trusted Remediator ejecuta el documento SSM para la corrección automática de acuerdo con su programa de remediación. OpsItems Para obtener instrucciones sobre cómo ver todas las correcciones OpsItems desde la OpsCenter consola de Systems Manager, consulte [Realice un seguimiento de las correcciones en Trusted Remediator](#).

Ejecute las correcciones manuales en Trusted Remediator

Puede corregir las Trusted Advisor comprobaciones manualmente mediante un RFC automatizado. Si elige la corrección manual, Trusted Remediator crea una ejecución manual. OpsItem Para obtener más información, consulte [Ejecute las correcciones manuales en Trusted Remediator](#).

Recomendaciones de Compute Optimizer respaldadas por Trusted Remediator

En la siguiente tabla, se enumeran las recomendaciones de Compute Optimizer compatibles, los documentos de automatización de SSM, los parámetros preconfigurados y el resultado esperado de los documentos de automatización. Revisa el resultado esperado para ayudarte a entender los posibles riesgos en función de los requisitos de tu empresa antes de utilizar un documento de automatización de SSM para corregir las comprobaciones.

Asegúrate de que la regla de configuración correspondiente para cada comprobación de Compute Optimizer esté presente en las comprobaciones compatibles para las que deseas habilitar la corrección. Para obtener más información, consulta [Cómo optar AWS Compute Optimizer por Trusted Advisor las comprobaciones](#).

Opción de optimización	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles

Redimensionamiento

Recomendaciones de EC2 instancias de Amazon	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation	• MinimumDaysSinceLastChange: el parámetro para especificar el número mínimo de días transcurridos desde el último cambio de tipo de instancia. El valor predeterminado es 7 días.
	El tipo de EC2 instancia de Amazon se actualizó de acuerdo con las recomendaciones de Compute Optimizer. Se eligen las opciones más óptimas manteniendo los mismos parámetros de plataforma (arquitectura, hipervisor, interfaz de red, tipo de virtualización, etc.) si existe la opción.	Sin restricciones • Crear AMIBefore cambio de tamaño: para crear la AMI de la instancia como copia de seguridad antes de cambiar el tamaño, establézcala en «Verdadero». Para no crear una copia de seguridad, establézcala en «False». El valor predeterminado es «Verdadero». Sin restricciones

Opción de optimización	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Recomendaciones de volumen de Amazon EBS	AWSManagedServices-ModifyEBSVolume El volumen de Amazon EBS se modifica de acuerdo con las recomendaciones de Compute Optimizer. La modificación puede incluir el tipo de volumen, el tamaño, las IOPS y la generación de volúmenes (gp2, gp3, etc.).	• CreateSnapshot: Para crear una instantánea antes de modificar el volumen, establézcalo en «Verdadero». Para no crear una instantánea, establézcala en «Falso». El valor predeterminado es «Verdadero». Sin restricciones • VolumeType: El tipo de volumen deseado. Si no se especifica ningún tipo, se conserva el tipo existente. Sin restricciones • VolumeSize: El tamaño deseado del volumen, en GiB. El tamaño del volumen objetivo debe ser mayor o igual al tamaño actual del volumen. Si no se especifica ningún tamaño, se conserva el tamaño existente. Sin restricciones • IOPS: el número solicitado de I/O operaciones por segundo (IOPS). Este parámetro solo es válido para los volúmenes io1, io2 y gp3. Sin restricciones • Rendimiento: el rendimiento para aprovisionar un volumen, con un máximo de 1000 MiB/s. Este parámetro solo es válido para los volúmenes gp3.

Opción de optimización	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
		Sin restricciones • RemediateStackDrift: Para iniciar la corrección de la desviación, si alguna desviación se debe a una modificación del volumen, establézcala en «Verdadero». Para no intentar corregir las desviaciones, establézcalo en «False». El valor predeterminado es «Verdadero». Sin restricciones
Recomendaciones de funciones Lambda	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda memoria de funciones optimizada de acuerdo con las recomendaciones de Compute Optimizer.	RecommendedMemorySize : tamaño de memoria personalizado, si es diferente de las opciones recomendadas. Sin restricciones

Recursos inactivos

Opción de optimización	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Volumen Amazon EBS inactivo	AWSManagedServices-DeleteUnusedEBSVolume Se eliminará el volumen Amazon EBS no adjunto.	• CreateSnapshot: Para crear una instantánea antes de eliminar el volumen, establézcalo en «Verdadero». Para no crear una instantánea, establézcala en «Falso». El valor predeterminado es «Verdadero». Sin restricciones • MinimumUnattachedDays: mínimo de días sin adjuntar del volumen de Amazon EBS para eliminar, hasta 62 días. El valor predeterminado es 7. Sin restricciones
EC2 Instancia de Amazon inactiva	AWSManagedServices-StopEC2Instance La EC2 instancia de Amazon inactiva se detendrá.	ForceStopWithInstanceStore: Para forzar la detención de las instancias que utilizan el almacén de instancias, establézcalo en «True». Para no forzar la parada, establézcalo en «False». El valor predeterminado «False» impide que la instancia se detenga. Sin restricciones

Opción de optimización	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Instancia de Amazon RDS inactiva	AWSManagedServices-StopIdleRDSInstance Detenga una instancia de Amazon RDS inactiva. Los motores compatibles son: MariaDB, Microsoft SQL Server, MySQL, Oracle y PostgreSQL. Este documento no se aplica a Aurora MySQL ni a Aurora PostgreSQL. La instancia se detendrá durante un máximo de 7 días y se volverá a lanzar automáticamente.	No se permiten parámetros preconfigurados. No hay restricciones

Trusted Advisor comprobaciones compatibles con Trusted Remediator

La siguiente tabla muestra las Trusted Advisor comprobaciones admitidas, los documentos de automatización de SSM, los parámetros preconfigurados y el resultado esperado de los documentos de automatización. Revise el resultado esperado para ayudarlo a comprender los posibles riesgos en función de los requisitos de su empresa antes de utilizar un documento de automatización de SSM para corregir las comprobaciones.

Asegúrese de que la regla de configuración correspondiente a cada Trusted Advisor comprobación esté presente en las comprobaciones compatibles para las que desee habilitar la corrección. Para obtener más información, consulte [Ver las AWS Trusted Advisor comprobaciones impulsadas por AWS Config](#). Si una comprobación tiene AWS Security Hub los controles correspondientes, asegúrese de que el control Security Hub esté activado. Para obtener más información, consulte [Habilitar los controles en Security Hub](#). Para obtener información sobre la gestión de los parámetros preconfigurados, consulte [Configurar la corrección de comprobaciones de Trusted Advisor en Trusted Remediator](#).

Trusted Advisor comprobaciones de optimización de costes compatibles con Trusted Remediator

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Z4 AUBRNSmz Direcciones IP elásticas no asociadas	AWSManagedServices-TrustedRemediatorReleaseElasticIP Libera una dirección IP elástica que no está asociada a ningún recurso.	No se permiten parámetros preconfigurados. No hay restricciones
c18d2gz150 - Instancias de Amazon detenidas EC2	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime: Se cancelan EC2 las instancias de Amazon detenidas durante varios días.	• CreateAMIBefore termination: para crear la AMI de la instancia como respaldo antes de terminar la EC2 instancia de Amazon, elija <code>true</code>. Para no crear una copia de seguridad antes de la finalización, elija <code>false</code>. El valor predeterminado es <code>true</code>. • AllowedDays: El número de días que la instancia estuvo detenida antes de ser cancelada. El valor predeterminado es 30. Sin restricciones
c18d2gz128 Repositorio de Amazon ECR sin política de ciclo de vida configurada	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy Crea una política de ciclo de vida para el repositorio especificado si aún no existe una política de ciclo de vida.	ImageAgeLimit: El límite de edad máximo en días (de 1 a 365) para «cualquier» imagen del repositorio de Amazon ECR. Sin restricciones
DAvU99Dc4C	AWSManagedServices-DeleteUnusedEBSVolume	• CreateSnapshot: Si se establece en <code>true</code>, la automatización crea

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Volúmenes de Amazon EBS infrautilizados	Elimina los volúmenes de Amazon EBS infrautilizados si los volúmenes no se adjuntaron durante los últimos 7 días. De forma predeterminada, se crea una instantánea de Amazon EBS.	una instantánea del volumen de Amazon EBS antes de eliminarlo. El ajuste predeterminado es <code>true</code>. Los valores válidos son <code>true</code> y <code>false</code> (distinguen mayúsculas de minúsculas). • <code>MinimumUnattachedDays</code>: Un mínimo de días sin adjuntar del volumen de EBS que se debe eliminar, hasta 62 días. Si se establece en <code>0</code>, el documento SSM no comprueba el período sin adjuntar y elimina el volumen si el volumen no está adjunto actualmente. El valor predeterminado es. 7 Sin restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
hola M8 LMh88u Balanceadores de carga inactivos	AWSManagedServices-DeleteIdleClassicLoadBalancer Elimina un Classic Load Balancer inactivo si no se utiliza y no hay ninguna instancia registrada.	IdleLoadBalancerDays: el número de días durante los que el Classic Load Balancer ha solicitado 0 conexiones antes de considerarlo inactivo. El valor predeterminado es de siete días. Si la ejecución automática está habilitada, la automatización elimina los balanceadores de carga clásicos inactivos si no hay instancias de back-end activas. Para todos los balanceadores de carga clásicos inactivos que tienen instancias de back-end activas, pero que no tienen instancias de back-end en buen estado, no se usa la corrección automática OpsItems y para la remediación manual se crea.
TI39HalfU8 Amazon RDS Idle DB Instances	AWSManagedServices-StopIdleRDSInstance Se detiene la instancia de base de datos de Amazon RDS que ha estado inactiva durante los últimos siete días.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
COr6dfpM05 AWS Lambda funciones sobreaprovisionadas para el tamaño de la memoria	AWSManagedServices-ResizeLambdaMemory AWS Lambda el tamaño de la memoria de la función se redimensiona al tamaño de memoria recomendado proporcionado por. Trusted Advisor	RecommendedMemorySize: la asignación de memoria recomendada para la función Lambda. El rango de valores está entre 128 y 10240. Si el tamaño de la función Lambda se modificó antes de que se ejecutara la automatización, esta automatización podría sobrescribir la configuración con el valor recomendado por. Trusted Advisor
QCH7dWoux1 EC2 Instancias Amazon de baja utilización	AWSManagedServices-StopEC2Instance (documento SSM predeterminado para el modo de ejecución automática y manual). Se detienen EC2 las instancias de Amazon que se utilizan poco.	ForceStopWithInstanceStore: Se configura en <code>true</code> para forzar la detención de las instancias mediante el almacén de instancias. De lo contrario, establézcala en <code>false</code> . El valor predeterminado de <code>false</code> impide que la instancia se detenga. Los valores válidos son verdadero o falso (distingue entre mayúsculas y minúsculas). Sin restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
QCH7DWOUx1 EC2 Instancias Amazon de baja utilización	AWSManagedServices-ResizeInstanceByOneLevel El tamaño de la EC2 instancia de Amazon se redimensiona en un tipo de instancia inferior en el mismo tipo de familia de instancias. La instancia se detiene e inicia durante la operación de cambio de tamaño y vuelve al estado inicial una vez finalizada la ejecución del documento SSM. Esta automatización no admite el cambio de tamaño de las instancias que se encuentran en un grupo de Auto Scaling.	• MinimumDaysSinceLastChange: Número mínimo de días desde el último cambio de tipo de instancia. Si el tipo de instancia se modificó dentro de un tiempo específico, el tipo de instancia no cambiará. Se usa 0 para omitir esta validación. El valor predeterminado es 7. • AMIBefore cambio de tamaño: para crear la AMI de la instancia como copia de seguridad antes de cambiar el tamaño, elija <code>true</code>. Para no crear una copia de seguridad, elija <code>false</code>. El valor predeterminado es <code>false</code>. Los valores válidos son <code>true</code> y <code>false</code> (distinguen mayúsculas de minúsculas). • ResizeIfStopped: Para continuar con el cambio de tamaño de la instancia, incluso si la instancia está detenida, elija <code>true</code>. Para no cambiar automáticamente el tamaño de la instancia si está detenida, elija <code>false</code>. Los valores válidos son <code>true</code> y <code>false</code> (distinguen mayúsculas de minúsculas). Sin restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
QCH7DWOUx1 EC2 Instancias Amazon de baja utilización	AWSManagedServices-TerminateInstance Las EC2 instancias de Amazon poco utilizadas se cancelan si no forman parte de un Auto Scaling Group y la protección de terminación no está habilitada. De forma predeterminada, se crea una AMI.	Crear AMI Before terminación: defina esta opción como <code>true</code> o <code>false</code> cree una AMI de instancia como respaldo antes de terminar la EC2 instancia. El valor predeterminado es <code>true</code> . Los valores válidos son <code>true</code> y <code>false</code> (distinguen mayúsculas de minúsculas). Sin restricciones
G31sq1e9u Underutilized Amazon Redshift Clusters	AWSManagedServices-PauseRedshiftCluster El clúster de Amazon Redshift está en pausa.	No se permiten parámetros preconfigurados. No hay restricciones
c1cj39rr6v Configuración incompleta de cancelación de carga multiparte de Amazon S3	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload El bucket de Amazon S3 está configurado con una regla de ciclo de vida para anular las cargas de varias partes que permanecen incompletas después de ciertos días.	DaysAfterInitiation: el número de días transcurridos los cuales Amazon S3 detiene una carga multiparte incompleta. El valor predeterminado es de 7 días. Sin restricciones
c1z7kmr00n Recomendaciones de optimización de EC2 costos de Amazon para instancias	Utilice las recomendaciones de EC2 instancias de Amazon y la EC2 instancia de Amazon inactiva de Recomendaciones de Compute Optimizer respaldadas por Trusted Remediator .	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
c1z7kmr02n Recomendaciones de optimización de costos de Amazon EBS para volúmenes	Utilice las recomendaciones de volumen de Amazon EBS y el volumen de Amazon EBS inactivo desde. Recomendaciones de Compute Optimizer respaldadas por Trusted Remediator	No se permiten parámetros preconfigurados. No hay restricciones
c1z7kmr03n Recomendaciones de optimización de costes de Amazon RDS para instancias de base de datos	Utilice la instancia inactiva de Amazon RDS de Recomendaciones de Compute Optimizer respaldadas por Trusted Remediator .	No se permiten parámetros preconfigurados. No hay restricciones
c1z7kmr05n AWS Lambda recomendaciones de optimización de costes para las funciones	Utilice las recomendaciones de funciones Lambda de. Recomendaciones de Compute Optimizer respaldadas por Trusted Remediator	No se permiten parámetros preconfigurados. No hay restricciones

Trusted Advisor controles de seguridad compatibles con Trusted Remediator

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
12Fnkpl8Y5 Exposed Access Keys	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey La clave de acceso IAM expuesta está desactivada.	No se permiten parámetros preconfigurados. Las aplicaciones configuradas con una clave de acceso de IAM expuesta no se pueden autenticar.
Hs4Ma3G127: el registro de ejecución de API Gateway REST WebSocket y API debe estar habilitado Verificación APIGateway ycorrespondiente AWS Security Hub : 1.	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging El registro de ejecución está habilitado en la fase de la API.	LogLevel: Nivel de registro para habilitar el registro de la ejecución , ERROR - El registro solo está habilitado para los errores. INFO - El registro está habilitado para todos los eventos. Debe conceder permiso a API Gateway para leer y escribir los registros de su cuenta a CloudWatch para habilitar el registro de ejecución; consulte Configurar el CloudWatch registro para REST APIs en API Gateway para obtener más información.
Hs4Ma3G129: las etapas de la API REST de API Gateway deberían tener el rastreo habilitado AWS X-Ray Verificación APIGateway	AWSManagedServices-EnableAPIGatewayXRayTracing El rastreo de X-Ray está habilitado en la fase API.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
ycorrespondiente AWS Security Hub : 3.		
Hs4Ma3G202 - Los datos de la caché de la API REST de API Gateway deben cifrarse en reposo Verificación APIGatewa ycorrespondiente AWS Security Hub: 5.	AWSManagedServices-EnableAPIGatewayCacheEncryption Habilite el cifrado en reposo para los datos de la caché de la API REST de API Gateway si la etapa de la API REST de API Gateway tiene la caché habilitada.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G177 - AWS Security Hub Comprobación correspondiente: los grupos de escalado automático asociados a un balanceador de cargas deben usar las comprobaciones de estado del balanceador de cargas .1 AutoScaling	AWSManagedServices-TrustedRoleEnableAutoScalingGroupELBHealthCheck Las comprobaciones de estado de Elastic Load Balancing están habilitadas para el grupo Auto Scaling.	HealthCheckGracePeriod: La cantidad de tiempo, en segundos, que Auto Scaling espera antes de comprobar el estado de una instancia de Amazon Elastic Compute Cloud que ha entrado en servicio. La activación de las comprobaciones de estado de Elastic Load Balancing puede provocar el reemplazo de una instancia en ejecución si alguno de los balanceadores de carga de Elastic Load Balancing adjuntos al grupo de Auto Scaling indica que está en mal estado. Para obtener más información, consulte Adjuntar un balanceador de cargas de Elastic Load Balancing a su grupo de Auto Scaling
Hs4Ma3G245: las AWS CloudFormation pilas deben integrarse con Amazon Simple Notification Service Verificación correspondiente AWS Security Hub CloudFormation: 1.	AWSManagedServices-EnableCloudFormationStackNotification Asocie una CloudFormation pila a un tema de Amazon SNS para la notificación.	NotificaciónARNs: uno ARNs de los temas de Amazon SNS que se van a asociar a las pilas seleccionadas CloudFormation . Para habilitar la corrección automática, se debe NotificaciónARNs proporcionar el parámetro preconfigurado.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G210: las distribuciones deben tener el registro habilitado CloudFront Verificación correspondiente AWS Security Hub : CloudFront.	AWSManagedServices-EnableCloudFrontDistributionLogging El registro está habilitado para las CloudFront distribuciones de Amazon.	• BucketName: el nombre del depósito de Amazon S3 en el que desea almacenar los registros de acceso. • S3KeyPrefix: el prefijo de la ubicación en el depósito de S3 de los registros de CloudFront distribución de Amazon. • IncludeCookies: Indica si se deben incluir las cookies en los registros de acceso. Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros preconfigurados: • BucketName • S3KeyPrefix • IncludeCookies Para conocer estas restricciones de corrección, consulte ¿Cómo activo el registro en mi distribución? CloudFront

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G109: CloudTrail La validación del archivo de registro debe estar habilitada Comprobación correspondiente AWS Security Hub CloudTrail: 4.	AWSManagedServices-TrustedRoleEnableCloudTrailLoggingValidation Permite la validación CloudTrail del registro de senderos.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G108: las CloudTrail rutas deberían integrarse con Amazon Logs CloudWatch Verificación correspondiente AWS Security Hub CloudTrail: 5.	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail está integrado con CloudWatch Logs.	- CloudWatchLogsLogGroupName: nombre del grupo de CloudWatch registros al que se envían los CloudTrail registros. Debe utilizar un grupo de registro que exista en su cuenta. - CloudWatchLogsRoleName: Nombre de la función de IAM que debe asumir el punto final de CloudWatch Logs para escribir en el grupo de registros de un usuario. Debe utilizar un rol que ya exista en su cuenta. Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros preconfigurados: - CloudWatchLogsLogGroupName - CloudWatchLogsRoleName

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G217: CodeBuild los entornos de proyecto deben tener una configuración de registro AWS Verificación correspondiente AWS Security Hub CodeBuild: 4.	AWSManagedServices-TrustedRolemediatorEnableCodeBuildLoggingConfig Habilita el registro del CodeBuild proyecto.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G306 - Los clústeres de base de datos de Neptune deberían tener habilitada la protección de eliminación AWS Security Hub Verificación correspondiente: documento DB.3	AWSManagedServices-TrustedRolemediatorDisablePublicAccessOnDocumentDBSnapshot Elimina el acceso público de la instantánea manual del clúster de Amazon DocumentDB.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G308: Los clústeres de Amazon DocumentDB deben tener habilitada la protección de eliminación AWS Security Hub Verificación correspondiente: documento DB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection Habilita la protección contra la eliminación del clúster de Amazon DocumentDB.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G323 - Las tablas de DynamoDB deben tener habilitada la protección de eliminación AWS Security Hub Comprobación correspondiente: DynamoDB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection Permite la protección contra la eliminación de tablas DynamoDB que no son de AMS.	No se permiten parámetros preconfigurados. No hay restricciones
EPS02JT06w: Instantáneas públicas de Amazon EBS	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot El acceso público a la instantánea de Amazon EBS está deshabilitado.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G118: Los grupos de seguridad predeterminados de VPC no deberían permitir el tráfico entrante o saliente Verificación EC2correspondiente AWS Security Hub: 2.	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG Se eliminan todas las reglas de entrada y salida del grupo de seguridad predeterminado.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G117: Los volúmenes EBS adjuntos deben cifrarse en reposo Verificación correspondiente AWS Security Hub EC2: 3.	AWSManagedServices-EncryptInstanceVolume El volumen de Amazon EBS adjunto a la instancia está cifrado.	• KMSKeyID: ID de AWS KMS clave o ARN para cifrar el volumen. • DeleteStaleNonEncryptedSnapshotBackups: un indicador que decide si se debe eliminar la copia de seguridad instantánea de los volúmenes antiguos no cifrados. La instancia se reinicia como parte de la corrección y es posible revertirla si DeleteStaleNonEncryptedSnapshotBackups está configurada de esta manera, lo que ayuda a falsear la restauración.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G120: las instancias detenidas EC2 deben eliminarse después de un período de tiempo específico Verificación EC2correspondiente AWS Security Hub: 4.	AWSManagedServices-TerminateInstance(documento SSM predeterminado para el modo de ejecución automática y manual) EC2 Las instancias de Amazon detenidas durante 30 días se cancelan.	Crear AMIBefore rescisión: Para crear la AMI de la instancia como respaldo antes de terminar la EC2 instancia, elija <code>true</code>. Para no crear una copia de seguridad antes de la finalización, elija <code>false</code>. El valor predeterminado es <code>true</code>. Sin restricciones
Hs4Ma3G120: las EC2 instancias detenidas deben eliminarse después de un período de tiempo específico Verificación EC2correspondiente AWS Security Hub: 4.	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime: EC2 Las instancias de Amazon detenidas durante el número de días definido en Security Hub (el valor predeterminado es 30) se cancelan.	Crear AMIBefore terminación: para crear la AMI de la instancia como respaldo antes de terminar la EC2 instancia, elija <code>true</code>. Para no crear una copia de seguridad antes de la finalización, elija <code>false</code>. El valor predeterminado es <code>true</code>. Sin restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G12 1: el cifrado por defecto de EBS debe estar activado Verificación correspondiente AWS Security Hub : EC27.	AWSManagedServices-EncryptEBSByDefault El cifrado de Amazon EBS está habilitado de forma predeterminada para el Región de AWS	No se permiten parámetros preconfigurados. El cifrado de manera predeterminada es una configuración específica de la región. Si lo habilita para una región, no podrá deshabilitarlo para volúmenes o instantáneas individuales de esa región.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G124: Las instancias de EC2 Amazon deberían usar la versión 2 del servicio de metadatos de instancias () IMDSv2 Verificación correspondiente AWS Security Hub EC2: .8.	AWSManagedServices-TrustedRolemediatorHabilitar instancia EC2 IMDSv2 EC2 Las instancias de Amazon utilizan Instance Metadata Service versión 2 (IMDSv2).	• IMDSv1MetricCheckPeriod: El número de días (42-455) para analizar las métricas de IMDSv1 uso CloudWatch. Si la EC2 instancia de Amazon se creó dentro del período de tiempo especificado, el análisis comienza a partir de la fecha de creación de la instancia. • HttpPutResponseHopLimit: el número máximo de saltos de red permitidos para el token de metadatos de la instancia. Este valor se puede configurar entre saltos 1 y 2. Un límite de saltos de 1 restringe el acceso del token a los procesos que se ejecutan directamente en la instancia, mientras que un límite de saltos de 2 permite el acceso desde los contenedores que se ejecutan en la instancia. Sin restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G207: las EC2 subredes no deberían asignar automáticamente direcciones IP públicas Verificación EC2correspondiente AWS Security Hub: 1.5	AWSManagedServices-UpdateAutoAssignPublicIpv4 direcciones Las subredes de VPC están configuradas para no asignar automáticamente direcciones IP públicas.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G209: se eliminan las listas de control de acceso a la red no utilizadas Verificación EC2correspondiente AWS Security Hub: 1.6	AWSManagedServices-DeleteUnusedNACL Eliminar la ACL de red no utilizada	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G215: Los grupos de seguridad de EC2 Amazon no utilizados deberían eliminarse Verificación correspondiente AWS Security Hub EC2: .22	AWSManagedServices-DeleteSecurityGroups Elimine los grupos de seguridad no utilizados.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G247: Amazon Transit EC2 Gateway no debería aceptar automáticamente las solicitudes de adjuntos de VPC Verificación EC2correspondiente AWS Security Hub: 2.3	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach- Desactiva la aceptación automática de las solicitudes de adjuntos de VPC para el Amazon Transit EC2 Gateway especificado que no sea de AMS.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G235: los repositorios privados de ECR deberían tener configurada la inmutabilidad de etiquetas Verificación correspondiente AWS Security Hub : ECR.2	AWSManagedServices-TrustedR emediatorSetImageTagImmutability Establece la configuración de mutabilidad de la etiqueta de imagen en INMUTABLE para el repositorio especificado.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G216: los repositorios de ECR deben tener configurada al menos una política de ciclo de vida Verificación AWS Security Hub correspondiente: ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy El repositorio de ECR tiene configurada una política de ciclo de vida.	LifecyclePolicyText: El texto de la política del repositorio JSON que se aplicará al repositorio. Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros preconfigurados: LifecyclePolicyText

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G325: los clústeres EKS deben tener habilitado el registro de auditoría Verificación correspondiente AWS Security Hub : EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog El registro de auditoría está habilitado para el clúster EKS.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G183: el balanceador de carga de aplicaciones debe configurarse para eliminar los encabezados HTTP Verificación AWS Security Hub correspondiente: ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer está configurado para campos de encabezado no válidos.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G184: Debe habilitarse el registro de los balanceadores de carga de aplicaciones y los balanceadores de carga clásicos Verificación correspondiente AWS Security Hub : ELB.5	AWSManagedServices-EnableELBLogging (documento SSM predeterminado para el modo de ejecución automática y manual) El registro de Application Load Balancer y Classic Load Balancer está habilitado.	• BucketName: el nombre del depósito (no el ARN). Asegúrese de que la política de bucket esté configurada correctamente para el registro. • S3KeyPrefix: el prefijo de la ubicación en el bucket de Amazon S3 para los registros de Elastic Load Balancing. Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros preconfigurados: • BucketName • S3KeyPrefix El bucket de Amazon S3 debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir los registros de acceso en el bucket.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G184: El registro de los balanceadores de carga de aplicaciones y los balanceadores de carga clásicos debe estar habilitado Verificación correspondiente AWS Security Hub : ELB.5	AWSManagedServices-EnableELBLoggingV2 El registro de Application Load Balancer y Classic Load Balancer está habilitado.	• TargetBucketTagKey: el nombre de la etiqueta (distingue entre mayúsculas y minúsculas) que se utiliza para identificar el bucket de Amazon S3 de destino. Utilícela junto con TargetBucketTagValue la etiqueta del bucket que servirá como bucket de destino para el registro de acceso. • TargetBucketTagValue: el valor de la etiqueta (distingue entre mayúsculas y minúsculas) que se utiliza para identificar el bucket de Amazon S3 de destino. Úselo para TargetBucketTagKey etiquetar el bucket que servirá como bucket de destino para el registro de acceso. • S3BucketPrefix: el prefijo (jerarquía lógica) del bucket de Amazon S3. El prefijo que especifique no debe incluir la cadena AWSLogs. Para obtener más información, consulte Organizar objetos con prefijos. Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros preconfigurados: • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
		El bucket de Amazon S3 debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir los registros de acceso en el bucket.
Hs4Ma3G326: La configuración de acceso público del bloque Amazon EMR debe estar habilitada AWS Security Hub Verificación correspondiente: EMR.2	AWSManagedServices-TrustedRoleMediatorEnableEMRBlockPublicAccess La configuración de acceso público del bloqueo de Amazon EMR está activada en la cuenta.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G135: las AWS KMS claves no deben borrarse involuntariamente Verificación correspondiente AWS Security Hub : KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS se cancela la eliminación de la clave.	No se permite ningún parámetro preconfigurado. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G299 - Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas AWS Security Hub Comprobación correspondiente: Neptune.4	AWSManagedServices-TrustedRoleMediatorEnableNeptuneDBClusterDeletionProtection Habilita la protección contra la eliminación del clúster de Amazon Neptune.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G319 - Los firewalls de Network Firewall deben tener habilitada la protección de eliminación Verificación AWS Security Hub correspondiente Network Firewall: 9.	AWSManagedServices-TrustedRoleMediatorEnableNetworkFirewallDeletionProtection- Habilita la protección de eliminación para AWS Network Firewall.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G223: los OpenSearch dominios deben cifrar los datos enviados entre nodos Verificación correspondiente AWS Security Hub OpenSearch h: 3.	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption El cifrado de nodo a nodo está habilitado para el dominio.	No se permiten parámetros preconfigurados. Una vez que se habilita el node-to-node cifrado, no se puede deshabilitar la configuración. En su lugar, haz una instantánea manual del dominio cifrado, crea otro dominio, migra tus datos y, a continuación, elimina el dominio anterior.
Hs4Ma3G222: el registro de errores de OpenSearch dominio en los registros debe estar habilitado CloudWatch Verificación correspondiente AWS Security Hub : Opensearch h.4	AWSManagedServices-EnableOpenSearchLogging El registro de errores está activado para el dominio. OpenSearch	CloudWatchLogGroupArn: El ARN de un grupo de registros de Amazon CloudWatch Logs. Para habilitar la corrección automática, se debe proporcionar el siguiente parámetro preconfigurado: CloudWatchLogGroupArn La política CloudWatch de recursos de Amazon debe configurarse con permisos. Para obtener más información, consulta Cómo habilitar los registros de auditoría en la Guía del usuario de Amazon OpenSearch Service

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G221: los OpenSearch dominios deben tener habilidad o el registro de auditoría Verificación correspondiente AWS Security Hub : Opensearch h.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch los dominios están configurados con el registro de auditoría activado.	CloudWatchLogGroupArn: el ARN del grupo de CloudWatch registros en el que se van a publicar los registros. Para habilitar la corrección automática, se debe proporcionar el siguiente parámetro preconfigurado: CloudWatchLogGroupArn La política CloudWatch de recursos de Amazon debe configurarse con permisos. Para obtener más información, consulta Cómo habilitar los registros de auditoría en la Guía del usuario de Amazon OpenSearch Service
Hs4Ma3G220: Las conexiones a los OpenSearch dominios deben cifrarse mediante TLS 1.2 Verificación correspondiente AWS Security Hub : Opensearch h.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 La política de TLS está configurada como `policy-MIN-TLS-1-2-2019-07` y solo se permiten las conexiones cifradas a través de HTTPS (TLS).	No se permiten parámetros preconfigurados. Se requieren conexiones a los OpenSearch dominios para usar TLS 1.2. El cifrado de los datos en tránsito puede afectar al rendimiento. Pruebe sus aplicaciones con esta función para comprender el perfil de rendimiento y el impacto del TLS.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G194: La instantánea de Amazon RDS debe ser privada Verificación correspondiente AWS Security Hub : RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 El acceso público a la instantánea de Amazon RDS está deshabilitado.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G192: las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible AWS Verificación correspondiente AWS Security Hub : RDS.2	AWSManagedServices-TrustedResourceDisablingPublicAccessOnRDSInstance Inhabilite el acceso público a la instancia de base de datos de RDS.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G189: la supervisión mejorada está configurada para las instancias de base de datos de Amazon RDS Verificación correspondiente AWS Security Hub : RDS.6	AWSManagedServices-TrustedR emediatorEnableRDSEnhancedM onitoring Habilite una supervisión mejorada para las instancias de base de datos de Amazon RDS	• MonitoringInterval: El intervalo, en segundos, entre los puntos en los que se recopilan las métricas de supervisión mejorada para la instancia de base de datos. Los intervalos válidos son 0, 1, 5, 10, 15, 30 y 60. Para deshabilitar la recopilación de métricas de monitorización mejorada, especifique 0. • MonitoringRoleName: el nombre de la función de IAM que permite a Amazon RDS enviar métricas de supervisión mejoradas a Amazon CloudWatch Logs. Si no se especifica un rol, se usa <code>aws-rds-monitoring-role</code> se crea el rol predeterminado, si no existe. Si se habilita la supervisión mejorada antes de la ejecución de la automatización, esta automatización podría sobrescribir los ajustes con los MonitoringRoleName valores MonitoringInterval y configurados en los parámetros preconfigurados.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G190: Los clústeres de Amazon RDS deben tener habilitada la protección de eliminación Verificación correspondiente AWS Security Hub : RDS.7	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection La protección contra la eliminación está habilitada para los clústeres de Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G198: Las instancias de base de datos de Amazon RDS deben tener habilitada la protección de eliminación Verificación correspondiente AWS Security Hub : RDS.8	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection La protección contra la eliminación está habilitada para las instancias de Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G199: las instancias de base de datos de RDS deberían publicar los registros en Logs CloudWatch Verificación correspondiente AWS Security Hub : RDS.9	AWSManagedServices-TrustedR emediatorEnableRDSLogExports La exportación de registros de RDS está habilitada para la instancia de base de datos de RDS o el clúster de base de datos de RDS.	No se permiten parámetros preconfigurados. Se requiere el rol AWSServiceRoleForRDS vinculado al servicio.
Hs4Ma3G160: la autenticación de IAM debe configurarse para las instancias de RDS Verificación correspondiente AWS Security Hub : RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management la autenticación está habilitada para la instancia de RDS.	ApplyImmediately: Indica si las modificaciones de esta solicitud y las modificaciones pendientes se aplican de forma asíncrona lo antes posible. Para aplicar el cambio inmediatamente, elija. <code>true</code> Para programar el cambio para el siguiente período de mantenimiento, seleccione. <code>false</code> Sin restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G16 1: la autenticación de IAM debe configurarse para los clústeres de RDS Verificación correspondiente AWS Security Hub : RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication La autenticación de IAM está habilitada para el clúster de RDS.	ApplyImmediately: Indica si las modificaciones de esta solicitud y las modificaciones pendientes se aplican de forma asíncrona lo antes posible. Para aplicar el cambio inmediatamente, seleccione. true Para programar el cambio para el siguiente período de mantenimiento, seleccione. false Sin restricciones
Hs4Ma3G16 2: las actualizaciones automáticas de las versiones secundarias de RDS deberían estar habilitadas Verificación correspondiente AWS Security Hub : RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade La configuración de actualización automática de versiones secundarias para Amazon RDS está habilitada.	No se permiten parámetros preconfigurados. La instancia de Amazon RDS debe estar en ese available estado para que se produzca esta corrección.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G163: Los clústeres de bases de datos de RDS deben configurarse para copiar etiquetas en las instantáneas Verificación correspondiente AWS Security Hub : RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagstosnapshot la configuración de los clústeres de Amazon RDS está habilitada.	No se permiten parámetros preconfigurados. Las instancias de Amazon RDS deben estar en estado disponible para que se produzca esta corrección.
Hs4Ma3G164: las instancias de base de datos de RDS deben configurarse para copiar etiquetas en las instantáneas Verificación correspondiente AWS Security Hub : RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagsToSnapshot la configuración de Amazon RDS está habilitada.	No se permiten parámetros preconfigurados. Las instancias de Amazon RDS deben estar en estado disponible para que se produzca esta corrección.
RsS93 HQwa1 Instantáneas públicas de Amazon RDS	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 El acceso público a la instantánea de Amazon RDS está deshabilitado.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G103: Los clústeres de Amazon Redshift deberían prohibir el acceso público AWS Security Hub Comprobación correspondiente: Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster El acceso público al clúster de Amazon Redshift está deshabilitado.	No se permiten parámetros preconfigurados. Al deshabilitar el acceso público, se bloquean todos los clientes que vienen de Internet. Además, el clúster de Amazon Redshift permanece en estado de modificación durante unos minutos mientras la corrección inhabilita el acceso público al clúster.
Hs4Ma3G106: Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría AWS Security Hub Comprobación correspondiente: Redshift.4	AWSManagedServices-TrustedRedshiftClusterAuditLogging El registro de auditoría se habilita en el clúster de Amazon Redshift durante el período de mantenimiento.	No se permiten parámetros preconfigurados. Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros preconfigurados. BucketName: El depósito debe estar en el mismo lugar. Región de AWS El clúster debe tener permisos de lectura y colocar objetos. Si el registro del clúster de Redshift está habilitado antes de la ejecución de la automatización, esta automatización podría sobrescribir los ajustes de registro con S3KeyPrefix los valores BucketName y configurados en los parámetros preconfigurados.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G105: Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las principales versiones AWS Security Hub Comprobación correspondiente: Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade- Las principales actualizaciones de las versiones se aplican automáticamente al clúster durante el período de mantenimiento. No hay un tiempo de inactividad inmediato para el clúster de Amazon Redshift, pero su clúster de Amazon Redshift podría sufrir un tiempo de inactividad durante el período de mantenimiento si se actualiza a una versión principal.	No se permiten parámetros preconfigurados. No hay restricciones
Hs4Ma3G104: Los clústeres de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado AWS Security Hub Comprobación correspondiente: Redshift.7	AWSManagedServices-TrustedRedshiftClusterEnhancedVPCRouting El enrutamiento de VPC mejorado está habilitado para los clústeres de Amazon Redshift.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G173: la configuración de acceso público del bloque S3 debe estar habilitada en el nivel del bucket Verificación correspondiente AWS Security Hub: S3.8	AWSManagedServices-TrustedRoleBlockS3BucketPublicAccess Los bloques de acceso público a nivel de bucket se aplican al bucket de Amazon S3.	No se permiten parámetros preconfigurados. Esta corrección podría afectar a la disponibilidad de los objetos de S3. Para obtener información sobre cómo Amazon S3 evalúa el acceso, consulte Bloquear el acceso público a su almacenamiento de Amazon S3.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G230: el registro de acceso al servidor de bucket S3 debe estar habilitado Verificación AWS Security Hub correspondiente: S3.9	AWSManagedServices-EnableBucketAccessLogging(documento SSM predeterminado para el modo de ejecución automática y manual) El registro de acceso al servidor Amazon S3 está activado.	• TargetBucket: El nombre del depósito de S3 para almacenar los registros de acceso al servidor. • TargetObjectKeyFormat: formato de clave de Amazon S3 para objetos de registro (los valores distinguen entre mayúsculas y minúsculas). Para usar el formato simple de las claves S3 para los objetos de registro, elijaSimplePrefix . Para usar la clave S3 particionada para los objetos de registro y usarla EventTime para el prefijo particionado, elija. PartitionedPrefixEventTime Para usar la clave S3 particionada para los objetos de registro y usarla DeliveryTime para el prefijo particionado, elija. PartitionedPrefixDeliveryTime Los valores admitidos son SimplePrefix , PartitionedPrefixEventTime y PartitionedPrefixDeliveryTime . Para habilitar la corrección automática, se debe proporcionar el siguiente parámetro preconfigurado:. TargetBucket El depósito de destino debe estar en el mismo depósito Región de

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
		AWS y Cuenta de AWS al de origen, con los permisos correctos para la entrega de registros. Para obtener más información, consulte Habilitación del registro de acceso al servidor de Amazon S3 .

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G230: el registro de acceso al servidor de bucket S3 debe estar habilitado Verificación AWS Security Hub correspondiente: S3.9	AWSManagedServices-TrustedRoleMediatorEnableBucketAccessLoggingV2: El registro de buckets de Amazon S3 está activado.	• TargetBucketTagKey: El nombre de la etiqueta (distingue entre mayúsculas y minúsculas) para identificar el bucket de destino. Utilícelo TargetBucketTagValue para etiquetar el depósito que se utilizará como depósito de destino para el registro de acceso. • TargetBucketTagValue: El valor de la etiqueta (distingue entre mayúsculas y minúsculas) para identificar el depósito de destino, TargetBucketTagKey utilícelo y etiquete el depósito para que se utilice como depósito de destino para el registro de acceso. • TargetObjectKeyFormat: Formato de clave de Amazon S3 para objetos de registro (los valores distinguen entre mayúsculas y minúsculas): para usar el formato simple de las claves S3 para objetos de registro, elija SimplePrefix. Para usar la clave S3 particionada para los objetos de registro y usarla EventTime para el prefijo particionado, elija PartitionedPrefixEventTime. Para usar la clave S3 particionada para los objetos de registro y usarla DeliveryTime para el prefijo particionado, elija PartitionedPrefixDeliveryTime. El

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
		valor predeterminado es PartitionedPrefixEventTime. Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros: TargetBucketTagKey TargetBucketTagValue. El depósito de destino debe estar en el mismo depósito Región de AWS y Cuenta de AWS como el depósito de origen, con los permisos correctos para la entrega de registros. Para obtener más información, consulte Habilitación del registro de acceso al servidor de Amazon S3.
Pfx0 RwgBli Permisos de bucket de Amazon S3	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Bloqueo del acceso público	No se permiten parámetros preconfigurados. Esta comprobación consta de varios criterios de alerta. Esta automatización soluciona los problemas de acceso público. Trusted Advisor No se admite la corrección de otros problemas de configuración señalados por. Esta corrección sí permite corregir los buckets de S3 Servicio de AWS creados (por ejemplo, cf-templates-000000000000).

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G272: Los usuarios no deberían tener acceso root a las instancias de notebook SageMaker Verificación SageMaker correspondiente AWS Security Hub: 3.	AWSManagedServices-TrustedRolemediatorDisableSageMakerNotebookInstanceRootAccess El acceso root para los usuarios está deshabilitado en la instancia de SageMaker Notebook.	No se permiten parámetros preconfigurados. Esta corrección provoca una interrupción si la instancia del SageMaker portátil está en ese estado. InService
Hs4Ma3G179: los temas de SNS deben cifrarse en reposo mediante AWS KMS Verificación correspondiente AWS Security Hub : SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest El tema de SNS está configurado con el cifrado del lado del servidor.	KmsKeyId: el ID de una clave maestra de cliente AWS gestionada (CMK) para Amazon SNS o una CMK personalizada que se utilizará para el cifrado del lado del servidor (SSE). El valor predeterminado es. <code>alias/aws/sns</code> Si se utiliza una AWS KMS clave personalizada, debe configurarse con los permisos correctos. Para obtener más información, consulte el tema Habilitar el cifrado del lado del servidor (SSE) para Amazon SNS

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G158: los documentos SSM no deben ser públicos Verificación correspondiente AWS Security Hub : SSM.4	AWSManagedServices-TrustedRolemediatorDisableSSMDocPublicSharing- Desactiva la compartición pública del documento SSM.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Hs4Ma3G136: las colas de Amazon SQS deben cifrarse en reposo Verificación correspondiente AWS Security Hub : SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest Los mensajes de Amazon SQS están cifrados.	• SqsManagedSseEnabled: Establecido en <code>true</code> para habilitar el cifrado de colas del lado del servidor mediante claves de cifrado propiedad de Amazon SQS, configurado en <code>false</code> para habilitar el cifrado de colas del lado del servidor mediante una clave. AWS KMS • KMSKeyID: el ID o el alias de una clave maestra de cliente AWS gestionada (CMK) para Amazon SQS o una CMK personalizada que se utilizará para cifrar la cola en el servidor. Si no se proporciona, se utiliza. <code>alias/aws/sqs</code> • KmsDataKeyReusePeriodSeconds: El tiempo, en segundos, durante el que Amazon SQS puede reutilizar una clave de datos para cifrar o descifrar los mensajes antes de volver a llamar. AWS KMS Un entero que represent a segundos, entre 60 segundos (1 minuto) y 86 400 segundos (24 horas). Esta configuración se ignora si <code>SqsManagedSseEnabled</code> se establece en. <code>true</code> Se rechazan <code>ReceiveMessage</code> las solicitudes anónimas <code>SendMessage</code> y a la cola cifrada. Todas las solicitudes hechas a las colas con

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
		SSE habilitado deben usar HTTPS y Signature Version 4.

Trusted Advisor las comprobaciones de tolerancia a errores son compatibles con Trusted Remediator

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
c18d2gz138 Recuperación de Amazon DynamoDB Point-in-time	AWSManagedServices-TrustedRemediatorEnableDDBPITR Permite point-in-time la recuperación de tablas de DynamoDB.	No se permiten parámetros preconfigurados. No hay restricciones
R365S2qddf Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning El control de versiones de bucket de Amazon S3 está activado.	No se permiten parámetros preconfigurados. Esta corrección no permite corregir los buckets de S3 Servicio de AWS creados (por ejemplo, cf-templates-0000000000000000).
BueAdJ7nRP Registro de bucket de Amazon S3	AWSManagedServices-EnableBucketAccessLogging El registro de buckets de Amazon S3 está activado.	- TargetBucket: el nombre del depósito de S3 para almacenar los registros de acceso al servidor. - TargetObjectKeyFormat: formato de clave Amazon S3 para objetos de registro, si desea utilizar el formato simple de claves S3 para objetos de registro, elija SimplePrefix . Para usar la clave S3 particionada

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
		para los objetos de registro y usarla EventTime para el prefijo particionado, elija. PartitionedPrefixEventTime Para usar la clave S3 particionada para los objetos de registro y usarla DeliveryTime para el prefijo particionado, elija. PartitionedPrefixDeliveryTime El valor predeterminado es PartitionedPrefixEventTime . Los valores válidos son SimplePrefix , PartitionedPrefixEventTime y PartitionedPrefixDeliveryTime (distinguen mayúsculas de minúsculas). Para habilitar la corrección automática, se deben proporcionar los siguientes parámetros preconfigurados: • TargetBucket El depósito de destino debe estar en el mismo depósito Región de AWS y Cuenta de AWS como el depósito de origen, con los permisos correctos para la entrega de registros. Para obtener más información, consulte Habilitación del registro de acceso al servidor de Amazon S3.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
f2ik5r6dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedR emediatorEnableRDSMultiAZ La implementación en zonas de disponibilidad múltiple está habilitada.	No se permiten parámetros preconfigurados. Es posible que se produzca una degradación del rendimiento durante este cambio.
H7 IgTzj TYb Instantáneas de Amazon EBS	AWSManagedServices-TrustedR emediatorCreateEBSSnapshot EBSsnapshots Se crea Amazon.	No se permiten parámetros preconfigurados. No hay restricciones
Top QPADk ZvH Copias de seguridad de RDS	AWSManagedServices-EnableRDS SBackupRetention La retención de copias de seguridad de Amazon RDS está habilitada para la base de datos.	• BackupRetentionPeriod: El número de días (de 1 a 35) para conservar las copias de seguridad automatizadas. • ApplyImmediately: Indica si el cambio de retención de la copia de seguridad de RDS y cualquier modificación pendiente se aplican de forma asíncrona lo antes posible. Elija true aplicar el cambio inmediatamente o programarlo false para el siguiente período de mantenimiento. Si el ApplyImmediately parámetro está establecido en true, los cambios pendientes en la base de datos se aplican junto con la configuración RDSBackup de retención.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
c1qf5bt013 Las instancias de base de datos de Amazon RDS tienen desactivado el escalado automático de almacenamiento	AWSManagedServices-TrustedRolemediatorEnableRDSInstanceStorageAutoScaling- El escalado automático del almacenamiento está habilitado para la instancia de base de datos de Amazon RDS.	MaxAllocatedStorageIncrease Percentage: El porcentaje de aumento de la corriente Allocated Storage, para establecer el. MaxAllocatedStorage El valor predeterminado es 26. Debe establecer el umbral de almacenamiento máximo en al menos un 10% más que el almacenamiento asignado actualmente. Se recomienda establecer el umbral máximo de almacenamiento en al menos un 26% más. Para obtener más información, consulte Administrar la capacidad automáticamente con el escalado automático del almacenamiento de Amazon Relational Database Service. Sin restricciones
7q GXs KIUw Conexión Classic Load Balancer: Draining	AWSManagedServices-TrustedRolemediatorEnableCLBConnectionDraining El drenaje de conexiones está activado en Classic Load Balancer.	ConnectionDrainingTimeout: El tiempo máximo, en segundos, para mantener abiertas las conexiones existentes antes de anular el registro de las instancias. El valor predeterminado está establecido en segundos. 300 Sin restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
c18d2gz106 Amazon EBS no está incluido en el plan AWS Backup	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS está incluido en el AWS Backup plan.	Remediation etiqueta el volumen de Amazon EBS con el siguiente par de etiquetas. El par de etiquetas debe coincidir con los criterios de selección de recursos basados en etiquetas de. AWS Backup • TagKey • TagValue Sin restricciones
c18d2gz107 La tabla Amazon DynamoDB no está incluida en el plan AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan La tabla Amazon DynamoDB se incluye en el plan. AWS Backup	Remediation etiqueta Amazon DynamoDB con el siguiente par de etiquetas. El par de etiquetas debe coincidir con los criterios de selección de recursos basados en etiquetas de. AWS Backup • TagKey • TagValue Sin restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
c18d2gz117 Amazon EFS no está incluido en el AWS Backup plan	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS está incluido en el AWS Backup plan.	Remediation etiqueta Amazon EFS con el siguiente par de etiquetas. El par de etiquetas debe coincidir con los criterios de selección de recursos basados en etiquetas de AWS Backup • TagKey • TagValue Sin restricciones
c18d2gz105 Equilibrador de carga cruzado del equilibrador de carga de red	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing El equilibrio de carga entre zonas está habilitado en Network Load Balancer.	No se permiten parámetros preconfigurados. No hay restricciones
c1qf5bt026 El synchronous_commit parámetro Amazon RDS está desactivado	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter synchronous_commit El parámetro está activado en Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
c1qf5bt030 El innodb_flush_log_at_trx_commit parámetro Amazon RDS no es 1	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter innodb_flush_log_at_trx_commit El parámetro está establecido en 1 Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones
c1qf5bt031 El sync_binlog parámetro Amazon RDS está desactivado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter sync_binlog El parámetro está activado en Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones
c1qf5bt036 La configuración de innodb_default_row_format parámetros de Amazon RDS no es segura	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter innodb_default_row_format El parámetro está establecido en DYNAMIC Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones
c18d2gz144 La monitorización EC2 detallada de Amazon no está habilitada	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring La monitorización detallada está habilitada para Amazon EC2.	No se permiten parámetros preconfigurados. No hay restricciones

Trusted Advisor las comprobaciones de rendimiento son compatibles con Trusted Remediator

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
COr6dfpM06 AWS Lambda funciones insuficientemente aprovisionadas para el tamaño de la memoria	AWSManagedServices-ResizeLambdaMemory El tamaño de la memoria de las funciones Lambda se redimensiona al tamaño de memoria recomendado proporcionado por. Trusted Advisor	RecommendedMemorySize: la asignación de memoria recomendada para la función Lambda. El rango de valores está entre 128 y 10240. Si el tamaño de la función Lambda se modifica antes de la ejecución de la automatización, esta automatización podría sobrescribir la configuración con el valor recomendado por. Trusted Advisor
ZRxQIPsb6c EC2 Instancias de Amazon de alta utilización	AWSManagedServices-ResizeInstanceByOneLevel Las EC2 instancias de Amazon se redimensionan en un tipo de instancia superior en el mismo tipo de familia de instancias. Las instancias se detienen e inician durante la operación de cambio de tamaño y vuelven al estado inicial una vez finalizada la ejecución. Esta automatización no admite el cambio de tamaño de las instancias que se encuentran en un grupo de Auto Scaling.	• MinimumDaysSinceLastChange: El número mínimo de días transcurridos desde el último cambio de tipo de instancia. Si el tipo de instancia se modificó dentro del tiempo especificado, el tipo de instancia no cambia. Se usa 0 para omitir esta validación. El valor predeterminado es 7. • Crear AMIBefore cambio de tamaño: para crear la AMI de la instancia como copia de seguridad antes de cambiar el tamaño, elija <code>true</code>. Para no crear una copia de seguridad, elija <code>false</code>. El valor predeterminado es <code>false</code>. Los valores válidos son <code>true</code> y <code>false</code> (distinguen mayúsculas de minúsculas).

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
		ResizeIfStopped: Para continuar con el cambio de tamaño de la instancia, incluso si la instancia está detenida, elija <code>true</code>. Para no cambiar automáticamente el tamaño de la instancia si está detenida, elija <code>false</code>. Los valores válidos son <code>true</code> y <code>false</code> (distinguen mayúsculas de minúsculas). Sin restricciones
c1qf5bt021 innodb_change_buffering Parámetro de Amazon RDS que utiliza un valor inferior al óptimo	AWSManagedServices-TrustedRemediatorRemediateRDSParmeterGroupParameter El valor del innodb_change_buffering parámetro se establece en NONE Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones
c1qf5bt025 El autovacuum parámetro Amazon RDS está desactivado	AWSManagedServices-TrustedRemediatorRemediateRDSParmeterGroupParameter autovacuum El parámetro está activado en Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
c1qf5bt028 El enable_indexonlyscan parámetro Amazon RDS está desactivado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter enable_indexonlyscan El parámetro está activado en Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones
c1qf5bt029 El enable_indexscan parámetro Amazon RDS está desactivado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter enable_indexscan El parámetro está activado en Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones
c1qf5bt032 El innodb_stats_persistent parámetro Amazon RDS está desactivado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter innodb_stats_persistent El parámetro está activado en Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones
c1qf5bt037 El general_logging parámetro Amazon RDS está activado	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter general_logging El parámetro está desactivado en Amazon RDS.	No se permiten parámetros preconfigurados. No hay restricciones

Trusted Advisor las comprobaciones de límites de servicio son compatibles con Trusted Remediator

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Ln7rR0l7j9 EC2-Dirección IP elástica de VPC	AWSManagedServices-UpdateVpcElasticIPQuota Se solicita un nuevo límite para las direcciones IP elásticas de EC2 - VPC. De forma predeterminada, el límite se incrementa en 3.	Incremento: el número que se va a aumentar la cuota actual. El valor predeterminado es 3. Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el OK estado, es posible que se produzca un aumento del límite superior.
Km7qq0l7j9 Gateways de Internet de VPC	AWSManagedServices-IncreaseServiceQuota- Se solicita un nuevo límite para las pasarelas de Internet de VPC. De forma predeterminada, el límite se incrementa en tres.	Incremento: el número que se va a aumentar la cuota actual. El valor predeterminado es 3. Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el OK estado, es posible que se produzca un aumento del límite superior.
JL7pp0l7j9 VPC	AWSManagedServices-IncreaseServiceQuota Se solicita un nuevo límite para la VPC. De forma predeterminada, el límite se incrementa en 3.	Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3. Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el OK estado, es posible que se produzca un aumento del límite superior.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
Fw7hh0I7j9 Grupos de Auto Scaling	AWSManagedServices-Increase ServiceQuota Se solicita un nuevo límite para los grupos de Auto Scaling. De forma predeterminada, el límite se incrementa en 3.	Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3. Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el OK estado, es posible que se produzca un aumento del límite superior.
3 Njm0 DJQO9 Grupos de opciones de RDS	AWSManagedServices-Increase ServiceQuota Se solicita un nuevo límite para los grupos de opciones de Amazon RDS. De forma predeterminada, el límite se incrementa en 3.	Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3. Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el OK estado, es posible que se produzca un aumento del límite superior.
EM8b3yLRTr Application Load Balancers de ELB	AWSManagedServices-Increase ServiceQuota Se solicita un nuevo límite para los balanceadores de carga de aplicaciones ELB. De forma predeterminada, el límite se incrementa en 3.	Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3. Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el OK estado, es posible que se produzca un aumento del límite superior.

Compruebe la ID y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
8WiQ K YSt25 Network Load Balancers de ELB	AWSManagedServices-IncreaseServiceQuota Se solicita un nuevo límite para los balanceadores de carga de red ELB. De forma predeterminada, el límite se incrementa en 3.	Incremento: el número para aumentar la cuota actual. El valor predeterminado es 3. Si esta automatización se ejecuta varias veces antes de que la Trusted Advisor comprobación se actualice con el OK estado, es posible que se produzca un aumento del límite superior.

Trusted Advisor comprobaciones de excelencia operativa respaldadas por Trusted Remediator

Compruebe la identificación y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
c18d2gz125 La Amazon API Gateway no registra los registros de ejecución	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging El registro de ejecución está habilitado en la fase API.	No se permiten parámetros preconfigurados. Debe conceder permiso a API Gateway para leer y escribir los registros de su cuenta a CloudWatch fin de habilitar el registro de ejecución; consulte Configurar el CloudWatch registro para REST APIs en API Gateway para obtener más información.
c18d2gz168 La protección contra eliminaci	AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection- La protección contra	No se permiten parámetros preconfigurados. No hay restricciones

Compruebe la identificación y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
El grupo de Elastic Load Balancing no está habilitado para los equilibradores de carga	La eliminación está activada en el Elastic Load Balancer.	
c1qf5bt012 Amazon RDS Performance Insights está desactivado	<code>AWSManagedServices-TrustedRole mediatorEnableRDSPerformanceInsights</code> Performance Insights está activado en Amazon RDS.	<code>PerformanceInsightsRetentionPeriod</code>: El número de días necesarios para conservar los datos de Performance Insights. Valores válidos: 7 o $\text{mes} * 31$, donde el mes es un número de meses comprendido entre 1 y 23. Ejemplos: 93 (3 meses * 31), 341 (11 meses * 31), 589 (19 meses * 31) o 731. <code>PerformanceInsightsKMSKeyID</code>: el identificador AWS KMS clave para el cifrado de los datos de Performance Insights. Si no especificas un valor para el <code>PerformanceInsightsKMSKey</code> identificador, Amazon RDS utilizará la AWS KMS clave predeterminada. Sin restricciones

Compruebe la identificación y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
c1fd6b96l4 Registros de acceso a Amazon S3 activados	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 El registro de acceso al bucket de Amazon S3 está activado.	• TargetBucketTagValue: Utilice el valor de la etiqueta (distingue entre mayúsculas y minúsculas) TargetBucketTagKey para identificar el bucket de destino y etiquetarlo como bucket de destino para el registro de acceso. • TargetObjectKeyFormat: formato de clave de Amazon S3 para objetos de registro (los valores distinguen entre mayúsculas y minúsculas). Para usar el formato simple de las claves S3 para los objetos de registro, elija SimplePrefix. Para usar la clave S3 particionada para los objetos de registro y usarla EventTime para el prefijo particionado, elija PartitionedPrefixEventTime. Para usar la clave S3 particionada para los objetos de registro y usarla DeliveryTime para el prefijo particionado, elija PartitionedPrefixDeliveryTime. Los valores admitidos son SimplePrefix, PartitionedPrefixEventTime y PartitionedPrefixDeliveryTime. Para habilitar la corrección automática, se debe proporcionar el siguiente

Compruebe la identificación y el nombre	Nombre del documento SSM y resultado esperado	Parámetros y restricciones preconfigurados compatibles
		parámetro preconfigurado: TargetBucketTagKey. TargetBucketTagValue El depósito de destino debe estar en el mismo depósito Región de AWS y Cuenta de AWS como el depósito de origen, con los permisos correctos para la entrega de registros. Para obtener más información, consulte Habilitación del registro de acceso al servidor de Amazon S3.

Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator

Las configuraciones se almacenan AWS AppConfig como parte de la aplicación Trusted Remediator. Cada categoría de Trusted Advisor comprobación tiene un perfil de configuración independiente. Para obtener más información sobre Trusted Advisor las categorías, consulte [Ver las categorías de verificación](#).

Puede solicitar la configuración de las correcciones por recurso o por Trusted Advisor comprobación. Puede aplicar excepciones mediante etiquetas de recursos.

Note

La corrección de Trusted Advisor los hallazgos se configura actualmente mediante AWS AppConfig, y esta función es totalmente compatible en la actualidad. AMS anticipa que esto cambiará en el futuro. Se recomienda evitar crear automatizaciones que dependan de ellas AWS AppConfig, ya que este método está sujeto a cambios. Tenga en cuenta que es posible que necesite actualizar o modificar las automatizaciones creadas en torno a la AWS AppConfig implementación actual en el futuro para garantizar la compatibilidad.

El indicador de función Compute Optimizer -> EC2 instances tiene parámetros adicionales:

- **allow-upscale**: permite escalar instancias no optimizadas, con aprovisionamiento insuficiente. EC2 El valor predeterminado es "false".
- **min-savings-opportunity-percentage** La oportunidad mínima de porcentaje de ahorro para la remediación automatizada. El valor predeterminado es el 10%

Configuraciones de corrección predeterminadas

Las configuraciones de las Trusted Advisor comprobaciones individuales se almacenan como AWS AppConfig indicadores. El nombre de la bandera coincide con el nombre del cheque. Cada configuración de verificación contiene los siguientes atributos:

- **modo de ejecución**: determina cómo Trusted Remediator realiza la corrección predeterminada:
 - **Automatizado**: Trusted Remediator corrige automáticamente los recursos creando un documento SSM OpsItem, ejecutándolo y resolviéndolo después tras una ejecución correcta. OpsItem
 - **Manual**: OpsItem se crea un documento, pero el documento SSM no se ejecuta automáticamente. La corrección se revisa OpsItem y se ejecuta mediante el RFC automatizado. Para obtener más información, consulte [Trabaje con las soluciones en Trusted Remediator](#).
 - **Condicional**: la corrección está deshabilitada de forma predeterminada. Puede habilitarla para recursos específicos mediante etiquetas. Para obtener más información, consulte las siguientes secciones [Personalice la remediación con etiquetas de recursos](#) y [Personalice la remediación con etiquetas de anulación de recursos](#).
- **Inactivo**: no se produce ninguna corrección y no OpsItem se crea ninguna. No puede anular el modo de ejecución de la Trusted Advisor comprobación que está configurada como inactiva.
- **parámetros preconfigurados**: introduzca valores para los parámetros del documento SSM necesarios para la corrección automática, en el formato de, separados por una coma (Parameter=Value,). Consulte los parámetros preconfigurados compatibles [Trusted Advisor comprobaciones compatibles con Trusted Remediator](#) para el documento SSM asociado a cada comprobación.
- **alternative-automation-document**: Este atributo ayuda a sustituir el documento de automatización existente por otro documento compatible (si está disponible para la comprobación específica). De forma predeterminada, este atributo no está seleccionado.

 Note

El `alternative-automation-document` atributo no admite documentos de automatización personalizados. Puede utilizar los documentos de automatización de Trusted Remediator compatibles existentes que figuran en [Trusted Advisor comprobaciones compatibles con Trusted Remediator](#).

Por ejemplo, para comprobarlo `Qch7DwouX1`, hay tres documentos SSM asociados: `AWSManagedServices-StopEC2Instance`, y `AWSManagedServices-ResizeInstanceByOneLevel`. `AWSManagedServices-TerminateInstance` El valor de `alternative-automation-document` puede ser uno de los dos `AWSManagedServices-ResizeInstanceByOneLevel` `AWSManagedServices-TerminateInstance` (`AWSManagedServices-StopEC2Instance` es el documento SSM predeterminado que se debe corregir). `Qch7DwouX1`

El valor de cada atributo debe coincidir con las restricciones de ese atributo.

 Tip

Antes de aplicar las configuraciones predeterminadas a las Trusted Advisor comprobaciones, se recomienda considerar el uso de las funciones de etiquetado y anulación de recursos que se describen en las siguientes secciones. Las configuraciones predeterminadas se aplican a todos los recursos de la cuenta, lo que puede no ser conveniente en todos los casos.

A continuación, se muestra un ejemplo de captura de pantalla de una consola con el modo de ejecución configurado en Manual y los atributos que coinciden con sus restricciones.

Personalice la remediación con etiquetas de recursos

Los `manual-for-tagged-only` atributos `automated-for-tagged-only` de la configuración de comprobación le permiten especificar etiquetas de recursos para corregir las comprobaciones individuales. Se recomienda utilizar este método cuando se necesita aplicar un comportamiento de corrección coherente a un grupo de recursos que comparten la misma etiqueta o etiquetas. Las siguientes son descripciones de estas etiquetas:

- **automated-for-tagged-only:** especifique las etiquetas de recursos (uno o más pares de etiquetas, separadas por comas) para que las comprobaciones se corrijan automáticamente, independientemente del modo de ejecución predeterminado.
- **manual-for-tagged-only:** especifique las etiquetas de recursos (uno o más pares de etiquetas, separadas por comas) para las correcciones que deben ejecutarse manualmente, independientemente del modo de ejecución predeterminado.

Por ejemplo, si desea habilitar la corrección automática para todos los recursos que no son de producción y aplicar la corrección manual para los recursos de producción, puede establecer la configuración de la siguiente manera:

```
"execution-mode": "Conditional",  
"automated-for-tagged-only": "Environment=Non-Production",  
"manual-for-tagged-only": "Environment=Production",
```

Con las configuraciones anteriores configuradas en sus recursos, compruebe que el comportamiento de la corrección sea el siguiente:

- Los recursos etiquetados con la etiqueta «Entorno = no producción» se corrigen automáticamente.
- Los recursos etiquetados con la etiqueta «Medio ambiente = producción» requieren una intervención manual para su remediación.
- Los recursos sin la etiqueta «Medio ambiente» siguen el modo de ejecución predeterminado («Condicional», en este caso). Por lo tanto, no se realiza ninguna acción con los recursos restantes).

Para obtener asistencia adicional con sus configuraciones, póngase en contacto con su arquitecto de nube.

Personalice la remediación con etiquetas de anulación de recursos

Las etiquetas de anulación de recursos permiten personalizar el comportamiento de corrección de los recursos individuales, independientemente de sus etiquetas. Al añadir una etiqueta específica a un recurso, se anula el modo de ejecución predeterminado para ese recurso y la comprobación. Trusted Advisor La etiqueta de anulación de recursos tiene prioridad sobre la configuración predeterminada y la configuración de etiquetado de recursos. Por lo tanto, si establece el modo de ejecución predeterminado en Automatizado, Manual o Condicional para un recurso mediante

la etiqueta de anulación de recursos, anulará el modo de ejecución predeterminado y cualquier configuración de etiquetado de recursos.

Para anular el modo de ejecución de un recurso, complete los siguientes pasos:

1. Identifique los recursos para los que desea anular la configuración de corrección.
2. Determine el Trusted Advisor identificador de la verificación que desea anular. Puedes encontrar la verificación de los IDs registros admitidos Trusted Advisor . [Trusted Advisor comprobaciones compatibles con Trusted Remediator](#)
3. Agregue una etiqueta a los recursos con la siguiente clave y valor mediante el tipo de cambio [Etiqueta | Actualización o Etiqueta | Actualización masiva](#):
 - Clave de etiqueta: TR-*Trusted Advisor check ID*-Execution-Mode (distingue entre mayúsculas y minúsculas)

En el ejemplo de clave de etiqueta anterior, Trusted Advisor check ID sustitúyala por el identificador único de la Trusted Advisor marca que deseas anular.

- Valor de etiqueta: utilice uno de los siguientes valores para el valor de etiqueta:
 - Automatizado: Trusted Remediator corrige automáticamente el recurso para esta Trusted Advisor comprobación.
 - Manual: OpsItem se crea una para el recurso, pero la corrección no se realiza automáticamente. La corrección se revisa y se ejecuta mediante la automatización. Para obtener más información, consulte [Trabaje con las soluciones en Trusted Remediator](#).
 - Inactivo: la corrección y OpsItem la creación no se realizan para este recurso ni para la comprobación especificada Trusted Advisor .

Por ejemplo, para corregir automáticamente un volumen de Amazon EBS con el identificador de Trusted Advisor verificación, DAvU99Dc4C añada una etiqueta al volumen de EBS. La clave de la etiqueta es TR-DAvU99Dc4C-Execution-Mode y el valor de la etiqueta es. Automated

A continuación, se muestra un ejemplo de la consola que muestra la sección Etiquetas:

Flujo de trabajo de decisiones en modo ejecución

Existen varios niveles para configurar el modo de ejecución de sus recursos y de cada Trusted Advisor comprobación. El siguiente diagrama muestra cómo Trusted Remediator decide qué modo de ejecución utilizar en función de sus configuraciones:

Configurar tutoriales de remediación

Los siguientes tutoriales proporcionan ejemplos de cómo crear soluciones comunes en Trusted Remediator

Corrija todos los recursos manualmente

Este ejemplo configura la corrección manual para todos los volúmenes de Amazon EBS con el identificador de Trusted Advisor comprobación DAv U99Dc4C (volúmenes de Amazon EBS subutilizados).

Configurar la corrección manual para los volúmenes de Amazon EBS con el identificador de comprobación U99Dc4C DAv

1. Utilice el tipo de cambio Configuration|Update de remediation para solicitar la actualización de la configuración.
2. Introduzca los siguientes parámetros:
 - CheckIds: U99Dc4C DAv
 - ExecutionMode: Manual

Note

Se pueden configurar varias comprobaciones en una sola solicitud. En el caso de las comprobaciones que requieren la misma configuración, incluya varias comprobaciones IDs en el CheckIdsparámetro. Para las comprobaciones que requieren una configuración diferente, cree un RemediationConfigurationobjeto nuevo.

3. Envíe el RFC.

Corrija todos los recursos automáticamente, excepto los recursos seleccionados

En este ejemplo, se configura la corrección automática para todos los volúmenes de Amazon EBS con el identificador de Trusted Advisor comprobación DAV U99Dc4C (volúmenes de Amazon EBS infrautilizados), con la excepción de los volúmenes especificados que no se van a corregir (denominados inactivos).

Configure la corrección automática para los volúmenes de Amazon EBS con el identificador de verificación DAV U99Dc4C, con la excepción de los recursos inactivos seleccionados

1. Anule la corrección automática para volúmenes de Amazon EBS seleccionados:

Utilice el tipo de cambio [Etiqueta | Actualización](#) o [Etiqueta | Actualización masiva](#) para aplicar la siguiente etiqueta a los volúmenes que se excluyan de la corrección automática:

- Clave: Modo de ejecución TR- U99Dc4C DAV
- Valor: Inactivo

2. Utilice el tipo de cambio Remediation Configuration|Update para solicitar la actualización de la configuración.

3. Introduzca los siguientes parámetros:

- CheckIds: U99Dc4C DAV
- ExecutionMode: Automatizado

4. Envíe el RFC.

Corrija los recursos etiquetados automáticamente

Este ejemplo configura la corrección automática para todos los volúmenes de Amazon EBS con la etiqueta Stage=NonProd con el identificador de Trusted Advisor comprobación DAV U99Dc4C (volúmenes de Amazon EBS subutilizados). Los demás recursos sin esta etiqueta no se corrigen.

Configure la corrección automática para los volúmenes de Amazon EBS con la etiqueta **Stage=NonProd** para el ID de comprobación U99Dc4C DAV

1. Utilice el tipo de cambio [Configuración | Actualización de remediación para solicitar la actualización](#) de la configuración.
2. Introduzca los siguientes parámetros:

- CheckIds: DAv U99Dc4C
- ExecutionMode: Condicional
- AutomatedForTaggedOnly: {"Etapa»:» NonProd «}

 Note

El valor especificado para el AutomatedForTaggedOnlyparámetro anula el valor previamente configurado. Para conservar las etiquetas existentes, inclúyalas en el nuevo valor.

3. Envíe el RFC.

Restablezca la configuración a los valores predeterminados

En este ejemplo, se elimina la automated-for-tagged-onlyconfiguración existente de la comprobación Hs4Ma3G104. Para eliminar la configuración de etiquetas aplicada anteriormente, defina el AutomatedForTaggedOnlyvalor del parámetro en {}.

Restablezca la configuración por defecto para comprobar Hs4Ma3G104

1. Utilice el tipo de cambio [Configuración de corrección | Actualización para solicitar la actualización](#) de la configuración.
2. Introduzca los siguientes parámetros:
 - CheckIds: Hs4Ma3G104
 - ExecutionMode: Introduzca el valor utilizado actualmente
 - AutomatedForTaggedOnly: {}
3. Envíe el RFC.

Trabaje con las soluciones en Trusted Remediator

Realice un seguimiento de las correcciones en Trusted Remediator

Para realizar un seguimiento de OpsItems las correcciones, siga estos pasos:

1. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>

2. Elija Administración de operaciones, OpsCenter.
3. (Opcional) Filtre la lista por Source=Trusted Remediator para incluir solo Trusted Remediator OpsItems en la lista.

A continuación se muestra un ejemplo de la OpsCenter pantalla filtrada por Source=Trusted Remediator:

 Note

Además OpsItems de verlos desde OpsCenter, puede ver los registros de corrección del bucket AMS S3. Para obtener más información, consulte [Registros de remediación en Trusted Remediator](#).

Ejecute las correcciones manuales en Trusted Remediator

Trusted Remediator crea comprobaciones configuradas OpsItems para la corrección manual. Debe revisar estas comprobaciones e iniciar el proceso de corrección manualmente.

Para solucionarlo manualmente OpsItem, complete los siguientes pasos:

1. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>
2. Elija Administración de operaciones, OpsCenter.
3. (Opcional) Filtre la lista por Source=Trusted Remediator para incluir solo Trusted Remediator OpsItems en la lista.
4. Elija lo OpsItem que desee revisar.
5. Revise los datos operativos del OpsItem. Los datos operativos incluyen los siguientes elementos:
 - trustedAdvisorCheckCategoría: la categoría del identificador del Trusted Advisor cheque. Por ejemplo, tolerancia a errores
 - trustedAdvisorCheckID: el identificador de Trusted Advisor verificación único.
 - trustedAdvisorCheckMetadatos: los metadatos del recurso, incluido el ID del recurso.
 - trustedAdvisorCheckNombre: el nombre de la Trusted Advisor comprobación.

- **trustedAdvisorCheckEstado**: el estado de la Trusted Advisor comprobación detectada para el recurso.
- **trustedAdvisorCheckManualRemediation**: los datos personalizados que proporcionan detalles de referencia para la corrección manual.
- **ManualExecutionInput**: un objeto que define los parámetros cuyos valores se pueden modificar al ejecutar la corrección manual.
 - **DocumentName**: el nombre del manual (documento SSM).
 - **CustomizableParameters**: nombres de parámetros que se pueden modificar.
- **DefaultInput**: un objeto que define los nombres y valores de los parámetros que se utilizarán en la corrección manual. Los valores se rellenan en función de parámetros preconfigurados.

6. Para solucionarlo manualmente, complete los siguientes pasos OpsItem:

- Utilice [Trusted Remediator | Finding | Remediate | Tipo de cambio ct-1c7ch8z5phrjp](#)
- Introduzca los valores de los siguientes parámetros:
 - **DocumentNameAWSManagedServices-RemediateTrustedRemediatorFinding**: Debe ser.
 - **Región**: La Región de AWS, en la forma us-east-1.
 - **Parámetros**: Introduzca los parámetros de corrección manual:
 - **OpsItemId**: El identificador del elemento de operaciones.
 - **RemediationDocumentName**: El nombre del documento de automatización de SSM que se va a utilizar. El documento debe estar asociado al elemento de operaciones. Si hay varios documentos asociados al elemento de operaciones, se DocumentName deben especificar.
 - **RemediationParameters**: Un key/value mapa de parámetros para la ejecución de la automatización, con el formato: `{"ParameterName1": ["ParameterValue1"], "ParameterName2": ["ParameterValue2"]}`. Solo puedes usar los parámetros que estén presentes en el objeto de operaciones **trustedAdvisorCheckManualRemediation CustomizableParameters**. Si no se especifica, los parámetros y valores se recuperan del elemento de operaciones.
- Seleccione 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.
- Supervise el progreso de la ejecución de la RFC.

- e. Una vez completada la ejecución, OpsItem se resuelve. Si el RFC falló, sigue los pasos que se indican. [Solucione los problemas de las correcciones en Trusted Remediator](#) Para obtener asistencia adicional para la solución de problemas, póngase en contacto con AMS.

Solucione los problemas de las correcciones en Trusted Remediator

Para obtener ayuda con las correcciones manuales y los errores de corrección, póngase en contacto con AMS.

Para ver el estado y los resultados de la reparación, complete los siguientes pasos:

1. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>
2. Elija Administración de operaciones, OpsCenter.
3. (Opcional) Filtre la lista por Source=Trusted Remediator para incluir solo Trusted Remediator OpsItems en la lista.
4. Elija lo OpsItem que desee revisar.
5. En la sección Ejecuciones automatizadas, revise el nombre y el estado del documento y los resultados.
6. Revise los siguientes errores comunes de automatización. Si sus problemas no aparecen aquí, póngase en contacto con su CSDM para obtener ayuda.

Errores de corrección comunes

No aparece ninguna ejecución en Automation Executions

Si no hay ninguna ejecución asociada a ella, OpsItem podría indicar que la ejecución no se pudo iniciar debido a valores de parámetros incorrectos.

Pasos para la solución de problemas

1. En los datos operativos, revise el valor de la `trustedAdvisorCheckAutoRemediation` propiedad.
2. Compruebe que los valores `DocumentName` y los parámetros sean correctos. Para obtener los valores correctos, consulte [Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator](#) los detalles sobre cómo configurar los parámetros del SSM. Para revisar los parámetros de comprobación admitidos, consulte [Trusted Advisor comprobaciones compatibles con Trusted Remediator](#)

3. Compruebe que los valores del documento SSM coincidan con los patrones permitidos. Para ver los detalles de los parámetros del contenido del documento, seleccione el nombre del documento en la sección Runbooks.
4. Tras revisar y corregir los parámetros, corrija manualmente el. OpsItem Para conocer los pasos de corrección, consulte. [Ejecute las correcciones manuales en Trusted Remediator](#)
5. Para evitar que se repita este error, asegúrese de configurar la corrección con los valores de parámetros correctos en su configuración. Para obtener más información, consulte [Configurar la corrección de Trusted Advisor comprobaciones en Trusted Remediator](#)

Ejecuciones fallidas en Automation Executions

Los documentos de remediación contienen varios pasos que interactúan con la Servicios de AWS realización de diversas acciones. APIs Para identificar la causa específica del error, complete los siguientes pasos:

Pasos para la solución de problemas

1. Para ver los pasos de ejecución individuales, selecciona el enlace del identificador de ejecución que se encuentra en la sección Ejecuciones automatizadas. A continuación, se muestra un ejemplo de la consola de Systems Manager que muestra los pasos de ejecución de una automatización seleccionada:

2. Elija el paso con el estado Fallido. Los siguientes son ejemplos de mensajes de error:

- NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist

Este error indica que se especificó un nombre de depósito incorrecto en los parámetros preconfigurados de la configuración de corrección.

Para resolver este error, [ejecute la automatización manualmente con el nombre](#) de bucket correcto. Para evitar que este problema vuelva a producirse, [actualice la configuración de corrección](#) con el nombre de bucket correcto.

- DB instance my-db-instance-1 is not in available status for modification.

Este error indica que la automatización no pudo realizar los cambios esperados porque la instancia de base de datos estaba en un estado no válido.

Para resolver este error, [ejecute la automatización manualmente](#).

Registros de remediación en Trusted Remediator

Trusted Remediator crea registros en formato JSON y los carga en Amazon Simple Storage Service. Los archivos de registro se cargan en un bucket de S3 creado por AMS y denominado. `ams-trusted-remediator-{your-account-id}-logs` AMS crea el bucket de S3 en la cuenta de administrador delegado. Puede importar los archivos de registro QuickSight para generar informes de corrección personalizados.

Registro de elementos de remediación

Trusted Remediator crea el Remediation item log cuando se crea una remediación OpsItem . Este registro contiene la remediación manual OpsItem y la remediación automática. OpsItem Puede utilizarlo Remediation item log para realizar un seguimiento de la visión general de todas las correcciones.

Ubicación del registro de elementos de corrección para las recomendaciones de Compute Optimizer

`s3://ams-trusted-remediator-delegated-administrator-account-id-logs/
compute_optimizer_remediation_items/remediation creation time in yyyy-mm-dd format/10 digits epoch time or unix timestamp-Trusted Advisor check ID-
Resource ID.json`

Ubicación del registro de elementos de corrección para las comprobaciones Trusted Advisor

`s3://ams-trusted-remediator-delegated-administrator-account-id-logs/
remediation_items/remediation creation time in yyyy-mm-dd format/10 digits
epoch time or unix timestamp-Trusted Advisor check ID- Resource ID.json`

URL del archivo de ejemplo del registro de elementos de remediación

`s3:///ams-trusted-remediator-111122223333-logs/
remediation_items/2023-02-06/1675660464-DAvU99Dc4C-
vol-00bd8965660b4c16d.json`

Formato de registro de elementos de Compute Optimizer Remediation

```
{
```

```

"AccountID": "Account_ID",
"ComputeOptimizerCheckID": "Compute Optimizer check ID",
"ComputeOptimizerCheckName": "Compute Optimizer check name",
"ResourceID": "Resource ID",
"RemediationTime": Remediation creation time,
"ExecutionMode": "Automated or Manual",
"OpsItemID": "OpsItem ID"
}

```

Trusted Advisor Formato de registro de elementos de corrección

```

{
  "TrustedAdvisorCheckID": Trusted Advisor check ID,
  "TrustedAdvisorCheckName": Trusted Advisor check name,
  "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
  "ResourceID": Resource ID,
  "RemediationTime": Remediation creation time,
  "ExecutionMode": Automated or Manual,
  "OpsItemID": OpsItem ID
}

```

Contenido de muestra en formato de registro de elementos de Compute Optimizer Remediation

```

{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}

```

Trusted Advisor Contenido de muestra en formato de registro de elementos de remediación

```

{
  "TrustedAdvisorCheckID": "DAvU99Dc4C",
  "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
  "TrustedAdvisorCheckResultTime": 1675614749,
  "ResourceID": "vol-00bd8965660b4c16d",
  "RemediationTime": 1675660464,
  "OpsItemID": "oi-cca5df7af718"
}

```

}

Registro automatizado de ejecución de correcciones, Compute Optimizer y Trusted Advisor

Trusted Remediator lo crea Automated remediation execution log cuando se completa la ejecución automática de un documento SSM. Este registro contiene detalles de ejecución de SSM únicamente para la corrección automática. OpsItem Puede utilizar este archivo de registro para realizar un seguimiento de las correcciones automatizadas.

Ubicación del registro de correcciones automatizadas de Compute Optimizer

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs//
remediation_executions/remediation creation time in yyyy-mm-dd format/10
digits epoch time or unix timestamp-Compute Optimizer recommendation
ID.json
```

Trusted Advisor Ubicación del registro de correcciones automatizado

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs//
remediation_executions/remediation creation time in yyyy-mm-dd format/10
digits epoch time or unix timestamp-Trusted Advisor check ID-Resource
ID.json
```

Ejemplo de ubicación del registro de correcciones automatizadas de Compute Optimizer

```
s3://ams-trusted-remediator-111122223333-logs/
remediation_executions/2025-06-26/1750908858-123456789012-compute-
optimizer-ec2-i-1235173471d2cd789.json
```

Trusted Advisor Ejemplo de ubicación del registro de correcciones automatizadas

```
s3://ams-trusted-remediator-111122223333-logs/
remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-
vol-00bd8965660b4c16d.json
```

Contenido de muestra en formato de registro de correcciones automatizado

```
{
  "OpsItemID": "oi-767c77e05301",
  "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
```



```
"SSMExecutionStatus": "Success"}
```

Mejores prácticas en Trusted Remediator

Las siguientes son las mejores prácticas para ayudarle a utilizar Trusted Remediator:

- Si no está seguro de los resultados de la reparación, comience con el modo de ejecución manual. A veces, aplicar la ejecución automática para las correcciones desde el principio puede provocar resultados inesperados.
- Realice una revisión semanal de las correcciones OpsItems para obtener información sobre los resultados de Trusted Remediator.
- Las cuentas de los miembros heredan las configuraciones de la cuenta de administrador delegado. Por lo tanto, es importante estructurar las cuentas de manera que te ayuden a administrar varias cuentas con las mismas configuraciones. Puede eximir los recursos de la configuración predeterminada mediante etiquetas.

Remediador de confianza FAQs

Las siguientes son preguntas frecuentes sobre Trusted Remediator:

¿Qué es Trusted Remediator y en qué me beneficia?

Cuando Compute Optimizer identifica un incumplimiento Trusted Advisor o emite una recomendación, Trusted Remediator responde de acuerdo con sus preferencias especificadas, ya sea aplicando una corrección, solicitando la aprobación mediante correcciones manuales o informando de las correcciones en su próxima revisión empresarial mensual (MBR). La subsanación se lleva a cabo en el momento o el cronograma de remediación que prefieras. Trusted Remediator le ofrece la posibilidad de autogestionar las Trusted Advisor comprobaciones y actuar en función de ellas, con la flexibilidad de configurar y corregir las comprobaciones de forma individual o masiva. Con una biblioteca de documentos de remediación comprobados, AMS aumenta constantemente sus cuentas aplicando controles de seguridad y siguiendo las mejores prácticas. AWS Solo se le notificará si así lo especifica en su configuración. Los usuarios de AMS pueden suscribirse a Trusted Remediator sin coste adicional.

¿Cómo se relaciona Trusted Remediator con otros y trabaja con ellos? Servicios de AWS

Tienes acceso a las Trusted Advisor comprobaciones y a las recomendaciones de Compute Optimizer como parte de tu plan Enterprise Support actual. Trusted Remediator se integra con

Trusted Advisor Compute Optimizer para aprovechar las capacidades de automatización de AMS existentes. En concreto, AMS utiliza documentos de AWS Systems Manager automatización (manuales de instrucciones) para las correcciones automatizadas. AWS AppConfig se utiliza para configurar los flujos de trabajo de remediación. Puede ver todas las correcciones actuales y pasadas a través del Systems Manager OpsCenter. Los registros de corrección se almacenan en un bucket de Amazon S3. Puede usar los registros para importar y crear paneles de informes personalizados en ellos. QuickSight

¿Quién configura las correcciones?

Usted es el propietario de las configuraciones de su cuenta. Administrar las configuraciones es su responsabilidad. También puede ponerse en contacto con AMS para obtener cambios en la configuración, asistencia y correcciones manuales, así como para solucionar los errores de corrección.

¿Cómo instalo los documentos de automatización de SSM?

Los documentos de automatización de SSM se comparten automáticamente con las cuentas AMS integradas.

¿También se remediarán los recursos propiedad de AMS?

Trusted Remediator no marca los recursos propiedad de AMS. Trusted Remediator se centra únicamente en sus recursos.

¿En qué Regiones de AWS está disponible Trusted Remediator y quién puede usarlo?

Trusted Remediator está disponible para los clientes de AMS Advanced. Para ver una lista actualizada de las regiones de soporte, consulte [Servicios de AWS por región](#).

¿Trusted Remediator provocará la pérdida de recursos?

Dado que los documentos de automatización de SSM actualizan directamente los recursos a través de la AWS API, es posible que se produzcan desviaciones de recursos. Puedes usar etiquetas para segregar los recursos creados a través de tus paquetes existentes CI/CD . Puede configurar Trusted Remediator para que ignore los recursos etiquetados y, al mismo tiempo, corrija los demás recursos.

¿Cómo puedo pausar o detener Trusted Remediator?

Utilice el tipo de cambio [Management | Trusted Remediator | State | Habilitar o deshabilitar](#) para detener el servicio Trusted Remediator. Utilice el mismo tipo de cambio para volver a activar Trusted Remediator.

¿Cómo puedo corregir las comprobaciones que no son compatibles con Trusted Remediator?

Puede seguir comunicándose con AMS a través de Operations On Demand (OOD) en caso de comprobaciones no admitidas. AMS le ayuda a corregir estas comprobaciones. Para obtener más información, consulte [Operations On Demand](#).

¿Qué recursos utiliza Trusted Remediator en sus cuentas?

Trusted Remediator implementa los siguientes recursos en la cuenta de administrador delegado de Trusted Remediator:

- Un bucket de Amazon S3 denominado `ams-trusted-remediator-{your-account-id}-logs`. Trusted Remediator crea la solución `Remediation item log` en formato JSON cuando se crea una solución y OpsItem carga los archivos de registro en este depósito.
- Una AWS AppConfig aplicación para almacenar las configuraciones de corrección para las Trusted Advisor comprobaciones compatibles y las recomendaciones de Compute Optimizer.

Trusted Remediator no despliega recursos en la cuenta de miembro de Trusted Remediator.

Administración de registros:

Temas

- [¿Qué es la administración de registros?](#)
- [Cómo funciona el registro de AMS](#)
- [Acceder a sus registros de](#)
- [Personalización de la configuración de registros](#)

La administración de registros de AMS recopila, agrega y controla la retención de los registros de la cuenta gestionada. AWS la administración de registros agrega a Logs los registros de EC2 las instancias y AWS los recursos de Amazon desplegados en tu cuenta CloudWatch . Puede encontrar la lista completa de los servicios a partir de los cuales se agregan los registros actualmente en [Registros de servicios agregados de AMS](#).

¿Qué es la administración de registros?

La administración de registros es el proceso de gestionar los eventos de registro generados por las instancias, las aplicaciones y los servicios de AWS. Esta función define la forma en que AMS procesa, almacena y rota los eventos de registro generados en su cuenta de AWS gestionada. Los registros de infraestructura se utilizan durante la resolución de incidentes y para respaldar las auditorías del sistema.

Cómo funciona el registro de AMS

La administración de registros de la zona de landing zone (SALZ) de una sola cuenta de AMS utiliza una variedad de agentes y herramientas preinstalados que se implementan cuando se incorporan o aprovisionan instancias y aplicaciones.

El registro se configura durante el proceso de incorporación de la cuenta y cuando se lanza una pila.

Los registros de zonas de aterrizaje multicuenta (MALZ) de AMS producidos por las instancias y los servicios de AWS están disponibles en CloudWatch Logs o en Amazon Simple Storage Service (Amazon S3), dentro de cada cuenta gestionada por AMS. La landing zone multicuenta de AMS proporciona una cuenta de registro central que actúa como ubicación de agregación central para algunos registros producidos por cuentas de aplicaciones individuales.

Las tablas de las [Acceder a sus registros de](#) subsecciones describen qué registros están disponibles en las cuentas individuales y cuáles están disponibles en la cuenta de registro central.

Acceder a sus registros de

Para acceder a sus registros, asegúrese de tener una de las funciones de IAM requeridas y de estar en su cuenta de AMS. A continuación, navegue hasta el directorio que se muestra.

Multi-Account Landing Zone (MALZ)

Proporciona cinco funciones de IAM predeterminadas, cada una de las cuales permite el acceso a todos los registros de la cuenta (todas van precedidas de): `AWSTManagedServices`

- `AdminRole`
- `CaseRole`
- `ChangeManagementRole`
- `ReadOnlyRole`
- `SecurityOpsRole`

El acceso a estas funciones se configura mediante federación, y cada función se asigna a un grupo dentro del dominio de Active Directory.

Para obtener más información sobre estas funciones, consulte [Función de usuario de IAM en AMS](#).

Single-Account Landing Zone (SALZ)

El valor predeterminado `Customer_ReadOnly_Role` de la landing zone de cuenta única de AMS te permite acceder a todos los registros de tu cuenta. El acceso a los registros se controla mediante las funciones de AWS Identity and Access Management (IAM) asignadas a los grupos de Active Directory.

Registros de servicios agregados de AMS

Cada AWS servicio inicia sesión en CloudWatch Logs o en una ubicación específica de un bucket de Amazon S3.

 Note

A menos que se indique específicamente, todas las ubicaciones de los registros son locales de la cuenta que generó los registros y no se agregan a la cuenta de registro central. Para encontrar los nombres predeterminados de las CloudTrail rutas de AMS en las cuentas de SALZ y MALZ, vaya a la consola de AWS CloudTrail y, a continuación, a la página de rutas y busque AMS. Como los recursos de AMS tienen etiquetas, puede encontrar los senderos de esta manera. Ejemplo de CloudTrail etiqueta AMS:

```
Environment    AMSInfrastructure
```

Para acceder a sus registros, asegúrese de tener una de las funciones de IAM requeridas y de estar en su cuenta de AMS. A continuación, navegue hasta el directorio que se muestra.

Multi-Account Landing Zone

Registros de servicios agregados de varias cuentas de AMS en las zonas de landing zone

	Nombre del servicio	Detalles del registro	Ubicación del registro
1	Amazon Aurora	Registros generales, de consultas lentas y de errores.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	AWS CloudFormation (CFN)	Solo registro de llamadas a la API.	AWS CloudFormation Las llamadas a la API se documentan mediante CloudTrail, que envía sus registros a un bucket de S3 CloudWatch LogGroup y, a continuación, los sincroniza en un bucket de S3. De forma predeterminada, los registros se conservan durante 14 días en el depósito CloudWatch LogGroup de S3 y se conservan indefinidamente en el depósito de S3.

	Nombre del servicio	Detalles del registro	Ubicación del registro
			CloudWatch LogGroup:/CloudTrail/Registros de zonas de aterrizaje Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs -ams-a {} -log-management- {} <i>account_ID region</i> Ruta:/{}/AWSLogs<i>account_ID</i> CloudTrail
3	Amazon CloudFront (CloudFront)	Registro de solicitudes de usuarios. CloudFront el registro debe estar habilitado de forma explícita. Para obtener información, consulte Habilitar el registro para los servicios compatibles .	Cubeta S3: ams-a {} <i>account_ID</i> } -log-management- {} <i>region</i> Ruta: AWS/RedShift/{}/<i>CloudFront distribution ID</i>
4	Amazon CloudWatch (CloudWatch)	Solo registro de llamadas a la API.	CloudWatch LogGroup:/CloudTrail/Registros de zonas de aterrizaje Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Ruta:AWSLogs/{}/<i>account_ID</i> }/CloudTrail/
5	Amazon Elastic Block Store (Amazon EBS)	El servicio EBS no genera ningún registro.	No aplicable

	Nombre del servicio	Detalles del registro	Ubicación del registro
6	Amazon Elastic Compute Cloud (Amazon EC2)	Registros del sistema y de la aplicación. Para obtener más información, consulte Amazon Elastic Compute Cloud (Amazon EC2): registros a nivel de sistema .	CloudWatch Registros:/{ <i>instance ID</i> }
7	Amazon Elastic File System (Amazon EFS)	Solo registro de llamadas a la API.	CloudWatch LogGroup:/CloudTrail/Registros de zonas de aterrizaje Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Ruta:AWSLogs/{ <i>account_ID</i> }/CloudTrail/

	Nombre del servicio	Detalles del registro	Ubicación del registro
8	Elastic Load Balancing (ELB)	Entradas del registro de accesos y errores. Los balanceadores de carga elásticos registran todas las solicitudes que se les envían, incluidas las solicitudes que no se envían a instancias de back-end. Por ejemplo, si un cliente envía una solicitud con un formato incorrecto o no hay instancias en buen estado que puedan responder, la solicitud seguirá siendo registrada. Para obtener más información sobre las entradas de registro de Elastic Load Balancing, consulte • Classic Load Balancers: acceda a las entradas del registro. • Equilibradores de carga de aplicaciones: accede a las entradas del registro. • Equilibradores de carga de red: acceda a las entradas del registro.	Registros de llamadas a la API: CloudWatch LogGroup:/CloudTrail/Registros de zonas de aterrizaje Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - {} - {} <i>account_ID</i> <i>region</i> Ruta:AWSLogs/{<i>account_ID</i> }/CloudTrail/ Registros de acceso: Cubeta S3: mc-a {<i>account_ID</i> }-logs {} <i>region</i> Ruta: aws/elbaccess

	Nombre del servicio	Detalles del registro	Ubicación del registro
9	Amazon OpenSearch Service (OpenSearch Servicio)	Registros de errores del servicio. Debe habilitar el OpenSearch registro de forma explícita. Para obtener información, consulte Habilitar el registro para los servicios compatibles	CloudWatch LogGroup:/CloudTrail/Registros de zonas de aterrizaje Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Ruta:AWSLogs/{ <i>account_ID</i> }/CloudTrail/
10	Amazon ElastiCache	Solo registro de llamadas a la API.	CloudWatch LogGroup://CloudTrail/Registros de zonas de aterrizaje Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - {} - {} <i>account_ID region</i> Ruta:AWSLogs/{ <i>account_ID</i> }/CloudTrail/
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Registros de conexiones, usuarios y actividad. El registro está activado de forma predeterminada cuando se crea el clúster de Redshift al invocar el clúster de Redshift CT (ct-1malj7snzxrkr). Para obtener más información, consulte Registro de auditorías de bases de datos.	Depósito de S3: ams-a { <i>account_ID</i> } -log-management- {} <i>region</i> Ruta: /AWS//{} RedShift <i>CloudFront Distribution ID</i>

	Nombre del servicio	Detalles del registro	Ubicación del registro
15	Amazon Relational Database Service (RDS)	Registros específicos del tipo de base de datos. Debe habilitar explícitamente el registro de RDS. Para obtener información, consulte Habilitar el registro para los servicios compatibles Solo puede acceder a los registros de MSSQL mediante un procedimiento almacenado; para obtener más información, consulte Archivar archivos de registro.	CloudWatch LogGroup: <code>/aws/rds/ (o)/{/} <i>instance cluster database_name log_name</i></code>

	Nombre del servicio	Detalles del registro	Ubicación del registro
16	Amazon S3 (S3)	Registros de acceso al bucket. Cada registro de acceso proporciona detalles sobre una sola solicitud de acceso, como el solicitante, el nombre del depósito, la hora de la solicitud, la acción de la solicitud, el estado de la respuesta y el código de error (si lo hubiera). La información del registro de acceso puede ser útil en auditorías de acceso y seguridad. También puede ayudarle a conocer mejor su base de clientes y entender su factura de Amazon S3. Para obtener más información sobre las entradas del registro de acceso de S3, consulte el formato del registro de acceso al servidor S3.	Bucket de S3: mc-a {<i>account_ID</i>} -log-management- {<i>region</i>} Ruta: /aws/s3access/ {<i>bucket_name</i>} Depósito S3 [en la cuenta de registro central]: aws-landing-zone-s 3-access-logs- {<i>account_ID</i>} - {<i>region</i>} Ruta: /
17	Amazon Simple Email Service (SES)	Llamadas al servicio de la API de SES.	CloudWatch LogGroup:/CloudTrail/Registros de zonas de aterrizaje Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - {<i>account_ID</i>} - {<i>region</i>} Ruta: AWSLogs/{<i>account_ID</i>}/CloudTrail/

	Nombre del servicio	Detalles del registro	Ubicación del registro
18	Amazon Virtual Private Cloud (VPC)	Datos de flujo de la VPC (información sobre el tráfico IP que entra y sale de las interfaces de red de la VPC).	CloudWatch LogGroup: /aws/vpcflow/ { } <i>VPC_ID</i>
19	Auto Scaling	Solo registro de llamadas a la API.	CloudWatch LogGroup:/CloudTrail/Registros de zonas de aterrizaje
20	AWS Certificate Manager		Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - { } - { } <i>account_ID region</i> Ruta:AWSLogs/{ <i>account_ID</i> }/CloudTrail/
21	AWS CodeDeploy	Registros de implementación específicos de la instancia.	En Instance
22	AWS Config	Llamadas al servicio de la API de AWS Config.	CloudWatch LogGroup:/CloudTrail/Landing-Zone-Logs Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - { } - { } <i>account_ID region</i> Ruta:AWSLogs/{ <i>account_ID</i> }/CloudTrail/

	Nombre del servicio	Detalles del registro	Ubicación del registro
		Cambios en la configuración de los recursos, controlados por AWS Config.	Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - { <i>account_ID</i> } - { <i>region</i> } Ruta:AWSLogs/{ <i>account_ID</i> } / Config/
23	AWS Database Migration Service (AWS DMS)	Registros de migración de bases de datos. Para obtener más información, consulte Introducción a la administración de registros en AWS Database Migration Service .	consola de migración de bases de datos
24	AWS Direct Connect (DX)	Solo registro de llamadas a la API.	CloudWatch LogGroup:/CloudTrail/Registros de zonas de aterrizaje
25	AWS Glaciar		Depósito S3 [en la cuenta de registro central]: aws-landing-zone-logs - {} - {} <i>account_ID region</i>
26	AWS IAM (IAM)		
27	AWS Key Management Service		Ruta:AWSLogs/{ <i>account_ID</i> } / CloudTrail/
28	Consola de administración de AWS (consola o consola de AWS)		

	Nombre del servicio	Detalles del registro	Ubicación del registro
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

Single-Account Landing Zone

Registros de servicios agregados de zonas de landing zone de cuentas únicas de AMS

	Nombre del servicio	Detalles del registro	Ubicación del registro
1	Amazon Aurora	Registros generales, de consultas lentas y de errores.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	Amazon CloudFormation (CloudFormation o CFN)	Solo registro de llamadas a la API.	CloudFormation Las llamadas a la API se documentan mediante CloudTrail, que envía sus registros a un bucket de S3 CloudWatch LogGroup y, a continuación, los sincroniza en un bucket de S3. CloudWatch LogGroup: /aws/ams/cloudtrail Cubeta de S3: ams-a {} -log-management- {<i>account_ID</i> } <i>region</i>

	Nombre del servicio	Detalles del registro	Ubicación del registro
3	Amazon CloudFront (CloudFront)	Registro de solicitudes de usuarios. Debe habilitar el CloudFront registro de forma explícita. Para obtener información, consulte Habilitar el registro para los servicios compatibles	Cubeta de S3: <code>ams-a</code> <code>{<i>account_ID</i>}</code> -log-management- <code>{<i>region</i>}</code> Ruta: <code>AWS/RedShift/{<i>CloudFront_distribution_ID</i>}</code>
4	Amazon CloudWatch (CloudWatch)	Solo registro de llamadas a la API.	CloudWatch LogGroup: <code>/aws/ams/cloudtrail</code>
5	Amazon Elastic Block Store (EBS)	El servicio EBS no genera registros.	No aplicable
6	Amazon Elastic Compute Cloud (EC2)	Registros del sistema y de la aplicación. Para obtener más información, consulte Amazon Elastic Compute Cloud (Amazon EC2): registros a nivel de sistema.	CloudWatch Registros: <code>{<i>instance_ID</i>}</code>
7	Amazon Elastic File System (Amazon EFS)	Solo registro de llamadas a la API.	CloudWatch LogGroup: <code>/aws/ams/cloudtrail</code>

	Nombre del servicio	Detalles del registro	Ubicación del registro
8	Elastic Load Balancing (ELB)	Entradas del registro de accesos y errores. Los balanceadores de carga elásticos registran todas las solicitudes que se les envían, incluidas las solicitudes que no se envían a instancias de back-end. Por ejemplo, si un cliente envía una solicitud con un formato incorrecto o no hay instancias en buen estado que puedan responder, la solicitud seguirá siendo registrada. Para obtener más información sobre las entradas de registro de Elastic Load Balancer, consulte • Classic Load Balancers: acceda a las entradas del registro. • Equilibradores de carga de aplicaciones: accede a las entradas del registro. • Equilibradores de carga de red: acceda a las entradas del registro.	CloudWatch LogGroup: /aws/ams/cloudtrail Cubeta S3: mc-a {<i>account_ID</i>} -logs- {} <i>region</i> Ruta: aws/elbaccess

	Nombre del servicio	Detalles del registro	Ubicación del registro
9	Amazon OpenSearch Service (OpenSearch Servicio)	Registros de errores del servicio. Debe habilitar el OpenSearch registro de forma explícita. Para obtener información, consulte Habilitar el registro para los servicios compatibles	CloudWatch LogGroup: /aws/ams/cloudtrail
10	Amazon ElastiCache	Solo registro de llamadas a la API.	CloudWatch LogGroup: /aws/ams/cloudtrail
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Registros de conexiones, usuarios y actividad. El registro está activado de forma predeterminada cuando se crea el clúster de Redshift al invocar el clúster de Redshift CT (ct-1malj7snzxrkr). Para obtener más información, consulte Registro de auditorías de bases de datos.	Depósito de S3: <code>ams-a-{<i>account_ID</i>}-log-management-{<i>region</i>}</code> Ruta: <code>/AWS/{<i>RedShiftCloudFront_Distribution_ID</i>}</code>

	Nombre del servicio	Detalles del registro	Ubicación del registro
15	Amazon Relational Database Service (RDS)	Registros específicos del tipo de base de datos. El registro de RDS debe estar habilitado de forma explícita. Para obtener información, consulte Habilitar el registro para los servicios compatibles Solo puede acceder a los registros de MSSQL mediante un procedimiento almacenado; para obtener más información, consulte Archivar archivos de registro.	CloudWatch LogGroup: /aws/rds/ (instance cluster)/{nombre de la base de datos}/{nombre del registro}

	Nombre del servicio	Detalles del registro	Ubicación del registro
16	Amazon S3 (S3)	Registros de acceso al bucket. Cada registro de acceso proporciona detalles sobre una sola solicitud de acceso, como el solicitante, el nombre del depósito, la hora de la solicitud, la acción de la solicitud, el estado de la respuesta y el código de error (si lo hubiera). La información del registro de acceso puede ser útil en las auditorías de seguridad y acceso; también puede ayudarle a conocer su base de clientes y a entender su factura de Amazon S3. Para obtener más información sobre las entradas del registro de acceso de S3, consulte el formato del registro de acceso al servidor S3.	Bucket de S3: mc-a {<i>account_ID</i>} -log-management- {<i>region</i>} Ruta: /aws/s3access/ {<i>bucket_name</i>}
17	Amazon Simple Email Service (SES)	Llamadas al servicio de la API de SES.	CloudWatch LogGroup: /aws/ams/cloudtrail Cubeta S3: ams-a {<i>account_ID</i>} -log-management- {<i>region</i>} Ruta: AWS/CloudTrail/AWSLogs/{}/{<i>account_ID</i>} CloudTrail <i>region</i>

	Nombre del servicio	Detalles del registro	Ubicación del registro
18	Amazon Virtual Private Cloud (VPC)	Datos de flujo de la VPC (información sobre el tráfico IP que entra y sale de las interfaces de red de la VPC).	CloudWatch LogGroup: /aws/vpcflow/ {vpc_id}
19	Auto Scaling	Solo registro de llamadas a la API.	CloudWatch LogGroup: /aws/ams/cloudtrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	Registros de implementación específicos de la instancia.	En una instancia
22	AWS Config	Llamadas al servicio de la API de AWS Config.	CloudWatch LogGroup: /aws/ams/cloudtrail Cubeta de S3: <code>ams-a-{account_ID}-log-management-{}region</code> Ruta: <code>AWS/CloudTrail/AWSLogs/{}/{account_ID} CloudTrail region</code>
23	AWS Database Migration Service (AWS DMS)	Registros de migración de bases de datos. Para obtener más información, consulte Introducción a la administración de registros en AWS Database Migration Service .	consola de migración de bases de datos
24	AWS Direct Connect (DX)	Solo registro de llamadas a la API.	CloudWatch LogGroup: /aws/ams/cloudtrail
25	AWS Glaciar		

	Nombre del servicio	Detalles del registro	Ubicación del registro
26	AWS IAM (IAM)		
27	AWS Key Management Service		
28	Consola de administración de AWS (consola o consola de AWS)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

Registros de servicios compartidos de AMS

En la siguiente tabla se describen los registros y la ubicación de los registros de los servicios compartidos de AMS de su cuenta.

Para acceder a sus registros, asegúrese de tener una de las funciones de IAM requeridas y de estar en su cuenta de AMS. A continuación, navegue hasta el directorio que se muestra.

Registro de servicios compartidos de zona de landing zone única AMS

	Nombre del servicio compartido	Detalles del registro	Ubicación del registro
1	Hosts bastión	Información sobre los usuarios que acceden al host del bastión.	Bastiones de Linux: CloudWatch Registros:/{id de instancia}/var/log/secure CloudWatch Registros:/{id de instancia}/var/log/audit/audit.log Bastiones de Windows: CloudWatch Registros:/{id de instancia}/SecurityEventLog
2	Hosts de administración	Producción de scripts, que ayudan a automatizar las acciones de administración del acceso dentro de la cuenta.	CloudWatch Registros:/{id de instancia}/ApplicationEventLog
4	Anfitriones EPS (DSM)	Información sobre la inscripción de instancias en la plataforma Deep Security Management.	CloudWatch Registros:/{id de instancia}/var/log/DSM.log
5	Servicios de directorio	Información sobre el inicio de sesión de la cuenta, la administración de la cuenta, el seguimiento detallado, el acceso a los objetos, el cambio de política y el uso de privilegios en el directorio de la cuenta. Debe habilitar de forma explícita el registro de los	CloudWatch Registros: /aws/directoryservice/ {identificador del directorio} - {nombre dns del directorio}

	Nombre del servicio compartido	Detalles del registro	Ubicación del registro
		servicios de directorio. Para obtener información, consulte Habilitar el registro para los servicios compatibles .	
6	Lambdas	Salida de varias lambdas, que ayudan a automatizar las acciones operativas dentro de la cuenta.	CloudWatch Registros: /aws/lambda/{nombre lambda}

Registro de servicios compartidos de zonas de landing zone multicuenta AMS

	Nombre del servicio compartido	Detalles del registro	Ubicación del registro
1	Bastiones	Resultado de los inicios de sesión de las instancias y de los errores de autenticación.	CloudWatch Registros de Linux Bastions:/{ <i>instance_ID</i> }.log var/log/secure CloudWatch Registros de Windows Bastions:/{ <i>instance_ID</i> } SecurityEventLog
2	Hosts de administración	Salida de scripts, que ayudan a automatizar las acciones de gestión del acceso dentro de la cuenta.	CloudWatch Registros:/{ <i>instance_ID</i> }/ApplicationEventLog
3	Anfitriones EPS (DSM)	Información sobre la inscripción de instancias en la plataforma Deep Security Management.	CloudWatch Registros:/{ <i>instance_ID</i> }/var/log/DSM.log

	Nombre del servicio compartido	Detalles del registro	Ubicación del registro
4	Servicios de directorio	Información sobre el inicio de sesión de la cuenta, la administración de la cuenta, el seguimiento detallado, el acceso a objetos, el cambio de política y el uso de privilegios en el directorio de la cuenta. Debe habilitar de forma explícita el registro de los servicios de directorio. Para obtener información, consulte Habilitar el registro para los servicios compatibles.	CloudWatch Registros: /aws/directoryservice/ {} - {} <i>directory_ID</i> <i>directory_DNS_name</i>
5	Lambdas	Salida de varias lambdas, que ayudan a automatizar las acciones operativas dentro de la cuenta.	CloudWatch Registros: /aws/lambda/ {} <i>Lambda_name</i>

Amazon Elastic Compute Cloud (Amazon EC2): registros a nivel de sistema

Los registros de la instancia los recopila un agente de CloudWatch registros que se ejecuta en la instancia y se puede acceder a ellos a través de un grupo de CloudWatch registros con el mismo nombre que la instancia. Por ejemplo, si el ID de la instancia es i-0123456789abcdef0 y el nombre del archivo de registro es /var/log/messages, the Log Group would be i-0123456789abcdef0 and the Log Stream /var/log/messages

Véase también [Registros de servicios agregados de AMS](#).

Para acceder a sus registros, asegúrese de tener una de las funciones de IAM requeridas y de estar en su cuenta de AMS. A continuación, navegue hasta el directorio que se muestra.

 Note

De forma predeterminada, se recopilan los siguientes registros.

Amazon Linux/Red Hat Linux/Centos Linux/Ubuntu /SUSE Linux

Archivo de registro/Secuencia de registro

```
/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
/var/log/yum.log
/var/log/aws/ams/bootstrap.log
/var/log/aws/ams/build.log
/var/log/syslog
/var/log/dpkg.log
/var/log/auth.log
/var/log/zypper.log
```

 Note

Para obtener información sobre el acceso a los registros de Amazon Linux 2023, consulte [¿Por qué faltan registros en el directorio /var/log en mi instancia de EC2 Amazon Linux 2023?](#)

Windows

Archivo de registro/flujo de registro

```
SecurityEventLog
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
AmazonSSMErrorLog
```

Integración con Splunk

AMS admite los servicios de análisis de registros de clientes basados en AWS Lambda, como Splunk.

AMS utiliza el complemento Splunk para Amazon Web Services, que permite transmitir los datos de AWS a Splunk. Consulte los requisitos de [hardware](#) y software.

Consulte esta entrada del blog de Splunk [sobre cómo transmitir CloudWatch los registros de AWS a Splunk \(Consejo: es más fácil de lo que piensa\)](#). Debido a que la transmisión de CloudWatch registros está habilitada de forma predeterminada para los clientes de AMS, AMS configura la función de AWS Lambda por usted, sin embargo, debe configurar la entrada del recopilador de eventos HTTP (HEC) de Splunk y enviar una solicitud a AMS para obtener la funcionalidad adicional.

Este es el aspecto que podrían tener los ajustes de entrada de datos:

Personalización de la configuración de registros

Puede modificar la retención de los datos de registro de CloudWatch los registros y habilitar el registro para otros servicios de AWS.

Alterar la retención de CloudWatch registros

Puede cambiar la configuración de retención de datos de registro de los CloudWatch registros. De forma predeterminada, los registros se conservan de forma indefinida y no caducan nunca. Puede ajustar la política de retención para cada grupo de registro, manteniendo la retención indefinida o

seleccionar un periodo de retención de entre 10 años y un día. Para ver el período de retención mínimo permitido en AMS, consulte el documento de normas técnicas de AMS disponible en AWS Artifact. Para acceder a AWS Artifact, póngase en contacto con su CSDM para obtener instrucciones o vaya a [Introducción a AWS](#) Artifact.

La función de retención de CloudWatch registros elimina los eventos de registro de una transmisión en función de la política de retención. No elimina los flujos de registros ni los grupos de registros. Para obtener información general, consulte la Guía del usuario de Amazon CloudWatch Logs [¿Qué es Amazon CloudWatch Logs?](#).

Para obtener información sobre cómo personalizar un período de retención de registros y obtener más información, consulte [Cambiar la retención de datos de registro en los CloudWatch registros](#).

Habilitar el registro para los servicios compatibles

Algunos servicios no tienen el registro activado de forma predeterminada y requieren una activación explícita.

Para habilitar el registro de Amazon RDS y Route53 CloudFront OpenSearch, envíe una RFC al tipo de cambio Management | Other | Other | Create (ct-1e1xtak34nx76) con los siguientes valores, sustituyéndolos según corresponda: *variables*

Subject: Enable logging for *SERVICE_NAME*
Description: Service ARN: *SERVICE_ARN*

Administración de la seguridad

La administración de la seguridad de AWS Managed Services (AMS) es el proceso mediante el cual AMS identifica los activos de una organización e implementa políticas y procedimientos para protegerlos.

Note

Ahora, AMS dispone de un tipo de cambio (CT): Implementación | Componentes de pila avanzados | Certificado ACM y, además, SANs | Create (ct-3l14e139i5p50), que puede utilizar para enviar una solicitud de certificado. AWS Certificate Manager Para obtener información, consulte [AWS::CertificateManager::Certificate](#). Este CT prevé la creación de un nombre alternativo (SAN) adicional para el sujeto.

Para comprender mejor la AWS seguridad general, consulte [las prácticas recomendadas en materia de seguridad, identidad y conformidad](#).

AMS clasifica los riesgos de seguridad de la siguiente manera:

- Riesgos conocidos detectados por el antimalware, que son gestionados por el proceso de mitigación del malware.
- Eventos de seguridad, incluidas las infracciones de acceso, que gestiona el proceso de gestión de los eventos de seguridad.

Temas

- [Protección de datos en AMS](#)
- [Identity and Access Management](#)
- [Respuesta a incidentes de seguridad en AMS](#)
- [Revisiones de seguridad de solicitudes de cambio en AMS Advanced](#)

Protección de datos en AMS

AMS supervisa continuamente sus cuentas gestionadas mediante el uso de AWS servicios nativos como Amazon GuardDuty, Amazon Macie (opcional) y otras herramientas y procesos internos

patentados. Una vez que se activa una alarma, AMS asume la responsabilidad de la clasificación inicial y de la respuesta a la alarma. Nuestros procesos de respuesta se basan en los estándares del NIST. AMS pone a prueba periódicamente sus procesos de respuesta utilizando la simulación de respuesta a incidentes de seguridad para alinear su flujo de trabajo con los programas de respuesta de seguridad existentes para los clientes.

Cuando AMS detecta cualquier infracción o amenaza inminente de infracción de sus políticas de AWS seguridad, recopilamos información, incluidos los recursos afectados y cualquier cambio relacionado con la configuración. AMS ofrece follow-the-sun asistencia las 24 horas del día, los 7 días de la semana, los 365 días del año, con operadores especializados que revisan e investigan activamente los paneles de supervisión, la lista de incidentes y las solicitudes de servicio en todas sus cuentas gestionadas. AMS investiga los resultados con nuestros expertos en seguridad para analizar la actividad y comunicártelo a través de los contactos de intensificación de la seguridad que figuran en tu cuenta.

Basándose en nuestras conclusiones, AMS interactúa con usted de forma proactiva. Si cree que la actividad no está autorizada o es sospechosa, AMS trabaja con usted para investigar y solucionar el problema o contener el problema. Existen determinados tipos de conclusiones GuardDuty que requieren que confirme el impacto antes de que AMS pueda tomar alguna medida. Por ejemplo, el tipo de GuardDuty búsqueda UnauthorizedAccess:IAMUser/ConsoleLogin, indica que uno de tus usuarios ha iniciado sesión desde una ubicación inusual; AMS te lo notifica y te pide que revises el hallazgo para confirmar si este comportamiento es legítimo.

Amazon Macie

AWS Managed Services recomienda utilizar Macie para detectar una lista amplia y completa de datos confidenciales, como información de salud personal (PHI), información de identificación personal (PII) y datos financieros.

Macie se puede configurar para que se ejecute periódicamente en cualquier bucket de Amazon S3, lo que automatiza la evaluación de cualquier objeto nuevo o modificado dentro de un bucket a lo largo del tiempo. A medida que se generen problemas de seguridad, AMS se lo notificará y colaborará con usted para solucionarlos según sea necesario.

Para obtener más información, consulte [Análisis de los hallazgos de Amazon Macie](#).

Seguridad de Amazon Macie

Macie es un servicio de seguridad intelligence/AI con tecnología artificial que le ayuda a evitar la pérdida de datos al descubrir, clasificar y proteger automáticamente los datos confidenciales

almacenados en AWS. Macie utiliza el aprendizaje automático para reconocer datos confidenciales, como la información de identificación personal (PII) o la propiedad intelectual, asigna un valor empresarial y proporciona visibilidad sobre dónde se almacenan estos datos y cómo se utilizan en su organización. Macie supervisa continuamente la actividad de acceso a los datos para detectar anomalías y envía alertas cuando detecta un riesgo de acceso no autorizado o de fugas inadvertidas de datos. El servicio Macie es compatible con Amazon S3 y fuentes AWS CloudTrail de datos.

AMS monitorea continuamente las alertas de Macie y, si recibe una alerta, toma medidas rápidas para proteger sus recursos y su cuenta. Con la incorporación de Macie a la lista de servicios compatibles con AMS, ahora también somos responsables de habilitar y configurar Macie en todas sus cuentas, según sus instrucciones. Puede ver las alertas de Macie y nuestras acciones a medida que se despliegan en la consola de AWS o en las integraciones compatibles. Durante la incorporación de la cuenta, puede indicar las cuentas que utiliza para almacenar su información de identificación personal. Para todas las cuentas nuevas con PII, te recomendamos usar Macie. En el caso de las cuentas existentes con información de identificación personal, ponte en contacto con nosotros y la activaremos en tu cuenta. Como resultado, puede disponer de una capa de protección adicional y disfrutar de todas las ventajas de Macie en su entorno de AWS gestionado por AMS.

AMS Macie FAQs

- ¿Por qué necesito a Macie si todas las cuentas de AMS tienen Trend Micro y GuardDuty están activadas?

Macie lo ayuda a proteger sus datos en Amazon S3 al ayudarlo a clasificar los datos que tiene, el valor que tienen para la empresa y el comportamiento asociado con el acceso a esos datos. Amazon GuardDuty ofrece una amplia protección de sus cuentas, cargas de trabajo y datos de AWS, ya que le ayuda a identificar amenazas como el reconocimiento de los actores de amenazas, los problemas de instancias y la actividad problemática de la cuenta. Ambos servicios incorporan el análisis del comportamiento de los usuarios, el aprendizaje automático y la detección de anomalías para detectar las amenazas en sus respectivas categorías. Trend Micro no se centra en identificar la PII ni las amenazas derivadas de la misma.

- ¿Cómo activo Macie en mi cuenta de AMS?

Si lo has PII/PHI guardado en tus cuentas o tienes pensado guardarlo, ponte en contacto con tu CSDM o envía una solicitud de servicio para habilitar Macie en tus cuentas nuevas o existentes gestionadas por AMS.

- ¿Cuáles son las implicaciones económicas de habilitar Macie en mi cuenta de AMS?

Los precios de Macie funcionan para AMS de forma similar a otros servicios, como Amazon Elastic Compute Cloud (Amazon EC2). Pagas por Amazon Macie en función del uso y un aumento de AMS en función del tuyo. SLAs Las tarifas de Macie se basan en el uso; consulte los precios de [Amazon Macie](#), que se miden AWS CloudTrail en función de los eventos y del almacenamiento de Amazon S3. Ten en cuenta que los cargos de Macie tienden a estabilizarse a partir del segundo mes después de su activación, ya que se cobran en función de los datos incrementales que se añaden a los buckets de Amazon S3.

Para obtener más información sobre Macie, consulte [Amazon Macie](#).

GuardDuty

GuardDuty es un servicio de supervisión continua de la seguridad que utiliza fuentes de inteligencia sobre amenazas, como listas de direcciones IP y dominios maliciosos, y aprendizaje automático para identificar actividades inesperadas, potencialmente no autorizadas y maliciosas en su entorno de AWS. Esto puede incluir problemas como la escalada de privilegios, el uso de credenciales expuestas o la comunicación con direcciones IP o dominios maliciosos. GuardDuty también supervisa el comportamiento de acceso a las cuentas de Amazon Web Services para detectar señales de peligro, como despliegues de infraestructura no autorizados, como instancias implementadas en una región que nunca se ha utilizado, o llamadas inusuales a la API, como un cambio en la política de contraseñas para reducir la seguridad de las contraseñas. Para obtener más información, consulte la [Guía del GuardDuty usuario](#).

Para ver y analizar sus GuardDuty hallazgos, utilice el siguiente procedimiento.

1. Abra la [consola de GuardDuty](#).
2. Elija Hallazgos y, a continuación, elija un hallazgo específico para ver los detalles. Los detalles de cada hallazgo varían según el tipo de hallazgo, los recursos involucrados y la naturaleza de la actividad.

Para obtener más información sobre los campos de búsqueda disponibles, consulte los [detalles de GuardDuty búsqueda](#).

GuardDuty seguridad

Amazon GuardDuty ofrece una detección de amenazas que le permite supervisar y proteger de forma continua sus cuentas y cargas de trabajo de AWS. Amazon GuardDuty analiza los flujos

continuos de metadatos generados a partir de la actividad de su cuenta y red que se encuentran en AWS CloudTrail los eventos, los registros de flujo de Amazon VPC y los registros del Sistema de nombres de dominio (DNS). También utiliza inteligencia de amenazas integrada, como direcciones IP maliciosas conocidas, detección de anomalías y aprendizaje automático, para identificar las amenazas con mayor precisión. GuardDuty es un servicio AMS supervisado. Para obtener más información sobre la GuardDuty supervisión de Amazon, consulta [GuardDuty supervisión](#). Para obtener más información GuardDuty, consulta [Amazon GuardDuty](#).

Todas las cuentas AMS nuevas están GuardDuty habilitadas de forma predeterminada. AMS se configura GuardDuty durante la incorporación de la cuenta. Puede enviar solicitudes de cambio para modificar la configuración en cualquier momento. GuardDuty Los precios funcionan para AMS de forma similar a otros servicios, como Amazon Elastic Compute Cloud (Amazon EC2). Usted paga en GuardDuty función del uso y un aumento de AMS en función del suyo. SLAs GuardDuty las tarifas se basan en el uso ([GuardDuty precios de Amazon](#)) y se miden en función de AWS CloudTrail los eventos y el volumen del registro de flujo de Amazon VPC.

GuardDuty En el caso de AMS, están habilitadas las siguientes categorías de detección principales:

- Reconocimiento: actividad que sugiere el reconocimiento por parte de un agente de amenazas, como una actividad inusual de la API, el escaneo de puertos dentro de la VPC, patrones inusuales de solicitudes de inicio de sesión fallidas o el sondeo de puertos desbloqueado desde una IP defectuosa conocida.
- Problema de instancia: actividad problemática de las instancias, como la minería de criptomonedas, el malware que utiliza algoritmos de generación de dominios (DGA), la actividad de denegación de servicio saliente, el volumen de tráfico de red inusualmente alto, los protocolos de red inusuales, la comunicación de la instancia saliente con una IP maliciosa conocida, EC2 las credenciales temporales de Amazon utilizadas por una dirección IP externa y la exfiltración de datos mediante DNS.
- Actividad de la cuenta: los patrones comunes que indican la actividad de la cuenta incluyen las llamadas a la API desde un proxy de geolocalización o anonimización inusual, los intentos de deshabilitar el AWS CloudTrail registro, los lanzamientos de instancias o infraestructuras inusuales, las implementaciones de infraestructura en una región de AWS inusual y las llamadas a la API desde direcciones IP maliciosas conocidas.

AMS utiliza las cuentas gestionadas para supervisar de forma continua los hallazgos y alertas procedentes de ellas y, GuardDuty en caso de recibir alertas, las operaciones de AMS toman medidas proactivas para proteger sus recursos GuardDuty y su cuenta. Puede ver GuardDuty los

resultados y nuestras acciones a medida que se van desarrollando en la consola de AWS o en las integraciones compatibles.

GuardDuty funciona con Trend Micro Deep Security Manager en su cuenta. Trend Micro Deep Security Manager ofrece servicios de detección y prevención de intrusiones basados en el host. Los servicios de reputación web de Trend Micro se solapan GuardDuty en cierta medida con la capacidad de detectar cuándo un host intenta comunicarse con un host o servicio web que se sabe que representa una amenaza. Sin embargo, GuardDuty proporciona categorías de detección de amenazas adicionales y, para ello, supervisa el tráfico de la red, un método que complementa la detección basada en el host de Trend Micro. La detección de amenazas basada en la red permite aumentar la seguridad, ya que no permite que los controles fallen si el anfitrión presenta un comportamiento problemático. AMS recomienda usarlo GuardDuty en todas sus cuentas de AMS.

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.

GuardDuty supervisión

GuardDuty le informa del estado de su entorno de AWS mediante la generación de [hallazgos de seguridad](#) que AMS captura y sobre los que puede alertar.

Amazon GuardDuty supervisa la seguridad de su entorno de AWS mediante el análisis y el procesamiento de los registros de flujo de VPC, los registros de AWS CloudTrail eventos y los registros del sistema de nombres de dominio. Puede ampliar este ámbito de supervisión configurándolo GuardDuty para utilizar también sus propias listas de IP de confianza y listas de amenazas personalizadas.

- Las listas de IP de confianza se componen de las direcciones IP que ha permitido para una comunicación segura con la infraestructura y las aplicaciones de AWS. GuardDuty no genera datos sobre las direcciones IP que figuran en las listas de IP de confianza. Solo puede tener una lista de IP de confianza cargada a la vez por cuenta y región de AWS.
- Las listas de amenazas se componen de direcciones IP maliciosas conocidas. GuardDuty genera resultados a partir de listas de amenazas. Solo puede tener hasta seis listas de amenazas cargadas a la vez por cuenta y región de AWS.

Para implementarlo GuardDuty, utilice el comando AMS CT Deployment | Monitoring and notification | GuardDuty IP set | Create (ct-08avs2e9mc7g) para crear un conjunto de direcciones IP aprobadas. También puede utilizar el conjunto AMS CT Deployment | Monitoring and Notification | GuardDuty Threat Intel Set | Create (ct-25v6r7t8gvkq5) para crear un conjunto de direcciones IP denegadas.

Para obtener una lista [¿Qué monitorea el sistema de monitoreo AMS?](#) de los servicios que monitorea AMS, consulte.

Firewall DNS Amazon Route 53 Resolver

Amazon Route 53 Resolver responde de forma recursiva a las consultas de DNS de AWS los recursos de registros públicos, los nombres de DNS específicos de Amazon VPC y las zonas alojadas privadas de Amazon Route 53, y está disponible de forma predeterminada en todos ellos. VPCs Con DNS Firewall de Route 53 Resolver, puede filtrar y regular el tráfico DNS de salida para su virtual private cloud (VPC). Para ello, cree colecciones reutilizables de reglas de filtrado en grupos de reglas de DNS Firewall, asocie los grupos de reglas a su VPC y, a continuación, monitoree la actividad en los registros y métricas de DNS Firewall. En función de la actividad, puede ajustar el comportamiento de DNS Firewall según corresponda. Para obtener más información, consulte [Uso del firewall de DNS para filtrar el tráfico DNS saliente](#).

Para ver y administrar la configuración del firewall DNS de Route 53 Resolver, utilice el siguiente procedimiento:

1. Inicie sesión en la consola de Amazon VPC AWS Management Console y ábrala en. <https://console.aws.amazon.com/vpc/>
2. En Firewall de DNS, selecciona Grupos de reglas.
3. Revisa, edita o elimina la configuración existente o crea un grupo de reglas nuevo. Para obtener más información, consulte [Cómo funciona el firewall DNS de Route 53 Resolver](#).

Supervisión y seguridad del firewall DNS de Amazon Route 53 Resolver

El firewall DNS de Amazon Route 53 utiliza los conceptos de asociaciones de reglas, acción de reglas y prioridad de evaluación de reglas. Una lista de dominios es un conjunto reutilizable de especificaciones de dominio que se utiliza en una regla de DNS Firewall, dentro de un grupo de reglas. Al asociar un grupo de reglas a una VPC, DNS Firewall compara las consultas de DNS con las listas de dominios que se utilizan en las reglas. Si el Firewall de DNS encuentra una coincidencia, gestiona la consulta de DNS de acuerdo con la acción de la regla coincidente. Para obtener más información sobre los grupos de reglas y las reglas, consulte Reglas [y grupos de reglas del Firewall DNS](#).

Las listas de dominios se dividen en dos categorías principales:

- Listas de dominios gestionadas, que se AWS crean y mantienen para usted.

- Sus propias listas de dominios, que usted crea y mantiene.

Los grupos de reglas se evalúan en función de su índice de prioridad de asociación.

De forma predeterminada, AMS implementa una configuración de referencia que consta de la siguiente regla y grupo de reglas:

- Un grupo de reglas denominado `DefaultSecurityMonitoringRule`. El grupo de reglas tiene la prioridad de asociación más alta disponible en el momento de la creación para cada VPC existente en cada una de las VPC habilitadas. Región de AWS
- Una regla nombrada `DefaultSecurityMonitoringRule` con la prioridad 1 dentro del grupo de `DefaultSecurityMonitoringRule` reglas, mediante la lista de dominios `AWSManagedDomainsAggregateThreatList` gestionados con la acción ALERT.

Si tiene una configuración existente, la configuración básica se implementa con una prioridad inferior a la configuración existente. La configuración actual es la predeterminada. Utiliza la configuración básica de AMS como una configuración general si la configuración existente no proporciona instrucciones de mayor prioridad sobre cómo gestionar la resolución de consultas. Para modificar o eliminar la configuración básica, realice una de las siguientes acciones:

- Póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) o con su arquitecto de nube (CA).
- Cree una solicitud de cambio (RFC) mediante [Management | Other | Other | Create CT \(ct-1e1xtak34nx76\)](#).
- Cree una solicitud de servicio.

Si su cuenta funciona en el modo Desarrollador o en el modo Cambio directo, puede realizar los cambios usted mismo.

AWS Certificate Manager Certificado (ACM)

AMS tiene un certificado CT, `Deployment | Advanced stack components | ACM` con un SANs | `Create (ct-3l14e139i5p50)` adicional, que puede utilizar para enviar una solicitud de certificado de AWS Certificate Manager, con hasta cinco nombres alternativos de sujeto (SAN) adicionales (como `example.com`, `example.net` y `example.org`). [Para obtener más información, consulte ¿Qué es? AWS Certificate Manager](#) y [característica del certificado ACM](#).

 Note

Esta configuración de tiempo de espera no se limita a la ejecución, sino también a la validación del certificado ACM mediante la validación por correo electrónico. Sin tu validación, la RFC fallará.

Cifrado de datos en AMS

AMS utiliza varios AWS servicios para el cifrado de datos, entre los que destacan Amazon Simple Storage Service AWS Key Management Service (AWS KMS), Amazon Elastic Block Store, Amazon Relational Database Service Amazon Redshift Amazon ElastiCache, AWS Lambda, y OpenSearch Amazon Service.

Amazon S3

Amazon S3 ofrece varias opciones de cifrado de objetos que protegen los datos en tránsito y en reposo. El cifrado del lado del servidor cifra el objeto antes de guardarlo en discos de sus centros de datos y, a continuación, lo descifra al descargar los objetos. Siempre que autentique su solicitud y tenga permiso de acceso, no existe diferencia alguna en la forma de obtener acceso a objetos cifrados o sin cifrar. Para obtener más información, consulte [Protección de los datos en Amazon S3](#).

Amazon EBS

Con el cifrado de Amazon EBS, no necesita crear, mantener ni proteger su propia infraestructura de administración de claves. El cifrado de Amazon EBS utiliza AWS KMS claves al crear volúmenes e instantáneas cifrados. Las operaciones de cifrado se realizan en los servidores que alojan EC2 las instancias de Amazon. Esto se hace para garantizar que tanto data-at-rest una instancia como data-in-transit entre ella y su almacenamiento Amazon EBS adjunto estén protegidos. Puede asociar volúmenes cifrados y no cifrados con una instancia simultáneamente. Para obtener más información, consulte [Cifrado de Amazon EBS](#).

Amazon RDS

Amazon RDS puede cifrar sus instancias de base de datos Amazon RDS. Los datos cifrados en reposo incluyen el almacenamiento subyacente de las instancias de base de datos, sus copias de seguridad automatizadas, las réplicas de lectura y las instantáneas. Las instancias de base de datos cifradas por Amazon RDS utilizan el algoritmo de cifrado AES-256 estándar del sector para cifrar los datos en el servidor que aloja las instancias de base de datos de Amazon RDS. Una vez cifrados los

datos, Amazon RDS se encarga de la autenticación de acceso y del descifrado de los datos de forma transparente, con un impacto mínimo en el desempeño. No es necesario modificar las aplicaciones cliente de base de datos para utilizar el cifrado. Para obtener más información, consulte [Cifrado de recursos de Amazon RDS](#).

Amazon Simple Queue Service

Además de la opción de cifrado gestionado del lado del servidor (SSE) predeterminada por Amazon SQS, el SSE gestionado por Amazon SQS (SSE-SQS) le permite crear un cifrado gestionado del lado del servidor personalizado que utiliza claves de cifrado gestionadas por Amazon SQS para proteger los datos confidenciales que se envían a través de las colas de mensajes. El cifrado del servidor (SSE) le permite transferir información confidencial en colas cifradas. El SSE protege el contenido de los mensajes en las colas mediante claves de cifrado administradas por Amazon SQS (SSE-SQS) o claves administradas en (SSE-KMS). AWS KMS [Para obtener información sobre cómo administrar el SSE mediante el, consulte Cifrado en reposo. AWS Management Console](#)

Cifrado de datos en reposo

OpenSearch Los dominios de servicio ofrecen el cifrado de los datos en reposo, una función de seguridad que ayuda a evitar el acceso no autorizado a los datos. La función utiliza AWS Key Management Service (AWS KMS) para almacenar y gestionar las claves de cifrado y el algoritmo del estándar de cifrado avanzado con claves de 256 bits (AES-256) para realizar el cifrado. Para obtener más información, consulte [Cifrado de datos en reposo para Amazon OpenSearch Service](#).

Administración de claves

AWS KMS es un servicio gestionado que le facilita la creación y el control de las claves maestras de los clientes (CMKs), las claves de cifrado que se utilizan para cifrar sus datos. AWS KMS CMKs están protegidos por módulos de seguridad de hardware (HSMs) validados por el programa de validación de módulos criptográficos FIPS 140-2, excepto en las regiones de China (Beijing) y China (Ningxia). Para obtener más información, consulte [¿Qué es AWS Key Management Service?](#)

Identity and Access Management

AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a AWS los recursos. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos. Durante la incorporación a AMS, usted es responsable de crear funciones de administrador de IAM multicuenta en cada una de sus cuentas gestionadas.

La IAM de Multi-Account Landing Zone (MALZ) protege

La zona de aterrizaje multicuenta (MALZ) de AMS requiere una confianza en Active Directory (AD) como objetivo de diseño principal de la gestión de acceso a AMS para permitir que cada organización (tanto AMS como cliente) gestione los ciclos de vida de sus propias identidades. Esto evita la necesidad de tener credenciales en el directorio de la otra. La confianza unidireccional está configurada de modo que el Active Directory administrado dentro de él Cuenta de AWS confíe en AD, propiedad del cliente o administrado, para autenticar a los usuarios. Como la confianza es unidireccional, no significa que el Active Directory del cliente confíe en el Active Directory del cliente.

En esta configuración, el directorio de clientes que gestiona las identidades de los usuarios se conoce como bosque de usuarios y el AD gestionado al que se adjuntan las EC2 instancias de Amazon se conoce como bosque de recursos. Se trata de un patrón de diseño de Microsoft que se utiliza habitualmente para la autenticación de Windows; para obtener más información, [consulte Forest Design Models](#).

Este modelo permite a ambas organizaciones automatizar sus respectivos ciclos de vida y permite a AMS y a usted revocar rápidamente el acceso si un empleado deja la organización. Sin este modelo, si ambas organizaciones utilizaran un directorio común (o lo crearan users/groups en los directorios de la otra), ambas organizaciones tendrían que incluir flujos de trabajo adicionales y sincronizaciones de usuarios para contabilizar los empleados que comienzan y se van. Esto supone un riesgo, ya que el proceso tiene latencia y puede ser propenso a errores.

Requisitos previos de acceso a MALZ

Integración del proveedor de identidad MALZ para acceder a la consola AWS/AMS, CLI y SDK.

Confianza unidireccional para las EC2 instancias de Amazon en tu cuenta de AMS.

Autenticación con identidades

AMS usa funciones de IAM, que son un tipo de identidad de IAM. Una función de IAM es muy similar a la de un usuario, ya que es una identidad con políticas de permisos que determinan lo que la identidad puede y no puede hacer en ella. AWS Sin embargo, un rol no tiene credenciales asociadas y, en lugar de estar asociado únicamente a una persona, está pensado para que lo pueda asumir cualquier persona que lo necesite. Un usuario de IAM puede asumir una función para disponer temporalmente de diferentes permisos para una tarea específica.

Los roles de acceso están controlados por la pertenencia a un grupo interno, que la Gerencia de Operaciones administra y revisa periódicamente.

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-roleo](#) 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).
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

Rol	Política o políticas
	AWSSupportAcceso
	AMSChangeManagementReadOnlyPolicy
	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 AWSsupport Ejemplo de acceso Esta política proporciona acceso a todas las operaciones y recursos de soporte.

Rol	Política o políticas
	AWSCertificateManagerFullAccess información, (Política pública gestionada de AWS)
	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

Rol	Política o políticas
	AMSCChangeManagementPolicy
	AWSCertificateManagerFullAccess
	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"
    }
]
}

```

AMSCChangeManagementReadOnlyPolicy

AMSCChangeManagementReadOnlyPolicy

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.

AMSCChangeManagementInfrastructurePolicy

AMSCChangeManagementInfrastructurePolicy(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 [ReadOnlyAccess](#) para 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": [
        "*"
      ]
    }
  ]
}

```

Registro y supervisión de eventos de seguridad

AMS monitorea continuamente el entorno gestionado para detectar amenazas a la seguridad. AMS o usted pueden detectar los eventos de seguridad. AMS actualiza periódicamente su proceso de automatización, según la Guía de gestión de incidentes de seguridad informática del Instituto Nacional de Estándares y Tecnología (NIST), para detectar mejor las amenazas a la seguridad.

Seguridad de terminales (EPS)

Los recursos que aprovisiona 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)
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

Opción	Valor predeterminado
	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
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	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
	Todos los Day/All días (24 horas)	

Opción	Valor predeterminado	Notas
		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.
Se permite el spyware o el grayware	Ninguno	N/A
Notificación de eventos locales	Sí	N/A

Proceso de mitigación de malware

AMS utiliza la plataforma Deep Security Platform (sistema antimalware) de Trend Micro para detectar y responder al malware en las instancias gestionadas por AMS. De forma predeterminada, el agente de detección de Trend Micro se ejecuta en todas las EC2 instancias de Amazon, incluidas las de los servicios compartidos y las subredes privadas, para los sistemas operativos Windows y Linux. El sistema antimalware está conectado a la supervisión de AMS, de modo que se genera un evento

cada vez que se detecta malware. Si se produce un impacto en el cliente, el evento se transfiere al proceso de gestión de incidentes (para obtener más información, consulte [Respuesta a incidentes de AMS](#)). Mientras AMS evalúa el impacto, se le notifica y se intenta mitigarlo.

Las definiciones antimalware de Trend Micro se actualizan automáticamente cuando Trend Micro publica actualizaciones.

Durante la incorporación de la aplicación, usted indica la acción que desea que AMS lleve a cabo cuando encuentre malware en una instancia:

- Asegúrese de que el archivo en cuarentena esté en la lista de archivos permitidos, elimínelo de la cuarentena y devuélvalo al sistema de archivos.
- Elimine el archivo en cuarentena y elimínelo de la instancia.
- Suspenda la instancia y sustitúyala. La instancia suspendida estará entonces a su disposición para utilizarla en una investigación forense.

Tras la incorporación de la aplicación:

- Cuando el sistema antimalware descubre malware en una instancia, AMS lo pone automáticamente en cuarentena. Esto desencadena un evento y una investigación de seguimiento.
- AMS le notifica el evento mediante una notificación de servicio y comienza a aplicar la acción de mitigación predeterminada que haya seleccionado.
- Si no has elegido una acción predeterminada, AMS te preguntará qué acción debes realizar. Tras recibir las instrucciones, AMS ejecuta la acción seleccionada y se lo notifica. AMS le vuelve a notificar una vez finalizada la acción, incluyendo los detalles necesarios para el análisis forense, si corresponde.

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.

Escaneos completos de malware del sistema

El estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) exige escaneos completos de malware del sistema, que están habilitados de forma predeterminada en la VPC gestionada por AMS. Los escaneos completos del sistema están programados para realizarse a las 2 de la madrugada (en la zona horaria establecida en el servidor) porque consumen una gran cantidad de CPU. Los escaneos completos del sistema se suman a los escaneos de malware habituales que no utilizan mucha CPU.

Existe un nuevo tipo de cambio de administración (CT), denominado Desactivar los escaneos de malware, que permite deshabilitar los escaneos de malware en todo el sistema. Puede encontrar el CT en Gestión | Seguridad del host | Análisis completo del sistema | Desactivar la clasificación, cambiar el ID ct-1pybwg08h8qsz. Para volver a activar los escaneos, utilice la función Administración | Otros | Otros | Actualización de CT. La desactivación de los escaneos completos del sistema no inhabilita los escaneos de malware habituales.

Seguridad de Amazon Inspector

El servicio Amazon Inspector supervisa la seguridad de las pilas gestionadas por AMS. Amazon Inspector es un servicio de evaluación de seguridad automatizado que ayuda a identificar las brechas en la seguridad y el cumplimiento de la infraestructura implementada AWS. Las evaluaciones de seguridad de Amazon Inspector le permiten evaluar automáticamente las pilas para detectar la exposición, las vulnerabilidades y las desviaciones de las mejores prácticas al comprobar la accesibilidad de la red y las vulnerabilidades no deseadas en sus instancias de Amazon EC2 . Después de la evaluación, Amazon Inspector genera una lista detallada de resultados relacionados con la seguridad priorizados por nivel de gravedad. Las evaluaciones de Amazon Inspector se ofrecen como paquetes de reglas predefinidas mapeados a las mejores prácticas y definiciones de seguridad comunes. Los investigadores de AWS seguridad actualizan periódicamente estas reglas. Para obtener más información sobre Amazon Inspector, visita [Amazon Inspector](#).

AMS Amazon Inspector FAQs

- ¿Amazon Inspector está instalado en mis cuentas de AMS de forma predeterminada?

No. Amazon Inspector no forma parte de la compilación de la AMI predeterminada ni de la ingesta de carga de trabajo.

- ¿Cómo puedo acceder a Amazon Inspector e instalarlo?

Envíe un RFC (Administración | Otros | Otros | Crear) para solicitar el acceso a la cuenta y la instalación al Inspector y el equipo de operaciones de AMS modificará el Customer_ReadOnly_Role para proporcionar acceso a la consola de Amazon Inspector (sin acceso a SSM).

- ¿El agente de Amazon Inspector debe estar instalado en todas las EC2 instancias de Amazon que quiero evaluar?

No, las evaluaciones de Amazon Inspector con el paquete de reglas de accesibilidad de la red se pueden ejecutar sin un agente para ninguna instancia de Amazon EC2 . El agente es obligatorio para alojar los paquetes de reglas de evaluación. Para obtener más información sobre la instalación de agentes, consulte [Instalación de los agentes de Amazon Inspector](#).

- ¿Este servicio tiene un coste adicional?

Sí. Los precios de Amazon Inspector se encuentran en el sitio de [precios de Amazon Inspector](#).

- ¿Cuáles son las conclusiones de Amazon Inspector?

Los hallazgos son posibles problemas de seguridad descubiertos durante la evaluación de Amazon Inspector del objetivo de evaluación seleccionado. Los resultados se muestran en la consola de Amazon Inspector o en la API y contienen una descripción detallada de los problemas de seguridad y recomendaciones para resolverlos.

- ¿Están disponibles los informes de la evaluación de Amazon Inspector?

Sí. Un informe de evaluación es un documento que detalla lo que se prueba en la ejecución de evaluación y los resultados de esta. Los resultados de la evaluación se organizan en informes estándar, los que se pueden generar para compartir los resultados dentro de su equipo para corregir errores, enriquecer los datos de auditorías de cumplimiento o almacenar referencias futuras. Se puede generar un informe de evaluación de Amazon Inspector para ejecutar una evaluación una vez que se haya completado correctamente.

- ¿Puedo usar etiquetas para identificar las pilas con las que quiero ejecutar los informes de Amazon Inspector?

Sí.

- ¿Los equipos de operaciones de AMS tendrán acceso a los resultados de la evaluación de Amazon Inspector?

Sí. Cualquier persona que tenga acceso a la consola de Amazon Inspector en AWS puede ver los resultados y los informes de evaluación.

- ¿Los equipos de operaciones de AMS recomendarán o tomarán medidas en función de las conclusiones de los informes de Amazon Inspector?

No. Si quieres que se realicen cambios en función de los resultados del informe de Amazon Inspector, debes solicitarlos mediante una RFC (Management | Other | Other | Update).

- ¿Recibirá una notificación a AMS cuando ejecute un informe de Amazon Inspector?

Cuando solicitas el acceso a Amazon Inspector, el operador de AMS que ejecuta la RFC notifica la solicitud a tu CSDM.

Para obtener más información, consulte [Amazon Inspector FAQs](#).

Respuesta a incidentes de AMS

AMS utiliza las mejores prácticas tradicionales de gestión de incidentes de gestión de servicios de TI (ITSM) para restablecer el servicio, cuando es necesario, lo más rápido posible.

Brindamos follow-the-sun asistencia las 24 horas del día, los 7 días de la semana, los 365 días del año a través de múltiples centros de operaciones en todo el mundo, con operadores especializados que supervisan activamente los paneles de control y las colas de incidentes.

Nuestros ingenieros de operaciones utilizan herramientas internas de seguimiento de incidentes para identificar, registrar, categorizar, priorizar, diagnosticar, resolver y cerrar incidentes y proporcionarle información actualizada sobre todas estas actividades a través de la consola AMS o mediante la API. Soporte Nuestros operadores, muchos de los cuales han trabajado en AWS Premium Support en distintos perfiles y funciones tecnológicas, utilizan una variedad de Soporte herramientas internas para ayudar en todas esas actividades. Estos operadores están muy familiarizados con las infraestructuras compatibles con AMS y tienen conocimientos técnicos de nivel experto para abordar todos los problemas de soporte identificados. En el raro caso de que nuestros operadores necesiten asistencia, los equipos de Soporte y AWS Servicio Premium están disponibles para ayudarlo según sea necesario.

En los casos en que los incidentes de alta prioridad estén afectando a sus cargas de trabajo críticas, AMS recomendará restaurar la infraestructura. Suele haber un equilibrio entre la solución de un

problema o la restauración a partir de una copia de seguridad de funcionalidad comprobada, y los riesgos e impactos derivados del tiempo de inactividad del servicio para los clientes son los factores decisivos. Si dispones de tiempo para resolver problemas, AMS te ayudará, pero si la restauración es urgente, podemos iniciar una restauración de inmediato.

Note

Se pierden los datos efímeros que no forman parte de la plantilla de pila o de la restauración de datos. AMS hace todos los esfuerzos razonables para restaurar la infraestructura cuando las ofertas de AWS servicios no están disponibles. La restauración de la infraestructura se completa una vez que las ofertas de AWS servicios están disponibles.

Si no autorizas la restauración de la infraestructura según lo recomendado por AMS, no podrás recibir un crédito de servicio equivalente al compromiso de servicio de AMS por el tiempo de resolución de incidentes.

Validación de conformidad

AMS implementa y administra una biblioteca de AWS Config reglas y medidas correctivas para protegerlo contra errores de configuración que podrían reducir la seguridad y la integridad operativa de sus cuentas.

Por ejemplo, cuando se crea un bucket de Amazon S3, AWS Config puede evaluar el bucket de Amazon S3 según una regla que exige que los buckets de Amazon S3 denieguen el acceso de lectura público. Si la política de buckets de Amazon S3 o la lista de control de acceso a los buckets (ACL) permiten el acceso de lectura AWS Config público, marcan tanto el bucket como la regla como no conformes. Estas Reglas de AWS Config marcan los recursos como conformes, no conformes o no aplicables, según el resultado de su evaluación. Para obtener más información sobre el AWS Config servicio, consulte la [Guía para AWS Config desarrolladores](#).

Puede usar la AWS Config consola, la AWS CLI o la AWS Config API para ver las reglas implementadas en su cuenta y el estado de cumplimiento de sus reglas y recursos. Para obtener más información, consulte la AWS Config documentación: [Visualización del cumplimiento de la configuración](#).

Note

Encontrará información adicional sobre este tema accediendo a los informes de AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#). Para

acceder a AWS Artifact, puede ponerse en contacto con su CSDM para obtener instrucciones o ir a [Introducción a AWS](#) Artifact. Esta información no se incluye en esta guía del usuario porque contiene contenido de seguridad confidencial.

Zona de destino multicuenta: visualización del estado de cumplimiento de su Reglas de AWS Config

La zona de aterrizaje multicuenta de AMS utiliza el servicio de AWS Config agregación para crear una visión centralizada del cumplimiento en todas sus cuentas. Esto significa que puedes ver el estado de conformidad de Reglas de AWS Config todo tu entorno de landing zone multicuenta de AMS en el AWS Config agregador de tu cuenta de seguridad.

El siguiente es un ejemplo del AWS Config agregador que muestra el estado de cumplimiento central de todas las cuentas. Reglas de AWS Config

Para obtener más información, consulte la documentación de AWS de [Config Aggregator](#).

- ¿Cómo usa AMS las reglas de AWS Config?

AMS Reglas de AWS Config las crea para dar visibilidad a la configuración de sus AWS recursos en función de las condiciones especificadas en las reglas. Si una regla no es conforme, puede solicitar un cambio y el equipo de operaciones de AMS trabajará con usted para tomar las medidas correctivas necesarias.

- En ese caso, verás que aparecen los siguientes cambios en tus cuentas de AMS:
 - Reglas de AWS Config en AWS Config > Reglas
 - Las reglas de Config personalizadas con sus funciones Lambda existen en su cuenta
 - Config Aggregator en la cuenta de seguridad y Config Authorization en todas las cuentas (solo en la zona de destino multicuenta)

La siguiente es una muestra de los resultados de Reglas de AWS Config su evaluación de conformidad, que se muestran a continuación:

Para obtener más información sobre AWS Config, consulte:

- AWS Config: [¿Qué es Config?](#)

- Reglas de AWS Config: [evaluación de los recursos con reglas](#)
- Reglas de AWS Config: [Comprobación de conformidad dinámica: Reglas de AWS Config — Comprobación de conformidad dinámica para recursos en la nube](#)
- AWS Config Aggregator: agregación de datos [multicuenta y multirregión](#)

Restricciones de la política de control del servicio de landing zone multicuenta de 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.

Resiliencia

La infraestructura AWS global se basa en zonas de disponibilidad Regiones de AWS y zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

[Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte la infraestructura global.AWS](#)

Seguridad de la infraestructura

Note

Encontrará información adicional sobre este tema accediendo a los informes de AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#). Para acceder a AWS Artifact, puede ponerse en contacto con su CSDM para obtener instrucciones o ir a [Introducción a AWS](#) Artifact. Esta información no se incluye en esta guía del usuario porque contiene contenido de seguridad confidencial.

Control de seguridad para sistemas end-of-support operativos

Los sistemas operativos que estén fuera del período de soporte general de la EOS o del fabricante end-of-support del sistema operativo y que no reciban actualizaciones de seguridad corren un mayor riesgo de seguridad.

AWS ofrece algunos servicios para ayudar a gestionar el sistema operativo end-of-support. Para obtener información acerca de Windows end-of-support, consulte [Programa de End-of-Support migración para Windows Server](#).

Note

Encontrará información adicional sobre este tema accediendo a los informes de AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#). Para acceder a AWS Artifact, puede ponerse en contacto con su CSDM para obtener instrucciones o ir a [Introducción a AWS Artifact](#). Esta información no se incluye en esta guía del usuario porque contiene contenido de seguridad confidencial.

Usar grupos de seguridad

Un grupo de seguridad funciona como un firewall virtual que controla el tráfico de una o varias instancias. Los grupos de seguridad AMS le permiten establecer reglas de tráfico entrante y saliente a nivel de instancia. Puede crear un grupo de seguridad y especificar recursos en su cuenta AMS, instancias de Amazon, EC2 instancias de base de datos de Amazon RDS, Load Balancers, instancias de replicación de Deep Security Manager (DSM), destinos de montaje de EFS y ElastiCache clústeres para asociarlos al grupo de seguridad. Una vez asociadas, el tráfico hacia o desde esas instancias está restringido por las reglas establecidas en el grupo de seguridad.

Para comprender mejor la seguridad general de AWS, consulte [Best Practices for Security, Identity and Compliance](#) y [Amazon EC2 Security Groups for Linux Instances](#).

AMS ahora cuenta con un conjunto de tipos de cambios para crear y administrar grupos de seguridad:

- Despliegue | Componentes de pila avanzados | Grupo de seguridad | Crear (ct-10xx2g2d7hc90)
- Administración | Componentes de pila avanzados | Grupo de seguridad | Eliminar (ct-3cp96z7r065e4)

- Administración | Componentes de pila avanzados | Grupo de seguridad | Actualización (ct-3memthlcmvc1b)

Para [ver ejemplos](#), consulte Grupos de seguridad.

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) Se permite el acceso SSH y RDP desde los bastiones	SentinelDefaultSecurityGroupPublic (no restringe el tráfico saliente)
Bastiones de MALZ:			

Tipo	Protocolo	Intervalo de puertos	Origen
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	
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-10xx2g2d7hc90).

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](#).

Biblioteca de controles preventivos y de detección AMS

AWS Managed Services (AMS) le proporciona una selección library/catalog de políticas de control de servicios comprobadas (SCPs) y ConfigRules que puede aprovechar para mejorar su postura de seguridad y mitigar las brechas de conformidad en sus cuentas de AMS.

Temas

- [Reglas seleccionadas SCPs y Config](#)
- [Notificación personalizada para las reglas de Config](#)

Reglas seleccionadas SCPs y Config

Reglas seleccionadas SCPs y de configuración para AMS Advanced.

- Políticas de control de servicios (SCPs): las que SCPs se proporcionan se suman a las de AMS predeterminadas.

Puede utilizar estos controles de biblioteca junto con los predeterminados para cumplir requisitos de seguridad específicos.

- Reglas de configuración: Como medida de referencia, AMS recomienda aplicar paquetes de conformidad (consulte los paquetes de [conformidad](#) en la AWS Config guía) además de las reglas de configuración de AMS predeterminadas (consulte AMS Artifacts para ver las reglas predeterminadas). Los paquetes de conformidad cubren la mayoría de los requisitos de conformidad y AWS los actualiza periódicamente.

Las reglas que se enumeran aquí se pueden usar para cubrir brechas específicas de cada caso de uso que no están cubiertas por los paquetes de conformidad

Note

A medida que las reglas y los paquetes de conformidad predeterminados de AMS se actualicen con el tiempo, es posible que veas duplicados de estas reglas.

AMS recomienda realizar una limpieza periódica de las Config Rules duplicadas en general.

En el caso de AMS Advanced, las reglas de configuración no deben utilizar correcciones automáticas (consulte [Remediar recursos de AWS no conformes mediante reglas de AWS Config Rules](#)) para evitar cambios. out-of-band

SCP-AMS-001: Restrinja la creación de EBS

Impida la creación de volúmenes de EBS si no tiene el cifrado activado.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:CreateVolume",
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-002: Restringe el lanzamiento EC2

Impida el lanzamiento de una EC2 instancia si el volumen de EBS no está cifrado. Esto incluye denegar un EC2 lanzamiento sin cifrar, AMIs ya que este SCP también se aplica a los volúmenes raíz.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Effect": "Deny"
}
```

SCP-ADV-001: Restrinja los envíos de RFC

Impida que las funciones de AMS predeterminadas envíen automatizaciones específicas, RFCs como Crear VPC o Eliminar VPC. Esto resulta útil si desea aplicar permisos más detallados a sus funciones federadas.

Por ejemplo, es posible que desee que la opción predeterminada sea `AWSManagedServicesChangeManagement` Role capaz de enviar la mayoría de las disponibles, RFCs excepto las que permiten la creación y eliminación de una VPC, la creación de subredes

adicionales, la desconexión de una cuenta de aplicación y la actualización o eliminación de los proveedores de identidad de SAML:

SCP-AMS-003: Restringe la creación de RDS en AMS EC2

Impida la creación de instancias de Amazon EC2 y RDS que no tengan etiquetas específicas y, al mismo tiempo, permita que el AMS Backup IAM rol predeterminado de AMS lo haga. Esto es necesario para la recuperación ante desastres o DR.

```
{
  "Sid": "DenyRunInstanceWithNoOrganizationTag",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances",
    "rds:CreateDBInstance"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:rds:*:*:db:*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/organization": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam:*:<Account_Number>:role/ams-backup-iam-role"
      ]
    }
  }
}
```

SCP-AMS-004: Restringe las subidas a S3

Impida la carga de objetos S3 no cifrados.

```
{
  "Sid": "DenyUnencryptedS3Uploads",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
}
```

```

        "Condition": {
            "StringNotLike": {
                "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]
            },
            "Null": {
                "s3:x-amz-server-side-encryption": "false"
            }
        }
    }
}

```

SCP-AMS-005: Restringe el acceso a la API y a la consola

Impida el acceso a la consola y a la API de AWS para las solicitudes procedentes de direcciones IP incorrectas conocidas como cliente determinado InfoSec.

SCP-AMS-006: Impide que la entidad de IAM elimine la cuenta de un miembro de la organización

Impedir que una AWS Identity and Access Management entidad elimine las cuentas de los miembros de la organización.

```

{
  "Effect": "Deny",
  "Action": ["organizations:LeaveOrganization"],
  "Resource": ["*"]
}

```

SCP-AMS-007: Impida compartir recursos con cuentas ajenas a su organización

Evite compartir recursos con cuentas externas ajenas a su AWS organización

```

{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {

```

```

    "Bool": {
      "ram:AllowsExternalPrincipals": "true"
    }
  },
  {
    "Effect": "Deny",
    "Action": [
      "ram:CreateResourceShare",
      "ram:UpdateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "ram:RequestedAllowsExternalPrincipals": "true"
      }
    }
  }
}

```

SCP-AMS-008: Impida compartir con organizaciones o unidades organizativas () OUs

Impida compartir recursos con una and/or unidad organizativa de cuentas que esté en una organización.

```

{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "ram:Principal": [
        "arn:aws:organizations::*:account/o-${OrganizationId}/${AccountId}",
        "arn:aws:organizations::*:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
      ]
    }
  }
}

```

SCP-AMS-009: Impide que los usuarios acepten invitaciones para compartir recursos

Impida que las cuentas de los miembros acepten invitaciones AWS RAM para unirse a recursos compartidos. Esta API no admite ninguna condición y solo impide que se comparta contenido desde cuentas externas.

```
{
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}
```

SCP-AMS-010: Impide las acciones de activación y desactivación de la región de la cuenta

Impida activar o desactivar nuevas AWS regiones para sus AWS cuentas.

```
{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

SCP-AMS-011: Impida las acciones de modificación de la facturación

Impida modificaciones en la configuración de facturación y pago.

```
{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ],
  "Resource": "*"
}
```

SCP-AMS-012: Impide la eliminación o modificación de datos específicos CloudTrails

Impida modificaciones en AWS CloudTrail senderos específicos.

```
{
  "Effect": "Deny",
  "Action": [
    "cloudtrail:DeleteEventDataStore",
    "cloudtrail:DeleteTrail",
    "cloudtrail:PutEventSelectors",
    "cloudtrail:PutInsightSelectors",
    "cloudtrail:UpdateEventDataStore",
    "cloudtrail:UpdateTrail",
    "cloudtrail:StopLogging"
  ],
  "Resource": [
    "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"
  ]
}
```

SCP-AMS-013: Impide la desactivación del cifrado EBS predeterminado

Impida la desactivación del cifrado predeterminado de Amazon EBS.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

SCP-AMS-014: Impedir la creación de una VPC y una subred predeterminadas

Impida la creación de una Amazon VPC y subredes predeterminadas.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc"
  ],
  "Resource": "*"
}
```

SCP-AMS-015: Impide la desactivación y la modificación GuardDuty

Evita que Amazon GuardDuty se modifique o desactive.

```
{
  "Effect": "Deny",
  "Action": [
    "guardduty:AcceptInvitation",
    "guardduty:ArchiveFindings",
    "guardduty:CreateDetector",
    "guardduty:CreateFilter",
    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty>DeleteDetector",
    "guardduty>DeleteFilter",
    "guardduty>DeleteInvitations",
    "guardduty>DeleteIPSet",
    "guardduty>DeleteMembers",
    "guardduty>DeletePublishingDestination",
    "guardduty>DeleteThreatIntelSet",
    "guardduty:DisableOrganizationAdminAccount",
    "guardduty:DisassociateFromMasterAccount",
    "guardduty:DisassociateMembers",
    "guardduty:InviteMembers",
    "guardduty:StartMonitoringMembers",
    "guardduty:StopMonitoringMembers",
    "guardduty:TagResource",
    "guardduty:UnarchiveFindings",
    "guardduty:UntagResource",
    "guardduty:UpdateDetector",
    "guardduty:UpdateFilter",
    "guardduty:UpdateFindingsFeedback",
    "guardduty:UpdateIPSet",
    "guardduty:UpdateMalwareScanSettings",
    "guardduty:UpdateMemberDetectors",
    "guardduty:UpdateOrganizationConfiguration",
    "guardduty:UpdatePublishingDestination",
    "guardduty:UpdateThreatIntelSet"
  ],
  "Resource": "*"
}
```

```
}
```

SCP-AMS-016: Impide la actividad de los usuarios root

Impida que el usuario root realice cualquier acción.

```
{
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:root"
      ]
    }
  }
}
```

SCP-AMS-017: Impide la creación de claves de acceso para el usuario root

Impida la creación de claves de acceso para el usuario root.

```
{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

SCP-AMS-018: Impide deshabilitar el bloqueo de acceso público de la cuenta S3

Evite deshabilitar el bloqueo de acceso público de una cuenta Amazon S3. Esto evita que cualquier segmento de la cuenta pase a ser público.

```
{
  "Effect": "Deny",
  "Action": "s3:PutAccountPublicAccessBlock",
  "Resource": "*"
}
```


SCP-AMS-019: Impedir la desactivación de AWS Config o la modificación de las reglas de Config

Impida la desactivación o modificación AWS Config de las reglas.

```
{
  "Effect": "Deny",
  "Action": [
    "config:DeleteConfigRule",
    "config:DeleteConfigurationRecorder",
    "config:DeleteDeliveryChannel",
    "config:DeleteEvaluationResults",
    "config:StopConfigurationRecorder"
  ],
  "Resource": "*"
}
```

SCP-AMS-020: Impide todas las acciones de IAM

Impida todas las acciones de IAM.

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": "*"
}
```

SCP-AMS-021: Impida la eliminación de registros, grupos y transmisiones CloudWatch

Evita que se eliminen grupos y transmisiones de Amazon CloudWatch Logs.

```
{
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": "*"
}
```

SCP-AMS-022: Impide la eliminación de Glacier

Impida la eliminación de Amazon Glacier.

```
{
  "Effect": "Deny",
  "Action": [
    "glacier:DeleteArchive",
    "glacier:DeleteVault"
  ],
  "Resource": "*"
}
```

SCP-AMS-023: Impida la eliminación del IAM Access Analyzer

Impida la eliminación del IAM Access Analyzer.

```
{
  "Action": [
    "access-analyzer:DeleteAnalyzer"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-024: Impedir modificaciones en el Security Hub

Impida la eliminación de AWS Security Hub.

```
{
  "Action": [
    "securityhub:DeleteInvitations",
    "securityhub:DisableSecurityHub",
    "securityhub:DisassociateFromMasterAccount",
    "securityhub:DeleteMembers",
    "securityhub:DisassociateMembers"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-025: Impedir la eliminación en Directory Service

Impida la eliminación de los recursos de AWS Directory Service.

```
{
  "Action": [
    "ds:DeleteDirectory",
    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",
    "ds:DisableLDAPS",
    "ds:DisableRadius",
    "ds:DisableSso",
    "ds:UnshareDirectory"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-026: Impida el uso de un servicio excluido

Impida el uso de servicios que figuran en la lista denegada.

Note

Sustituya *service1* y por *service2* sus nombres de servicio. Ejemplo *access-analyzer* o *IAM*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"]
}
```

SCP-AMS-027: Impedir el uso de un servicio excluido en regiones específicas

Impida el uso de servicios que figuran en la lista de personas excluidas en regiones específicas.

AWS

 Note

Sustituya *service1* y por *service2* los nombres de sus servicios. Ejemplo *access-analyzer* o *IAM*.

Sustituya *region1* y *region2* por sus nombres de servicio. Ejemplo *us-west-2* o *use-east-1*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"],
  "Condition": {
    "StringEquals": {
      "aws:RequestedRegion": [
        "region1",
        "region2"
      ]
    }
  }
}
```

SCP-AMS-028: Impide que las etiquetas sean modificadas excepto por directores autorizados

Impida que cualquier usuario modifique las etiquetas, excepto los directores autorizados. Utilice etiquetas de autorización para autorizar a los directores. Las etiquetas de autorización deben estar asociadas a los recursos y a los directores. A solo user/role se considera autorizada si la etiqueta del recurso y la principal coinciden. Para obtener más información, consulte los siguientes recursos:

- [Proteger las etiquetas de recursos utilizadas para la autorización mediante una política de control de servicios en AWS Organizations](#)
- [Impida que las etiquetas se modifiquen excepto por parte de responsables autorizados](#)

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
```

```

"Resource": [
  "*"
],
"Condition": {
  "StringNotEquals": {
    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
    "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
  },
  "Null": {
    "ec2:ResourceTag/access-project": false
  }
}
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
    },
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
        "access-project"
      ]
    }
  }
}
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {

```

```

    "StringNotEquals": {
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "Null": {
      "aws:PrincipalTag/access-project": true
    }
  }
}

```

SCP-AMS-029: Impedir que los usuarios eliminen los registros de flujo de Amazon VPC

Impida la eliminación de los registros de flujo de Amazon VPC.

```

{
  "Action": [
    "ec2:DeleteFlowLogs",
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:PutLifecycleConfiguration",
    "firehose:DeleteDeliveryStream"
  ],
  "Resource": "*",
  "Effect": "Deny"
}

```

SCP-AMS-030: Impedir compartir la subred de VPC con una cuenta que no sea la cuenta de red

Impida compartir las subredes de Amazon VPC con cuentas distintas de la cuenta de red.

Note

NETWORK_ACCOUNT_ID Sustitúyalo por el ID de su cuenta de red.

```

{
  "Effect": "Deny",
  "Action": [
    "ram:AssociateResourceShare",

```

```

    "ram:CreateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "ram:Principal": "NETWORK_ACCOUNT_ID"
    },
    "StringEquals": {
      "ram:RequestedResourceType": "ec2:Subnet"
    }
  }
}

```

SCP-AMS-031: Impida el lanzamiento de instancias con tipos de instancias prohibidos

Impida el lanzamiento de tipos de EC2 instancias de Amazon prohibidos.

Note

Sustituya *instance_type1* y *instance_type2* por los tipos de instancias que desee restringir, por ejemplo, *t2.micro* o por una cadena comodín, por ejemplo. **.nano*

```

{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}

```

SCP-AMS-032: Impide el lanzamiento de instancias sin IMDSv2

Evite las EC2 instancias de Amazon sin IMDSv2.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*"
  }
]
```

SCP-AMS-033: Impide que se modifique una función específica de IAM

Impida que se modifiquen funciones de IAM específicas.

```
{
```



```

"Action": [
  "iam:AttachRolePolicy",
  "iam>DeleteRole",
  "iam>DeleteRolePermissionsBoundary",
  "iam>DeleteRolePolicy",
  "iam:DetachRolePolicy",
  "iam:PutRolePermissionsBoundary",
  "iam:PutRolePolicy",
  "iam:TagRole",
  "iam:UntagRole",
  "iam:UpdateAssumeRolePolicy",
  "iam:UpdateRole",
  "iam:UpdateRoleDescription"
],
"Resource": [
  "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
],
"Effect": "Deny"
}

```

SCP-AMS-034: Impide la modificación de funciones específicas de IAM AssumeRolePolicy

Impida que se modifiquen las cuatro AssumeRolePolicy funciones de IAM especificadas.

```

{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}

```

ConfigRule: Etiquetas obligatorias

Comprueba si EC2 las instancias tienen las etiquetas personalizadas que has necesitado. Además InfoSec, esto también es útil para la gestión de costes

```

ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the required tags.

```

```
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
  SourceIdentifier: REQUIRED_TAGS
```

ConfigRule: La clave de acceso está girada

Compruebe que las claves de acceso se estén rotando dentro del período de tiempo especificado. Por lo general, se establece en 90 días según los requisitos de conformidad típicos.

```
ConfigRuleName: access-keys-rotated
Description: >-
  A config rule that checks whether the active access keys are rotated
  within the number of days specified in maxAccessKeyAge. The rule is
  NON_COMPLIANT if the access keys have not been rotated for more than
  maxAccessKeyAge number of days.
InputParameters:
  maxAccessKeyAge: '90'
Source:
  Owner: AWS
  SourceIdentifier: ACCESS_KEYS_ROTATED
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: clave de acceso raíz de IAM en AMS

Compruebe que la clave de acceso raíz no esté presente en la cuenta. En el caso de las cuentas AMS Advanced, se espera que sea compatible out-of-the-box.

```
ConfigRuleName: iam-root-access-key-check
Description: >-
  A config rule that checks whether the root user access key is available. The
  rule is COMPLIANT if the user access key does not exist.
Source:
  Owner: AWS
  SourceIdentifier: IAM_ROOT_ACCESS_KEY_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: gestionado por SSM EC2

Compruebe que EC2s está siendo gestionado por SSM Systems Manager.

```
ConfigRuleName: ec2-instance-managed-by-systems-manager
Description: >-
  A Config rule that checks whether the EC2 instances in the
  account are managed by AWS Systems Manager.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
    - 'AWS::SSM::ManagedInstanceInventory'
Source:
  Owner: AWS
  SourceIdentifier: EC2_INSTANCE_MANAGED_BY_SSM
```

ConfigRule: Usuario de IAM no utilizado en AMS

Compruebe si hay credenciales de usuario de IAM que no se hayan utilizado durante un período específico. Al igual que la comprobación de rotación de claves, esta suele tener un valor predeterminado de 90 días según los requisitos de conformidad típicos.

```
ConfigRuleName: iam-user-unused-credentials-check
Description: >-
  A config rule that checks whether IAM users have passwords
  or active access keys that have not been used within the
  specified number of days provided.
InputParameters:
  maxCredentialUsageAge: '90'
Source:
  Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: registro de cubos en S3

Comprueba que el registro esté habilitado para los depósitos de S3 de la cuenta.

```
ConfigRuleName: s3-bucket-logging-enabled
Description: >-
  A Config rule that checks whether logging is enabled for S3 buckets.
Scope:
```

```
ComplianceResourceTypes:
  - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_LOGGING_ENABLED
```

ConfigRule: Control de versiones de cubos de S3

Compruebe que el control de versiones y la eliminación de MFA (opcional) estén habilitados en todos los buckets de S3

```
ConfigRuleName: s3-bucket-versioning-enabled
Description: >-
  A Config rule that checks whether versioning is enabled for S3
  buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
  Source:
    Owner: AWS
SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED
```

ConfigRule: Acceso público a S3

Comprueba que la configuración de acceso público (ACL pública, política pública, buckets públicos) esté restringida en toda la cuenta

```
ConfigRuleName: s3-account-level-public-access-blocks
Description: >-
  A Config rule that checks whether the required public access block
  settings are configured from account level. The rule is only
  NON_COMPLIANT when the fields set below do not match the corresponding
  fields in the configuration item.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::AccountPublicAccessBlock'
InputParameters:
  IgnorePublicAcls: 'True'
  BlockPublicPolicy: 'True'
  BlockPublicAcls: 'True'
  RestrictPublicBuckets: 'True'
Source:
```

Owner: AWS

SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

ConfigRule: Hallazgos no archivados GuardDuty

Compruebe si hay GuardDuty hallazgos no archivados que tengan una duración superior a la especificada. La duración predeterminada es de 30 días para los resultados de baja resolución, 7 días para los de media y de 1 día para los de alta.

ConfigRuleName: guardduty-non-archived-findings

Description: >-

A Config rule that checks whether the Amazon GuardDuty has findings that are non archived. The rule is NON_COMPLIANT if GuardDuty has non archived low/medium/high severity findings older than the specified number.

InputParameters:

daysLowSev: '30'

daysMediumSev: '7'

daysHighSev: '1'

Source:

Owner: AWS

SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS

MaximumExecutionFrequency: TwentyFour_Hours

ConfigRule: Eliminación de CMK

Compruebe si hay claves maestras AWS Key Management Service personalizadas (CMKs) cuya eliminación esté programada (también conocida como pendiente). Esto es crucial, ya que el hecho de no darse cuenta de la eliminación de la CMK puede provocar que los datos sean irrecuperables

ConfigRuleName: kms-cmk-not-scheduled-for-deletion

Description: >-

A config rule that checks whether customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is NON_COMPLIANT if CMKs are scheduled for deletion.

Source:

Owner: AWS

SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION

MaximumExecutionFrequency: TwentyFour_Hours

ConfigRule: Rotación CMK

Comprueba que la rotación automática esté habilitada para cada CMK de la cuenta

```
ConfigRuleName: cmk-backing-key-rotation-enabled
Description: >-
  A config rule that checks that key rotation is enabled for each customer
  master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
  for specific key object. The rule is not applicable to CMKs that have
  imported key material.
Source:
  Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
MaximumExecutionFrequency: TwentyFour_Hours
```

Notificación personalizada para las reglas de Config

Es posible que se produzcan casos de reglas de Config críticas que no cumplan con las normas y que requieran una mayor sensibilización directamente con sus equipos InfoSec y con los de liderazgo. En estos casos, AMS recomienda configurar una notificación personalizada basada en eventos de incumplimiento.

Por ejemplo:

```
ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the mandated tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
SourceIdentifier: REQUIRED_TAGS
NotificationEventRule:
  Type: 'AWS::Events::Rule'
Properties:
  Name: CWEventForrequired-tags
  Description: >-
    SNS Notification for Non-Compliant Events of Config Rule:
    required-tags
  State: ENABLED
  EventPattern:
    detail-type:
      - Config Rules Compliance Change
```

```

    source:
      - aws.config
    detail:
      newEvaluationResult:
        complianceType:
          - NON_COMPLIANT
      configRuleARN:
        - 'Fn::GetAtt':
            - RequiredEC2Tags
            - Arn
    Targets:
      - Id: RemediationNotification
      Arn:
        Ref: SnsTopic
      InputTransformer:
        InputTemplate: >-
          "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
COST_CENTER, APP_ID, Name, and Backup."
        InputPathsMap:
          instance_id: $.detail.resourceId
    SnsTopic:
      Type: 'AWS::SNS::Topic'
      Properties:
        Subscription:
          - Endpoint: Cloud_Ops_Leaders@customer.com
            Protocol: email
          TopicName: noncompliant-instance-notification
    SnsTopicPolicy:
      Type: 'AWS::SNS::TopicPolicy'
      Properties:
        PolicyDocument:
          Statement:
            - Sid: __default_statement_ID
              Effect: Allow
              Principal:
                AWS: '*'
              Action:
                - 'SNS:GetTopicAttributes'
                - 'SNS:SetTopicAttributes'
                - 'SNS:AddPermission'
                - 'SNS:RemovePermission'
                - 'SNS>DeleteTopic'
                - 'SNS:Subscribe'
                - 'SNS:ListSubscriptionsByTopic'

```

```
- 'SNS:Publish'
- 'SNS:Receive'
Resource:
  Ref: SnsTopic
Condition:
  StringEquals:
    'AWS:SourceOwner':
      Ref: 'AWS::AccountId'
- Sid: TrustCWEToPublishEventsToMyTopic
  Effect: Allow
  Principal:
    Service: events.amazonaws.com
  Action: 'sns:Publish'
  Resource:
    Ref: SnsTopic
Topics:
  - Ref: SnsTopic
```

Función vinculada al servicio de EventBridge reglas de Amazon para AMS Advanced

AMS Advanced usa el rol vinculado a servicios (SLR) denominado `AWSServiceRoleForManagedServices_Events`: este rol confía en que uno de los directores del servicio de AWS Managed Services (`events.managedservices.amazonaws.com`) asuma el rol por usted. El servicio usa el rol para crear una regla administrada. EventBridge Esta regla es la infraestructura necesaria en su AWS cuenta para enviar información sobre el cambio de estado de alarma de su cuenta a AWS Managed Services.

Permisos de EventBridge SLR para AMS Advanced

El rol vinculado al servicio `AWSServiceRoleForManagedServices_Events` depende de los siguientes servicios para asumir el rol:

- `events.managedservices.amazonaws.com`

Esta función incluye la política `AWSManagedServices_EventsServiceRolePolicy` AWS administrada (consulte la [política administrada de AWS: AWSManagedServices_EventsServiceRolePolicy](#)).

El servicio utiliza la función para enviar información sobre el cambio de estado de alarma de su cuenta a AWS Managed Services. Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de AWS Identity and Access Management.

[Puede descargar el JSON `AWSServiceRoleForManagedServices\_EventsServiceRolePolicy` en este ZIP: `EventsServiceRolePolicy.zip`.](#)

Creación de una cámara EventBridge réflex para AMS Advanced

No necesita crear manualmente un rol vinculado a servicios. Cuando se incorpora a AMS en la consola AWS de administración AWS CLI, la o la AWS API, AMS Advanced crea automáticamente la función vinculada al servicio.

Important

Este rol vinculado al servicio puede aparecer en su cuenta si utilizaba el servicio AMS Advanced antes del 7 de febrero de 2023, cuando comenzó a admitir funciones vinculadas al servicio y, posteriormente, AMS Accelerate creó el rol en su cuenta. `AWSServiceRoleForManagedServices_Events` Para obtener más información, consulte [Un nuevo rol ha aparecido en mi cuenta de IAM](#).

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando te incorporas a AMS, AMS Advanced vuelve a crear el rol vinculado al servicio para ti.

Edición de una cámara EventBridge réflex para AMS Advanced

AMS Advanced no permite editar el rol vinculado al `AWSServiceRoleForManagedServices_Events` servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminar una EventBridge SLR para AMS Advanced

No es necesario eliminar manualmente el rol de `AWSServiceRoleForManagedServices_Events`. Cuando te desconectas de AMS en la consola AWS de administración, la AWS API AWS CLI o la consola, AMS Advanced limpia los recursos y elimina automáticamente la función vinculada al servicio.

También puede utilizar la consola de IAM AWS CLI o la AWS API para eliminar manualmente el rol vinculado al servicio. Para ello, primero debe limpiar manualmente los recursos del rol vinculado al servicio para poder eliminarlo después manualmente.

 Note

Si el servicio AMS Advanced utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de AMS Advanced utilizados por el rol `AWSServiceRoleForManagedServices_Events` vinculado al servicio

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al `AWSServiceRoleForManagedServices_Events` servicio.

Para obtener más información, consulte [Eliminación de un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

Prácticas recomendadas de seguridad

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.

Configuración no predeterminada del EPS de la zona de landing zone multicuenta de 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.

Barandillas AMS

Una barandilla es una regla de alto nivel que proporciona un control continuo del entorno AMS en general.

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.

Políticas de control del servicio MALZ

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.

Respuesta a incidentes de seguridad en AMS

La seguridad es la principal prioridad de AWS Managed Services (AMS). AMS despliega recursos y controles en sus cuentas para administrarlas. AWS tiene un modelo de responsabilidad compartida: AWS gestiona la seguridad de la nube y usted es responsable de la seguridad en la nube. AMS protege sus datos y activos y ayuda a mantener su AWS infraestructura segura mediante el uso de controles de seguridad y una supervisión activa para detectar problemas de seguridad. Estas capacidades le ayudan a establecer una base de seguridad para las aplicaciones que se ejecutan en la AWS nube. AMS colabora con usted a través de la respuesta a incidentes de seguridad para evaluar el efecto y, luego, llevar a cabo la contención y las remediaciones en función de las recomendaciones de mejores prácticas.

Cuando se produce una desviación de la línea base, por ejemplo, debido a un error de configuración o a un cambio en factores externos, es necesario responder e investigar. Para hacerlo correctamente, debe comprender los conceptos básicos de la respuesta a incidentes de seguridad en su entorno AMS. También debe comprender los requisitos para preparar, formar y capacitar a los equipos de nube antes de que se produzcan problemas de seguridad. Es importante conocer los controles y las capacidades que puede utilizar, preparar planes de respuesta para los problemas de seguridad más comunes, como una cuenta de usuario comprometida o el uso indebido de cuentas privilegiadas, e identificar métodos de corrección que utilicen la automatización para mejorar la velocidad y la coherencia de la respuesta. Además, debe comprender sus requisitos normativos y de cumplimiento en lo que respecta a la creación de un programa de respuesta a incidentes de seguridad que cumpla con esos requisitos.

La respuesta a los incidentes de seguridad puede ser compleja, pero si se implementa un enfoque iterativo, se puede simplificar el proceso y permitir que el equipo de respuesta a incidentes mantenga satisfechos a las partes interesadas de los activos al proporcionar una detección y respuesta tempranas y continuas. En esta guía, le proporcionamos la metodología que utiliza AMS para la

respuesta a incidentes, la matriz de responsabilidad de AMS (RACI), cómo puede prepararse para un incidente de seguridad, cómo interactuar con AMS durante los incidentes de seguridad y algunos de los manuales de respuesta a incidentes que utiliza AMS.

Cómo funciona la respuesta a incidentes de seguridad de AMS

AWS Managed Services se ajusta a la [Guía de gestión de incidentes de seguridad informática NIST 800-61 para la respuesta a incidentes](#) de seguridad. Al cumplir con este estándar del sector, ofrecemos un enfoque coherente para la gestión de eventos de seguridad y seguimos las mejores prácticas para proteger y responder a los incidentes de seguridad en la nube.

Ciclo vital de respuesta a incidentes

Cuando la detección identifica y genera una alerta de seguridad, o si solicita asistencia de seguridad, el equipo de operaciones de AWS Managed Services se asegura de que se lleva a cabo una investigación a tiempo, ejecuta automatizaciones para realizar la recopilación, clasificación y análisis de datos, le informa del análisis, lleva a cabo la investigación y cualquier actividad de contención y, a continuación, publica el análisis de los eventos.

Las actividades de recopilación, clasificación, análisis y contención de datos que se llevan a cabo durante la respuesta al incidente varían en función del tipo de incidente de seguridad que se investigue. Al final de este documento, encontrará ejemplos de flujos de trabajo de respuesta a incidentes de seguridad para escenarios seleccionados.

Durante los incidentes, AMS determina el curso de acción correcto de forma dinámica, lo que puede provocar que los pasos documentados se reordenen o se omitan según corresponda para garantizar que se obtenga el resultado correcto.

Preparación

A medida que el panorama de amenazas evoluciona, AMS sigue ampliando sus capacidades de detección y respuesta. A medida que se añaden nuevas detecciones, AMS incorpora las alertas de estas nuevas detecciones a la plataforma de detección y respuesta. Los equipos de seguridad de AMS están capacitados para investigar y colaborar con usted durante todo el ciclo de vida de la respuesta a los incidentes de seguridad.

Debido a este enfoque de asociación, es importante que sus equipos de seguridad y aplicaciones estén preparados para colaborar con AMS para gestionar los eventos de seguridad a medida que se

produzcan. Esta documentación explica qué esperar durante un incidente de seguridad y le ayuda a prepararse para una respuesta rápida en caso de que se produzca un incidente de seguridad.

Esta documentación utiliza la definición 800-61 del NIST de un evento como cualquier suceso observable en un sistema o una red y un incidente como una infracción o amenaza inminente de violación de las políticas, las políticas de uso aceptable o las prácticas de seguridad estándar.

Lista de verificación de preparación

Realice la siguiente lista de verificación con su administrador de entrega de soluciones en la nube (CSDM) de AMS y su arquitecto de nube (CA) de AMS:

- Comprenda qué cargas de trabajo se ejecutan en qué cuentas.
- Comprenda qué equipos internos son responsables de las distintas cargas de trabajo y etiquételos adecuadamente en las cargas de trabajo.
- Conserve internamente los datos de contacto de otros equipos que puedan ser necesarios durante la investigación de un incidente de seguridad y para tomar decisiones de contención.
- Confirma que los contactos de seguridad estén actualizados y se hayan agregado a todas las AWS cuentas gestionadas. Los contactos se administran por cuenta.
- Sepa cómo denunciar un incidente de seguridad a AMS y familiarícese con la gravedad y los tiempos de respuesta esperados.
- Asegúrese de que, cuando reciba las notificaciones de seguridad, se envíen a las personas y los sistemas adecuados, como los buscapersonas o el centro de operaciones de seguridad.
- Sepa qué fuentes de registro tiene a su disposición, dónde se almacenan en sus cuentas y quién tiene acceso a ellas.
- Aprenda a utilizar CloudWatch Insights para consultar los registros durante las investigaciones.
- Comprenda las opciones de contención disponibles por recurso (IAM, S3EC2, etc.) y las consecuencias en la disponibilidad de la carga de trabajo cuando se encuentra en situación de contención.

Detect

Durante la administración de sus AWS cuentas, AMS supervisa las anomalías en el comportamiento de los usuarios, las actividades de las cuentas y los posibles eventos de seguridad mediante los datos recopilados de las fuentes y los controles de detección, incluidos, entre otros, Amazon,

GuardDuty VPC Flow Logs, CloudWatch Amazon Macie y los feeds internos de Threat Intelligence de AWS Config Amazon.

AMS utiliza AWS servicios nativos y otras tecnologías de detección para responder a los eventos de seguridad creados por:

- Config: tipos de búsqueda de conformidad
- GuardDuty Búsqueda de tipos
- Tipos de búsqueda de Macie
- Eventos del firewall DNS de Amazon Route 53 Resolver
- Eventos de seguridad de AMS (alarmas de vigilancia en la nube)

Se añaden nuevos hallazgos a medida que evolucionan los servicios, los productos y los ecosistemas de amenazas.

Informe sobre los eventos de seguridad a AMS

Presente un incidente a través del portal o Soporte centro de soporte de AMS para notificar a AMS de un incidente de seguridad o solicitar una investigación.

Análisis

Tras identificar e informar de un suceso de seguridad, el siguiente paso consiste en analizar si se trata de un falso positivo o de un incidente real. AMS utiliza técnicas automatizadas y de investigación manual para gestionar los eventos de seguridad. El análisis incluye la investigación de los registros de diferentes fuentes de detección, como los registros de tráfico de red, los registros del host, CloudTrail los eventos, los registros de AWS servicio, etc. El análisis también busca patrones que muestren un comportamiento anómalo por correlación.

Su colaboración es necesaria para comprender el contexto específico del entorno de la cuenta y establecer lo que es normal para su cuenta y sus cargas de trabajo. Esto ayuda a AMS a identificar una anomalía más rápido y a acelerar la respuesta a los incidentes.

Gestione las comunicaciones de AMS sobre eventos de seguridad

AMS lo mantiene informado durante la investigación al contactar con sus contactos de seguridad mediante una denuncia de incidente. El administrador de prestación de servicios en la nube de AMS

(CSDM) y el arquitecto de la nube (CA) de AMS son los puntos de contacto a los que acudir para cualquier tipo de comunicación durante una investigación de seguridad activa.

La comunicación incluye la notificación automática cuando se genera una alerta de seguridad, la comunicación después del análisis del evento, el establecimiento de puentes de llamadas y la entrega continua de artefactos como archivos de registro, una instantánea de los recursos infectados y la obtención de los resultados de las investigaciones durante el evento de seguridad.

Los campos estándar incluidos en las notificaciones de alerta de seguridad de AMS se enumeran a continuación. Estos campos le proporcionan información para que pueda remitir los eventos a los equipos correspondientes de su organización para que los corrijan.

- Tipo de búsqueda
- Identificador de búsqueda (cuando proceda)
- Detectar la gravedad
- Descripción del hallazgo
- Buscando la fecha y hora de creación
- AWS ID de cuenta
- Región (si procede)
- AWS Recursos (IAMuser/role/policy, S3 EC2, EKS)

Se proporcionan campos adicionales según el tipo de hallazgo; por ejemplo, los hallazgos de EKS incluyen detalles del pod, el contenedor y el clúster.

Contención

El enfoque de AMS en materia de contención consiste en asociarse con usted. Usted comprende el impacto en su empresa y en la carga de trabajo que pueden derivarse de las actividades de contención, como el aislamiento de la red, el desaprovechamiento de usuarios o roles de IAM, la reconstrucción de instancias, etc.

Una parte esencial de la contención es la toma de decisiones. Por ejemplo, apague un sistema, aisle un recurso de la red o desactive el acceso o finalice las sesiones. Estas decisiones son más fáciles de tomar si existen estrategias y procedimientos predeterminados para contener el incidente. AMS proporciona la estrategia de contención y, a continuación, implementa la solución después de haber considerado el riesgo que implica la implementación de las acciones de contención.

Existen diferentes opciones de contención en función de los recursos que se analicen. AMS espera que se desplieguen varios tipos de contención simultáneamente durante la investigación de un incidente. Algunos de estos ejemplos incluyen:

- Aplique reglas de protección para bloquear el tráfico no autorizado (grupo de seguridad, NACL, reglas WAF, reglas SCP, denegar la inclusión en la lista, establecer una acción de firma en cuarentena o bloqueo)
- Aislamiento de recursos
- Aislamiento de red
- Inhabilitar los usuarios, las funciones y las políticas de IAM
- Modificar o reducir el privilegio de usuario y rol de IAM
- Terminación, suspensión o eliminación de recursos informáticos
- Restringir el acceso público desde el recurso afectado
- Claves de acceso, claves de API y contraseñas rotativas
- Eliminar las credenciales divulgadas y la información confidencial

AMS lo alienta a considerar el tipo de estrategias de contención para cada tipo de incidente grave que esté dentro de sus posibilidades de riesgo, con criterios claramente documentados que ayuden a la toma de decisiones en caso de que se produzca un incidente. Los criterios para determinar la estrategia adecuada incluyen:

- Posibles daños a los recursos
- Preservación de las pruebas
- Falta de disponibilidad del servicio (por ejemplo, conectividad de red, servicios prestados a terceros)
- Tiempo y recursos necesarios para implementar la estrategia
- Efectividad de la estrategia (por ejemplo, contención parcial, contención total)
- Permanencia de la solución (por ejemplo, decisiones entre puertas unidireccionales y puertas bidireccionales)
- Duración de la solución (por ejemplo, una solución alternativa de emergencia que se eliminará en cuatro horas, una solución temporal que se eliminará en dos semanas o una solución permanente).
- Aplique controles de seguridad que pueda activar para reducir el riesgo y disponer de tiempo para definir e implementar una contención más eficaz.

La velocidad de la contención es fundamental, por lo que AMS recomienda adoptar un enfoque gradual para lograr una contención eficiente y eficaz mediante la elaboración de estrategias a corto y largo plazo.

Utilice esta guía para considerar su estrategia de contención, que incluye diferentes técnicas según el tipo de recurso.

- Estrategia de contención
 - ¿Puede AMS identificar el alcance del incidente de seguridad?
 - En caso afirmativo, identifique todos los recursos (usuarios, sistemas, recursos).
 - En caso contrario, investigue en paralelo mientras ejecuta el siguiente paso en los recursos identificados.
 - ¿Se puede aislar el recurso?
 - En caso afirmativo, proceda a aislar los recursos afectados.
 - En caso contrario, colabore con los propietarios y administradores del sistema para determinar las medidas adicionales necesarias para contener el problema.
 - ¿Están todos los recursos afectados aislados de los no afectados?
 - En caso afirmativo, continúe con el siguiente paso.
 - Si no, continúe aislando los recursos afectados hasta que se logre contenerlos a corto plazo para evitar que el incidente se agrave aún más.
- Backup del sistema
 - ¿Se crearon copias de seguridad de los sistemas afectados para su posterior análisis?
 - ¿Están las copias forenses cifradas y almacenadas en una ubicación segura?
 - En caso afirmativo, continúe con el siguiente paso.
 - En caso contrario, cifre las imágenes forenses y almacénelas en una ubicación segura para evitar el uso accidental, los daños y las manipulaciones.

Erradicación

Una vez contenido un incidente, puede ser necesario erradicarlo para eliminar por completo las fuentes de amenaza y proteger el sistema antes de pasar a la siguiente fase de recuperación. Las medidas de erradicación podrían incluir eliminar el malware y eliminar las cuentas de usuario comprometidas, así como identificar y mitigar todas las vulnerabilidades que se explotaron. Durante

la erradicación, es importante identificar todas las cuentas, los recursos y las instancias afectadas del entorno para poder solucionarlas.

Se recomienda que la erradicación y la recuperación se realicen de forma gradual, de modo que se prioricen las medidas de remediación. En el caso de los incidentes a gran escala, la recuperación puede llevar meses. La intención de las primeras fases debe ser aumentar la seguridad general con cambios de gran valor relativamente rápidos (días o semanas) para evitar futuros incidentes. Las fases posteriores deben centrarse en los cambios a largo plazo (por ejemplo, cambios en la infraestructura) y en el trabajo continuo para mantener la empresa lo más segura posible.

En el caso de algunos incidentes, la erradicación no es necesaria o se lleva a cabo durante la recuperación.

Considere lo siguiente:

- ¿Se puede cambiar la imagen del sistema y luego reforzarlo con parches u otras contramedidas para prevenir o reducir el riesgo de ataques?
- ¿Se ha eliminado todo el malware y otros artefactos que han dejado los atacantes y se han reforzado los sistemas afectados para evitar nuevos ataques?

Recuperar

AMS colabora con usted para restablecer el funcionamiento normal de los sistemas, confirmar que funcionan con normalidad y (según proceda) corregir las vulnerabilidades para evitar incidentes similares.

Considere lo siguiente:

- ¿Están los sistemas afectados parcheados y reforzados contra el ataque reciente y los posibles ataques futuros?
- ¿Qué día y hora es posible restablecer la producción de los sistemas afectados?
- ¿Qué herramientas utilizará para probar, supervisar y comprobar que los sistemas que restaure para ponerlos en producción no son vulnerables a las técnicas de ataque iniciales?

Informe posterior al incidente

Tras el suceso, AMS lleva a cabo un proceso de revisión de la investigación de todos los incidentes de seguridad. Además, AMS inicia un proceso de corrección de errores (COE) para abordar

los incidentes de seguridad causados por un error del sistema o de un procedimiento que, de forma plausible, tiene margen de mejora. AMS colabora con usted para mejorar continuamente la experiencia de investigación de seguridad. El proceso COE ayuda a AMS a identificar los factores que contribuyen a que los eventos afecten a los clientes y relaciona esas causas con las siguientes acciones, elementos que pueden evitar que se repitan eventos similares o ayuda a mitigar la duración o el nivel de impacto.

El proceso de revisión de la investigación de los incidentes de seguridad aborda los siguientes elementos para identificar las oportunidades de mejora:

- ¿Cuánto tiempo transcurrió desde el inicio del incidente hasta su descubrimiento, la evaluación inicial del impacto y cada etapa del proceso de gestión del incidente (por ejemplo, contención o recuperación)?
- ¿Cuánto tiempo tardó el equipo de respuesta a incidentes en responder al informe inicial del incidente?
- ¿Cuánto tiempo se tardó en realizar un análisis de impacto inicial?
- ¿Se pudo prevenir esto y cómo? ¿Existe alguna herramienta o proceso que pudiera haberlo evitado?
- ¿Podríamos haberlo detectado antes y cómo?
- ¿Qué pudo haber hecho que la investigación fuera más rápida?
- ¿Se siguieron los procedimientos de respuesta a incidentes documentados? ¿Fueron adecuados?
- ¿El intercambio de información con otras partes interesadas se realizó de manera oportuna? ¿Cómo podría mejorarse?
- ¿Fue eficaz la colaboración con otros equipos (de AWS seguridad, de cuentas, de AWS desarrollo y de seguridad del cliente)? Si no, ¿qué podría mejorarse?
- ¿Qué pasos de preparación faltaban que pudieran haber ayudado: matrices de escalamiento, RACI, modelos de responsabilidad compartida, etc.? ¿Es necesario actualizar algún Runbook?
- ¿Cuál fue la diferencia entre la evaluación de impacto inicial y la evaluación de impacto final? ¿Qué podemos hacer para mejorar la precisión de las evaluaciones en una fase temprana de la respuesta al incidente?
- ¿Cuáles son los elementos de acción que se derivan de las lecciones aprendidas?

Guías de respuesta a incidentes de seguridad en AMS

Esta sección contiene dos manuales:

- [Respuesta a la actividad del usuario root](#)
- [Respuesta a eventos de malware](#)

Respuesta a la actividad del usuario root

El [usuario raíz](#) es el superusuario de su AWS cuenta. Tenga en cuenta que AMS monitorea el uso de root. Se recomienda utilizar el usuario root solo para las pocas tareas que lo requieran, como cambiar la configuración de la cuenta, activar el acceso AWS Identity and Access Management (IAM) a la facturación y la gestión de costes, cambiar la contraseña root y activar la autenticación multifactor (MFA). Para obtener más información, consulte [Tareas que requieren credenciales de usuario raíz](#).

Para obtener más información sobre cómo informar a AMS del uso raíz planificado, consulte [Cuándo y cómo usar la cuenta raíz en AMS](#).

Cuando se detecta actividad por parte del usuario root (intentos fallidos de iniciar sesión que podrían indicar un ataque de fuerza bruta o actividad en la cuenta tras iniciar sesión correctamente), se genera un evento y se envía un incidente a tus contactos de seguridad definidos.

AWS Managed Services Operations investiga la actividad no planificada de los usuarios raíz, lleva a cabo la recopilación, clasificación y análisis de datos y realiza actividades de contención según sus instrucciones, seguidas de un análisis posterior al evento.

Si tiene el modelo operativo AMS Advanced, recibirá comunicaciones adicionales de los ingenieros de AMS CSDM y AMS Ops en las que se confirmará la actividad no planificada de los usuarios raíz debido a la responsabilidad de AMS de proteger las credenciales de los usuarios raíz. AMS investiga la actividad de los usuarios root hasta que se confirme el camino a seguir.

Preparación

Informe a AMS de cualquier uso planificado del usuario root enviando una solicitud de servicio de AMS con los datos y las horas del evento planificado para evitar actividades innecesarias de respuesta a incidentes.

Póngase en contacto periódicamente GameDays con AMS para validar que los procesos de respuesta a incidentes de los clientes de AMS, las personas y los sistemas estén actualizados, y desarrolle la memoria muscular con las personas responsables para lograr una respuesta más rápida a los incidentes.

Fase A: Detectar

AMS supervisa la actividad raíz de las cuentas a través de fuentes de detección, incluida GuardDuty la supervisión de AMS.

Si tiene AMS Accelerate, el modelo operativo responde al incidente y solicita que se investigue la actividad inesperada del usuario root. Cuando esto ocurre, AMS Operations inicia el manual de cuentas comprometidas.

Si dispone de AMS Advanced, el modelo operativo responde al incidente o informa al CSDM de cualquier actividad planificada por parte de un usuario root para poner fin a una investigación en curso sobre una situación comprometida en la cuenta.

Fase B: analizar

AMS lleva a cabo una investigación exhaustiva de los eventos del usuario raíz cuando determina que la actividad no está autorizada. Utilizando tanto las automatizaciones como el equipo de respuesta de seguridad de AMS, los registros y los eventos se analizan para detectar anomalías y comportamientos inesperados en los usuarios root. Se proporcionan registros para ayudar a determinar si la actividad es desconocida, si se trata de un evento de un usuario raíz autorizado o si requiere una investigación más profunda.

Algunos ejemplos de la información proporcionada durante la investigación para respaldar las comprobaciones internas son:

- Información de la cuenta: ¿En qué cuenta se utilizó la cuenta raíz?
- Dirección de correo electrónico del usuario raíz: cada usuario raíz está asociado a una dirección de correo electrónico de su organización
- Detalles de autenticación: ¿desde dónde y cuándo accedió el usuario raíz a su entorno?
- Registros de actividad: ¿Qué hizo el usuario cuando inició sesión como root? Estos registros se presentan en forma de CloudWatch eventos. Comprender cómo leer estos registros ayuda en la investigación.

Se recomienda estar preparado para recibir la información de análisis y tener un plan sobre cómo llegar a los puntos de contacto autorizados para las cuentas de su organización. Como los usuarios raíz no se nombran como individuos, determinar quién tiene acceso a la dirección de correo electrónico raíz utilizada para la cuenta en su organización ayuda a dirigir rápidamente las preguntas internamente.

Fase C: Contener y erradicar

AMS colabora con sus equipos de seguridad para llevar a cabo la contención siguiendo las instrucciones de sus contactos autorizados de Customer Security. Las opciones de contención incluyen:

- Rotación de las credenciales y claves apropiadas.
- Finalizar las sesiones activas de las cuentas y los recursos.
- Erradicar los recursos creados.

Durante las actividades de contención, AMS trabaja en estrecha colaboración con su equipo de seguridad para garantizar que se minimice cualquier interrupción en sus cargas de trabajo y que las credenciales raíz estén debidamente protegidas.

Una vez completado el plan de contención, trabajará con el equipo de operaciones de AMS para tomar las medidas de recuperación necesarias.

Informe posterior al incidente

Según sea necesario, AMS inicia el proceso de revisión de la investigación para identificar las lecciones aprendidas. Como parte de completar un COE, AMS comunica cualquier hallazgo relevante a los clientes afectados para ayudarlos a mejorar su proceso de respuesta a los incidentes.

AMS documenta todos los detalles finales de la investigación, recopila las métricas adecuadas y, a continuación, informa del incidente a los equipos internos de AMS que necesiten información, incluidos el CSDM y la CA asignados.

Respuesta a eventos de malware

Las EC2 instancias de Amazon se utilizan para alojar diversas cargas de trabajo, incluido software de terceros y software desarrollado a medida que implementan los equipos de aplicaciones de las organizaciones. AMS le ofrece y le anima a implementar sus cargas de trabajo en imágenes parcheadas y mantenidas de forma continua por AMS.

Durante el funcionamiento de las instancias, AMS monitorea las anomalías en el comportamiento o la actividad a través de una variedad de controles de detección de seguridad, incluidos Amazon, Endpoint Protection GuardDuty, Network Traffic y los feeds internos de Inteligencia de Amenazas de Amazon.

Los clientes de AMS que utilizan el modelo operativo AMS Advanced instalan automáticamente el cliente de supervisión de Endpoint Security (EPS) en los recursos aprovisionados. Esto garantiza que los recursos se supervisen y admitan las 24 horas del día, los 7 días de la semana, lo que incluye la creación de un incidente de seguridad cuando se detecta un evento.

AMS también monitorea los hallazgos de GuardDuty malware. Están disponibles tanto en AMS Advanced como en AMS Accelerate, si están activados. Consulta [Protección contra malware en Amazon GuardDuty](#) para obtener más información.

 Note

Si has optado por [Bring Your Own EPS](#), el proceso de respuesta a los incidentes es diferente al que se describe en esta página. Para obtener más información, consulte la documentación a la que se hace referencia.

Cuando se detecta malware, se crea un incidente y se le notifica del mismo. Esta notificación va seguida de cualquier actividad de reparación que se haya producido. AMS Operations investiga, recopila, clasifica y analiza los datos y, a continuación, lleva a cabo actividades de contención según sus instrucciones, seguidas de un análisis posterior al suceso.

Fase A: Detectar

AMS monitorea los eventos en las instancias con GuardDuty una solución de seguridad de punto final. AMS determina las actividades de enriquecimiento y clasificación adecuadas para ayudarle a tomar decisiones de contención o aceptación de riesgos en función del tipo de hallazgo o alerta.

La recopilación de datos se realiza en función del tipo de hallazgo. La recopilación de datos implica consultar múltiples fuentes de datos, tanto internas como externas, a la cuenta afectada para obtener una idea de la actividad observada o de las configuraciones preocupantes.

AMS correlaciona el hallazgo con cualquier otra alarma y alerta o telemetría de cualquier cuenta afectada o plataforma de inteligencia de amenazas de AMS.

Fase B: analizar

Una vez recopilados los datos, se analizan para identificar cualquier actividad o indicador preocupante. Durante esta fase de la investigación, AMS colabora con usted para integrar el conocimiento empresarial y el dominio de las instancias y las cargas de trabajo a fin de comprender qué se espera y qué es lo que está fuera de lo común.

Algunos ejemplos de la información proporcionada durante la investigación para respaldar las comprobaciones internas son:

- Información de la cuenta: ¿En qué cuenta se observó la actividad del malware?
- Detalles de la instancia: ¿Qué instancias están implicadas en los eventos de malware?
- Fecha y hora del evento: ¿Cuándo se activó la alerta?
- Información sobre la carga de trabajo: ¿Qué se está ejecutando en la instancia?
- Detalles sobre el malware, si corresponde: familias de malware e información de código abierto sobre el malware.
- Detalles sobre los usuarios o las funciones: ¿Qué usuarios o funciones se ven afectados por la actividad o participan en ella?
- Registros de actividad: ¿Qué actividades se registran en la instancia? Se presentan en forma de CloudWatch eventos y eventos del sistema de la instancia. Saber cómo leer estos registros le ayudará en la investigación
- Actividad de red: ¿Qué puntos finales se conectan a la instancia, a qué se conecta la instancia y cuál es el análisis del tráfico?

Se recomienda estar preparado para recibir información sobre la investigación y tener un plan sobre cómo contactar con los puntos de contacto adecuados para las cuentas, las instancias y las cargas de trabajo de la organización. Comprender la topología de la red y la conexión prevista puede ayudar a acelerar el análisis de impacto. El conocimiento de las pruebas de penetración planificadas en el entorno y de las implementaciones recientes realizadas por los propietarios de las aplicaciones también puede acelerar la investigación.

Si determina que la actividad está planificada y autorizada, el incidente se actualiza y la investigación finaliza. Si se confirma el compromiso, usted y AMS determinarán el plan de contención adecuado.

Fase C: Contener y erradicar

AMS colabora con usted para determinar las actividades de contención adecuadas en función de los datos recopilados y la información conocida. Las opciones de contención incluyen, pero no se limitan a:

- Preservar los datos mediante instantáneas
- Modificar las reglas de red para limitar el tráfico entrante o saliente de las instancias
- Modificar las políticas de usuarios y roles de SCP e IAM para limitar el acceso

- Finalización, suspensión o desactivación de instancias
- Finalizar cualquier conexión persistente
- Rotación de las credenciales y claves apropiadas

Si opta por realizar una actividad de erradicación contra la instancia, AMS lo ayudará a lograrlo. Las opciones incluyen, pero no se limitan a:

- Eliminar cualquier software no deseado
- Reconstruir la instancia a partir de una imagen limpia y completamente parcheada y volver a implementar las aplicaciones y la configuración
- Restauración de la instancia a partir de una copia de seguridad anterior
- Implementar aplicaciones y servicios en otra instancia de su cuenta que pueda ser adecuada para alojar las cargas de trabajo.

Es importante determinar cómo se distribuyó y ejecutó el malware en la instancia antes de restablecer el servicio para asegurarse de que se aplican todos los controles adicionales que impidan que el malware vuelva a aparecer en la instancia. AMS proporciona información o información adicional a sus socios o equipos forenses, según sea necesario, para respaldar la labor forense.

En este punto, trabajará con AMS Operations para las actividades de recuperación. AMS trabaja en estrecha colaboración con usted para minimizar las interrupciones en las cargas de trabajo y proteger las instancias.

Informe posterior al incidente

Según sea necesario, AMS inicia el proceso de revisión de la investigación para identificar las lecciones aprendidas. Como parte de completar un COE, AMS le comunica los hallazgos relevantes para ayudarlo a mejorar su proceso de respuesta a incidentes.

AMS documenta los detalles finales de la investigación, recopila las métricas adecuadas e informa del incidente a los equipos internos de AMS que requieren información, incluidos el CSDM y el CA asignados.

Revisiones de seguridad de solicitudes de cambio en AMS

Advanced

El proceso de revisión de las solicitudes de cambio de AWS Managed Services garantiza que AMS lleve a cabo una revisión de seguridad de los cambios solicitados a medida que se implementan en su nombre en su cuenta.

[Estándares técnicos AMS Advanced](#) define los criterios de seguridad, las configuraciones y los procesos mínimos para establecer la seguridad básica de sus cuentas. Cuando AMS implementa los cambios solicitados, seguimos estos estándares.

AMS evalúa todas las solicitudes de cambio 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 un proceso de revisión de seguridad. Durante este proceso, AMS resalta el riesgo relevante y el responsable de la aprobación de riesgos autorizado lo revisa y aprueba para lograr un equilibrio entre las necesidades empresariales y de seguridad.

Proceso de gestión de riesgos de seguridad del cliente

El proceso de gestión avanzada de riesgos para la seguridad del cliente (CSRM) de AMS ayuda a identificar y comunicar claramente los riesgos a los propietarios adecuados. Este proceso minimiza los riesgos de seguridad en su entorno y reduce la sobrecarga operativa continua en caso de identificar los riesgos.

De forma predeterminada, cuando alguien de su organización solicita que AMS implemente un cambio en su entorno gestionado, AMS revisa el cambio para determinar si la solicitud no cumple los estándares técnicos, lo que podría alterar la postura de seguridad de su cuenta. Si existe un riesgo de seguridad alto o muy alto, el personal de seguridad autorizado acepta o rechaza la revisión del cambio. Los cambios solicitados también se evalúan para determinar si tienen efectos adversos en la capacidad de AMS para gestionar la cuenta. Si la revisión detecta posibles impactos adversos, AMS requerirá revisiones y aprobaciones adicionales.

Puede excluirse del flujo de trabajo basado en la aprobación en el proceso de CSRM en caso de riesgos altos o muy altos. Para cambiar la opción de CSRM para cuentas específicas, de la CSRM estándar a la de solo notificación, colabore con sus gerentes de prestación de servicios en la nube para crear una aceptación única del riesgo. Si opta por la opción de solo notificación, AMS implementará los cambios solicitados independientemente de la categoría de riesgo. Además, AMS envía una notificación de riesgo a los responsables de la aprobación de riesgos autorizados en lugar

de solicitar la aprobación antes de la implementación del cambio. Hable con sus arquitectos de nube o gerentes de prestación de servicios en la nube para obtener más información sobre el proceso de CSRM de AMS, cómo cambiar la opción de CSRM predeterminada al incorporar nuevas cuentas de AMS o cómo actualizar las cuentas existentes.

 Note

AMS recomienda encarecidamente que utilice la opción predeterminada de CSRM estándar en todas sus cuentas.

Estándares técnicos AMS Advanced

Las siguientes son las categorías de estándares técnicos de AMS Advanced:

ID	Categoría
AMS-STD-001	Configuración de etiquetado
AMS-STD-002	AWS Identity and Access Management
AMS-STD-003	Seguridad de la red
AMS-STD-004	Pruebas de penetración
AMS-STD-005	Amazon GuardDuty
AMS-STD-006	Seguridad del host
AMS-STD-007	Registro
AMS-STD-008	AMS-MAD
AMS-STD-009	Misceláneo

Controles estándar en AMS Advanced

Los siguientes son los controles estándar del AMS:

AMS-STD-001: Configuración de etiquetado

El siguiente es el control estándar para 001: Configuración de etiquetado.

1. Todos los AWS recursos requeridos por el equipo de AMS para fines operativos y de administración deben tener el siguiente par clave-valor.
 - AppId= AMSInfrastructure
 - Entorno = AMSInfrastructure
 - AppName = AMSInfrastructure
 - AMSResource=Verdadero
2. Todas las etiquetas requeridas por el equipo de AMS, distintas de las enumeradas anteriormente, deben tener prefijos tal como se menciona en la lista de prefijos de AMS (consulte la nota).
3. Los valores de etiqueta requeridos por el equipo de AMS (AppIdentorno y AppName) se pueden cambiar en cualquiera de los recursos que haya creado en función de sus solicitudes de cambio.
4. No debes eliminar ninguna etiqueta de las pilas que AMS requiera en función de tus solicitudes de cambio.
5. No puede utilizar la convención de nomenclatura de etiquetas AMS para su infraestructura, como se menciona en el punto 2.
6. Puede hacer que se creen etiquetas personalizadas en los recursos que necesite AMS (normalmente para casos de uso de facturación e informes de costes). Las etiquetas personalizadas se conservan si los recursos se actualizan mediante la actualización de la pila y no mediante la actualización de la plantilla.

Note

Lista de prefijos AMS

1. ams-*
2. AWSManagedServicios*
3. /ams/ *
4. Ams*
5. AMS*
6. Ams*
7. mc*

- 8. MC*
- 9. Mc*
- 10.centinella*
- 11.Centinela*
- 12.Servicios_gestionados*
- 13.Nuevo AMS*
- 14.AWS_*
- 15.aws*
- 16.VPC_*
- 17.CloudTrail*
- 18.Cloudtrail*
- 19/aws_reservado/
- 20.INGERIR*
- 21.EPSDB*
- 22.MMS*
- 23.TemplateId*
- 24.StackSet-ams*
- 25.StackSet-Zona de aterrizaje de AWS
- 26.IAMPolicy*
- 27.cliente-mc-*
- 28.Raíz*
- 29.LandingZone*
- 30.StateMachine*
- 31.codedeploy_service_role
- 32.host de administración
- 33.sentinel.int.
- 34.eps
- 35.UnhealthyInServiceBastion
- 36.ms-

AMS-STD-002 - (IAM) AWS Identity and Access Management

ID	Norma técnica
1.0	Duración del tiempo de espera
1.1	El tiempo de espera predeterminado de un usuario federado es de una hora y puede aumentarse hasta cuatro horas.
1.2	El tiempo de acceso predeterminado a la pila es de 12 horas.
2.0	AWS Uso de la cuenta raíz
2.1	Si se utiliza una cuenta raíz por cualquier motivo, Amazon GuardDuty debe estar configurado para generar los resultados pertinentes.
2.2	En el caso de las cuentas de una sola cuenta en la zona de aterrizaje (SALZ) y en las cuentas de administración de varias cuentas de la zona de aterrizaje (MALZ) (anteriormente denominada Master/Billing cuenta), la cuenta del usuario raíz debe tener habilitada la MFA virtual y el token virtual de MFA se descarta durante la incorporación de la cuenta, de modo que ni AMS ni los clientes puedan iniciar sesión como root. Debe seguir el proceso estándar de pérdida de la contraseña AWS raíz junto con su gestor de prestación de servicios en la nube (CSDM) de AMS. Esta configuración debe permanecer durante el ciclo de vida de las cuentas gestionadas por AMS.
2.3	No debe crear claves de acceso para la cuenta raíz.

ID	Norma técnica
3.0	Creación y modificación de usuarios
3.1	Se pueden crear IAM users/roles con acceso programático y permisos de solo lectura sin ninguna política de tiempo limitado. Sin embargo, no se permite el permiso para permitir la lectura de objetos (por ejemplo, S3:GetObject) en todos los depósitos de Amazon Simple Storage Service de la cuenta.
3.1.1	Se pueden crear usuarios humanos de IAM para el acceso a la consola y con permisos de solo lectura con la política de límite de tiempo (hasta 180 días), mientras que la política removal/renewal/extension de límite de tiempo limitado generará la notificación de riesgo. Sin embargo, no se permite el permiso para leer objetos (por ejemplo, S3:GetObject) en todos los depósitos de S3 de la cuenta.
3.2	No se deben crear usuarios y roles de IAM para el acceso programático y de consola con permisos que modifiquen la infraestructura (escritura y administración de permisos) en la cuenta del cliente sin una aceptación arriesgada. Existen excepciones para los permisos de escritura a nivel de objeto de S3, que se permiten sin riesgo de aceptación siempre que los segmentos específicos estén dentro del ámbito de aplicación y las operaciones de etiquetado en etiquetas no relacionadas con AMS.

ID	Norma técnica
3.3	Los usuarios de IAM con acceso programático, nombrados <code>customer_servicenow_user</code> y <code>customer_servicenow_logging_user</code> necesarios para la ServiceNow integración en la cuenta de aplicación SALZ o MALZ y las *cuentas principales* se pueden crear sin ninguna política de tiempo limitado.
3.4	Los usuarios de IAM con acceso programático, que utilizan <code>customer_cloud_endure_policy</code> y <code>customer_cloud_endure_deny_policy</code> (con acceso de solo lectura) que se requieren para la CloudEndure integración en SALZ pueden crearse cuentas de MALZ, pero necesitan una política de tiempo limitado durante el período de migración planificado. El límite de tiempo puede ser de un período máximo de 180 días sin ningún tipo de RA. El SCP también está autorizado a cambiar las cuentas de MALZ para permitir que estas políticas funcionen durante el período requerido. Usted define los períodos de migración adecuados a sus necesidades y los ajusta según sea necesario.
4.0	Políticas, acciones y APIs
4.1	Todos los usuarios y funciones de IAM en las cuentas de SALZ deben tener incorporada la Política de rechazo de clientes (CDP) predeterminada para proteger la infraestructura de AMS de daños accidentales o intencionados.

ID	Norma técnica
4.2	El AMS SCPs debe estar activado en todas las cuentas gestionadas por AMS en MALZ.
4.3	Las identidades capaces de realizar acciones administrativas en las claves de KMS, por ejemplo PutKeyPolicy ScheduleKeyDeletion , deben estar restringidas únicamente a los operadores de AMS y a los responsables de automatización.
4.4	Una política no debe proporcionar acceso al administrador con una declaración equivalente a «Efecto»: «Permitir» con «Acción»: «*» en lugar de «Recurso»: «*» sin riesgo de aceptación.
4.5	La política de IAM no debe incluir ninguna acción que incluya la acción Permitir S3: *** en cualquier segmento sin riesgo de aceptación.
4.6	No se deben permitir las llamadas a la API contra las políticas clave de KMS para las claves de infraestructura de AMS en las políticas de IAM del cliente.
4.7	No se deben permitir acciones que eludan el proceso de administración de cambios (RFC), como iniciar o detener la instancia, crear un bucket de S3 o una instancia de RDS, etc.
4.8	No se deben permitir acciones que realicen cambios en los registros DNS de la infraestructura de AMS en Amazon Route 53.

ID	Norma técnica
4.9	Los usuarios humanos de IAM con acceso a la consola creados después de seguir el debido proceso no deben tener ninguna política asociada directamente, excepto la política de confianza, el rol y la política de tiempo limitado.
4.10	Se pueden EC2 crear perfiles de instancias de Amazon con acceso de lectura a un secreto o espacio de nombres específico AWS Secrets Manager dentro de la misma cuenta.
4.11	Los permisos de AWS Managed Services Change Management (AMSCM) o AWS Managed Services Service Knowledge Management System (AMSSKMS) se pueden añadir a cualquier función (capacidad de apertura). SR/Incident/RFC
4.12	La política de IAM no debe incluir ninguna acción que incluya la acción Permitir registros (DeleteLogGroup y registros) DeleteLogStream en cualquier grupo de CloudWatch registros de AMS Amazon.
4.13	No se deben permitir los permisos para crear claves multirregionales.
4.14	Para proporcionar acceso a un bucket de S3 ARNs que aún no esté creado en sus cuentas, utilice la clave de condición de S3 específica del servicio <code>s3:ResourceAccount</code> para especificar el número de cuenta.

ID	Norma técnica
4.15	Puedes tener acceso a ver, crear, enumerar y eliminar tu panel personalizado, pero solo puedes ver y enumerar en los CloudWatch paneles de Amazon.
4.15.1	Puede ver, crear, enumerar y eliminar el acceso a su panel de control personalizado de S3 Storage Lens.
4.16	Se pueden conceder todos los permisos relacionados con SQL Workbench roles/users para trabajar en las bases de datos de Amazon Redshift.
4.17	Se puede conceder cualquier AWS CloudShell permiso a los roles de los clientes como alternativa a la CLI.
4.18	Una función de IAM Servicio de AWS como director de confianza también debe cumplir con las normas técnicas de la IAM.
4.19	Los roles vinculados a servicios (SLRs) no están sujetos a los estándares técnicos de AMS IAM, ya que los crea y mantiene el equipo de servicio de IAM.

ID	Norma técnica
4.20	Las políticas de IAM no deben permitir el acceso de lectura sin restricciones a los objetos del bucket de Amazon S3 (por ejemplo, Amazon S3:GetObject) en todos los buckets de una cuenta: • En las cuentas en modo desarrollador: las infracciones dan lugar a una notificación de riesgo • En las cuentas que no están en modo desarrollador: las infracciones requieren la aceptación del riesgo
4.21	Todos los permisos de IAM para el tipo de recurso «savingsplan» se pueden conceder a los clientes.
4.22	Los ingenieros de AMS no pueden copiar ni mover los datos de los clientes (archivos, objetos S3, bases de datos) manualmente en ninguno de los servicios de almacenamiento de datos, como Amazon S3, Amazon Relational Database Service, Amazon DynamoDB, etc., ni en el sistema de archivos del sistema operativo .
4.23	La política de SCP no debe modificarse para permitir ningún acceso adicional a ninguna de las cuentas gestionadas por AMS.

ID	Norma técnica
4.24	No se debe permitir ningún cambio en la política de SCP que pueda infringir la infraestructura o las capacidades de administración de AMS. (Nota: los recursos de AMS tienen la etiqueta AppId= AMSInfrastructure y siguen el espacio de nombres protegido de AMS).
4.25	La función de aprovisionamiento automatizado de IAM de AMS debe estar habilitada en sus cuentas como una función opcional.
4.26	Los roles o usuarios de AMS asumidos por humanos no deben tener acceso al contenido del cliente en S3, RDS, DynamoDB, Redshift, ElastiCache, EFS y FSx. Además, en las funciones de operador se debe denegar explícitamente el acceso a una publicación conocida o nueva APIs publicada por otra persona. Servicios de AWS que permita el acceso al contenido de los clientes.
5.0	Federación
5.1	La autenticación debe configurarse mediante la federación en la cuenta gestionada por AMS.
5.2	Solo debe haber una confianza de salida unidireccional entre AMS AD y su Active Directory (AMS AD confía en el AD local).
5.3	Los almacenes de identidades utilizados para autenticarse en AMS no deben existir en las cuentas de aplicaciones gestionadas por AMS.
6.0	Políticas de cuentas cruzadas

ID	Norma técnica
6.1	Se pueden configurar las funciones de IAM y las políticas de confianza entre las cuentas de AMS que pertenecen al mismo cliente según los registros de los clientes.
6.2	Las políticas de confianza de los roles de IAM entre las cuentas AMS y las que no son de AMS solo se deben configurar si la cuenta que no es de AMS pertenece al mismo cliente de AMS (confirmando que están bajo la misma AWS Organizations cuenta o haciendo coincidir el dominio de correo electrónico con el nombre de la empresa del cliente).
6.3	Las políticas de confianza de las funciones de IAM entre las cuentas de AMS y las cuentas de terceros no deben configurarse sin correr el riesgo de aceptarlas.
6.4	Se pueden configurar políticas multicuentas para acceder a cualquier cuenta de AMS CMKs del mismo cliente gestionada por un cliente.
6.5	Se pueden configurar políticas multicuenta para acceder a cualquier clave de KMS de una cuenta que no sea de AMS mediante una cuenta de AMS.
6.6	No se deben permitir las políticas multicuenta para acceder a cualquier clave de KMS de una cuenta de AMS por parte de una cuenta de terceros sin una aceptación arriesgada.

ID	Norma técnica
6.6.1	Las políticas multicuentas para acceder a cualquier clave de KMS de una cuenta de AMS desde una cuenta que no sea de AMS solo se pueden configurar si la cuenta que no es de AMS es propiedad del mismo cliente de AMS.
6.7	Se pueden configurar políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) entre cuentas de AMS del mismo cliente.
6.8	Se pueden configurar políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) en una cuenta que no sea de AMS desde una cuenta de AMS con acceso de solo lectura.
6.9	Las políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) con permisos de escritura de AMS a una cuenta que no sea de AMS (o de una cuenta que no sea de AMS a AMS) solo deben configurarse si la cuenta que no es de AMS es propiedad del mismo cliente de AMS (confirmando que está en la misma cuenta o haciendo coincidir el dominio de correo electrónico con AWS Organizations el nombre de la empresa del cliente).

ID	Norma técnica
6,10	Se pueden configurar políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) en una cuenta de terceros desde una cuenta de AMS con acceso de solo lectura.
6.11	No se deben configurar políticas multicuenta para acceder a cualquier dato o recurso del bucket de S3 donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) en una cuenta de terceros desde una cuenta de AMS con acceso de escritura.
6.12	Las políticas multicuentas de cuentas de terceros para acceder a un bucket de S3 de un cliente de AMS o a los recursos en los que se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift) no deben configurarse sin una aceptación arriesgada.
7.0	User Groups (Grupos de usuarios)
7.1	Se permiten los grupos de IAM con permisos de solo lectura y no mutativos.
8.0	Políticas basadas en recursos
8.1	Los recursos de la infraestructura de AMS deben protegerse de la administración por parte de identidades no autorizadas mediante la incorporación de políticas basadas en los recursos.

ID	Norma técnica
8.2	Sus recursos deben configurarse con políticas basadas en recursos con privilegios mínimos, a menos que especifique explícitamente una política diferente.
9.0	Servicios aprovisionados de autoservicio (SSPS)
9.1	El rol o la política de IAM predeterminados de AMS (incluidos el perfil de la instancia, el SSPS y el patrón) no deben modificarse con o sin ningún riesgo. Se permiten excepciones (sin riesgo de aceptación) a las políticas de confianza. En las funciones predeterminadas del SSP también se permite etiquetar los cambios de rol, política o usuario.
9.3	La política de SSPS para el rol de consola de Systems Manager Automation no se puede adjuntar a ningún rol personalizado aparte del rol predeterminado. Las demás políticas de SSPS solo se deben adjuntar a las funciones de IAM personalizadas después de garantizar que la vinculación de la política a una función personalizada no proporciona permisos adicionales fuera del diseño previsto para el servicio SSPS predeterminado.

AMS-STD-003: Seguridad de red

El siguiente es el control estándar para 003 - Network Security:

ID	Norma técnica
	Redes

ID	Norma técnica
1.0	Se debe acceder a todas las EC2 instancias mediante SSH o RDP únicamente a través de hosts Bastion, rango CIDR de VPC del host bastión o desde el rango CIDR de VPC de la misma instancia.
2.0	EC2 Se permite la IP elástica en las instancias
3.0	Se debe utilizar el plano de control AMS y, por extensión, en el plano de datos, el TLS 1.2+.
4.0	Todo el tráfico de salida debe pasar por la cuenta IGW o TGW.
5.0	Un grupo de seguridad no debe tener el origen 0.0.0.0/0 en la regla de entrada si no está conectado a un balanceador de cargas según la versión 9.0
6.0	El depósito o los objetos de S3 no deben hacerse públicos sin riesgo de ser aceptados.
7.0	No se debe permitir el acceso a la administración de servidores en los puertos SSH/22 o SSH/2222 (no SFTP/2222), TELNET/23 , RDP/3389, WinRM/5985-5986, VNC/5900-5901 TS/CITRIX/1494 o 1604, LDAP/389 o 636 y RPC/135, NETBIOS/137-139 desde fuera de la VPC a través de grupos de seguridad.

ID	Norma técnica
8.0	No se debe permitir el acceso a la administración de bases de datos en los puertos (MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433) o en un puerto personalizado desde el público ni se debe enrutar a una VPC a través de DX, VPC-Peer o una VPN a través de un grupo de seguridad. IPs
8.1	Cualquier recurso en el que se puedan almacenar los datos de los clientes no debe exponerse directamente a la Internet pública.
9.0	El acceso directo a las aplicaciones a través de los puertos HTTP/80, HTTPS/8443 y HTTPS/443 desde Internet solo está permitido a los balanceadores de carga, pero no a ningún recurso de cómputo directamente, por ejemplo, instancias, contenedores, etc. EC2 ECS/EKS/Fargate
10.0	Se puede permitir el acceso de las aplicaciones a través de los puertos HTTP/80 y HTTPS/443 desde el rango de IP privadas del cliente.
11.0	No se debe permitir ningún cambio en los grupos de seguridad que controlan el acceso a la infraestructura de AMS sin que ello suponga un riesgo.
12.0	AMS Security hace referencia a los estándares cada vez que se solicita que un grupo de seguridad se adjunte a una instancia.

ID	Norma técnica
13.0	El acceso al bastión del cliente en los puertos 3389 y 22 solo debe permitirse desde los rangos de IP privadas que se enruten a la VPC a través de DX, VPC-peer o VPN.
14.0	La asociación entre cuentas de zonas alojadas privadas VPCs desde una cuenta de AMS a una cuenta que no es de AMS (o que no es de AMS a una cuenta de AMS) solo debe configurarse si la cuenta que no es de AMS es propiedad del mismo cliente de AMS (confirmando que están bajo la misma cuenta de la organización de AWS o haciendo coincidir el dominio de correo electrónico con el nombre de la empresa del cliente) mediante herramientas internas.
15.0	Se pueden permitir las conexiones de emparejamiento de VPC entre cuentas que pertenecen al mismo cliente.
16.0	La base de AMS se AMIs puede compartir con cuentas ajenas a AMS siempre que ambas cuentas sean propiedad del mismo cliente (confirmando que están bajo la misma AWS Organizations cuenta o haciendo coincidir el dominio de correo electrónico con el nombre de la empresa del cliente) mediante herramientas internas.
17.0	El puerto FTP 21 no debe configurarse en ninguno de los grupos de seguridad sin una aceptación del riesgo.

ID	Norma técnica
18.0	Se permite la conectividad de red entre cuentas a través de Transit Gateway siempre que todas las cuentas sean propiedad del cliente.
19.0	No está permitido convertir una subred privada en pública
20.0	No se deben permitir las conexiones de emparejamiento de VPC con cuentas de terceros (que no sean propiedad del cliente).
21.0	No se debe permitir la conexión de Transit Gateway a una cuenta de terceros (que no sea propiedad del cliente).
22.0	El tráfico de red necesario para que AMS preste los servicios a los clientes no debe bloquearse en el punto de salida de la red del cliente.
23.0	Se permite compartir las reglas de resolución con aquellas que Cuenta de AWS sean propiedad del mismo cliente mediante una notificación de riesgo
19.0	ICMP
19.1	La solicitud ICMP entrante a Amazon por EC2 parte del cliente infra requerirá una notificación del riesgo.
19.2	Se permiten las solicitudes entrantes del público IPs enrutadas a Amazon VPC a través de DX, VPC-peer o VPN a través de un grupo de seguridad.

ID	Norma técnica
19.3	Las solicitudes entrantes del público que IPs no se enruten a Amazon VPC a través de DX, VPC-peer o VPN a través de un grupo de seguridad requerirían una aceptación de riesgo.
19.4	Se permiten solicitudes ICMP salientes desde Amazon EC2 a cualquier destino.
20.0	Uso compartido de grupos de seguridad
20.1	Si un grupo de seguridad cumple con este estándar de seguridad, se puede compartir entre cuentas VPCs de la misma cuenta y entre cuentas de la misma organización.
20.2	Si un grupo de seguridad no cumple con este estándar y anteriormente se requería la aceptación del riesgo para este grupo de seguridad, no se permite el uso de la función de uso compartido de grupos de seguridad entre la misma cuenta o entre cuentas de la misma organización sin la aceptación del riesgo para esa nueva VPC o cuenta. VPCs

AMS-STD-004: Pruebas de penetración

El siguiente es el control estándar para el 004: Pruebas de penetración

1. AMS no admite la infraestructura de pentest. Es responsabilidad del cliente. Por ejemplo, Kali no es una distribución de Linux compatible con AMS.
2. Los clientes deben cumplir con las [pruebas de penetración](#).
3. En caso de que el cliente desee realizar pruebas de penetración de la infraestructura en las cuentas, se debe avisar previamente a AMS con 24 horas de antelación.

4. AMS proporcionará al cliente una infraestructura de pentesting según los requisitos del cliente que se especifiquen explícitamente en la solicitud de cambio o servicio presentada por el cliente.
5. La gestión de la identidad de la infraestructura de pentesting del cliente es responsabilidad del cliente.

AMS-STD-005 - GuardDuty

El siguiente es el control estándar para 005 - GuardDuty

1. GuardDuty debe estar activado en todas las cuentas de los clientes en todo momento.
2. GuardDuty Los resultados de la cuenta de aplicaciones gestionada por el cliente (CMA) en MALZ no generarán alarmas para el equipo de operaciones.
3. GuardDuty las alertas deben almacenarse en la misma cuenta o en cualquier otra cuenta gestionada de la misma organización.
4. No se GuardDuty debe utilizar la función de lista de IP confiables de. En su lugar, se puede utilizar el archivado automático como alternativa, lo que resulta útil para fines de auditoría.
5. GuardDuty La delegación de administradores no debe estar habilitada en MALZ, ya que el administrador delegado podría realizar acciones con altos privilegios, como deshabilitar las demás cuentas, sin correr el riesgo GuardDuty de aceptarlas.
6. GuardDuty Los filtros de archivado automático deben utilizar el alcance mínimo para obtener el máximo rendimiento. Por ejemplo, si AMS ve varios bloques impredecibles IPs en distintos bloques de CIDR y hay un ASN corporativo que es adecuado utilizar, utilice el ASN. Sin embargo, si puedes limitar el alcance a rangos específicos o a /32 direcciones, entonces acércate a esos rangos.

AMS-STD-006: Seguridad del host

El siguiente es el control estándar para 006 - Host Security

- Debe haber un agente antivirus en ejecución en todas las EC2 instancias y en todo momento. (por ejemplo, Trend Micro DSM).
- El módulo antimalware debe estar activado.
- El agente EPS debe incluir todos los directorios y archivos que se van a escanear.
- Los archivos puestos en cuarentena por la solución antivirus se pueden compartir con usted cuando lo desee.

- No se debe instalar una solución de seguridad para terminales de terceros.
- La frecuencia de actualización de las firmas antivirus debe configurarse como mínimo una vez al día.
- La frecuencia de escaneo programada debe configurarse como mínimo una vez al mes.
- El escaneo en tiempo real (en tiempo real) debe estar activado y en funcionamiento en todo momento.
- AMS no debe ejecutar ningún script personalizado que no sea propiedad de AMS ni esté creado por AMS en sus instancias. (Nota: Puede hacerlo mediante el acceso de administrador de pila a través del acceso de administrador de pila CT o mediante la [AWS Systems Manager automatización \(AMS SSPS\)](#).
- La autenticación a nivel de red (NLA) no debe estar deshabilitada en el host de Windows.
- El sistema operativo host debe estar actualizado con los últimos parches de seguridad según el ciclo de parches configurado.
- Una cuenta gestionada por AMS no debe tener una instancia no gestionada en la cuenta.
- No debe permitirse la creación de cuentas de administrador local en su instancia por parte de AMS.
- No se EC2 debe crear el par de claves activado.
- No debe utilizar sistemas operativos declarados al final de su vida útil (EOL) y el proveedor o un tercero no proporcionan ningún otro soporte de seguridad.

AMS-STD-007: Registro

El siguiente es el control estándar para 007: Registro

ID	Norma técnica
1.0	Tipos de registro
1.1	Registros del sistema operativo: todos los hosts deben registrar como mínimo los eventos de autenticación del host, los eventos de acceso para todos los usos de privilegios elevados y los eventos de acceso para todos los cambios en la configuración de acceso y privilegios, tanto si se realizan correctamente como si no.

ID	Norma técnica
1.2	AWS CloudTrail: el registro CloudTrail de eventos de administración debe estar habilitado y configurado para enviar los registros a un bucket de S3.
1.3	Registros de flujo de VPC: todos los registros de tráfico de red deben registrarse mediante registros de flujo de VPC.
1.4	Registro de acceso al servidor Amazon S3: los buckets S3 obligatorios por AMS que almacenan registros deben tener habilitado el registro de acceso al servidor.
1.5	AWS Config Instantáneas: AWS Config deben registrar los cambios de configuración de todos los recursos compatibles en todas las regiones y entregar los archivos de instantáneas de configuración a los depósitos de S3 al menos una vez al día.
1.6	Registros del Endpoint Protection System (EPS): el registro de la solución EPS debe estar habilitado y configurado para enviar los registros a un grupo de CloudWatch registros.
1.7	Registros de aplicaciones: los clientes pueden habilitar el inicio de sesión en sus aplicaciones y almacenarlos en un grupo de CloudWatch registros o en un depósito de S3.
1.8	Registro a nivel de objeto de S3: los clientes pueden habilitar el registro a nivel de objeto en sus depósitos de S3.

ID	Norma técnica
1.9	Registro de servicios: los clientes pueden habilitar y reenviar los registros de los servicios de SSPS como cualquier otro servicio principal.
1.10	Registros de Elastic Classic/Application Load Balancer/Network Load Balancing (Load Balancer): las entradas de los registros de acceso y errores deben almacenarse en los buckets S3 gestionados por AMS 2.0.
2.0	Control de acceso
2.1	No debe tener acceso de escritura o eliminación en los depósitos de S3 necesarios para AMS que almacenan registros y CloudWatch registros (grupos de registros).
2.2	Debe tener acceso de solo lectura a todos los registros de sus cuentas.
2.3	Los depósitos S3 exigidos por AMS que almacenan registros no deben permitir el uso de cuentas de terceros como norma en las políticas de los depósitos.
2.4	Los registros de CloudWatch los grupos de registros de Logs no se deben eliminar sin la aprobación explícita de su contacto de seguridad autorizado.
3.0	Retención de registros
3.1	Los grupos de CloudWatch registros exigidos por AMS deben tener un período de retención mínimo de 90 días en los registros.

ID	Norma técnica
3.2	Los depósitos S3 exigidos por AMS que almacenan los registros deben tener un período de retención mínimo de 18 meses.
3.3	AWS Backup las instantáneas deberían estar disponibles con una retención mínima de 31 días en los recursos compatibles.
4.0	Cifrado
4.1	El cifrado debe estar habilitado en todos los depósitos de S3 que necesiten los equipos de AMS que almacenen los registros.
4.2	Cualquier reenvío de registros desde las cuentas de los clientes a cualquier otra cuenta debe estar cifrado.
5.0	Integridad
5.1	El mecanismo de integridad del archivo de registro debe estar activado. La «validación del archivo de registro» debe estar configurada en las AWS CloudTrail rutas requeridas por los equipos de AMS.
6.0	Reenvío de registros
6.1	Cualquier registro se puede reenviar de una cuenta AMS a otra cuenta AMS del mismo cliente.
6.2	Cualquier registro se puede reenviar de AMS a una cuenta que no sea de AMS solo si la cuenta que no es de AMS es propiedad del mismo cliente de AMS.

ID	Norma técnica
6.3	Los registros de una cuenta de cliente no deben reenviarse a una cuenta de terceros (que no sea propiedad del cliente).

AMS-STD-008 - AMS-MAD

El siguiente es el control estándar para 008 - AMS-MAD

ID	Norma técnica
1.0	Administración de accesos
1.1	Solo los usuarios con privilegios de AMS con inicios de sesión interactivos y tareas de automatización deben poder iniciar sesión en el host de administración para administrar el AD administrado en las cuentas de los clientes.
1.2	Los administradores de AD solo deben tener privilegios de administrador delegado (grupo de administradores delegados de AMS).
1.3	Los ingenieros que inicien sesión en los entornos de AD de los clientes (instancias o hosts de administración) deben tener un acceso limitado en el tiempo.
1.4	En una EC2 instancia, los clientes tienen acceso de solo lectura a los objetos de AD mediante las herramientas de administración remota del servidor.
1.5	No se deben permitir derechos administrativos al usuario o grupo de Active Directory.

ID	Norma técnica
1.6	AWS Se permite compartir el directorio con un Cuenta de AWS propietario del mismo cliente con una notificación de riesgo.
2.0	Cuentas de servicio
2.1	Las cuentas de servicios gestionados grupales (gMSA) se deben usar siempre que las aplicaciones las admitan en lugar de la cuenta de servicio estándar.
2.2	Todas las demás cuentas de servicio deben crearse después del proceso de aceptación del riesgo.
2.3	Los grupos de seguridad de AD no se deben reutilizar a menos que el cliente lo solicite explícitamente. Se deben crear nuevos grupos de AD. Los objetos informáticos que soliciten acceso a la cuenta de servicio deben agregarse al nuevo grupo de seguridad.
2.4	Todas las cuentas de servicio de gMSA deben añadirse a la unidad organizativa (OU) «Cuenta de servicio gestionada».
2,5	Todas las cuentas de servicio que no sean de GMSA deben agregarse a la OU «Usuarios →Cuentas de servicio».
3.0	Objetos de política de grupo (GPO)
3.1	No se debe modificar ninguna configuración del GPO «Configuración de Windows > Configuración de seguridad» si reduce la seguridad de la cuenta de alguna manera con respecto al estado actual.

ID	Norma técnica
3.2	En MALZ, que RFCs se envía desde una cuenta de aplicación que solicita la creación de un GPO, el GPO debe estar vinculado a la OU correspondiente a la cuenta de la aplicación. Los GPOs que afecten a todas las cuentas deben provenir de la cuenta de servicio compartido.
3.3	El tiempo de espera predeterminado de la sesión inactiva de RDP debe establecerse en 15 minutos para todos los servidores del dominio de Active Directory.
4.0	Confianza en Active Directory
4.1	Se permite la confianza saliente unidireccional (del directorio al directorio de clientes hospedado por AMS) si los reenviadores condicionales se enrutan a una VPC a través IPs de DX, VPC-peer o VPN.
5.0	Otros
5.1	El mecanismo de integridad del archivo de registro debe estar activado. La «validación del archivo de registro» debe estar configurada en las AWS CloudTrail rutas requeridas por los equipos de AMS.
6.0	Reenvío de registros
6.1	Los usuarios, grupos, objetos informáticos, unidades organizativas u otras entidades del cliente no deben utilizar la convención de nomenclatura de AMS según la convención de nomenclatura de AMS.

ID	Norma técnica
6.2	Todo OUs debe ser gestionado por AMS.

AMS-STD-009 - Diverso

El siguiente es el control estándar para 009 - Miscelánea

- Si el cifrado está activado en un recurso, objeto, base de datos o sistema de archivos, no debe deshabilitarse.

Cambios que introduzcan riesgos de seguridad altos o muy altos en su entorno

Los siguientes cambios introducen un riesgo de seguridad alto o muy alto en su entorno:

AWS Identity and Access Management

- High_risk-IAM-001: Cree claves de acceso para la cuenta raíz
- High_risk-IAM-002: modificación de la política de SCP para permitir un acceso adicional
- High_risk-IAM-003: modificación de la política de SCP que podría dañar la infraestructura de AMS
- High_Risk-IAM-004: Creación de una cuenta de cliente role/user con permisos variables en la infraestructura (escritura, gestión de permisos o etiquetado)
- High_Risk-IAM-005: IAM aplica políticas de confianza entre las cuentas de AMS y las cuentas de terceros (que no son propiedad del cliente)
- High_risk-IAM-006: políticas multicuenta para acceder a cualquier clave de KMS desde una cuenta de AMS (desde una cuenta de terceros)
- High_risk-IAM-007: políticas multicuenta de cuentas de terceros para acceder a un bucket de S3 de un cliente de AMS o a recursos donde se puedan almacenar datos (como Amazon RDS, Amazon DynamoDB o Amazon Redshift)
- High_Risk-IAM-008: asigne los permisos de IAM a cualquier infraestructura que modifique el permiso de la cuenta del cliente
- High_risk-IAM-009: Permite publicar y leer todos los depósitos de S3 de la cuenta
- High_risk-IAM-010: aprovisionamiento automatizado de IAM con permisos read/write

Seguridad de la red

- High_RISK-NET-001: Abra los puertos de administración del sistema operativo SSH/22 o SSH/2222 (no SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/ CITRIX/1494 o 1604, LDAP/389 o 636 y NETBIOS/137-139 desde Internet
- High_risk-net-002: Abra los puertos de administración de bases de datos MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 o cualquier puerto de administración de clientes desde Internet
- High_risk-net-003: abra los puertos de aplicaciones HTTP/80, HTTPS/8443 y HTTPS/443 directamente en cualquier recurso informático. Por ejemplo, instancias, contenedores, etc. desde Internet EC2 ECS/EKS/Fargate
- High_Risk-Net-004: cualquier cambio en los grupos de seguridad que controlan el acceso a la infraestructura AMS
- High_risk-net-006: interconexión de VPC con la cuenta de terceros (que no es propiedad del cliente)
- High_risk-net-007: Se ha añadido el firewall del cliente como punto de salida para todo el tráfico de AMS
- High_risk-net-008: No se permite adjuntar archivos adjuntos a Transit Gateway a la cuenta de terceros
- High_Risk-S3-001: Aprovisiona o habilita el acceso público en el bucket S3

Registro

- CloudTrailHigh_risk-log-001: Desactivar. (Se requiere la aprobación del administrador del sitio de operaciones)
- High_risk-log-002: inhabilita los registros de flujo de la VPC. (Se requiere la aprobación del administrador del sitio de operaciones)
- High_risk-log-003: reenvío de registros mediante cualquier método (notificación de eventos S3, extracción mediante un agente SIEM, inserción mediante un agente SIEM, etc.) desde una cuenta gestionada por AMS a una cuenta de terceros (no propiedad del cliente)
- High_risk-log-004: Utilice un registro que no sea de AMS para CloudTrail

Seguridad del host

- High_risk-HOST-001: deshabilita la seguridad de End Point en la cuenta por cualquier motivo. (Se requiere la aprobación del administrador del sitio de operaciones)
- High_Risk-Host-002: deshabilita la aplicación de parches en un recurso o a nivel de cuenta.
- High_risk-host-003: Implementación de una instancia no administrada en la cuenta. EC2
- High_risk-host-004: ejecutar un script personalizado proporcionado por el cliente.
- High_risk-host-005: creación de cuentas de administrador local en las instancias.
- High_Risk-Host-006: Excluye el escaneo de tipos o extensiones de archivo EPS de Trend Micro o deshabilita la protección contra malware en los terminales.

 Note

No es obligatorio aceptar el riesgo para las normas de exclusión o GuardDuty supresión de antimalware de la EPS relacionadas con las pruebas de penetración o los análisis de vulnerabilidades o los problemas de rendimiento que afecten al servicio y que justifiquen la adopción de medidas proactivas. events/known En estas situaciones, basta con una notificación de riesgo.

- High_risk-host-007: Crear para KeyPair EC2
- High_risk-host-008: Deshabilite la seguridad del punto final en el EC2
- High_risk-host-009: Cuentas que utilizan el sistema operativo End of Life (EOL)

Misceláneo

- High_risk-enc-001: deshabilita el cifrado en cualquier recurso si está activado

Active Directory administrado

- High_Risk-AD-001: proporciona derechos de administrador al usuario o grupo de Active Director
- High_Risk-AD-002: políticas de GPO capaces de reducir la postura de seguridad de la cuenta

Gestión de la continuidad en AMS Advanced

Como parte de la gestión de la continuidad, AWS Managed Services (AMS) proporciona acceso automatizado a AWS Backup un servicio nativo con AWS. Esto facilita el acceso a un servicio compatible con Amazon EBS, Amazon EC2, Amazon RDS, Amazon EFS y más.

Para obtener más información, consulte [AWS Backup: Cómo funciona](#).

Temas

- [¿Qué es la gestión de la continuidad?](#)
- [Cómo funciona la gestión de la continuidad](#)
- [Respuesta de recuperación ante desastres](#)
- [Planificación de la recuperación ante desastres](#)

¿Qué es la gestión de la continuidad?

La administración de la continuidad es el proceso que utiliza AMS para proporcionar copias de seguridad e instantáneas de su cuenta.

AMS proporciona acceso a ellos AWS Backup mediante tipos de cambios que se utilizan para crear y gestionar tareas y planes de copia de seguridad.

Cómo funciona la gestión de la continuidad

AMS lo utiliza [AWS Backup](#) para la gestión de la continuidad.

Al empezar a trabajar con AWS Backup AMS:

1. Ejecute una copia de seguridad bajo demanda
2. Cree un plan de respaldo (opcional, AMS proporciona planes de respaldo predeterminados)
3. Utilice el AMS predeterminado en las bóvedas de respaldo (opcional)
4. Administre (ejecute, refine, elimine, etc.) sus planes de respaldo y puntos de recuperación

Planes de respaldo de AMS

Un plan de respaldo es una expresión de política que define cuándo y cómo desea realizar copias de seguridad de los recursos de AWS compatibles, como las bases de datos de RDS, los volúmenes de EBS, las tablas de DynamoDB y los sistemas de archivos EFS. Las políticas de programación y retención se administran mediante planes de respaldo personalizados, que puede crear mediante un tipo de cambio (CT) con AMS Advanced o con AWS Backup AMS Accelerate. Asigne recursos a sus planes de copia de seguridad mediante etiquetas y AWS Backup realice y conserve automáticamente las copias de seguridad de los recursos asignados de acuerdo con el plan de copia de seguridad definido. Puede crear varios planes de copia de seguridad si tiene cargas de trabajo con requisitos de copia de seguridad diferentes.

Un plan de respaldo puede tener hasta seis reglas de respaldo que definen un cronograma y un período de retención, entre otros detalles. El programa de copias de seguridad determina cuándo se AWS Backup inicia un trabajo de copia de seguridad y con qué frecuencia se crea una copia de seguridad. Puede elegir una frecuencia por hora, por día, por semana o por mes. La configuración de días de eliminación determina cuántos días se almacena la instantánea antes de que se elimine automáticamente.

Note

AMS Advanced: si se migra desde el sistema de copias de seguridad AMS anterior, AMS crea un plan de copias de seguridad predeterminado para garantizar la compatibilidad con versiones anteriores. El par clave-valor en este escenario es Backup:True. Para garantizar la compatibilidad con versiones anteriores, el valor aquí no distingue entre mayúsculas y minúsculas, por lo que Backup:True o Backup:True son todas etiquetas válidas. Todos los demás pares clave:valor distinguen entre mayúsculas y minúsculas.

AWS Backup puede funcionar a nivel de volumen de EBS o a nivel de EC2 instancia de Amazon, pero no haga ambas cosas al mismo tiempo, ya que esto puede provocar una situación de carrera en la que las copias de seguridad podrían chocar.

Planes de respaldo predeterminados, landing zone multicuenta

Durante el RFC de creación de una nueva cuenta, AMS se asegura de que haya un plan de respaldo predeterminado general a nivel de cuenta para proteger sus cargas de trabajo. Los valores de los campos obligatorios se establecen de forma predeterminada, como se muestra en la siguiente sección:

Plan de respaldo de AMS predeterminado

default-backup-plan

Clave TAG: Backup

Valor TAG: True

```
RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for
23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for
23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for
23:30 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Plan de respaldo de AMS predeterminado	Start Time	Retención
copia de seguridad por hora	N/A	N/A
copia de seguridad diaria	todos los días a las 11:30 p.m. UTC	7 días
copia de seguridad semanal	semanalmente a las 23:30, hora peninsular española, solo los sábados	4 semanas
copia de seguridad mensual	mensual a las 23:30, hora peninsular española, el primer día del mes	26 semanas
respaldo anual	A las 23:30, hora península r española, el primer día del mes	2 años

Plan de respaldo AMS predeterminado mejorado

Este plan es un modelo de prácticas AWS Backup recomendadas para protegerse contra los ataques de ransomware. Implementa una estrategia de respaldo diaria, semanal, mensual y anual. AWS Backup El [backup continuo](#) está habilitado con una retención máxima (31 días) de [los recursos compatibles](#).

ams-enhanced-default-backup-plan

Clave TAG: backup-orchestrator-enhanced

Valor TAG: true

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00 UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for 02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Plan de respaldo AMS mejorado	Start Time	Retención
copia de seguridad por hora	N/A	N/A
copia de seguridad diaria	todos los días a las 4:00 UTC	31 días
copia de seguridad semanal	sábado, 2:00 UTC	6 semanas
copia de seguridad mensual	El 1 de cada mes, a las 2:00 UTC	26 semanas
respaldo anual	1 de enero a las 2:00 UTC	2 años

Plan de respaldo AMS para datos confidenciales

Este plan es un modelo de prácticas recomendadas de AWS Backup para proteger contra los ataques de ransomware en aplicaciones sensibles a los datos. Implementa una estrategia de copias de seguridad por hora, por día, por semana, por mes y por año. La copia de seguridad [continua de AWS Backup](#) está habilitada con una retención máxima (31 días) en [los recursos compatibles](#).

ams-data-sensitive-backup-plan

Clave TAG: backup-orchestrator-data-sensitive

Valor TAG: true

```
RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Plan de respaldo AMS sensible a los datos	Start Time	Retención
copia de seguridad por hora	en la marca de la hora	7 días
copia de seguridad diaria	todos los días a las 4:00 UTC	31 días
copia de seguridad semanal	sábado, 2:00 UTC	6 semanas
copia de seguridad mensual	El 1 de cada mes, a las 2:00 UTC	26 semanas
respaldo anual	1 de enero a las 2:00 UTC	2 años

Bóvedas de respaldo de AMS

AWS Backup organiza las instantáneas en unidades de almacenamiento lógico denominadas bóvedas.

Puede controlar las notificaciones del almacén de copias de seguridad a nivel de almacén individual mediante etiquetas. Puede inhabilitar las notificaciones de un almacén específico añadiendo la etiqueta `AMSNotificationOptOut` y configurando el valor `True` en un almacén específico. Para volver a recibir notificaciones del almacén, elimina la etiqueta.

Para ver una lista de las copias de seguridad de AMS, abra la [AWS Backup consola](#). En el panel de navegación, elija Backup Vaults y seleccione uno de los almacenes de respaldo AMS de las siguientes tablas. En la sección Copias de seguridad, consulte la lista de todas las copias de seguridad del almacén de copias de seguridad. Seleccione una copia de seguridad para editarla, eliminarla o restaurarla.

Planes de respaldo de Vaults for AMS

Nombre de la bóveda de AMS	Descripción
ams-automated-backups	Esta bóveda recibe todos los puntos de recuperación ocupados por el AWS Backup plan predeterminado de AMS Advanced default-backup-plan.
ams-automated-enhanced-backups	Esta bóveda recibe todos los puntos de recuperación ocupados por el plan o AWS Backup plan predeterminado mejorado ams-enhanced-default-backupde AMS Advanced.
ams-automated-data-sensitive-copias de seguridad	Esta bóveda recibe todos los puntos de recuperación acumulados por el AWS Backup plan ams-data-sensitive-backup-plan AMS Advanced.
ams-manual-backups	Esta es la ubicación predeterminada para todas las copias de seguridad de los planes de copia de seguridad de Start Backup Job

Nombre de la bóveda de AMS	Descripción
	RFC (ct-2hhud2lx01tq7), si no se ha definido un nombre de almacén.
ams-custom-backups	Esta es la ubicación predeterminada para las instantáneas que AMS toma antes de parchear una instancia mediante Patch Orchestrator o las actividades de parches mensuales. Estas se eliminan automáticamente de acuerdo con la política predeterminada de 60 días durante el ciclo de vida de los parches de AMS.

Tipos de cambios de respaldo de AMS

AMS ofrece varios planes CTs para crear y utilizar planes de respaldo.

Important

No edite los planes de respaldo predeterminados de AMS, ya que los cambios podrían perderse. En su lugar, cree nuevos planes para sus configuraciones personalizadas.

- [Plan de Backup: Crear](#)
- [Backup Job: Inicio](#)
- [Backup Job: detener](#)
- [Punto de recuperación: eliminar](#)
- [DynamoDB | Crear a partir de Backup](#)
- [Volumen de EBS: Crear a partir de Backup](#)
- [Amazon Elastic File System \(EFS\): creación a partir de Backup](#)

Monitoreo e informes de copias de seguridad de AMS

Important

La supervisión y los informes de las copias de seguridad de AMS solo están disponibles en las regiones compatibles con AMS. Estos son EE.UU. Este (Virginia), EE.UU. Oeste (Norte de California), EE.UU. Oeste (Oregón), EE.UU. Este (Ohio), Canadá (Centro), Sudamérica (São Paulo), UE (Irlanda), UE (Fráncfort), UE (Londres), UE (París), Asia Pacífico (Bombay), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Asia Pacífico (Tokio).

AMS genera informes de autoservicio diarios, así como informes mensuales sobre la cobertura de los recursos y el estado de las tareas de respaldo. Los informes mensuales se comparten en Monthly Business Reviews (MBRs). Para obtener más información sobre los informes de respaldo diarios, consulte [de respaldo diario](#).

Los expertos de AMS supervisan todas las tareas de copia de seguridad configuradas mediante AWS Backup. En caso de que se produzcan errores en la copia de seguridad, AMS la investigará y le notificará la causa principal y las opciones de reparación, si están disponibles. Para evitar el ruido de las alertas, durante los eventos que provocan un gran número de fallos en las copias de seguridad de sus cuentas, AMS hace una recomendación colectiva, a través de su CSDM, en lugar de notificarle cada fallo individual.

Tenga en cuenta que AMS no supervisa ninguna copia de seguridad configurada mediante la función de copia de seguridad independiente de un AWS servicio.

Respuesta de recuperación ante desastres

Además de las opciones que se describen en las siguientes secciones, es bueno que sepa qué pasos debe seguir para iniciar una recuperación ante desastres (DR) con AMS.

Si se produce un desastre y necesita iniciar una recuperación, siga estas pautas generales:

1. Abra un incidente de alta prioridad con la categoría Disponibilidad. AMS abrirá un puente de conferencias e invitará a su equipo a unirse.
2. Conozca la lista de recursos que necesita para recuperarse.
3. Conoce la zona de landing zone (LZ) objetivo en la que necesitas recuperarte (por ejemplo, la misma cuenta, diferente AZ o diferente cuenta y diferente región).

4. Envía solicitudes de recuperación para cada recurso de la landing zone de destino. Siga su plan de recuperación ante desastres actual o consulte las opciones de la siguiente sección (por ejemplo [Protección ante desastres EC2 con instantáneas de EBS en AMS](#), o [Protección ante desastres EC2 con Elastic Disaster Recovery en AMS](#)).
5. Restaure la funcionalidad de la aplicación y utilice la asistencia de AMS para solucionar problemas relacionados con la infraestructura.

AMS puede ayudarlo a prepararse para este evento y a crear un plan de recuperación ante desastres para su organización que aborde estas cuestiones. Para obtener más información, póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) o arquitecto de la nube (CA).

Planificación de la recuperación ante desastres

La recuperación ante desastres (DR) es un servicio fundamental para la continuidad empresarial y el cumplimiento normativo. AMS colabora con usted para ayudarlo a planificar, implementar y mantener su estrategia de DR en AMS.

AMS landing zone (LZ), con varias cuentas y una sola cuenta, proporciona componentes nativos, Multi-AZ y de alta disponibilidad para los componentes de la infraestructura de AMS que cumplen con la mayoría de los escenarios de protección ante desastres. Sin embargo, en función de la cobertura geográfica de su empresa, es posible que necesite protección regional. Para la disponibilidad entre regiones y la DR, se requiere otra cuenta de AMS en una región diferente (esto es válido tanto para la zona de aterrizaje multicuenta como para la zona de aterrizaje de una sola cuenta).

AMS se ajusta a las directrices de recuperación ante desastres de AWS que se describen en este blog, [Recuperación rápida de sistemas de misión crítica en caso de desastre](#), y admite las cuatro opciones siguientes:

- Varios sitios (o de alta disponibilidad)
- Modo de espera cálido
- Luz piloto
- Copia de seguridad y restauración

Estas opciones y la compatibilidad con AMS se describen en las siguientes secciones.

Multisitio o de alta disponibilidad (HA)

La solución de alta disponibilidad suele proporcionarse mediante la funcionalidad integrada de la aplicación, como la agrupación en clústeres o la replicación sincrónica. Los usuarios son dirigidos tanto a Prod como a los nodos. HA/DR El DNS apunta a los nodos directamente o a través de un balanceador de carga elástico (ELB).

Su arquitecto de nube (CA) de AMS trabajará con usted como parte de su planificación Well-Architected-Review y la de recuperación ante desastres.

HA DR utiliza funciones y servicios AWS nativos y de aplicaciones, como se muestra en el siguiente gráfico:

El sitio de DR puede estar en el mismo sitio o en uno diferente. Región de AWS

Note

Una región diferente (entre regiones) tendrá un entorno de Active Directory diferente.

Pasos de DR (conmutación por error): conmutación por error automática, no se requieren pasos manuales. En caso de que se produzca un error en la LZ principal, los usuarios se redirigirán automáticamente al nodo. DR/HA Esto se logra mediante la configuración del DNS y de la aplicación.

Métricas de DR de HA:

- Objetivo de punto de recuperación (RPO): <5 minutos
- Objetivo de tiempo de recuperación (RTO): <5 min
- Mantenimiento: alto (se requieren cambios sincrónicos en ambos entornos, como la configuración de las aplicaciones, los parches, el SG o ALB, los certificados, etc.).
- Costo: alto

Espera semiactiva

El término «modo de espera en espera» se utiliza para describir un escenario de recuperación ante desastres (DR) en el que una versión reducida del entorno se ejecuta en la nube.

La replicación de datos la realiza la capa de aplicación, normalmente de forma asíncrona, a una instancia en línea, mientras que el resto de las instancias (por ejemplo, los niveles de aplicación y web) pueden desactivarse para ahorrar costes. A los usuarios se les dirige únicamente al sitio de producción. También se pueden aprovisionar previamente otros AWS recursos, como el balanceador de carga elástico (ELB), en el sitio de DR.

Su AMS Cloud Architect (CA) trabajará con usted como parte de su Well-Architected-Review planificación y la de recuperación ante desastres.

Warm Standby DR utiliza funciones y servicios AWS nativos y de aplicaciones, como se muestra en el siguiente gráfico:

El sitio de DR puede estar en el mismo sitio o en uno diferente. Región de AWS

 Note

Una región diferente (entre regiones) tendrá un entorno de Active Directory diferente.

Pasos de DR (conmutación por error):

1. Frena la replicación de los datos y convierte la instancia de datos en el sitio de DR en la maestra
2. Actualice la configuración de la aplicación según sea necesario (nueva IP, nombre del servidor, etc.)
3. Redirija el DNS al sitio de DR (ELB)
4. Dependencias de AD si es necesario (cuentas de servicio SPNs, GPOs, etc.)

Métricas de DR de HA:

- Objetivo de punto de recuperación (RPO): <1 hora
- Objetivo y objetivo de tiempo de recuperación (RTO): menos de 1 hora (depende del número de instancias y de la orquestación)
- Mantenimiento: alto (se requieren cambios sincrónicos en ambos entornos, como la configuración de las aplicaciones, la aplicación de parches, los grupos de seguridad (SG) o el equilibrador de carga de aplicaciones (ALB), los certificados, etc.)
- Costo: medio

Luz piloto

En este enfoque de recuperación ante desastres (DR), se replica parte de su entorno Prod para un conjunto limitado de servicios principales. Una pequeña parte de la infraestructura está siempre en funcionamiento y sincroniza simultáneamente datos mutables (como bases de datos o documentos), mientras que otras partes de la infraestructura se apagan y se utilizan únicamente durante las pruebas. A diferencia de un enfoque de respaldo y recuperación, debes asegurarte de que tus elementos principales más importantes ya estén configurados y funcionando en la zona de aterrizaje de DR (la luz piloto).

Su arquitecto de nube de AMS trabajará con usted como parte de su planificación Well-Architected-Review y de recuperación ante desastres.

Pilot Light DR utiliza funciones y servicios AWS nativos y de aplicaciones, como se muestra en el siguiente gráfico:

El sitio de DR puede estar en el mismo sitio o en uno diferente. Región de AWS

Note

Una región diferente (entre regiones) tendrá un entorno de Active Directory diferente.

Pasos de DR (conmutación por error):

1. Frena la replicación de los datos y convierte la instancia de datos en el sitio de DR en la maestra
2. Inicie las instancias y la infraestructura desactivadas
3. Actualice la configuración de la aplicación según sea necesario (nueva IP, nombre del servidor, etc.)
4. Añada las instancias al ELB según sea necesario
5. Redirija el DNS al sitio de DR (ELB)
6. Dependencias de AD, si es necesario (cuentas de servicio SPNs GPOs, etc.)

Métricas de Pilot Light DR:

- Objetivo de punto de recuperación (RPO): <1 hora

- Objetivo y objetivo de tiempo de recuperación (RTO): aproximadamente 1 hora (depende del número de instancias y de la orquestación)
- Mantenimiento: Medio
- Costo: Medio

Copia de seguridad y restauración

Este enfoque de recuperación ante desastres (DR) simple y de bajo coste hace copias de seguridad de sus datos y aplicaciones desde cualquier lugar hasta la landing zone de DR para utilizarlos durante la recuperación tras un desastre.

Su AMS Cloud Architect trabaja con usted como parte de su planificación de Backup y DR.

Backup and Restore DR utiliza herramientas y procesos automatizados de AMS, como se muestra en el siguiente gráfico:

Se pueden utilizar dos métodos de copia de seguridad y replicación:

- Instantánea de EBS (objetivo de punto de recuperación (RPO) > 1 hora), conocida como «EBS»
- AWS Elastic Disaster Recovery (Objetivo de punto de recuperación (RPO) de aproximadamente 0,25 horas), conocido como «DRS»

El sitio de recuperación ante desastres puede estar en el mismo sitio o en uno diferente. Región de AWS

Note

Una región diferente (entre regiones) tiene un entorno de Active Directory diferente.

Pasos de DR (conmutación por error):

1. Restaure las instancias a partir de instantáneas (proceso de dos pasos, primero con la instancia de marcador de posición)
2. Actualice la configuración de la aplicación (nueva IP, nombre del servidor, etc.)
3. Configure otra infraestructura según sea necesario (SG, ELB, etc.)

4. Redirija el DNS al sitio de DR (ELB)
5. Actualice o restaure las dependencias de AD si es necesario (cuentas de servicio, nombres principales de servicio (SPNs), objetos de política de grupo (GPOs), etc.)

Métricas de recuperación ante desastres de Backup and Restore:

- Objetivo de punto de recuperación (RPO): más de 1 hora o aproximadamente 0,25 horas (depende de la solución seleccionada: EBS o DRE)
- Objetivo de tiempo de recuperación y (RTO): aproximadamente 1 hora (depende del número de instancias y de la orquestación)
- Mantenimiento: alto (se requieren cambios sincrónicos en ambos entornos, como la configuración de las aplicaciones, los parches, los grupos de seguridad o los balanceadores de carga de las aplicaciones, los certificados, etc.)
- Costo: medio

Protección ante desastres EC2 con instantáneas de EBS en AMS

Requisitos previos:

- Zona de aterrizaje de AMS Prod (fuente)
- Zona de aterrizaje AMS DR (objetivo DR)
- Las instantáneas de EBS están habilitadas para las EC2 instancias (AWS Backup)

Solución de replicación de instantáneas:

- Cross AZ: no se aplica: las instantáneas de EBS están muy disponibles en la región por diseño
- Entre regiones: AWS Backup

El siguiente diagrama representa el proceso de EC2 restauración a partir de las instantáneas de EBS en AMS:

EC2 Pasos de recuperación ante desastres en AMS:

1. Genere una RFC para compartir las instantáneas de EBS con la cuenta de destino (necesaria para la recuperación ante desastres entre regiones).

: Administración, componentes avanzados de Stack, EBS Snapshot, Share

2. Cree una pila EC2 AMS de marcador de posición en la subred de destino (subred del sitio de DR). La recomendación es utilizar la ingesta de CFN para crear la pila, ya que el cliente puede combinar los pasos de asignación de grupos de seguridad y otros (como añadir la instancia a un ELB) en la misma pila.

Tipo de cambio: implementación, ingestión, apilamiento a partir de una plantilla, creación CloudFormation

3. Genere un RFC para restaurar el volumen de la EC2 pila.

Tipo de cambio: administración, componentes de pila avanzados, pila de EC2 instancias, restauración de volúmenes.

El CT restaura los volúmenes a partir de las instantáneas compartidas en el paso 1 y los adjunta a la instancia de marcador de posición creada en el paso 2.

Funcionalidad CT de restauración de volúmenes:

- Cierre la instancia de marcador de posición
- Restaure los volúmenes a partir de las instantáneas
- Cambie los volúmenes
- Inicie la instancia
- Abandone el dominio anterior
- Cambiar el nombre de host
- Reiniciar. Los scripts bootstrap de AMS unen la instancia al dominio de destino (DR) al iniciarse

Entrada CT de restauración de volumen:

- InstanceId (ID de instancia de marcador de posición)
- RootDeviceSnapshotId, la instantánea de EBS del volumen raíz restaurado
- KMSKeyID, el identificador de clave de KMS o ARN, para cifrar todos los volúmenes restaurados de la instancia EC2
- DeviceNames, hasta 25 (opcional)
- SnapshotIds, hasta 25 (opcional). Lista de instantáneas de los volúmenes que se van a restaurar

Protección ante desastres EC2 con Elastic Disaster Recovery en AMS

Requisitos previos:

- Zona de aterrizaje de AMS Prod (fuente)
- Zona de aterrizaje AMS DR (objetivo DR)
- Primero debes inicializar el servicio Elastic Disaster Recovery para todas las Regiones de AWS aplicaciones en las que planeas usarlo.

Crea un rol de IAM en tu DR landing zone (LZ) para el acceso a la consola de Elastic Disaster Recovery.

- Importante: Un documento SSM se crea como una acción posterior al lanzamiento en DRS. Esta acción debe estar habilitada en todos sus servidores en la PostLaunch configuración.
- la instancia de destino (marcador de posición) debe tener una clave de etiqueta: "AWSDRS«, valor:"AllowLaunchingIntoThisInstance». La instancia de marcador de posición debe estar detenida. De lo contrario, AMS no podrá seleccionar la instancia de marcador de posición en la configuración de lanzamiento y Elastic Disaster Recovery no podrá restaurarla sobre la instancia de marcador de posición.

Para ver un diagrama del proceso de configuración y restauración de Elastic Disaster Recovery EC2 en AMS, consulta la arquitectura [general AWS Elastic Disaster Recovery \(AWS DRS\)](#).

EC2 Pasos de recuperación ante desastres con Elastic Disaster Recovery en AMS:

1. Cree una pila EC2 AMS de marcador de posición en la subred de destino (subred del sitio de DR) con las etiquetas adecuadas; para obtener más información, consulte la sección anterior. Recomendamos utilizar la ingesta de CFN para crear la pila, ya que puede combinar los pasos de asignar grupos de seguridad y etiquetar la instancia, el volumen de EBS y otros (como añadir la instancia a un ELB) en la misma pila.

Tipo de cambio: implementación, ingestión, apilamiento a partir de una plantilla, creación CloudFormation

2. Detenga la instancia del marcador de posición.

Tipo de cambio: administración, componentes de pila avanzados, EC2 instancia, parada

3. Si no lo ha hecho en el paso 1, etiquete la instancia de marcador de posición y su volumen de EBS con la clave: "AWSDRS«, valor:">»AllowLaunchingIntoThisInstance.

Tipo de cambio: administración, componentes de pila avanzados, etiqueta, actualización.

4. Utilice la instancia de marcador de posición del paso 1 como destino en Launch into instance ID, DRS Launch Settings, para el servidor de origen. Inicie el simulacro de recuperación de instancias desde la consola de Elastic Disaster Recovery para el servidor de origen.

 Note

Los volúmenes de instancias marcadores de posición se conservan en la cuenta. Para eliminar estos volúmenes, envíe un archivo Management | Advanced stack components | EBS Volume | Delete change type (ct-3e3h8u0sp5z80) al final de la operación de recuperación ante desastres.

Flujo de trabajo de recuperación ante desastres de Elastic:

- La instancia de destino (marcador de posición) debe estar detenida
- Cambie los volúmenes y elimine el volumen raíz de origen (marcador de posición)
- Inicie la instancia
- Ejecuta las acciones posteriores al lanzamiento para completar los siguientes elementos:
 - Activa el agente SSM.
 - Cambie los volúmenes y elimine el volumen raíz de origen (marcador de posición).
 - Inicie la instancia
 - Ejecute PostLaunchScript el documento SSM. Este documento hace lo siguiente:
 1. Abandona el dominio anterior.
 2. Cambia el nombre de servidor.
 3. Reiniciar. Los scripts bootstrap de AMS unen la instancia al dominio de destino (DR) durante el inicio.

Administración de parches en AMS

Temas

- [AMS Patch Orchestrator: un modelo de parches basado en etiquetas](#)
- [Uso de Patch Orchestrator](#)
- [Aplicación de parches bajo demanda](#)
- [Parcheo estándar AMS](#)
- [Compromisos de servicio de parcheo](#)

En AMS, la administración de parches es un servicio que le ayuda a mantener las actualizaciones del proveedor del sistema operativo en sus instancias de Amazon Elastic Compute Cloud (Amazon EC2). Tiene la libertad de personalizar la frecuencia y el proceso de aplicación de parches a sus EC2 instancias de Amazon.

La administración de parches se configura durante la incorporación y se puede actualizar mediante el proceso de RFC. Las pilas creadas con el sistema de gestión de cambios y una plantilla compatible con parches (para Amazon, EC2 Auto Scaling group, HA de uno o dos niveles) se suscriben automáticamente a la gestión de parches.

AMS ofrece una función, Patch Orchestrator, que consiste en aplicar parches basados en etiquetas, para configurar los parches.

Para ver las definiciones de los términos de aplicación de parches, consulte. [Términos clave de AMS](#)

Important

- No es posible que las pilas o las instancias que las componen opten por no participar en la administración de parches si la plantilla AMS a partir de la cual se crea la pila es compatible con la administración de parches. Actualmente, la aplicación de parches es compatible con las siguientes plantillas de pila:
 - Amazon EC2 stack | Create y Amazon EC2 stack | Create (con volúmenes adicionales)
 - EC2 Instancia de Amazon lanzada con AWS CloudFormation ingest
 - Grupo Auto Scaling | Crear (las EC2 instancias de Amazon del grupo están parcheadas)
 - Pila de un nivel de alta disponibilidad | Crear y pila de dos niveles de alta disponibilidad | Crear

- Si hay un incidente continuo que afecte a una pila, los operadores de AMS pueden reprogramar o cancelar la aplicación de parches programada.
- De forma predeterminada, todas las instancias de una pila específica compatible con parches se parchean in situ. Para parchear grupos de Auto Scaling con un reemplazo de Amazon Machine Image (AMI) mediante la AMI de latest/patched AMS, envíe una solicitud de servicio. AMIs Las actualizaciones se comparten en las cuentas todos los meses.

Important

Puede especificar repositorios de parches alternativos para los nodos gestionados. Mientras AMS implementa las configuraciones de parches solicitadas, usted es responsable de seleccionar y validar la seguridad de los repositorios elegidos. También debe aceptar cualquier riesgo derivado del uso de estos repositorios, como los riesgos de la cadena de suministro.

Las siguientes son las prácticas recomendadas para la seguridad del proceso de administración de parches:

- Utilice únicamente fuentes de repositorio confiables y verificadas
- Utilice de forma predeterminada los repositorios de los proveedores de sistemas operativos estándar cuando sea posible
- Audite periódicamente las configuraciones de los repositorios personalizados

Tip

AMS recomienda habilitar las copias de seguridad para las instancias que tengan aplicaciones o servicios valiosos. Para obtener información sobre cómo habilitar las copias de seguridad, consulte [Gestión de la continuidad en AMS Advanced](#).

AMS Patch Orchestrator: un modelo de parches basado en etiquetas

Si se ha incorporado al nuevo modelo de parches basado en etiquetas de AMS Patch Orchestrator, puede utilizar etiquetas para aplicar la configuración de parches a un conjunto preciso de recursos,

denominado grupo de parches, que van desde una instancia hasta todas las instancias. [Para obtener información sobre las etiquetas AMS, consulte Uso de etiquetas.](#) En la siguiente sección se proporcionan instrucciones sobre cómo configurar las etiquetas de Patch Orchestrator.

Los parches se instalan durante las ventanas de parches que defina en [SSM Patch Window | Create](#). Cada ventana de parches es una ventana de mantenimiento de AWS Systems Manager que se ejecuta según el programa que elija, tiene una duración configurada y se aplica a un grupo de parches. Las instancias que no forman parte de una ventana de parches específica se parchean durante el período de mantenimiento predeterminado que usted define al incorporarse a Patch Orchestrator.

 Important

Si está previsto que se ejecuten varios períodos de mantenimiento de parches al mismo tiempo, deben tener menos de 1001 instancias procesándose en un momento dado. Se trata de una limitación de AWS Systems Manager. AMS recomienda al menos una hora por cada cincuenta instancias.

De forma predeterminada, todos los parches del sistema operativo (SO) proporcionados por el proveedor se instalan durante un período de mantenimiento o durante un parche bajo demanda. Esto se denomina línea base de parches predeterminada. Si desea restringir los parches que se instalan, puede definir una línea base de parche personalizada con una línea base de parches creada CTs (por OSes), consulte la [subcategoría](#) Parches. Por ejemplo, puede usar una línea base de parches personalizada para que solo se instalen las actualizaciones de seguridad críticas e importantes para uno o más grupos de parches.

Una vez instalados los parches en una instancia, la instancia se reinicia. Las notificaciones de los parches se envían antes y después de aplicar el parche, y se envía un recordatorio adicional 96 horas antes del inicio programado. Además, AMS aplica actualizaciones a las herramientas de administración de infraestructura (como el agente SSM de AWS) durante el período de mantenimiento seleccionado.

 Important

AMS está desaprobandando los informes mensuales sobre el cumplimiento de los parches en las instancias a las que les faltan parches y no los enviará cada mes. Este cambio se ha realizado teniendo en cuenta los informes operativos de autoservicio publicados

recientemente, que se actualizan cada 24 horas y están disponibles a pedido y proporcionan los datos más recientes y detallados. Para obtener más información sobre los informes, consulte Informes de autoservicio. Para obtener más información sobre los informes, consulte [Informes de autoservicio](#).

Para obtener más información sobre las notificaciones, consulte [Notificaciones de parches](#).

Uso de Patch Orchestrator

Habilite AMS Patch Orchestrator para su cuenta enviando una solicitud de servicio que incluya los siguientes detalles:

- Categoría: Otros
- Asunto: A bordo de Patch Orchestrator
- Correos electrónicos de CC: las direcciones de correo electrónico de CC reciben notificaciones cuando cambia el estado de esta RFC de incorporación
- Detalles: pegue la siguiente información en el correo electrónico e indique sus valores. Tenga en cuenta que ThirdTagKey es opcional. Para ver recomendaciones y ejemplos, consulte la siguiente tabla.

```
Default maintenance window Schedule:  
Default Maintenance Window Schedule TimeZone:  
Default Maintenance Window Duration:  
Default Maintenance Window Cutoff:  
Default Patch Backup Retention In Days:  
Default Maintenance Window Notification Emails:  
First Tag Key:  
Second Tag Key:  
Third Tag Key:
```

En la siguiente tabla se describen el formato y las recomendaciones para los valores proporcionados.

Configuraciones de parches basadas en etiquetas de Patch Orchestrator

Nombre del parámetro	Información	Recomendación o ejemplo
Programa de ventanas de mantenimiento predeterminado	El cronograma del período de mantenimiento predeterminado en forma de cron o expresión de tasa. Por ejemplo: • <code>cron(0 3 ? * 6L *)</code>: el último viernes de cada mes a las 03:00 • <code>rate(7 days)</code>: Cada siete días Para obtener más información sobre la creación de expresiones cron y enlaces a recursos de expresiones cron y rate, consulta Cron y rate expresiones para ver los períodos de mantenimiento.	Recomendamos que el período se ejecute al menos una vez al mes en un día laborable constante.
Ventana de mantenimiento predeterminada: programa la zona horaria	La zona horaria en la que se ejecuta el período de mantenimiento predeterminado se basa en el formato de la Autoridad de Números Asignados de Internet (IANA).	Por ejemplo: • <code>America/Los_Angeles</code> • <code>etc/UTC</code>
Duración predeterminada del período de mantenimiento	La duración del período de mantenimiento predeterminado en horas.	Al menos 1 hora por cada 50 instancias, más 2 horas de cierre.
Límite predeterminado de la ventana de mantenimiento	El número de horas que faltan para que finalice el período de mantenimiento	Al menos 2 horas.

Nombre del parámetro	Información	Recomendación o ejemplo
	predeterminado en el que no se inician nuevos comandos de aplicación de parches. Este intervalo existe para dejar tiempo suficiente para que se complete la aplicación de parches antes de que finalice el período.	
Retención predeterminada de Patch Backup en días (opcional)	El tiempo predeterminado en días para conservar los puntos de restauración de EBS creados antes de aplicar parches a las instancias.	Recomendamos mantener el valor predeterminado, que es 60.
Correos electrónicos de notificación de la ventana de mantenimiento predeterminada	De una a cinco direcciones de correo electrónico o listas de distribución para recibir notificaciones sobre el estado predeterminado de los parches del período de mantenimiento.	Recomendamos utilizar listas de distribución grupales en lugar de correos individuales.
Primera clave de etiqueta	La primera clave de etiqueta que se utilizará para crear los valores de las etiquetas de su grupo de parches.	Por ejemplo, . Appld Especificue nulo si ya ha definido sus propios grupos de parches con una etiqueta de grupo de parches.
Segunda clave de etiqueta	La segunda clave de etiqueta que se utilizará para crear los valores de las etiquetas de su grupo de parches.	Por ejemplo, Medio ambiente. Especifique nulo si ya ha definido sus propios grupos de parches con una etiqueta de grupo de parches.

Nombre del parámetro	Información	Recomendación o ejemplo
Tercera clave de etiqueta (opcional)	La tercera clave de etiqueta opcional que se utilizará para crear los valores de las etiquetas de su grupo de parches.	Por ejemplo, Grupo.

Una vez que te hayas incorporado al nuevo modelo de servicio de parches de Patch Orchestrator, todas las instancias de tu cuenta debidamente etiquetadas pertenecerán a un grupo de parches con una etiqueta de grupo de parches. Patch Orchestrator usa tu etiqueta de grupo de parches existente o una etiqueta creada por AMS que consta de los dos o tres valores de etiqueta concatenados que especificaste durante la incorporación de Patch Orchestrator. Por ejemplo, {} - {} - {}*Tag Value 1. Tag Value 2 Tag Value 3* AMS actualiza estas etiquetas del grupo de parches aplicadas por AMS cada 12 horas. Si es necesario, puede actualizar los valores de las etiquetas del grupo de parches con los tipos de cambio [Tag | Update \(se requiere revisión\)](#) o [Tag | Update \(se requiere revisión\)](#).

Por ejemplo, si tu EC2 instancia de Amazon tiene los siguientes pares de etiquetas key:value:

- AppId:MyApplication
- Environment:Production
- Group:1

Durante la incorporación, especificaste las siguientes claves de etiqueta:

- First Tag Key = AppId
- Second Tag Key = Environment
- Third Tag Key = Group

AMS crea la siguiente etiqueta de grupo de parches y la aplica a sus instancias: Patch Group:MyApplication-Production-1.

 Note

Las alertas de error de los parches no se crean para las instancias que tienen sistemas operativos no compatibles o que se detienen durante el período de mantenimiento.

Requisitos previos de Patch Orchestrator

El flujo de trabajo de Patch Orchestrator se dirige a las EC2 instancias de Amazon que están parcheadas con la última versión del documento de automatización de System Manager:.

`AWSManagedServices-PatchInstanceFromMaintenanceWindow`

Como parte del flujo de trabajo del documento, el documento de comandos de ejecución «AWS-RunPatchBaseline» se ejecuta en cada una de las EC2 instancias de Amazon de los miembros del grupo de parches. Para obtener más información, consulte [Acerca del documento SSM AWS-RunPatchBaseline](#).

Requisitos:

- EC2 Instancia de Amazon implementada desde Amazon Machine Image (AMI) proporcionada por AMS o en una AMI a través del CT «Stack from migration partner migration instance» (ct-257p9zjk14ija).
- Conexión a Internet de salida habilitada. Para firewall/proxy las soluciones, el requisito es permitir que Windows Update Endpoint, el repositorio de and/or Linux refleje los puntos de enlace, la configuración del proxy del administrador del sistema de AWS y la configuración del proxy de metadatos. Para obtener más información, consulte [Configurar el agente SSM para usar un proxy](#) y [Usar un](#) proxy HTTP
- El rol de IAM coincide con el acceso mínimo permisivo para el servicio SSM del rol de IAM. `customer-mc-ec2-instance-profile`
- Recomendamos 10 GB de espacio disponible en la partición raíz. Para el sistema operativo Linux, hay al menos 2 GB disponibles en la `/var` partición.
- Autoridad de certificación válida y activa para la descarga de actualizaciones.
- Windows Server Update Services (WSUS): el registro incluye, entre otros: `DisableWindowsUpdateAccess`, `NoWindowsUpdate`; Las actualizaciones automáticas no deben impedir el funcionamiento del proceso de Windows Update.

Validación:

- Para las instancias de sistema operativo Linux que utilizan el administrador de paquetes yum, puede validar la disponibilidad de las actualizaciones ejecutando `#yum check-update`
- Para los sistemas operativos Linux RedHat 5.7 y posteriores, 6.1 y 7.0 y posteriores; las EC2 instancias de Amazon migradas a su cuenta AMS mediante el CT «Stack from migration partner migration instance» (ct-257p9zjk14ija), debe validar el estado del administrador de suscripciones para garantizar el rendimiento de la actualización.
- En el sistema operativo Windows, habilite Windows Server Update Services (WSUS). Ninguna política local debe bloquear la capacidad de WSUS para escanear o instalar actualizaciones. Una vez registrado como administrador, puede validarlo escaneando las actualizaciones disponibles desde la consola de Windows Update Service. Las versiones del sistema operativo Windows Server, incluidas la 2012R2, la 2016 y la 2019, tienen la configuración predeterminada de Windows Update para descargar e instalar. Puede configurar los ajustes que desee antes del escaneo. En versiones posteriores del sistema operativo, esta operación puede activar la instalación; configure previamente el comportamiento deseado.
- Solicita la validación al equipo de operaciones de AMS enviando una solicitud de servicio: «Documento de AWSManagedServices-CheckPatchingPrerequisites automatización que se ejecutará en una EC2 instancia de Amazon para evaluar la disponibilidad de los parches».

Note

Las alertas de error de los parches no se crean para las instancias que tienen sistemas operativos no compatibles o que se detienen durante el período de mantenimiento.

Ventanas de parches

Las instancias de un grupo de parches específico se parchean durante una o más ventanas de parches. Las ventanas de parches se ejecutan según un cronograma definido como una expresión cron o tasa, y tienen una duración configurable destinada a mantener las interrupciones relacionadas con los parches dentro de un intervalo de tiempo elegido. AMS recomienda crear varias ventanas de parches que cubran todas las instancias de forma conjunta, de forma que se adapten a las rutinas de aplicación de parches específicas de su organización, y utilizar la ventana de mantenimiento predeterminada como alternativa. Las ventanas de parches se crean con el tipo de cambio RFC Deployment | Patching | SSM patch window | Create (ct-0el2j07llrxs7). Todas las instancias que no forman parte de una ventana de parches se parchean durante el período de mantenimiento predeterminado que se crea durante la incorporación.

Normalmente, no es necesario actualizar una ventana de parches para incluir nuevas instancias. Por lo general, esto se hace modificando las etiquetas de las instancias. Por ejemplo, considere la siguiente secuencia de eventos:

1. Dos instancias se etiquetan con `conAppId:MyApplication,Environment:Production,Group:1`.

Esto genera una etiqueta en estas instancias, suponiendo que la primera clave de etiqueta = `AppId`, la segunda clave de etiqueta = entorno, la tercera clave de etiqueta = grupo y se crea una ventana de parches para el grupo de parches `MyApplication -Production-1`.

2. Se crean tres instancias más y se etiquetan con `conAppId:MyApplication,,Environment:Production Group:1`

Esto produce una etiqueta para Patch Group: `MyApplication -Production-1`.

No es necesario cambiar la ventana de parches, ya que recoge las cinco instancias en el momento de la próxima ejecución programada.

Para obtener un análisis más detallado y un tutorial sobre el uso de este tipo de cambio, consulte [SSM Patch Window | Create](#).

Notificaciones de parches

Important

A partir del 1 de febrero de 2025, los clientes de AMS dejarán de recibir notificaciones de las ventanas de mantenimiento de parches vacías en sus cuentas gestionadas.

Las direcciones de correo electrónico suscritas (hasta cinco) recibirán un correo similar al siguiente justo antes de que comience el período de mantenimiento del parche:

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME was started at:
2020-02-21T12:02:18.196Z.
Details:
Maintenance Window AccountId: YOUR_ACCOUNT_ID
Maintenance Window Region: YOUR_ACCOUNT_REGION
Maintenance Window Id: THE_MAINTENANCE_WINDOW_ID
Maintenance Window Name: THE_MAINTENANCE_WINDOW_NAME
```

Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*

Maintenance Window ExecutionId: *THE_EXECUTION_ID*

Targets:

InstanceId	InstanceName	StackId
-----	-----	-----
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>

A follow-up message with a detailed report is sent as soon as the maintenance window is over.

Please raise a service request if you have any inquiries about AMS Patch Orchestrator by following this URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

Al final de la actividad del parche, las direcciones de correo electrónico suscritas reciben un correo similar al siguiente:

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* ended at:
2020-02-21T12:03:20.058Z, with status: SUCCESS.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*

Maintenance Window Region: *YOUR_ACCOUNT_REGION*

Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*

Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*

Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*

Maintenance Window ExecutionId: *THE_EXECUTION_ID*

Targets:

RfcId	InstanceId	InstanceName	StackId
Status			
-----	-----	-----	
-----	-----		

THE_RFC_ID *THE_INSTANCE_ID* *THE_INSTANCE_NAME* *THE_STACK_NAME*
STATUS

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

Please raise an Incident if an issue is impacting one of your production applications by following this URL:

<https://console.aws.amazon.com/managedservices/incident/new>

Kind Regards,

Amazon Web Services
 Amazon Managed Services
 Patch Team

Cada 96 horas, el sistema de parches AMS identifica todos los próximos períodos de mantenimiento gestionados con parches dentro de esas 96 horas y envía una notificación de recordatorio a todas las direcciones de correo electrónico suscritas que estén dentro de ese período de 96 horas. Esto podría ocurrir tan solo una hora antes de que finalice el período o las 96 horas completas. Por ejemplo:

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* will start at:
 2020-05-06T16:35:36.523Z.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
 Maintenance Window Region: *YOUR_ACCOUNT_REGION*
 Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
 Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
 Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
 Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z
 Maintenance Window Schedule: rate(24 hours)
 Maintenance Window Timezone: *THE_TIMEZONE*

At this time, these are the instances in the "*PATCH_GROUP_NAME*" Patch Group:

InstanceId	InstanceName	StackId	InstanceState

<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped

<code>THE_INSTANCE_ID</code>	<code>THE_INSTANCE_NAME</code>	<code>THE_STACK_NAME</code>	running/stopped
<code>THE_INSTANCE_ID</code>	<code>THE_INSTANCE_NAME</code>	<code>THE_STACK_NAME</code>	running/stopped

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

If you would like to disable this maintenance window or you have inquires about the AMS Patch Orchestrator click on the following URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

If you would like to delete this maintenance window, you can run the CT with id "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

líneas de base de revisiones

De forma predeterminada, todos los parches del sistema operativo (SO) proporcionados por el proveedor se instalan utilizando la línea base de parches predeterminada por AMS. Si desea restringir los parches que se instalan, si lo desea, puede crear una línea base de parches utilizando el tipo de cambio RFC Deployment | Patching | SSM patch baseline | Create **OS** (el ID de CT varía según el sistema operativo).

[Para obtener información sobre el uso de estos tipos de cambios, consulte la subcategoría Parches.](#)

Etiquetas reservadas de Patch Orchestrator

Patch Orchestrator también genera las siguientes etiquetas que no se pueden modificar:

- **AMSPatchGrupo**: esta etiqueta se usa para generar el valor de las etiquetas de Patch Group. No debes modificar el AMSPatch grupo. Puedes modificar la etiqueta «Grupo de parches» si quieres usar un valor personalizado de «Grupo de parches». Patch Orchestrator sigue generando un valor para el AMSPatch grupo en función de las claves de etiquetas proporcionadas durante la incorporación, pero no modificará el valor de la etiqueta «Grupo de parches» si tú lo has

establecido en un valor personalizado. Para dejar de usar un valor personalizado de «Grupo de parches», puedes configurar el valor de «Grupo de parches» para que coincida con el valor de la AMSPatch etiqueta de grupo.

- AMSDefaultPatchGroup— Esta etiqueta indica si una instancia forma parte del período de mantenimiento predeterminado, con un valor verdadero o falso. Si el grupo de parches de una instancia no está asignado a una ventana de mantenimiento, este valor se establece en True.

Aplicación de parches bajo demanda

AMS tiene un tipo de cambio que se adapta a la línea base del parche, para que pueda ejecutar un parche en las instancias bajo demanda. Puede ser la línea base predeterminada que establezca al incorporarse o la línea base del parche de Patch Orchestrator Systems Manager que establezca con el tipo de cambio de la línea base del parche (el ID de CT varía según el sistema operativo).

Puede utilizar el tipo de cambio de parches bajo demanda con o sin Patch Orchestrator.

Para obtener información sobre el uso de este tipo de cambio, consulte [On Demand Patching](#) | Run.

Note

No puede usar instancias que formen parte de un grupo de Auto Scaling en un tipo de cambio de parches bajo demanda.

Parcheo estándar AMS

AMS apoya a los clientes actuales que utilizan el modelo de parches estándar de AMS, pero este modelo no está disponible para nuevos clientes y se está retirando en favor de AMS Patch Orchestrator.

El contenido habitual de los parches estándar de AMS incluye las actualizaciones de los proveedores para los sistemas operativos compatibles y el software preinstalado con los sistemas operativos compatibles (por ejemplo, IIS y Apache Server).

Durante la incorporación de AMS, se especifican los requisitos de aplicación de los parches, la política, la frecuencia y las ventanas de parches preferidas. Gracias a estas configuraciones, puede evitar que las aplicaciones se desconecten de una sola vez para aplicar parches a la infraestructura, de modo que puede controlar qué infraestructura se parchea y cuándo.

 Note

El proceso de aplicación de parches descrito en este tema solo se aplica a sus pilas. La infraestructura de AMS se parchea durante un proceso independiente. 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. Puede configurar la ventana de parches de AMS en el momento de la incorporación o aprobar o rechazar la notificación mensual del servicio de parches.

AMS escanea periódicamente las EC2 instancias gestionadas de Amazon en busca de actualizaciones disponibles a través de la funcionalidad de actualización del sistema operativo. También proporcionamos actualizaciones periódicas a la base de AMS Amazon Machine Images (AMIs) compatible con nuestro entorno.

Una vez validadas, las versiones de AMI de AMS se comparten con todas las cuentas de AMS. Puede ver las versiones de las AMI de AWS disponibles mediante la llamada a la EC2 API de [DescribeImages](#) Amazon o la EC2 consola de Amazon. Para encontrar los AMS disponibles AMIs, consulte [Encuentra AMI IDs, AMS](#).

AMS ejecuta programas de aplicación de parches ad hoc solo cuando usted lo solicita. Anteriormente, AMS enviaba una notificación; actualmente, no envía ninguna notificación.

 Note

De forma predeterminada, AMS usa Systems Manager para aplicar parches haciendo que el administrador de paquetes (Linux) o el servicio de actualización del sistema (Windows) consulten su repositorio predeterminado para ver qué paquetes nuevos están disponibles. Si, durante sus day-to-day operaciones, ha instalado un paquete en un host Linux mediante el administrador de paquetes predeterminado, ese administrador de paquetes también selecciona los paquetes nuevos para ese software cuando están disponibles. En tal caso, es posible que desee realizar una acción de parcheo (descrita en esta sección) para excluirse de esa instancia.

Sistemas operativos compatibles

Sistemas operativos compatibles (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (fecha prevista de finalización del soporte para AMS el 30 de junio de 2026)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux (RHEL) 9.x, 8.x
- Servidor SUSE Linux Enterprise 15 SP6
- SUSE Linux Enterprise Server para SAP 15 SP3 y versiones posteriores
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Sistemas operativos compatibles () ARM64

- Amazon Linux 2023
- Amazon Linux 2 (fecha prevista de finalización del soporte para AMS el 30 de junio de 2026)

Parches compatibles

AWS Managed Services admite la aplicación de parches principalmente a nivel del sistema operativo. Los parches que se instalan pueden variar según el sistema operativo.

Important

Todas las actualizaciones se descargan de los repositorios remotos del servicio de referencia de parches de Systems Manager configurados en la instancia y se describen más adelante en este tema. La instancia debe poder conectarse a los repositorios para poder realizar los parches.

Para excluirte del servicio básico de parches en los repositorios que entreguen paquetes que desees mantener tú mismo, ejecuta el siguiente comando para deshabilitar el repositorio:

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

Recupera la lista de repositorios actualmente configurados con el siguiente comando:

```
yum repolist
```

- Repositorios preconfigurados de Amazon Linux (normalmente cuatro):

ID de repositorio	Nombre del repositorio
amzn-main/latest	AMZN-base principal
amzn-updates/más recientes	Base de actualizaciones de AMZN
epel/x86_64	Paquetes adicionales para Enterprise Linux 6: x86_64
pbis	Actualizaciones de paquetes PBIS

- Repositorios preconfigurados de Red Hat Enterprise Linux (cinco para Red Hat Enterprise Linux 7 y cinco para Red Hat Enterprise Linux 6):

ID de repositorio	Nombre del repositorio
RHUI-Region- -7/x86_64 client-config-server	Conjunto de configuración de clientes de Red Hat Update Infrastructure 2.0
RHUI-Region-/7Server/x86_64 rhel-server-releases	Servidor Red Hat Enterprise Linux 7
Región RHUI: /7server/x86_64 rhel-server-releases	Red Hat Enterprise Linux Server 7 RH Common () RPMs
epel/x86_64	Paquetes adicionales para Enterprise Linux 7: x86_64
pbis	Actualizaciones de paquetes PBIS

ID de repositorio	Nombre del repositorio
Región RHUI- -6 client-config-server	Red Hat Update Infrastructure 2.0
Región RHUI- rhel-server-releases	Servidor Red Hat Enterprise Linux (6) RPMs
RHUI - Región - rhel-server-rh-common	Red Hat Enterprise Linux Server 6 RH Common () RPMs
Repel	Paquetes adicionales para Enterprise Linux 6: x86_64
pbis	Actualizaciones de paquetes PBIS

- Repositorios preconfigurados de CentOS 7 (normalmente cinco):

ID de repositorio	Nombre del repositorio
base/7/x86_64	CentOS-7 - Base
actualizaciones/7/x86_64	CentOS-7 - Actualizaciones
extras/7/x86_64	CentOS-7 - Extras
epel/x86_64	Paquetes adicionales para Enterprise Linux 7: x86_64
pbis	Actualizaciones de paquetes PBIS

- Para Microsoft Windows Server, todas las actualizaciones se detectan e instalan mediante el Agente de Windows Update, que está configurado para usar el catálogo de Windows Update (esto no incluye las actualizaciones de Microsoft Update).

En los sistemas operativos Microsoft Windows, Patch Manager utiliza el archivo cab wsusscn2.cab de Microsoft como fuente de las actualizaciones de seguridad del sistema operativo disponibles. Este archivo contiene información sobre las actualizaciones relacionadas con la seguridad publicadas por Microsoft. Patch Manager descarga este archivo de Microsoft con regularidad y lo utiliza para actualizar el conjunto de parches disponibles para las instancias de Windows. El

archivo contiene únicamente las actualizaciones que Microsoft identifica como relacionados con la seguridad. Cuando la información del archivo se procesa, Patch Manager también elimina las actualizaciones que se han reemplazado por actualizaciones posteriores. Por lo tanto, solo se muestra la última actualización y, en su caso, están disponibles para su instalación. Por ejemplo, si KB4 012214 reemplaza KB3135456, solo KB4 012214 estará disponible como actualización en Patch Manager.

Para obtener más información sobre el archivo wsusscn2.cab, consulte el artículo de Microsoft [Uso de WUA para buscar actualizaciones sin conexión](#).

Diseño de parches e infraestructura

AMS emplea diferentes métodos de aplicación de parches en función del diseño de la infraestructura: mutable o inmutable (para obtener definiciones detalladas, consulte). [Términos clave de AMS](#)

Con las infraestructuras mutables, los ingenieros de operaciones de AMS instalan las actualizaciones directamente en las EC2 instancias de Amazon, de forma individual, mediante una metodología tradicional in situ. Este método de aplicación de parches se usa para pilas que no son grupos de Auto Scaling y contienen una sola EC2 instancia de Amazon o varias instancias. En este escenario, reemplazar la AMI en la que se basaba la instancia o la pila destruiría todos los cambios realizados en ese sistema desde que se implementó por primera vez, por lo que no se hace. Las actualizaciones se aplican al sistema en ejecución y es posible que se produzca un tiempo de inactividad del sistema (según la configuración de la pila) debido al reinicio de la aplicación o del sistema. Esto se puede mitigar con una estrategia de Blue/Green actualización. Para obtener más información, consulte [AWS CodeDeploy Introduce Blue/Green las implementaciones](#).

Con infraestructuras inmutables, el método de aplicación de parches es el reemplazo de la AMI. Las instancias inmutables se actualizan de manera uniforme mediante una AMI actualizada que reemplaza a la AMI especificada en la configuración del grupo de Auto Scaling. Las versiones de AMS se actualizan (es decir, se parchean) AMIs todos los meses, normalmente la semana del martes de parches. En la siguiente sección se describe cómo funciona esto.

Cómo funcionan los parches estándar AMS

AMS utiliza el servicio Run Command de Systems Manager para la aplicación periódica de parches críticos, mensuales y según sea necesario, con dos métodos principales de aplicación de parches, in situ y reemplazo de la AMI, según la estrategia de despliegue de la infraestructura (mutable o

inmutable). En esta sección se describen el servicio de parches, los tipos, los métodos y los procesos de AMS.

AMS define dos tipos de parches, que se programan de forma diferente:

- Parches críticos: las actualizaciones se aplican lo más rápido posible, tras la aceptación del aviso.
- Parches estándar: los proveedores del sistema operativo se actualizan periódicamente y se aplican mensualmente.

Los parches se aplican mediante parches in situ o mediante el reemplazo de la AMI (previa solicitud).

Escaneo de actualizaciones

AMS utiliza el [Amazon EC2 Run Command Service](#) para ponerse en contacto con sus EC2 pilas de Amazon e implementar los scripts de escaneo y aplicación de parches necesarios. AMS utiliza el componente nativo de administración de paquetes ya instalado en el sistema operativo compatible para realizar todo el comportamiento de escaneo y aplicación de parches necesario en la EC2 pila de Amazon. Para Red Hat y Amazon Linux, el servicio usa yum. Para Windows, el servicio usa el agente de Windows Update.

Los escaneos se realizan a diario mediante [SSM Maintenance Windows](#) y el RunPatchBaseline documento AWS- predeterminado de AMS. Se escanean todas las EC2 pilas de Amazon accesibles mediante los repositorios de actualizaciones para Linux y Windows. El proceso de parcheo de AMS detecta todas las EC2 pilas de Amazon a las que se puede acceder y, a continuación, realiza los escaneos en un proceso por lotes para que la pila permanezca siempre en buen estado, incluso si se produce un error al ejecutar el escaneo. Luego, los resultados del escaneo se guardan para cada EC2 pila de Amazon.

Para ver los resultados del escaneo de una pila o instancia, envía una solicitud de servicio con el ID de pila o el ID de instancia.

El proceso de aplicación de parches de AMS predeterminado consiste en instalar todos los parches disponibles, independientemente de su clasificación o gravedad (por ejemplo, si son críticos o estándares). La excepción son los parches que se hayan excluido explícitamente de la pila (no se deben excluir los parches definidos como obligatorios por AMS).

Se le envía una notificación del servicio de aplicación de parches 14 días antes del período de mantenimiento propuesto. Esto le da tiempo para probar los parches propuestos y aceptarlos o rechazarlos. Si no respondes a la notificación del servicio de parches, tus instancias no están

parcheadas. Cuando llega el momento de instalar los parches, AMS crea una solicitud de cambio (RFC) para cada pila y esa RFC aparece en la lista de RFC de su cuenta.

AMS configuró la ventana y el aviso de mantenimiento

Con los parches configurados por AMS, cada cuenta tiene un período de mantenimiento mensual, que usted define al incorporar su cuenta. 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.

La ventana de aplicación de parches es diferente. La solicitud de servicio saliente de aplicación de parches (también conocida como notificación de servicio) incluye una ventana de parches sugerida.

Note

Para obtener información sobre cómo responder a la notificación del servicio de aplicación de parches, consulte [Acciones que puede realizar en la aplicación de parches estándar de AMS](#)

La notificación del servicio de aplicación de parches se envía por correo electrónico a la dirección de correo electrónico de contacto registrada en su cuenta. La notificación incluye un enlace a la consola de AWS Support donde puede responderla. También puede responder a la notificación mediante la página de solicitud de servicio de AMS. La notificación de servicio incluye:

- Una lista de las actualizaciones IDs (CSUs IUs, y OUs) que se aplican a la pila y las actualizaciones que ha solicitado que se excluyan de la aplicación de parches (si las hubiera).
- IDs de las instancias que se verán afectadas.
- Una ventana de parcheo propuesta en la que se aplicarán las actualizaciones. Puede solicitar una ventana de aplicación de parches diferente.
- Una solicitud para que acepte el parche propuesto o solicite información adicional. AMS le da tiempo para probar el impacto de las actualizaciones y aprobar o rechazar los parches, o solicitar que se excluyan actualizaciones específicas. Si necesita más tiempo para realizar las pruebas y desea que las actualizaciones se apliquen después de las pruebas, responda a la notificación de servicio y describa lo que desea, o envíe una solicitud de servicio para solicitar una nueva RFC de parche basándose en los detalles de la RFC anterior. Si no respondes en absoluto a la notificación de servicio, no se tomará ninguna medida para aplicar los parches y se cancelará la RFC.

Si aprueba la notificación de servicio, AMS ejecuta la RFC del parche y aplica las actualizaciones dentro del plazo de parches acordado, de acuerdo con el compromiso de servicio.

Una vez finalizada la aplicación de parches, AMS le envía una correspondencia en la solicitud de servicio con un resumen del resultado de la actividad de aplicación de parches (es decir, si se ha realizado correctamente o no).

Parcheo in situ

La aplicación de parches in situ hace referencia a un método en el que AMS inicia sesión en cada instancia de la pila y aplica los parches.

La aplicación de parches in situ se realiza en infraestructuras mutables que utilizan EC2 instancias de Amazon que ejecutan un sistema operativo compatible. Los parches aplican todas las actualizaciones no excluidas disponibles hasta ese momento. Cuando se publican los parches críticos, hay un proceso adicional de aplicación de parches críticos.

Parcheo estándar: in situ

La aplicación estándar de parches se realiza según el calendario de parches acordado que se indica en la notificación del servicio de parches, e incluye las actualizaciones periódicas de los parches que no se consideran críticas.

Antes del plazo de aplicación de parches propuesto, y con su respuesta afirmativa a la notificación, se crea una RFC de parche que aparece en su panel de RFC.

Parcheo crítico: in situ

Cuando un proveedor de sistemas operativos publica una actualización de seguridad importante, AMS le notifica la RFC del parche enviándole una notificación de servicio (al correo electrónico de contacto de su cuenta) para cada paquete, de acuerdo con el compromiso de servicio de AMS. La notificación de servicio incluye lo siguiente para cada actualización:

- Fecha de lanzamiento de la actualización
- Criticidad de la actualización
- Detalles de la actualización (referencia de KB, etc.)
- IDs de las pilas afectadas

Puede probar las actualizaciones que aparecen en la notificación y aprobar o rechazar los parches respondiendo a la notificación de servicio. Si aprueba la notificación, debe proporcionar una ventana de parches específica por pila para instalar las actualizaciones.

 Note

Los períodos de revisión que estén dentro de las 24 horas siguientes a la respuesta a la notificación del servicio pueden reprogramarse en función de la capacidad disponible.

Si no responde en un plazo de 10 días o si rechaza el parche propuesto, el parche se cancela.

Si desea aplicar las actualizaciones una vez transcurrido el período permitido (indicado en la notificación), envíe una solicitud de servicio para establecer un nuevo programa de parches en función de los detalles de la notificación anterior.

Si aprueba la notificación de servicio, AMS aplicará las actualizaciones dentro del período de parches especificado, de acuerdo con el compromiso de servicio.

En el caso de actualizaciones múltiples, puede excluir actualizaciones específicas de la aplicación de parches especificando las actualizaciones que se van a excluir en su respuesta a la notificación de servicio.

AMS le envía una notificación de servicio para cada pila, con el resultado de cada actualización (es decir, si se ha realizado correctamente o no).

La AMI actualiza los parches (utilizando los parches AMIs para los grupos de Auto Scaling)

Los parches de reemplazo de la AMI se realizan en infraestructuras inmutables mediante la actualización del ID de AMI que está configurado para implementar nuevas instancias de Amazon en EC2 un grupo de Auto Scaling.

Amazon Machine Images (AMIs) se publica periódicamente para los sistemas operativos compatibles. Los proveedores de sistemas operativos publican nuevos parches periódicamente. AMS toma la AMI proporcionada por Amazon, la actualiza con los últimos parches y, a continuación, añade los componentes adecuados para que pueda funcionar en el entorno AMS. Luego, pone la nueva AMI de AMS a disposición de todos los clientes de AMS al compartir la AMI con las cuentas. Las pilas de grupos de Auto Scaling se pueden actualizar mensualmente con estos AMS recién lanzados. AMIs El siguiente gráfico ilustra cómo AMIs se utilizan sus entornos en AMS.

Los grupos de Auto Scaling crean sus instancias en función de la AMI configurada para el grupo de Auto Scaling. Cuando se actualizan los recursos compartidos de AMS AMIs, dispone de las siguientes opciones en función de cómo gestione las actualizaciones de AMI:

- Si utiliza una herramienta de despliegue de aplicaciones (por ejemplo UserData, CodeDeploy,, etc.) que personalice las instancias automáticamente una vez creadas, puede hacer lo siguiente:
 - Responda a la notificación del servicio de aplicación de parches o envíe una solicitud de servicio para que la AMI de AMS más reciente sustituya a la AMI de configuración de su grupo de Auto Scaling actual. Tras sustituir el ID de AMI en la configuración de los grupos de Auto Scaling, AMS inicia las actualizaciones sucesivas de las instancias y las configuraciones de las instancias del grupo de Auto Scaling (por ejemplo, la instalación de aplicaciones, scripts de arranque, etc.) se aplican automáticamente a las nuevas instancias creadas con la nueva AMI de AMS.
- Si utiliza una custom/golden AMI en la configuración de sus grupos de Auto Scaling, puede:
 - Crea una instancia con la nueva AMI de AMS, personaliza la instancia y crea una nueva AMI dorada. Comparta la nueva AMI dorada con AMS mediante la EC2 consola de Amazon y envíe una solicitud de servicio a AMS para actualizar la configuración de sus grupos de Auto Scaling para usar su nueva AMI personalizada.
 - Comparte tu AMI dorada actual con AMS mediante la EC2 consola de Amazon y envía una solicitud de servicio para que AMS actualice tu AMI dorada. Para ello, AMS crea una instancia a partir de tu AMI dorada, aplica los parches a esa instancia, crea una nueva AMI dorada para ti y, a continuación, actualiza la configuración de tus grupos de Auto Scaling para usar la nueva AMI. El inconveniente es que AMS no puede comprobar si su nueva AMI personalizada funciona de la forma que usted desea. En su lugar, deberías probar la instancia creada con la nueva AMI y comprobar que todo funciona correctamente antes de crear una nueva AMI dorada, compartirla y solicitar que AMS actualice tus grupos de Auto Scaling. AMS no recomienda esta opción.

Parcheo estándar: actualizaciones de AMI

Cada mes, AMS publica nuevas Amazon Machine Images (AMIs) con mejoras en el servicio y nuevos parches que se aplican a AMIs.

Note

Los nuevos AMS AMIs se generan después del martes de parches desde la versión actualizada de AWS AMIs. A continuación, AMS los prueba antes de ponerlos a disposición.

Tras AMIs pasar las nuevas pruebas, las acciones de AMS se actualizaron AMIs a cuentas gestionadas.

Parches críticos: actualizaciones de la AMI

Cuando es necesario, AMS proporciona AMIs actualizaciones con los parches de seguridad críticos publicados desde la última versión mensual de la AMI.

El proceso de actualizaciones de seguridad críticas para infraestructuras inmutables es idéntico al proceso mensual de AMI para infraestructuras inmutables, excepto que se crea una nueva AMI de AMS fuera del horario normal (martes de parches), en función del lanzamiento de nuevas actualizaciones críticas. AMS pone a disposición una nueva AMI con los parches de seguridad críticos de acuerdo con los acuerdos de nivel de servicio (SLAs) definidos para su cuenta. Las actualizaciones de AMS de los grupos de Auto Scaling se realizan únicamente a pedido. Utilice una solicitud de servicio para enviar solicitudes de reemplazo de la AMI.

Fallos de parcheo estándar AMS

En caso de errores en las actualizaciones, AMS realiza un análisis para determinar la causa del error y le comunica el resultado del análisis. Si el error se debe a AMS, volvemos a intentar realizar las actualizaciones si se encuentra dentro del período de mantenimiento. De lo contrario, AMS crea notificaciones de servicio para la actualización fallida de la instancia y espera tus instrucciones.

En el caso de errores atribuibles a su sistema, puede enviar una solicitud de servicio con una nueva RFC de parche para actualizar las instancias.

Acciones que puede realizar en la aplicación de parches estándar de AMS

Además de probar los nuevos AMIs, hay varias medidas que puede tomar para administrar los parches de su infraestructura:

- Si la prueba de las actualizaciones ha tardado más de lo que permitía la ventana de parches, puede solicitar que AMS aplique las actualizaciones que se cancelaron cuando esté listo enviando una solicitud de servicio (utilice los detalles de la notificación de servicio original como base).
- Puede solicitar que se aplique una actualización importante (IU) u otra actualización (OU) antes de la siguiente ventana de actualización automática enviando una solicitud de servicio con una lista de las actualizaciones, las instancias aplicables y otros detalles, según proceda. Como este CT no

está automatizado, se tarda más en programarlo y ejecutarlo. Compruebe los objetivos del nivel de servicio (SLOs) durante el tiempo adecuado. Para obtener más información, consulte [Objetivos de nivel de servicio de AMS \(SLOs\)](#).

Además, puede utilizar los AMS existentes y parchados AMIs para crear diseños personalizados AMIs. Para obtener más información, consulte [AMI | Create](#).

Note

No puede solicitar una nueva AMI de AMS en función de una actualización importante u otra actualización antes del siguiente período de mantenimiento, ya que el proceso de publicación de la AMI de AMS sigue un ritmo uniforme para beneficio de todos los clientes de AMS.

Cambiar lo que sale patched/optioning

Con los parches configurados por AMS, en respuesta a la notificación del servicio de aplicación de parches o en una solicitud de servicio, puede cambiar los recursos a los que se van a aplicar los parches. Puede hacer lo siguiente:

- Defina una lista de parches que deben excluirse de la corrección, por pila y por sistema operativo.
- Defina una lista de recursos que deben excluirse de algunos parches o de todos los parches.
- Defina una lista de recursos que deben excluirse siempre de todas las aplicaciones de parches.
- Defina una lista de recursos a los que se deben aplicar los parches en un día y una hora determinados (esta opción es válida si no ha definido un período de mantenimiento).

Para excluir uno o más parches, envíe una solicitud de servicio o responda a la notificación del servicio de aplicación de parches mediante la plantilla que se proporciona a continuación. No envíe un RFC. Incluya en la solicitud el nombre o los nombres del parche que desea excluir y por qué. Incluya esta información en una solicitud de servicio de la siguiente manera:

- Nombre: el nombre del parche. En el caso de los parches de Windows, este es el nombre de la base de conocimientos, por ejemplo KB3145384. En el caso de los parches de Linux, este es el nombre del paquete, por ejemplo openssl-6.6.1p1-25.61.amzn1.x86_64.
- Motivo: un comentario que indica por qué se excluye el parche.
- Hora de caducidad: date/time fecha de caducidad de la exclusión.

Si un parche excluido ya está instalado, se elimina.

Un operador revisará la solicitud y analizará con usted si la exclusión de esos parches supone un riesgo de seguridad significativo. También se negocia la fecha de caducidad de los parches excluidos. Tras la fecha de caducidad acordada, la exclusión caduca y el parche se instala en cualquier parche posterior.

Los parches de la lista de exclusiones siguen apareciendo en los resultados del escaneo, si corresponde.

Note

A diferencia de Windows, los parches de Linux son específicos de cada versión. Esta distinción es importante porque las nuevas versiones de un parche excluido no se excluyen automáticamente. Es su responsabilidad notificar a AMS para que excluya las nuevas versiones de un parche de Linux si así lo desea.

Plantillas de respuesta a las notificaciones del servicio de parches

Debe responder a las notificaciones del servicio de parches utilizando el formato especificado para poder aplicar los parches a sus instancias. Debe hacerlo si aún no ha establecido un período de mantenimiento con AMS.

Cuando responda a una notificación de servicio, utilice el formato indicado.

Si no hay ningún período de mantenimiento establecido, díganos cuándo aplicar los parches, tal y como se muestra a continuación:

UTC	StartTime	StackId	InstanceId (Optional)
2019-04-01	15:00	stack-123456789012	i-1234566789
2019-04-01	15:00	stack-123456789013	i-1234566784
2019-04-01	15:00	stack-123456789014	i-1234566783
2019-04-01	15:00	stack-123456789015	i-1234566782

Si ha establecido un período de mantenimiento y desea que determinados recursos se excluyan de determinados parches, utilice el siguiente formato:

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	<i>PATCH</i>
stack-123456789013	i-1234566784	<i>PATCH</i>

stack-123456789014	i-1234566783	PATCH
stack-123456789015	i-1234566782	PATCH

Si ha establecido un período de mantenimiento y desea que determinados recursos se excluyan siempre de todos los parches, utilice el siguiente formato:

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	ALL
stack-123456789015	i-1234566782	ALL

Preparándose para la aplicación de parches

Para preparar su entorno para la aplicación automática de parches, le recomendamos lo siguiente:

- Asegúrese de tener un inventario completo de todas las instancias que desee parchear.
- Asegúrese de realizar copias de seguridad periódicas de sus recursos como parte de su estrategia de continuidad empresarial. Se crean copias de seguridad adicionales como parte de la secuencia de parches y se eliminan automáticamente de acuerdo con la política de retención de Patch Orchestrator que haya configurado (el valor predeterminado es de 60 días).
- Asegúrese de que todas las licencias pertinentes estén actualizadas.
- Modifique las ventanas de mantenimiento de las pilas para escalar los parches, de modo que las pilas de pruebas se parcheen antes que las pilas de producción. De esta forma, cualquier error relacionado con la aplicación de parches se detecta en las pilas de pruebas y se puede identificar antes de aplicar los parches a las pilas de producción.

Visualizar la configuración de los parches

Para saber cuál es su configuración de parches actual, puede hacer lo siguiente:

- Envíe una solicitud de servicio a AMS junto con la consulta.
- Espere una notificación del servicio de parches. En el aviso de aplicación de parches se indican todos los parches que se deben aplicar y los casos en los que se debe aplicar el parche, y también se sugiere una ventana de parches.

Puede enviar una solicitud de servicio para modificar lo siguiente:

- Intervalo de escaneo: cantidad de tiempo, en minutos, entre los escaneos de conformidad realizados en las instancias de esta pila.

El valor predeterminado es 240 (4 horas).

- NotificationWindow: Con qué antelación (en minutos) se te debe enviar la notificación a un cambio programado (parche). El valor predeterminado es 10080 (7 días).

Parcheo estándar AMS FAQs

En esta sección se proporcionan respuestas a algunas de las preguntas más frecuentes.

- P: ¿Cómo puedo dejar de aplicar parches a nivel mundial?

R: Para excluirse de la aplicación de parches en todo el mundo, presente una solicitud de servicio. Ten en cuenta que no puedes excluirte de los parches obligatorios de AMS. Se seguirán escaneando todas las pilas para que podamos informar sobre las vulnerabilidades.

- P: ¿Cómo puedo excluir pilas específicas de la aplicación de parches?

R: Para excluir permanentemente pilas específicas de la aplicación de parches, envía una solicitud de servicio. Para excluir determinadas pilas de un ciclo de parches concreto, responde a la próxima notificación de aplicación de parches con la lista de pilas que desee excluir. Para obtener información, consulte [Cambiar lo que sale patched/opting](#). Ten en cuenta que no puedes excluirte de los parches obligatorios.

- P: ¿Qué ocurre si no apruebo una notificación del servicio de parches?

R: Dispones de 14 días para aprobar una solicitud de servicio de aplicación de parches estándar y de 10 días para aprobar una notificación de aplicación de parches crítica. Si no aprueba la solicitud de servicio dentro del período de tiempo, el compromiso de servicio se anula y no se aplica ningún parche. En el caso de los parches obligatorios, los parches se aplican independientemente de la respuesta a la solicitud de servicio.

- P: ¿Cómo puedo excluir la instalación de parches y paquetes específicos?

R: Para excluir permanentemente parches o paquetes específicos, envíe una solicitud de servicio. Para excluir determinados parches o paquetes de un ciclo de parches concreto, responde a

la próxima notificación de aplicación de parches con la lista de parches o paquetes que desee excluir. Para obtener más información, consulte [Cambiar lo que sale patched/opting](#) . Tenga en cuenta que no puede excluirse de los parches obligatorios.

- P: ¿Qué ocurre si un sistema falla como resultado de una aplicación de parches?

R: AMS monitorea cada sistema. AMS le envía una notificación de servicio con el resultado de cada actualización (es decir, si se ha realizado correctamente o no) por pila e instancia. Si se detecta un error, AMS lo investiga, restaura la instancia y, a continuación, un ingeniero de operaciones de AMS intenta aplicar el parche manualmente. Para obtener información, consulte [Fallos de parcheo estándar AMS](#).

- P: ¿Qué actualizaciones gestiona AMS?

R: AMS gestiona las actualizaciones a nivel del sistema operativo que el proveedor notifica a AMS. Para obtener más información, consulte [Parches compatibles](#).

- P: ¿Qué actualizaciones no gestiona AMS?

R: AMS no gestiona las actualizaciones a nivel de aplicación.

- P: ¿Cómo se actualizan los grupos de Auto Scaling?

R: Los grupos de Auto Scaling se actualizan con un reemplazo de AMI en la configuración del grupo de Auto Scaling y realizan una actualización progresiva. Una actualización progresiva observa la HealthyHostThreshold configuración de la aplicación de parches, que determina cuántas EC2 instancias de Amazon de una pila deben mantenerse activas durante la aplicación de parches. Para obtener más información, consulte [La AMI actualiza los parches \(utilizando los parches AMIs para los grupos de Auto Scaling\)](#).

- P: ¿Cómo puedo instalar las actualizaciones fuera del ciclo normal?

R: En el caso de las actualizaciones a nivel de sistema operativo que desee instalar fuera del programa normal de aplicación de parches, envíe una solicitud de servicio utilizando la notificación

de aplicación de parches que haya recibido. Esto puede ocurrir si las pruebas de un parche propuesto tardaron más de 21 días (en el caso de un parche estándar) o 14 días (en el caso de un parche crítico). Out-of-band los parches se pueden realizar in situ para las instancias de Amazon EC2 independientes.

- P: ¿Cómo se parchean las pilas o instancias recién implementadas?

R: Al crear una nueva instancia de Amazon EC2 stack o un grupo de Auto Scaling, siempre debes especificar la AMI de AMS más reciente, que ya incluirá los parches más recientes. En el caso de infraestructuras mutables, la aplicación de parches en línea debe realizarse tan pronto como se despliegue la pila.

Compromisos de servicio de parcheo

En función del tipo de implementación de la infraestructura y de la importancia de la actualización, establecemos compromisos de servicio para las actualizaciones de seguridad críticas para infraestructuras mutables e inmutables, y para las actualizaciones importantes para infraestructuras mutables e inmutables.

Aplicación de parches estándar

Estos son los compromisos de servicio de AMS para la aplicación de parches estándar.

Aplicación de parches estándar e infraestructura mutable (aplicación de parches in situ)

Evento/acción	Medición del compromiso de servicio
Las actualizaciones importantes se publican en un mes.	El reloj comienza
Catorce días después de la creación de la notificación de parche estándar, AMS le notificará las próximas actualizaciones planificadas mediante una notificación de servicio y por correo electrónico para cada paquete. La notificación de servicio incluye:	El reloj se detiene después de enviar la notificación de servicio.

Evento/acción	Medición del compromiso de servicio
• Una lista de las actualizaciones IDs (CSUs y IUs) aplicables (necesarias y no aplicadas) a la pila y de las actualizaciones excluidas de la aplicación de parches • IDs de las pilas afectadas • El período de mantenimiento en el que se aplicarán las actualizaciones	
Usted comprueba el impacto de las actualizaciones y aprueba o rechaza la RFC. Si no responde en un plazo de 14 días o rechaza la aplicación de parches en su respuesta a la notificación de servicio, no se tomará ninguna medida. Si tarda más de 14 días en realizar la prueba y desea que las actualizaciones se apliquen una vez transcurrido el período de 14 días, envíe una solicitud de servicio para solicitar un nuevo parche basándose en los detalles de la RFC anterior.	Si no lo aprueba o no responde en un plazo de 14 días, el cambio pendiente se cancela y no se aplica el compromiso de servicio relativo a las actualizaciones.
Si aprueba la notificación de servicio en un plazo de 14 días, AMS aplicará las actualizaciones. Puede optar por excluir actualizaciones específicas de una RFC especificando las actualizaciones que se van a excluir en su respuesta a la notificación de servicio.	El reloj comienza si aprueba la notificación de servicio en un plazo de 14 días a partir de su recepción. El reloj se detiene cuando se ha intentado instalar la actualización.

Evento/acción	Medición del compromiso de servicio
AMS le envía una notificación de servicio con el resultado de cada intento de actualización. La notificación de servicio incluye los siguientes detalles: • ID de EC2 instancia de Amazon • Actualización 1 exitosa/fallida: ARN a1, ARN a2... • Actualización 2 exitosa/fallida: ARN b1, ARN b2... • La actualización no se realizó correctamente o falló: ARN c1, ARN c2...	No se usa.
En caso de errores en las actualizaciones, AMS realiza un análisis para determinar la causa del error y le comunica el resultado del análisis. Si el error se debe a AMS, AMS vuelve a intentar las actualizaciones dentro del período de mantenimiento; de lo contrario, AMS crea notificaciones de servicio para la combinación de instancia y actualización fallida y espera sus instrucciones en un período de mantenimiento.	No se usa.
En el caso de errores atribuibles a usted, envíe una solicitud de servicio para obtener una nueva RFC de parche a fin de actualizar las instancias.	No se usa.

Parches críticos

Estos son los compromisos de servicio de AMS para las actualizaciones de seguridad críticas.

Actualizaciones de seguridad críticas, infraestructura mutable

Evento/acción	Medición del compromiso de servicio
Se publica la CSU.	Arranca el reloj
AMS le notifica el RFC del parche mediante una notificación de servicio (que también envía un correo electrónico) para cada pila. La notificación de servicio incluye: • Actualiza la fecha de lanzamiento • Criticidad de la actualización • Detalles de la actualización: referencia de KB, etc. • IDs de las pilas afectadas	El reloj se detiene después de enviar la notificación de servicio.
Usted prueba las actualizaciones que figuran en la RFC y aprueba o rechaza la RFC en un plazo de 10 días respondiendo a la notificación de servicio.	Si no lo aprueba o no responde en un plazo de 14 días, el cambio pendiente se cancela y no se aplica el compromiso de servicio para la actualización.
Debe proporcionar un período de mantenimiento específico (por pila) para instalar las actualizaciones. Los períodos de mantenimiento especificados en un plazo de 24 horas a partir de la respuesta a la notificación de servicio pueden reprogramarse en función de la capacidad disponible.	
Si no responde en un plazo de 10 días o si rechaza la solicitud de confirmación del parche, la acción pendiente se cancela.	
Si desea aplicar las actualizaciones después del período de 14 días, envíe una solicitud de servicio para una nueva RFC de parche basada en los detalles de la RFC anterior.	

Evento/acción	Medición del compromiso de servicio
Si aprueba la notificación de servicio, AMS aplicará las actualizaciones. En el caso de varias actualizaciones, puede optar por excluir determinadas actualizaciones del cambio especificando las actualizaciones que se van a excluir en su respuesta a la notificación de servicio.	Si el período de mantenimiento deseado no está dentro del plazo de compromiso de servicio, solo se incumplirá el compromiso de servicio para la actualización si la RFC no se ejecuta dentro del período de mantenimiento deseado.
AMS le envía una notificación de servicio con el resultado de cada actualización que se haya aplicado. La notificación de servicio incluye los siguientes detalles: • ID de EC2 instancia de Amazon • La actualización se realizó correctamente: ARN a1, ARN a2... • Error de actualización: ARN c1, ARN c2...	No se usa.
En caso de errores en las actualizaciones, AMS realiza un análisis para determinar la causa del error y le comunica el resultado del análisis. Si el error se debe a AMS, AMS vuelve a intentar las actualizaciones dentro del período de mantenimiento; de lo contrario, AMS crea notificaciones de servicio para la combinación de instancia y actualización fallida y espera sus instrucciones en un nuevo período de mantenimiento.	No se usa.
En el caso de errores atribuibles a usted, envíe una solicitud de servicio para obtener una nueva RFC de parche a fin de actualizar las instancias.	No se usa.

Actualizaciones de seguridad críticas, infraestructura inmutable

Evento/acción	Medición del compromiso de servicio
Se publica la CSU.	Arranca el reloj
AMS le notifica lo siguiente mediante una notificación de servicio: • Fecha de lanzamiento de la actualización • Criticidad de la actualización • Detalles de la actualización (referencia de KB, etc.) • Imágenes de Amazon Machine Images (AMI) de AMS afectadas • Fecha y hora de publicación previstas de la nueva actualización AMIs	El reloj sigue funcionando.
Las versiones de AMS se actualizan AMIs en la cuenta gestionada.	El reloj se detiene.
Si aprueba la notificación de servicio, AMS aplicará las actualizaciones. AMS le notifica lo AMIs compartido en su cuenta mediante una notificación de servicio y por correo electrónico.	No se usa.
Si la prueba del nuevo AMIs tarda más del tiempo asignado (una semana), puede enviar una solicitud de servicio a AMS para actualizar sus grupos de Auto Scaling con la nueva AMI de AMS (tal cual). Si desea modificar la nueva AMI de AMS con sus configuraciones, utilice una RFC con el CT Management Other Other Update (ct-0xdawir96cy7k) para solicitar que actualicemos sus grupos de Auto Scaling.	No se usa.

Informes y opciones

AWS Managed Services (AMS) recopila datos de varios servicios nativos de AWS para proporcionar informes con valor añadido sobre las principales ofertas de AMS.

AMS ofrece dos tipos de informes detallados:

- **Informes a pedido:** puede solicitar determinados informes ad hoc a través de su Cloud Service Delivery Manager (CSDM). Estos informes no tienen un límite porque es posible que tengas que solicitarlos varias veces durante la fase de incorporación o en algún momento crítico. Sin embargo, ten en cuenta que estos informes no están diseñados para proporcionarse siguiendo un cronograma, como los informes semanales. Para comprender mejor sus necesidades o para obtener más información sobre el uso de los informes de autoservicio, póngase en contacto con su CSDM.
- **Informes de autoservicio:** los informes de autoservicio de AMS le permiten consultar y analizar datos directamente con la frecuencia que necesite. Utilice los informes de autoservicio para acceder a los informes desde la consola AMS y genere informes sobre los conjuntos de datos mediante grupos de S3 (un grupo por cuenta). Esto le permite integrar los datos en su herramienta de inteligencia empresarial (BI) favorita para poder personalizar los informes según sus necesidades.

Temas

- [Informes a petición](#)
- [Informes de autoservicio](#)

Informes a petición

Temas

- [Informes de parches de AMS](#)
- [Informes de AMS Backup](#)
- [Informes de Top Talkers prevenidos y seguimiento](#)
- [Informe de detalles de cargos de facturación](#)
- [Informes de Trusted Remediator](#)

AMS recopila datos de varios servicios nativos de AWS para proporcionar informes de valor añadido sobre las principales ofertas de AMS. Para obtener una copia de estos informes, solicite a su administrador de prestación de servicios en la nube (CSDM).

Informes de parches de AMS

Informes disponibles

- [Informe resumido de los detalles de las instancias de parches](#)
- [Informe de detalles del parche](#)
- [Informe de casos en los que no se detectaron parches](#)
- [Informe de cobertura de SSM para parchear](#)

Informe resumido de los detalles de las instancias de parches

El informe resumido de los detalles de las instancias de parches proporciona los detalles de las instancias recopiladas para las instancias que están incorporadas a la elaboración de informes. Se trata de un informe informativo que ayuda a identificar todas las instancias incorporadas, el estado de la cuenta, los detalles de las instancias, la cobertura del período de mantenimiento, el tiempo de ejecución del período de mantenimiento, los detalles de la pila y el tipo de plataforma. Este informe proporciona lo siguiente:

1. Datos sobre las instancias de producción y no producción de una cuenta. Nota: Las etapas de producción y no producción se derivan del nombre de la cuenta y no de las etiquetas de la instancia.
2. Datos sobre la distribución de las instancias por tipo de plataforma. Nota: El tipo de plataforma «N/A» es cuando no se AWS Systems Manager puede recuperar la información de la plataforma.
3. Datos sobre la distribución del estado de las instancias y el número de instancias en ejecución, detenidas o finalizadas.

Nombre del campo	Definición
Fecha y hora del informe	Fecha y hora en que se generó el informe.
ID de cuenta	ID de cuenta de AWS a la que pertenece el ID de instancia

Nombre del campo	Definición
Nombre de la cuenta	Nombre de la cuenta de AWS
Cuenta de producción	Identificador de las cuentas de AMS producidas y no producidas, en función de si el nombre de la cuenta incluye el valor «PROD» o «NONPROD». Ejemplo: PROD, NONPROD, no disponible
Estado de la cuenta	Estado de la cuenta AMS. Por ejemplo: ACTIVO, INACTIVO
Compromiso de servicio de cuenta de AMS	PREMIUM, ADEMÁS
Zona de aterrizaje	Marca para el tipo de zona de landing zone de la cuenta. Por ejemplo: MALZ, NON-MALZ
Restricciones de acceso	Regiones a las que está restringido el acceso. Por ejemplo: US SOIL
ID de instancia	ID de la EC2 instancia
Nombre de instancia	Nombre de la EC2 instancia
Tipo de plataforma de instancia	Tipo de sistema operativo (SO). Por ejemplo: Windows, Linux, etc.
Nombre de la plataforma de la instancia	Nombre del sistema operativo (SO). Por ejemplo: MicrosoftWindowsServer 2012R2 Standard, RedHatEnterpriseLinuxServer
Nombre de la pila	Nombre de la pila que contiene la instancia
Tipo de pila	Pila de AMS (infraestructura de AMS dentro de la cuenta del cliente) o pila de clientes (infraestructura gestionada por AMS que admite las aplicaciones de los clientes). Ejemplos: AMS, CUSTOMER

Nombre del campo	Definición
Nombre del grupo de escalado automático	Nombre del Grupo de Auto Scaling (ASG) que contiene la instancia
Grupo de parches de instancias	Nombre del grupo de parches utilizado para agrupar las instancias y aplicar el mismo período de mantenimiento. Si el grupo de parches no está asignado, el valor será «Sin asignar»
Tipo de grupo de parches de instancias	Tipo de grupo de parches. PREDETERMINADO: grupo de parches predeterminado con el intervalo de mantenimiento predeterminado, determinado por la <code>AMSDefaultPatchGroup:True</code> etiqueta de la instancia. CLIENTE: grupo de parches creado por el cliente. NOT_ASSIGNED: no se ha asignado ningún grupo de parches
Estado de la instancia	Estado dentro del ciclo de vida de la EC2 instancia. Ejemplos: TERMINADA, EN EJECUCIÓN, DETENIDA, DETENIDA, CERRADA, PENDIENTE. Para obtener más información, consulte Ciclo de vida de la instancia.
Cobertura del período de mantenimiento	Si hay una ventana de mantenimiento futura en esta instancia. Ejemplos: COVERED o NOT_COVERED

Nombre del campo	Definición
Fecha y hora de ejecución de la ventana de mantenimiento	La próxima vez se espera que se ejecute la ventana de mantenimiento. Si es NULL, ejecución en ventana única, es decir, no recurrente

Informe de detalles del parche

El informe de detalles del parche de AWS Managed Services (AMS) proporciona detalles del parche y la cobertura del período de mantenimiento de varias instancias, entre las que se incluyen:

1. Datos sobre los grupos de parches y sus tipos.
2. Datos sobre las ventanas de mantenimiento, la duración, el límite, las fechas futuras de ejecución de las ventanas de mantenimiento (programación) y las instancias afectadas en cada ventana.
3. Datos sobre todos los sistemas operativos de la cuenta y el número de instancias en las que está instalado el sistema operativo.

Nombre del campo	Definición
Fecha y hora del informe	Fecha y hora en que se generó el informe.
ID de cuenta	ID de cuenta de AWS a la que pertenece el ID de instancia
Nombre de la cuenta	Nombre de la cuenta de AWS
ID de instancia	ID de la EC2 instancia
Cuenta de producción	Identificador de las cuentas de AMS producidas y no producidas, en función de si el nombre de la cuenta incluye el valor «PROD» o «NONPROD». Si los datos no están disponibles, el valor será «No disponible»
Estado de la cuenta	Estado de la cuenta AMS. Por ejemplo: ACTIVO, INACTIVO

Nombre del campo	Definición
Tipo de plataforma de instancia	Tipo de sistema operativo (SO). Por ejemplo: Windows, Linux
Nombre de la plataforma de la instancia	Nombre del sistema operativo (SO). Por ejemplo: MicrosoftWindowsServer 2012R2 Standard, RedHatEnterpriseLinuxServer
Tipo de pila	Pila de AMS (infraestructura de AMS dentro de una cuenta de cliente) o pila de clientes (infraestructura gestionada por AMS que admite las aplicaciones de los clientes). Por ejemplo: AMS, CUSTOMER
Grupo de parches de instancias	Nombre del grupo de parches utilizado para agrupar las instancias y aplicar el mismo período de mantenimiento. Si el grupo de parches no está asignado, el valor será «Sin asignar»
Tipo de grupo de parches de instancias	Tipo de grupo de parches. PREDETERMINADO: grupo de parches predeterminado con ventana de mantenimiento predeterminada, determinada por la <code>AMSDefaultPatchGroup:True</code> etiqueta de la instancia CLIENTE: grupo de parches creado por el cliente SIN ASIGNAR: no se ha asignado ningún grupo de parches

Nombre del campo	Definición
Estado de la instancia	Estado dentro del ciclo de vida de la EC2 instancia. Por ejemplo: FINALIZADO, EN EJECUCIÓN, EN ESPERA, DETENIDO, CERRADO, PENDIENTE Para obtener más información, consulte Ciclo de vida de la instancia.
ID de ventana de mantenimiento	Identificador de ventana de mantenimiento
Estado de la ventana de mantenimiento	Los valores posibles son ACTIVADO o DESACTIVADO.
Tipo de ventana de mantenimiento	Tipo de ventana de mantenimiento
Fecha y hora de la próxima ejecución de la ventana de mantenimiento	Se espera que la próxima vez se ejecute la ventana de mantenimiento. Si es NULL, ejecución en ventana única, es decir, no recurrente
Ventana de mantenimiento de última ejecución	La última vez que se ejecutó la ventana de mantenimiento
Duración del período de mantenimiento (horas)	La duración del período de mantenimiento en horas
Cobertura del período de mantenimiento	La cobertura del período de mantenimiento
ID de referencia del parche	La línea base del parche está actualmente conectada a la instancia
Estado del parche	Estado general de cumplimiento de los parches. Por ejemplo: COMPLIANT, NON_COMPLIANT. Si falta al menos un parche, la instancia se considera no compatible; de lo contrario, es compatible.

Nombre del campo	Definición
Cumple: total	Recuento de parches compatibles (todos los niveles de gravedad)
No conformes: total	Recuento de parches no conformes (todos los grados de gravedad)
Cumple con las normas: crítico	Número de parches compatibles con una gravedad «crítica»
Cumple con las normas: alta	Recuento de parches compatibles con una gravedad «alta»
Cumple con las normas: media	Número de parches compatibles con una gravedad «media»
Cumple con las normas: bajo	Recuento de parches compatibles con una gravedad «baja»
Cumple con los requisitos: informativo	Recuento de parches compatibles con una gravedad «informativa»
Cumple con las normas: sin especificar	Número de parches compatibles con una gravedad «no especificada»
No conformes: crítico	Recuento de parches no conformes con una gravedad «crítica»
No conformes: alto	Recuento de parches no conformes con una gravedad «alta»
No conforme: medio	Recuento de parches no conformes con una gravedad «media»
No conformes: bajo	Recuento de parches no conformes con una gravedad «baja»
No conformes: informativo	Recuento de parches no conformes con una gravedad «informativa»

Nombre del campo	Definición
No conforme: sin especificar	Recuento de parches no conformes con una gravedad «no especificada»

Informe de casos en los que no se detectaron parches

El informe Instances That Missed Patches de AWS Managed Services (AMS) proporciona detalles sobre las instancias a las que no se les aplicaron parches durante la última ejecución del período de mantenimiento, entre los que se incluyen:

1. Datos sobre los parches faltantes a nivel de ID de parche.
2. Datos sobre todas las instancias a las que les falta al menos un parche, junto con atributos como la gravedad del parche, los días sin corregir, el intervalo y la fecha de lanzamiento del parche.

Nombre del campo	Definición
Fecha y hora del informe	Fecha y hora en que se generó el informe.
ID de cuenta	ID de cuenta de AWS a la que pertenece el ID de instancia
Nombre de la cuenta	Nombre de la cuenta de AWS
Cuenta de producción	Identificador de las cuentas de AMS producidas y no producidas, en función de si el nombre de la cuenta incluye el valor «PROD» o «NONPROD».
Estado de la cuenta	Estado de la cuenta AMS. Por ejemplo: ACTIVO o INACTIVO
Nivel de servicio de la cuenta AMS	PREMIUM o PLUS
ID de instancia	ID de EC2 instancia

Nombre del campo	Definición
Tipo de plataforma de instancia	Tipo de sistema operativo (SO). Por ejemplo: Windows
Estado de la instancia	Estado del ciclo de vida de la EC2 instancia . Por ejemplo: TERMINED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING Para obtener más información, consulta el ciclo de vida de la instancia.
ID del parche	ID del parche publicado. Por ejemplo: KB3172729
Gravedad del parche	Gravedad del parche por fabricante. Por ejemplo: CRÍTICO, IMPORTANTE, MODERADO, BAJO, SIN ESPECIFICAR
Clasificación de parches	Clasificación de los parches por editor. Por ejemplo: CRITICALUPDATES, SECURITUPDATES, UPDATEROLLUPS, UPDATES, FEATUREPACKS
Fecha y hora de lanzamiento del parche (UTC)	Fecha de lanzamiento del parche por editor
Estado de instalación del parche	Estado de instalación del parche en la instancia por SSM. Por ejemplo: INSTALADO, FALTANTE, NO APLICABLE
Días sin parches	Número de días sin parchear la instancia desde el último escaneo de SSM
Rango de días sin parchear	Grupos de días sin parchear. Por ejemplo: <30 DÍAS, 30-60 DÍAS, 60-90 DÍAS, MÁS DE 90 DÍAS

Informe de cobertura de SSM para parchear

El informe de cobertura de SMS con parches de AMS le informa de si las EC2 instancias de la cuenta tienen el agente SSM instalado o no.

Nombre del campo	Definición
Nombre del cliente	Nombre del cliente para situaciones en las que hay varios subclientes
Región de recursos	AWS Región en la que se encuentra el recurso
Nombre de cuenta	El nombre de la cuenta
AWS ID de cuenta	El ID de la AWS cuenta
ID de recurso	ID de la EC2 instancia
Nombre del recurso	Nombre de la EC2 instancia
Bandera compatible	Indica si el recurso tiene el agente SSM instalado («compatible») o no («NO CUMPLE»)

Informes de AMS Backup

Informes disponibles

- [Informe de éxito o fracaso de Backup Job](#)
- [Informe resumido de Backup](#)
- [Summary/Coverage Informe de Backup](#)

Informe de éxito o fracaso de Backup Job

El Success/Failure informe Backup Job proporciona información sobre las copias de seguridad ejecutadas en las últimas semanas. Para personalizar el informe, especifique el número de semanas durante las que desea recuperar los datos. El número predeterminado de semanas es 12. En la siguiente tabla se enumeran los datos incluidos en el informe:

Nombre del campo	Definición
ID de la cuenta de AWS	ID de cuenta de AWS a la que pertenece el recurso
Nombre de la cuenta	Nombre de la cuenta de AWS
ID de trabajo de Backup	El ID del trabajo de Backup
ID de recurso	El ID del recurso del que se ha hecho una copia de seguridad
Tipo de recurso	El tipo de recurso del que se está haciendo una copia de seguridad
Región de recursos	La AWS región del recurso respaldado
Estado de Backup	El estado de la copia de seguridad. Para obtener más información, consulte Estados de los trabajos de Backup
ID del punto de recuperación	El identificador único del punto de recuperación
Mensaje de estado	Descripción de los errores o advertencias que se produjeron durante el trabajo de copia de seguridad
Tamaño del Backup	Tamaño de la copia de seguridad en GB
Punto de recuperación ARN	El ARN de la copia de seguridad creada
Antigüedad del punto de recuperación en días	Número de días transcurridos desde que se creó el punto de recuperación
Hace menos de 30 días	Indicador de copias de seguridad con menos de 30 días

Informe resumido de Backup

Nombre del campo	Definición
Nombre del cliente	Nombre del cliente para situaciones en las que hay varios subclientes
Mes del Backup	Mes de la copia de seguridad
Año de Backup	Año de la copia de seguridad
Tipo de recurso	El tipo de recurso del que se está haciendo la copia de seguridad
Número de recursos	La cantidad de recursos de los que se hizo una copia de seguridad
Número de puntos de recuperación	Número de instantáneas distintas
Copias de seguridad con menos de 30 días	El recuento de copias de seguridad que tienen menos de 30 días
Antigüedad máxima de los puntos de recuperación	El punto de recuperación más antiguo en días
Edad mínima de puntos de recuperación	Edad del punto de recuperación más reciente en días

Summary/Coverage Informe de Backup

El Summary/Coverage informe Backup indica cuántos recursos no están protegidos actualmente por ningún AWS Backup plan. Hable con su CDSM sobre un plan adecuado para aumentar la cobertura, siempre que sea posible, y reducir el riesgo de pérdida de datos.

Nombre del campo	Definición
Nombre del cliente	Nombre del cliente para situaciones en las que hay varios subclientes

Nombre del campo	Definición
Región	AWS región donde se encuentra el recurso
Nombre de cuenta	El nombre de la cuenta
AWS ID de cuenta	El ID de la AWS cuenta
Tipo de recurso	Tipo del recurso. Los recursos son compatibles con AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EC2 EFS, RDS y S3) FSx
ARN de recurso	ARN del recurso
ID de recurso	ID del recurso
Cobertura	Indica si el recurso está cubierto o no («CUBIERTO» o «NOT_COVERED»)
Número de recursos	Número de recursos compatibles en la cuenta
perc_coverage	Porcentaje de recursos compatibles con una copia de seguridad ejecutada en los últimos 30 días.

Informes de Top Talkers prevenidos y seguimiento

Informes disponibles

- [Informe de incidentes evitados](#)
- [Monitoreando el informe de Top Talkers](#)

Informe de incidentes evitados

El informe Incidentes prevenidos enumera las CloudWatch alarmas de Amazon que se corrigieron automáticamente, lo que evitó un posible incidente. Para obtener más información, consulte [Corrección automática](#). En la siguiente tabla se muestra la información incluida en este informe:

Nombre del campo	Definición
execution_start_time_utc	Fecha en la que se ejecutó la automatización
customer_name	Nombre del cliente de la cuenta
account_name	El nombre de la cuenta
AwsAccountId	El ID de la cuenta de AWS
nombre_documento	El nombre del documento SSM o de la automatización ejecutada
duración_en_minutos	La duración de la automatización en minutos
Región	AWS Región en la que se encuentra el recurso
automation_execution_id	El ID de la ejecución
automation_execution_status	El estado de la ejecución

Monitoreando el informe de Top Talkers

El informe Monitoring Top Talkers presenta el número de CloudWatch alertas de Amazon generadas durante un período de tiempo específico y proporciona visualizaciones de los recursos que generan el mayor número de alertas. Este informe le ayuda a identificar los recursos que generan el mayor número de alertas. Estos recursos pueden ser adecuados para realizar un análisis de la causa raíz a fin de solucionar el problema o para modificar los umbrales de alarma a fin de evitar que se activen innecesariamente cuando no se trata de un problema real. En la siguiente tabla se muestra la información incluida en este informe:

Nombre del campo	Definición
Nombre del cliente	Nombre del cliente
AccountId	El ID de la AWS cuenta
Categoría de alerta	El tipo de alerta que se ha activado

Nombre del campo	Definición
Descripción	Descripción de la alerta
ID de recurso	ID del recurso que activó la alerta
Nombre del recurso	Nombre del recurso que activó la alerta
Región	AWS Región en la que se encuentra el recurso
Estado del incidente	Estado más reciente del incidente generado por la alarma
Primera aparición	La primera vez que se activó la alerta
Incidencia reciente	La última vez que se activó la alerta
Recuento de alertas	Número de alertas generadas entre la primera aparición y la reciente

Informe de detalles de cargos de facturación

El informe de detalles de los cargos de facturación de AWS Managed Services (AMS) proporciona detalles sobre los cargos de facturación de AMS con las cuentas vinculadas y los servicios de AWS correspondientes, que incluyen:

- Cargos a nivel de servicio de AMS, porcentajes de aumento, niveles de servicio de AMS a nivel de cuenta y tarifas de AMS.
- Cuentas vinculadas y cargos AWS por uso

Nombre del campo	Definición
Mes de facturación	El mes y el año del servicio facturado
ID de la cuenta del pagador	El identificador de 12 dígitos que identifica la cuenta que será responsable de pagar los cargos de AMS

Nombre del campo	Definición
ID de cuenta vinculada	El identificador de 12 dígitos que identifica la cuenta AMS que consume los servicios que generan gastos
AWS Nombre del servicio	El AWS servicio que se utilizó
AWS Cargos	Los AWS cargos del nombre del AWS servicio que figuran en el nombre del AWS servicio
Plan de precios	El nombre del plan de precios asociado a la cuenta vinculada
Aumenta la proporción	El porcentaje de aumento (expresado en V.WXYZ decimal) basado en pricing_plan, SLA y el servicio de AWS
Cargos ajustados AWS	AWS uso ajustado para AMS
Aumento de los cargos de AWS	El porcentaje de cargos de AWS que se cobrará por AMS; $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$
EC2 Instancias gastadas por RDS	Invierta en instancias EC2 de RDS
Cargos de AMS	Cargos totales de AMS del producto: $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
Tarifa mínima prorrateada	El importe que cobramos para cumplir con el mínimo contractual
Tarifa mínima	Tarifas mínimas de AMS (si corresponde)
Cargos totales de AMS por cuenta vinculada	Suma de todos los cargos de la linked_account
Cargos totales de AMS de la cuenta del pagador	Suma de todos los cargos de la cuenta del pagador

Informes de Trusted Remediator

Informes disponibles

- [Informe resumido de Trusted Remediator Remediation](#)
- [Informe resumido de la configuración de Trusted Remediator](#)
- [Trusted Advisor Compruebe el informe resumido](#)

Informe resumido de Trusted Remediator Remediation

El informe sobre el estado de las correcciones de Trusted Remediator proporciona información sobre las correcciones que se produjeron durante los ciclos de remediación anteriores. El número predeterminado de semanas es 1. Para personalizar el informe, especifique el número de semanas en función de su programa de remediación.

Nombre del campo	Definición
Date	Fecha en la que se recopilaron los datos.
ID de cuenta	El identificador de AWS cuenta al que pertenece el recurso
Nombre de la cuenta	El nombre AWS de la cuenta
Compruebe la categoría	La categoría de AWS Trusted Advisor verificación
Nombre del cheque	El nombre de la comprobación corregida Trusted Advisor
ID de la verificación	El identificador de la comprobación corregida Trusted Advisor
Modo de ejecución	El modo de ejecución que se configuró para la Trusted Advisor comprobación específica
OpsItem ID	El ID del OpsItem creado por Trusted Advisor para su corrección

Nombre del campo	Definición
OpsItem Estado	El estado del objeto OpsItem creado por Trusted Advisor en el momento de elaborar el informe
ID de recurso	El ARN del recurso creado para la remediación

Informe resumido de la configuración de Trusted Remediator

El informe resumido de la configuración de Trusted Remediator proporciona información sobre las configuraciones actuales de Trusted Remediator Remediation para cada comprobación. Trusted Advisor

Nombre del campo	Definición
Date	Fecha en la que se recopilaron los datos.
ID de cuenta	El ID de AWS cuenta al que se aplica la configuración
Nombre de la cuenta	El nombre AWS de la cuenta
Compruebe la categoría	La categoría de AWS Trusted Advisor verificación
Nombre del cheque	El nombre de la Trusted Advisor comprobación corregida a la que se aplica la configuración
ID de la verificación	El ID de la Trusted Advisor comprobación corregida a la que se aplica la configuración
Modo de ejecución	El modo de ejecución que se configuró para la Trusted Advisor comprobación específica
Sustituir a automatizado	El patrón de etiquetas, si está configurado, para anular el modo de ejecución a Automatizado

Nombre del campo	Definición
Sustituir a Manual	El patrón de etiquetas, si está configurado, para anular el modo de ejecución a Manual

Trusted Advisor Compruebe el informe resumido

El informe resumido de Trusted Advisor comprobaciones proporciona información sobre las Trusted Advisor comprobaciones actuales. Este informe recopila datos después de cada programa de remediación semanal. El número predeterminado de semanas es 1. Para personalizar el informe, especifique el número de semanas en función del ciclo de corrección.

Nombre del campo	Definición
Date	Fecha en la que se recopilaron los datos.
ID de cuenta	El ID de AWS cuenta al que se aplica la configuración
Nombre del cliente	El nombre AWS de la cuenta
Compruebe la categoría	La categoría de AWS Trusted Advisor verificación
Nombre del cheque	El nombre de la Trusted Advisor comprobación corregida a la que se aplica la configuración
ID de la verificación	El ID de la Trusted Advisor comprobación corregida a la que se aplica la configuración
Estado	El estado de alerta de la comprobación. Los estados posibles son correcto (verde), advertencia (amarillo), error (rojo) o not_available
Recursos marcados	El número de AWS recursos que se marcaron (enumeraron) en la Trusted Advisor lista.

Nombre del campo	Definición
Recursos ignorados	El número de AWS recursos que se ignoraron Trusted Advisor porque los marcaste como suprimidos.
Recursos en estado crítico	El número de recursos en estado crítico
Recursos en estado de advertencia	El número de recursos en estado de advertencia

Informes de autoservicio

Los informes de autoservicio (SSR) de AWS Managed Services (AMS) son una función que recopila datos de varios AWS servicios nativos y proporciona acceso a informes sobre las principales ofertas de AMS. El SSR proporciona información que puede utilizar para respaldar las operaciones, la administración de la configuración, la administración de activos, la administración de la seguridad y el cumplimiento.

Utilice SSR para acceder a los informes desde la consola AMS y genere informes a los conjuntos de datos a través de buckets de Amazon S3 (un bucket por cuenta). Puede conectar los datos a su herramienta de inteligencia empresarial (BI) favorita para personalizar los informes en función de sus necesidades específicas. AMS crea este depósito de S3 (nombre del depósito de S3: (ams-reporting-data-a<Account_ID>)) en su AWS región principal y los datos se comparten desde el plano de control de AMS alojado en la región us-east-1.

Important

Para acceder a esta función, debe tener uno de los siguientes roles:

- Zona de destino para varias cuentas: AWSManagedServicesReadOnlyRole
- Zona de destino para una sola cuenta: Customer_ _Role ReadOnly

Important

Uso de claves personalizadas con AWS Glue

Para cifrar sus AWS Glue metadatos con una clave KMS administrada por el cliente, debe realizar los siguientes pasos adicionales para permitir que AMS agregue datos de la cuenta:

1. Abra la AWS Key Management Service consola en <https://console.aws.amazon.com/kms> y, a continuación, elija Claves gestionadas por el cliente.
2. Seleccione el ID de clave que planea usar para cifrar los AWS Glue metadatos.
3. Seleccione la pestaña Alias y, a continuación, elija Crear alias.
4. En el cuadro de texto, introduzca y AmsReportingFlywheelCustomKey, a continuación, seleccione Crear alias.

Temas

- [Operaciones de API internas](#)
- [Informe de parches \(diario\)](#)
- [Informe de Backup \(diario\)](#)
- [Informe de incidentes \(semanal\)](#)
- [Informe de facturación \(mensual\)](#)
- [Informes agregados](#)
- [Paneles de informes de autoservicio de AMS](#)
- [Política de conservación de los datos](#)
- [Fuera de SSR](#)

Operaciones de API internas

Si supervisas las operaciones de la API, es posible que veas llamadas a las siguientes operaciones únicamente internas:

- `GetDashboardUrl`
- `ListReportsV2`

Funcionamiento interno de la API: `GetDashboardUrl`

Esta operación aparece en los registros del sistema cuando la consola AMS la invoca. No tiene otro caso de uso. No está disponible para su uso directo.

Devuelve la URL del panel de control incrustado para el informe correspondiente. Esta operación acepta un mensaje `dashboardName` devuelto por `ListReports`.

Sintaxis de la solicitud

```
HTTP/1.1 200
Content-type: application/json
{
  "dashboardName": "string"
}
```

Elementos de la solicitud

dashboardName: el nombre del QuickSight panel para el que se solicita la URL. El nombre del panel se devuelve en la `ListReports` versión 2.

Tipo: cadena

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200. El servicio devuelve los datos siguientes en formato JSON.

url: Devuelve la QuickSight URL de la solicitud `dashboardName`.

Tipo: cadena

Errores

Para obtener información sobre los errores comunes a todas las acciones, consulte [Errores comunes](#).

BadRequestException:

La solicitud presentada no es válida. Por ejemplo, si la entrada está incompleta o es incorrecta. Consulte el mensaje de error adjunto para obtener más información.

Código de estado HTTP: 400

NotFoundException:

No se encuentra el recurso solicitado. Asegúrese de que el URI de la solicitud sea correcto.

Código de estado HTTP: 404

TooManyRequestsException:

La solicitud ha alcanzado su límite máximo. Vuelva a intentarlo una vez transcurrido el período de tiempo especificado.

Código de estado HTTP: 429

UnauthorizedException:

La solicitud se deniega porque la persona que llama no tiene permisos suficientes.

Código de estado HTTP: 401

Funcionamiento de la API interna: V2 ListReports

Esta API aparece en los registros del sistema cuando la consola AMS la invoca. No tiene otro caso de uso. No está disponible para su uso directo.

Devuelve una lista de los informes operativos que están disponibles para una cuenta específica.

Sintaxis de la solicitud

La solicitud no tiene un cuerpo de solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
      "dashboard": "string",
      "lastUpdatedTime": "string",
```

```
}  
],  
  "reportsType": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200. El servicio devuelve los datos siguientes en formato JSON.

reportsList: La lista de informes operativos disponibles.

Tipo: matriz de objetos del panel

reportsType: Indica si un informe está agregado en varias cuentas o no.

Tipo: cadena

Errores

Para obtener información sobre los errores comunes a todas las acciones, consulte [Errores comunes](#).

BadRequestException:

La solicitud presentada no es válida. Por ejemplo, la entrada está incompleta o es incorrecta. Consulte el mensaje de error adjunto para obtener más información.

Código de estado HTTP: 400

NotFoundException:

No se encuentra el recurso solicitado. Asegúrese de que el URI de la solicitud sea correcto.

Código de estado HTTP: 404

TooManyRequestsException:

La solicitud ha alcanzado su límite máximo. Vuelva a intentarlo una vez transcurrido el período de tiempo especificado.

Código de estado HTTP: 429

UnauthorizedException:

La solicitud se deniega porque la persona que llama no tiene permisos suficientes.

Código de estado HTTP: 401

Informe de parches (diario)

Informes disponibles

-
- [Detalles del parche](#)
- [Instancias en las que no se incluyeron parches](#)

Se trata de un informe informativo que ayuda a identificar todas las instancias incorporadas a Patch Orchestrator (PO), el estado de la cuenta, los detalles de la instancia, la cobertura del período de mantenimiento, el tiempo de ejecución del período de mantenimiento, los detalles de la pila y el tipo de plataforma.

Este conjunto de datos proporciona:

- Datos sobre las instancias de producción y no producción de una cuenta. Las etapas de producción y no producción se derivan del nombre de la cuenta y no de las etiquetas de las instancias.
- Datos sobre la distribución de las instancias por tipo de plataforma. El tipo de plataforma «N/A» se produce cuando AWS Systems Manager (SSM) no puede obtener la información de la plataforma.
- Datos sobre la distribución del estado de las instancias y el número de instancias en ejecución, detenidas o finalizadas.

Nombre del campo de la consola	Nombre del campo del conjunto de datos	Definición
Restricciones de acceso	access_restrictions	Regiones a las que está restringido el acceso
ID de cuenta	aws_account_id	AWS ID de cuenta al que pertenece el ID de instancia

Nombre del campo de la consola	Nombre del campo del conjunto de datos	Definición
ID de cuenta de administrador	aws_admin_account_id	Cuenta de confianza habilitada por usted. AWS Organizations
Nombre de la cuenta	account_name	AWS nombre de cuenta
Estado de la cuenta	estado_de la cuenta	Estado de la cuenta AMS
	account_sla	Compromiso de servicio de la cuenta AMS
Account Type	malz_role	Función MALZ
Nombre del grupo de escalado automático	instance_asg_name	Nombre del Grupo de Auto Scaling (ASG) que contiene la instancia
ID de instancia	instance_id	ID de la EC2 instancia
Nombre de instancia	nombre_instancia	Nombre de la instancia EC2
Grupo de parches de instancias	instance_patch_groups	Nombre del grupo de parches utilizado para agrupar las instancias y aplicar el mismo período de mantenimiento
Tipo de grupo de parches de instancias	instance_patch_group_type	Tipo de grupo de parches
Tipo de plataforma de instancia	instance_platform_type	Tipo de sistema operativo (SO)
Nombre de la plataforma de la instancia	instance_platform_name	Nombre del sistema operativo (SO)
Estado de la instancia	instance_state	Estado dentro del ciclo de vida de la instancia EC2

Nombre del campo de la consola	Nombre del campo del conjunto de datos	Definición
Etiquetas de instancia	ec2_tags	Las etiquetas asociadas al ID de EC2 instancia de Amazon
Zona de aterrizaje	malz_flag	Marcar una cuenta relacionada con Malz
Cobertura del período de mantenimiento	mw_covered_flag	Si una instancia tiene al menos una ventana de mantenimiento habilitada con una fecha de ejecución futura, se considera cubierta y, de lo contrario, no está cubierta
Fecha y hora de ejecución de la ventana de mantenimiento	Hora de ejecución más temprana de la ventana	La próxima vez se espera que se ejecute la ventana de mantenimiento
Fecha y hora de ejecución de la ventana de mantenimiento	Hora de ejecución más temprana de la ventana	La próxima vez se espera que se ejecute la ventana de mantenimiento
Cuenta de producción	prod_account	Identificador de las cuentas AMS prod y no prod, en función de si el nombre de la cuenta incluye el valor «PROD» o «NONPROD».
Fecha y hora del informe	dataset_datetime	La fecha y la hora en que se generó el informe.
Nombre de la pila	instance_stack_name	Nombre de la pila que contiene la instancia

Nombre del campo de la consola	Nombre del campo del conjunto de datos	Definición
Tipo de pila	instance_stack_type	Pila de AMS (infraestructura de AMS dentro de la cuenta del cliente) o pila de clientes (infraestructura gestionada por AMS que admite las aplicaciones de los clientes)

Detalles del parche

Este informe proporciona los detalles del parche y la cobertura del período de mantenimiento de varias instancias.

Este informe proporciona:

- Datos sobre los grupos de parches y sus tipos.
- Datos sobre las ventanas de mantenimiento, la duración, el límite, las fechas futuras de ejecución de las ventanas de mantenimiento (programación) y las instancias afectadas en cada ventana.
- Datos sobre todos los sistemas operativos de la cuenta y el número de instancias en las que está instalado el sistema operativo.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Fecha y hora del informe	dataset_datetime	La fecha y la hora en que se generó el informe.
ID de cuenta	aws_account_id	AWS ID de cuenta al que pertenece el ID de instancia
Nombre de cuenta	account_name	AWS nombre de cuenta
Estado de la cuenta	estado_de la cuenta	Estado de la cuenta AMS

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Cumple con las normas: crítico	compliant_crítico	Recuento de parches compatibles con una gravedad «crítica»
Cumple con las normas: alta	compliant_high	Recuento de parches compatibles con una gravedad «alta»
Cumple con las normas: media	compliant_medium	Recuento de parches compatibles con una gravedad «media»
Cumple con las normas: bajo	compliant_low	Recuento de parches compatibles con una gravedad «baja»
Cumple con los requisitos: informativo	compliant_informativo	Recuento de parches compatibles con una gravedad «informativa»
Cumple con las normas: sin especificar	compliant_unspecified	Número de parches compatibles con una gravedad «no especificada»
Cumple con las normas: total	compliant_total	Recuento de parches compatibles (todos los niveles de gravedad)
ID de instancia	instance_id	ID de la EC2 instancia
Nombre de instancia	nombre_instancia	Nombre de la instancia EC2
	account_sla	Nivel de servicio de cuentas AMS

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Tipo de plataforma de instancia	instance_platform_type	Tipo de sistema operativo (SO)
Nombre de la plataforma de la instancia	instance_platform_name	Nombre del sistema operativo (SO)
Tipo de grupo de parches de instancias	instance_patch_group_type	DEFAULT: grupo de parches predeterminado con ventana de mantenimiento predeterminada, determinada por la etiqueta: True de la instancia AMSDefault PatchGroup CLIENTE: grupo de parches creado por el cliente NOT_ASSIGNED: no se ha asignado ningún grupo de parches
Grupo de parches de instancias	instance_patch_group	Nombre del grupo de parches utilizado para agrupar las instancias y aplicar el mismo período de mantenimiento
Estado de la instancia	instance_state	Estado dentro del ciclo de vida de la instancia EC2
Etiquetas de instancia	ec2_tags	Las etiquetas asociadas al ID de EC2 instancia de Amazon
Ventana de mantenimiento de última ejecución	last_execution_window	La última vez que se ejecutó la ventana de mantenimiento
ID de la ventana de mantenimiento	window_id	ID de la ventana de mantenimiento

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Estado de la ventana de mantenimiento	window_state	Estado de la ventana de mantenimiento
Tipo de ventana de mantenimiento	tipo_ventana	Tipo de ventana de mantenimiento
Fecha y hora de la próxima ejecución de la ventana de mantenimiento	window_next execution_time	La próxima vez se espera que se ejecute la ventana de mantenimiento
Duración del período de mantenimiento (horas)	duración de la ventana	La duración del período de mantenimiento en horas
Cobertura del período de mantenimiento	mw_covered_flag	Si una instancia tiene al menos una ventana de mantenimiento habilitada con una fecha de ejecución futura, se considera cubierta y, de lo contrario, no está cubierta
No compatible: crítico	noncompliant_critical	Recuento de parches no conformes con una gravedad «crítica»
No conformes: alto	noncompliant_high	Recuento de parches no conformes con una gravedad «alta»
No conforme: medio	noncompliant_medium	Recuento de parches no conformes con una gravedad «media»
No conformes: bajo	noncompliant_low	Recuento de parches no conformes con una gravedad «baja»

Nombre del campo	Nombre del campo del conjunto de datos	Definición
No conformes: informativo	no conforme _informativo	Recuento de parches no conformes con una gravedad «informativa»
No conforme: sin especificar	no conforme _sin especificar	Recuento de parches no conformes con una gravedad «no especificada»
No conformes: total	noncompliant_total	Recuento de parches no conformes (todos los grados de gravedad)
ID de referencia del parche	patch_baseline_id	La línea base del parche está actualmente conectada a la instancia
Estado del parche	patch_status	Estado general de cumplimiento de los parches. Si falta al menos un parche, la instancia se considera no compatible; de lo contrario, es compatible.
Cuenta de producción	prod_account	Identificador de las cuentas AMS prod y no prod, en función de si el nombre de la cuenta incluye el valor «PROD» o «NONPROD».
Tipo de pila	instance_stack_type	Pila de AMS (infraestructura de AMS dentro de la cuenta del cliente) o pila de clientes (infraestructura gestionada por AMS que admite las aplicaciones de los clientes)

Nombre del campo	Nombre del campo del conjunto de datos	Definición
	window_next_exec_yyyyyy	El año forma parte de window_next_execution_time
	window_next_exec_mm	El mes forma parte de window_next_execution_time
	Window_Next_Exec_D	Día: parte de window_next_execution_time
	window_next_exec_HHMM	Hora: parte minuciosa de window_next_execution_time

Instancias en las que no se incluyeron parches

Este informe proporciona detalles sobre las instancias a las que no se les aplicaron los parches durante la última ejecución del período de mantenimiento.

Este informe proporciona:

- Datos sobre los parches faltantes a nivel de ID de parche.
- Datos sobre todas las instancias a las que les falta al menos un parche y atributos como la gravedad del parche, los días sin corregir, el intervalo y la fecha de lanzamiento del parche.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Fecha y hora del informe	dataset_datetime	La fecha y la hora en que se generó el informe
ID de cuenta	aws_account_id	AWS ID de cuenta al que pertenece el ID de instancia
Nombre de cuenta	account_name	AWS nombre de cuenta

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Nombre del cliente: padre	customer_name_parent	
Nombre del cliente	customer_name	
Cuenta de producción	prod_account	Identificador de las cuentas AMS prod o no prod, en función de si el nombre de la cuenta incluye el valor «PROD» o «NONPROD».
Estado de la cuenta	estado_de la cuenta	Estado de la cuenta AMS
Account Type	tipo_cuenta	
	account_sla	Nivel de servicio de cuentas AMS
ID de instancia	instance_id	ID de tu EC2 instancia
Nombre de instancia	nombre_instancia	Nombre de la instancia EC2
Tipo de plataforma de instancia	instance_platform_type	Tipo de sistema operativo (SO)
Estado de la instancia	instance_state	Estado dentro del ciclo de vida de la instancia EC2
Etiquetas de instancia	ec2_tags	Las etiquetas asociadas al ID de EC2 instancia de Amazon
ID del parche	patch_id	ID del parche publicado
Gravedad del parche	patch_sev	Gravedad del parche por editor
Clasificación de los parches	patch_class	Clasificación del parche según el editor del parche

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Fecha y hora de lanzamiento del parche (UTC)	release_dt_utc	Fecha de lanzamiento del parche por editor
Estado de instalación del parche	install_state	Estado de instalación del parche en cada instancia por SSM
Días sin parches	days_unpatched	Número de días sin parchear la instancia desde el último escaneo de SSM
Rango de días sin parchear	days_unpatched_bucket	Grupo de días sin parchear

Informe de Backup (diario)

El informe de respaldo cubre las regiones principales y secundarias (cuando corresponda). Abarca el estado de las copias de seguridad (éxito o error) y los datos sobre las instantáneas realizadas.

Este informe proporciona:

- Estado de Backup
- Número de instantáneas tomadas
- Punto de recuperación
- Información sobre el plan de Backup y el almacén

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Fecha y hora del informe	dataset_datetime	La fecha y la hora en que se generó el informe.
ID de cuenta	aws_account_id	ID de cuenta de AWS a la que pertenece el ID de instancia

Nombre del campo	Nombre del campo del conjunto de datos	Definición
ID de cuenta de administrador	aws_admin_account_id	Cuenta de confianza habilitada por usted. AWS Organizations
Nombre de la cuenta	account_name	Nombre de la cuenta de AWS
SLA de la cuenta	account_sla	Compromiso de servicio de la cuenta AMS
	malz_flag	Marcar para una cuenta relacionada con Malz
	malz_role	Función MALZ
	access_restrictions	Regiones a las que está restringido el acceso
Snapshot de backup: fecha y hora de inicio programadas	start_by_dt_utc	Marca de tiempo en la que está previsto que comience la instantánea
Fecha y hora de inicio reales de la instantánea de backup	creation_dt_utc	Marca de tiempo en que comienza realmente la instantánea
Fecha y hora de finalización de la instantánea de Backup	completion_dt_utc	Marca de tiempo en que se completa la instantánea
Fecha y hora de caducidad de la instantánea de Backup	expiration_dt_utc	Fecha y hora de caducidad de la instantánea
Estado de Backup Job	backup_job_status	Estado de la instantánea
Tipo de Backup	backup_type	Tipo de copia de seguridad
ID del trabajo de Backup	backup_job_id	El identificador único del trabajo de copia de seguridad

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Tamaño del Backup en bytes	tamaño_de_copia de seguridad en bytes	El tamaño de la copia de seguridad en bytes
Plan de Backup (ARN)	backup_plan_arn	El plan de respaldo (ARN)
ID del plan de Backup	backup_plan_id	Identificador único del plan de Backup
Nombre del plan de copias de seguridad	backup_plan_name	El nombre del plan de Backup
Versión del plan de Backup	backup_plan_version	La versión del plan de respaldo
ID de regla de Backup	backup_rule_id	El identificador de la regla de respaldo
ARN de Backup Vault	backup_vault_arn	ARN de Backup Vault
Nombre del almacén de copias de seguridad	backup_vault_name	El nombre del almacén de respaldo
ARN del rol de IAM	iam_role_arn	El rol de IAM (ARN)
ID de instancia	instance_id	ID de instancia único
Estado de la instancia	instance_state	Estado de la instancia
Etiquetas de instancia	ec2_tags	Las etiquetas asociadas al ID de instancia EC2
ARN de recurso	resource_arn	El nombre del recurso de Amazon
ID de recurso	resource_id	El identificador único del recurso

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Región de recursos	región_recurso	Las regiones principales (y secundarias, cuando proceda) del recurso.
Tipo de recurso	resource_type	El tipo de recurso
Punto de recuperación (ARN)	recovery_point_arn	El ARN del punto de recuperación
ID del punto de recuperación	recovery_point_id	El identificador único del punto de recuperación
Estado del punto de recuperación	recovery_point_status	Estado del punto de recuperación
El punto de recuperación se elimina después de días	recovery_point_delete_after_days	El punto de recuperación se elimina después de días
El punto de recuperación se traslada a una cámara frigorífica después de días	recovery_point_move_to_cold_storage_after_days	Número de días transcurridos desde la fecha de finalización en que la instantánea de la copia de seguridad se traslada a una cámara frigorífica
Estado de cifrado del punto de recuperación	recovery_point_is_encrypted	Estado de cifrado del punto de recuperación
Clave de cifrado de punto de recuperación (ARN)	recovery_point_encryption_key_arn	Clave de cifrado del punto de recuperación (ARN)
ID de pila	stack_id	Identificador único de la pila de Cloudformation
Nombre de la pila	stack_name	Nombre de la pila

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Etiqueta: Grupo de parches predeterminado de AMS	tag_ams_default_patch_group	Valor de etiqueta: Grupo de parches predeterminado de AMS
Etiqueta: ID de aplicación	tag_app_id	Valor de etiqueta: ID de aplicación
Etiqueta: Nombre de la aplicación	tag_app_name	Valor de etiqueta: nombre de la aplicación
Etiqueta: Backup	tag_backup	Valor de etiqueta: Backup
Etiqueta: Marco de cumplimiento	tag_compliance_framework	Valor de etiqueta: Marco de cumplimiento
Etiqueta: Centro de costos	tag_cost_center	Valor de etiqueta: Centro de costes
Etiqueta: Cliente	tag_customer	Valor de etiqueta: Cliente
Etiqueta: Clasificación de datos	tag_data_classification	Valor de etiqueta: Clasificación de datos
Etiqueta: Tipo de entorno	tag_environment_type	Valor de etiqueta: Tipo de entorno
Etiqueta: Horas de operación	tag_horas_de_operación	Valor de etiqueta: Horas de operación
Etiqueta: Equipo propietario	tag_owner_team	Valor de etiqueta: equipo propietario
Etiqueta: Correo electrónico del equipo propietario	tag_owner_team_email	Valor de etiqueta: correo electrónico del equipo propietario

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Etiqueta: Patch Group	tag_patch_group	Valor de etiqueta: Patch Group
Etiqueta: Support Priority	tag_support_priority	Valor de etiqueta: Support Priority
Estado del volumen	estado_volumen	Estado del volumen

Informe de incidentes (semanal)

Este informe proporciona la lista agregada de incidentes junto con su prioridad, gravedad y estado más reciente, e incluye:

- Datos sobre los casos de soporte clasificados como incidentes en la cuenta gestionada
- Información sobre incidentes necesaria para visualizar las métricas de incidentes de la cuenta gestionada
- Datos sobre las categorías de incidentes y el estado de la solución de cada incidente

Tanto la visualización como los datos están disponibles para el informe semanal de incidentes.

- Se puede acceder a la visualización a través de la consola AMS de la cuenta a través de la página de informes.
- Se puede acceder al conjunto de datos con el siguiente esquema a través del bucket de S3 de la cuenta gestionada.
- Utilice los campos de fecha proporcionados para filtrar los incidentes según el mes, el trimestre, la semana y el and/or día en que se creó o resolvió el incidente.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Fecha y hora del informe	dataset_datetime	La fecha y la hora en que se generó el informe.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
ID de cuenta	aws_account_id	AWS ID de cuenta a la que pertenece el incidente.
ID de cuenta de administrador	aws_admin_account_id	Cuenta de confianza habilitada por usted. AWS Organizations
Nombre de la cuenta	account_name	AWS nombre de cuenta.
ID de caso	case_id	El identificador del incidente.
Mes de creación	created_month	El mes en que se creó el incidente.
Prioridad	priority	La prioridad del incidente.
Gravedad	severity	La gravedad del incidente.
Estado	status	El estado del incidente.
Categoría	yuma_category	La categoría del incidente.
Día de creación	created_day	El día en que se creó el incidente en el formato. YYYY-MM-DD

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Semana de creación	created_wk	La semana en que se creó el incidente en formato YYYY-WW. De domingo a sábado se contabilizan el principio y el final de la semana. La semana es del 01 al 25. La semana 01 es siempre la semana que contiene el primer día del año. Por ejemplo, el 31 de diciembre de 2021 y el 1 de enero de 2022 corresponden a la semana 2024-01.
Trimestre creado	created_qtr	El trimestre en el que se creó el incidente en formato AAAA. Del 01/01 al 31/03 se definen como Q1, y así sucesivamente.
Día resuelto	resolved_day	El día en que se resolvió el incidente en el formato. YYYY-MM-DD
Semana resuelta	resolved_wk	La semana en que se resolvió el incidente en formato YYYY-WW. De domingo a sábado se contabilizan el principio y el final de la semana. La semana es del 01 al 25. La semana 01 es siempre la semana que contiene el primer día del año. Por ejemplo, el 31-12-2021 y el 2024-01-01 están en la semana 2024-01.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Mes resuelto	mes_resuelto	El mes en que se resolvió el incidente en formato AAAA-MM.
Trimestre resuelto	resolved_qtr	El trimestre en el que se resolvió el incidente en formato AAAA. Del 01/01 al 31/03 se definen como Q1, y así sucesivamente.
Se creó la regla de agrupación	regla_agrupamiento	La regla de agrupación que se aplica al incidente. Ya sea «no_grouping» o «instance_grouping».
Instancia IDs	instance_ids	La instancia asociada al incidente.
Número de alertas	número_de_alertas	El número de alertas asociadas a ese incidente. Si tiene habilitada la agrupación, este número puede ser mayor que 1. Si no tiene habilitada la agrupación, siempre será 1.
Creado en	created_at	La marca de tiempo en que se creó el incidente.
Alarma ARNs	alarm_arns	El nombre del recurso de Amazon («arn») de las alarmas asociadas al incidente .

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Alarmas relacionadas	alarmas_relacionadas	Los nombres legibles para el ser humano de todas las alarmas asociadas al incidente .

Informe de facturación (mensual)

Detalles de los cargos de facturación

Este informe proporciona detalles sobre los cargos de facturación de AMS con las cuentas vinculadas y los servicios de AWS correspondientes.

Este informe proporciona:

- Datos sobre los cargos a nivel de servicio de AMS, los porcentajes de aumento, los niveles de servicio de AMS a nivel de cuenta y las tarifas de AMS.
- Datos sobre las cuentas vinculadas y los cargos por uso de AWS.

Important

El informe de facturación mensual solo está disponible en su cuenta de administrador pagador (MPA) o en la cuenta de cargos definida. Estas son las cuentas a las que se envía la factura mensual de AMS. Si no puede localizar estas cuentas, póngase en contacto con su administrador de prestación de servicios en la nube (CSDM) para obtener ayuda.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Fecha de facturación	date	El mes y el año del servicio facturado
ID de la cuenta del pagador	payer_account_id	El identificador de 12 dígitos que identifica la cuenta

Nombre del campo	Nombre del campo del conjunto de datos	Definición
		responsable del pago de los cargos de AMS
ID de la cuenta vinculada	linked_account_id	El identificador de 12 dígitos que identifica la cuenta AMS que consume los servicios que generan expansiones
AWS Nombre del servicio	product_name	El AWS servicio que se utilizó
AWS Cargos	aws_charges	Los AWS cargos por el nombre del AWS servicio en AWS el nombre del servicio
Plan de precios	plan_de precios	El plan de precios asociado a la cuenta vinculada
Grupo de servicios AMS	tier_uplifting_groups	Código de grupo de servicios AMS que determina el porcentaje de aumento
Proporción de elevación	porcentaje de aumento	El porcentaje de aumento (expresado como V.WXYZ decimal) se basa en el pricing_plan, el SLA y el servicio AWS
Cargos ajustados AWS	adjusted_aws_usage	AWS uso ajustado para AMS
Cargos elevados AWS	Uplifted_aws_charges	El porcentaje de cargos que se cobrarán AWS por AMS; $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$
EC2 Instancias gastadas por RDS	instances_ec2_rds_spend	Invierta en instancias de RDS EC2

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Cargos por instancia reservada	ris_charges	Cargos por instancia reservada
Aumento de los cargos por instancia reservada	uplifted_ris	El porcentaje de cargos de instancia reservada que se cobrará por AMS; $\text{ris\_charges} * \text{uplift\_percent}$
Cargos del Savings Plan	sp_charges	SavingsPlan cargos de uso
Cargos elevados del Plan de Ahorros	uplifted_sp	El porcentaje de cargos de los planes de ahorro que se cobrarán por el AMS; $\text{sp\_charges} * \text{uplift\_percent}$
Cargos de AMS	ams_charges	Costos totales de ams del producto: $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
Tarifa mínima prorrateada	mínimo prorrateado	El importe que cobramos para cumplir con el mínimo contractual
Cargos totales de AMS en la cuenta vinculada	linked_account_total ams_charges	Suma de todos los cargos de la linked_account
Cargos totales de AMS de la cuenta del pagador	pays_account_total ams_charges	Suma de todos los cargos de la cuenta del pagador
Cuota mínima	tarifas_mínimas	Tarifas mínimas de AMS (si corresponde)

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Reserved Instance y Savings Plan discount	adj_ri_sp_charges	RI/SP discount to be applied against RI/SPcargos (aplicables en determinadas circunstancias)

Informes agregados

Los informes de autoservicio agregados (SSR) le proporcionan una vista de los informes de autoservicio existentes agregados a nivel de la organización y de forma transversal. Esto le permite ver los indicadores operativos clave, como el cumplimiento de los parches, la cobertura de respaldo y los incidentes, en todas las cuentas gestionadas por AMS dentro de su empresa. AWS Organizations

El SSR agregado está disponible en todos los anuncios comerciales en los Regiones de AWS que AWS Managed Services esté disponible. Para obtener una lista completa de las regiones disponibles, consulte la [tabla de regiones](#).

Habilite los informes agregados

Debe gestionar la SSR agregada desde una cuenta de AWS Organizations [administración](#). La cuenta de administración es la AWS cuenta que utilizó para crear su organización.

Para habilitar el SSR agregado en una cuenta de AWS Organizations administración integrada en AMS, acceda a la consola de AMS y vaya a Informes. Seleccione Organization Access en la top-right-hand esquina para abrir el panel [AWS Managed Services Console: Organization View](#). Desde este panel, puede administrar la funcionalidad de SSR agregado.

AWS Organizations Las cuentas de administración que no están integradas en AMS no tienen acceso a la consola AMS. Para habilitar el SSR agregado para una cuenta AWS Organizations de administración que no esté integrada en AMS, primero autentifíquese en su cuenta Cuenta de AWS, vaya a la [AWS consola](#) y busque Managed Services. Se abrirá la página de marketing de AMS. En esta página, seleccione el enlace Organization Access en la barra de navegación para abrir la consola de AWS Managed Services: Organization View, donde puede administrar la funcionalidad de SSR agregada.

La primera vez que acceda a [AWS Managed Services Console: Organization View](#), complete los siguientes pasos:

1. Si aún no lo ha hecho AWS Organizations, seleccione Activar en AWS Organizations la consola. Para obtener información adicional sobre la configuración AWS Organizations, consulta la [Guía del AWS Organizations usuario](#). Puede omitir este paso si ya lo utiliza AWS Organizations.
2. Para habilitar el servicio agregado de informes de autoservicio, seleccione Habilitar el acceso confiable en la consola.
3. (Opcional) Registre a un administrador delegado para que tenga acceso de lectura a la vista de la organización.

Vea los informes agregados como administrador delegado

Un administrador delegado es la cuenta que usted elige para tener acceso de lectura a los informes agregados. El administrador delegado debe ser una cuenta incorporada a AMS y ser la única cuenta que tenga acceso de lectura a los informes agregados.

Para elegir un administrador delegado, introduzca el ID de la cuenta en el paso 3 de la AWS Managed Services Console: Organization View. Solo puede tener registrada una cuenta de administrador delegado a la vez. Tenga en cuenta que la cuenta de administrador delegado debe ser una cuenta administrada por AMS.

Para actualizar una cuenta de administrador delegado, vaya a la [AWS Managed Services Console: Organization View](#) y seleccione Eliminar el administrador delegado. La consola le pide que introduzca un nuevo ID de cuenta para registrarse como administrador delegado.

Lea los informes agregados

Si no registras a un administrador delegado y tu cuenta de AWS Organizations administración está integrada en AMS, la cuenta de AWS Organizations administración tendrá acceso de lectura a los informes agregados de forma predeterminada. Si AMS no administra la cuenta de AWS Organizations administración, debe elegir una cuenta de administrador delegado para tener acceso de lectura a los informes agregados.

En cualquier momento, solo una cuenta incorporada a AMS tiene acceso de lectura a los informes agregados, ya sea la cuenta de AWS Organizations administración o el administrador delegado registrado. Todas las demás cuentas de miembros de su organización (e incorporadas a AMS) seguirán teniendo acceso únicamente a los informes de una sola cuenta para cada cuenta individual.

[Después de activar el SSR agregado, navegue hasta sus informes.](#) Todos los informes de autoservicio existentes aparecen en esta sección y una etiqueta azul indica que se han agregado. Tenga en cuenta que debe acceder a la consola AMS desde la cuenta que eligió para tener acceso

de lectura a los informes agregados. Se trata de la cuenta AWS Organizations de administración o de administrador delegado.

Tras activar la SSR agregada, los informes agregados estarán disponibles a partir del siguiente ciclo de elaboración de informes.

Deshabilite los informes agregados

Para deshabilitar el SSR agregado, abra la [consola de AWS Managed Services: Organization View](#). Seleccione Inhabilitar el acceso de confianza. Tras deshabilitar el acceso de confianza para el SSR agregado, los informes de autoservicio de AMS dejarán de agregarse a nivel de la organización, en todas las cuentas. Tenga en cuenta también que la desactivación se efectuará a partir del siguiente ciclo de presentación de informes.

Tras desactivar el SSR agregado, hay que esperar hasta que los informes de la consola AMS aparezcan como informes de una sola cuenta. Este retraso se debe a que la desactivación de la función se produce a partir del siguiente ciclo de generación de informes.

Paneles de informes de autoservicio de AMS

Los informes de autoservicio de AMS ofrecen dos paneles: y. [Panel de control de Resource Tagger](#)
[Panel de reglas de configuración de seguridad](#)

Panel de control de Resource Tagger

El panel de control del etiquetador de recursos de AMS proporciona información detallada sobre los recursos compatibles con Resource Tagger, así como el estado actual de las etiquetas que Resource Tagger está configurado para aplicar a esos recursos.

Cobertura del etiquetador de recursos por tipo de recurso

Este conjunto de datos consta de una lista de recursos que tienen etiquetas administradas por Resource Tagger.

La cobertura de recursos por tipo de recurso se visualiza en cuatro gráficos de líneas que describen las siguientes métricas:

- Recuento de recursos: el número total de recursos de la región, por tipo de recurso.
- Recursos a los que les faltan etiquetas administradas: el número total de recursos de la región, por tipo de recurso, que requieren etiquetas administradas pero que no están etiquetados por el etiquetador de recursos.

- **Recursos no gestionados:** el número total de recursos de la región, por tipo de recurso, a los que Resource Tagger no les ha aplicado etiquetas gestionadas. Por lo general, esto significa que estos recursos no coinciden con ninguna configuración de Resource Tagger o que están excluidos explícitamente de las configuraciones.
- **Recursos gestionados:** métrica equivalente a la de recursos no gestionados (recuento de recursos: recursos no gestionados).

En la siguiente tabla se enumeran los datos proporcionados por este informe.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Fecha y hora del informe	dataset_datetime	Fecha y hora en que se generó el informe (hora UTC)
Cuenta de AWS ID	aws_account_id	Cuenta de AWS ID
ID de cuenta de administrador	aws_admin_account_id	Cuenta de confianza habilitada por usted. AWS Organizations
Región	region	Región de AWS
Tipo de recurso	resource_type	Este campo identifica el tipo de recurso. Solo se incluyen los tipos de recursos compatibles con Resource Tagger.
Recuento de recursos	conteo de recursos	Número de recursos (del tipo de recurso especificado) desplegados en esta región.
ResourcesMissingManagedTags	resource_missing_managed_tags_count	Número de recursos (del tipo de recurso especificado) que requieren etiquetas administradas, según los perfiles de configuración, pero que

Nombre del campo	Nombre del campo del conjunto de datos	Definición
		Resource Tagger aún no los ha etiquetado.
UnmanagedResources	unmanaged_resource_count	Número de recursos (del tipo de recurso especificado) a los que Resource Tagger no ha aplicado etiquetas administradas. Por lo general, estos recursos no coincidían con ningún bloque de configuración de Resource Tagger o se excluyen explícitamente de los bloques de configuración.

Cumplimiento de las reglas de configuración de Resource Tagger

Este conjunto de datos consiste en una lista de recursos Región de AWS, clasificados por tipo de recurso, a los que se les ha aplicado un perfil de configuración determinado. Se visualiza como un gráfico de líneas.

En la siguiente tabla se enumeran los datos proporcionados por este informe.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Fecha y hora del informe	dataset_datetime	Fecha y hora en que se generó el informe (hora UTC)
Cuenta de AWS ID	aws_account_id	Cuenta de AWS ID
ID de cuenta de administrador	aws_admin_account_id	Cuenta de confianza habilitada por usted. AWS Organizations
Región	region	Región de AWS

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Tipo de recurso	resource_type	Este campo identifica el tipo de recurso. Solo se incluyen los tipos de recursos compatibles con Resource Tagger.
ID del perfil de configuración	configuration_profile_id	El ID del perfil de configuración del etiquetador de recursos. Se utiliza un perfil de configuración para definir las políticas y reglas que se utilizan para etiquetar los recursos.
MatchingResourceCount	resource_count	Número de recursos (del tipo de recurso especificado) que coinciden con el ID del perfil de configuración del etiquetador de recursos. Para que un recurso coincida con el perfil de configuración, el perfil debe estar habilitado y el recurso debe coincidir con la regla del perfil.

Resource Tagger: recursos no compatibles

Este conjunto de datos consta de una lista de recursos que no son compatibles con una única configuración de Resource Tagger. Estos datos son un resumen diario del cumplimiento de los recursos y muestran el estado de los recursos de los clientes en el momento en que se envían estos informes a las cuentas de los clientes (no hay una vista histórica). Se visualiza como una tabla dinámica que consta de recursos que no cumplen con los requisitos de una configuración determinada.

En la siguiente tabla se enumeran los datos proporcionados por este informe.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Fecha y hora del informe	dataset_datetime	Fecha y hora en que se generó el informe (hora UTC)
Cuenta de AWS ID	aws_account_id	Cuenta de AWS ID
ID de cuenta de administrador	aws_admin_account_id	Cuenta de confianza habilitada por usted. AWS Organizations
Región	region	Región de AWS
Tipo de recurso	resource_type	Este campo identifica el tipo de recurso. Solo se incluyen los tipos de recursos compatibles con Resource Tagger.
ID de recurso	resource_id	El identificador único de los recursos compatibles con Resource Tagger.
Estado de cobertura	estado_de cobertura	Este campo indica si el recurso está etiquetado como lo configuró el ID de configuración del etiquetador de recursos.
ID del perfil de configuración	configuration_profile_id	El ID del perfil de configuración del etiquetador de recursos. Se utiliza un perfil de configuración para definir las políticas y reglas que se

Nombre del campo	Nombre del campo del conjunto de datos	Definición
		utilizan para etiquetar los recursos.

Panel de reglas de configuración de seguridad

El panel de reglas de Security Config ofrece una visión detallada del cumplimiento de los recursos y las AWS Config reglas de las cuentas AMS. Puede filtrar el informe por el nivel de severidad de las reglas para priorizar los hallazgos más importantes. En la siguiente tabla se enumeran los datos proporcionados por este informe.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
Cuenta de AWS ID	Cuenta de AWS ID	El identificador de la cuenta vinculado a los recursos relacionados.
ID de cuenta de administrador	aws_admin_account_id	Cuenta de confianza habilitada por usted. AWS Organizations
fecha y hora del informe	Fecha del informe	La fecha y la hora en que se generó el informe.
customer_name	Nombre del cliente	El nombre del cliente.
account_name	Nombre de la cuenta	El nombre asociado al ID de la cuenta
resource_id	ID de recurso	Un identificador de un recurso.
resource_region	Región de recursos	El Región de AWS lugar donde se encuentra el recurso.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
resource_type	Tipo de recurso	El tipo de recurso Servicio de AWS or.
nombre_recurso	Nombre del recurso	El nombre del recurso.
resource_ams_flag	Indicador AMS del recurso	Si el recurso es propiedad de AMS, este indicador se establece en TRUE. Si el recurso es propiedad del cliente, este indicador se establece en FALSE. Si no se conoce la propiedad, este indicador se establece en DESCONOCIDO.
config_rule	Regla de configuración	El nombre no personalizable de la regla de configuración.
config_rule_description	Descripción de la regla de configuración	Una descripción de la regla de configuración.
source_identifier	Identificador de fuente	Un identificador único para la regla de configuración gestionada y ningún identificador para una regla de configuración personalizada.
compliance_flag	Indicador de cumplimiento	Muestra si los recursos cumplen o no con las reglas de configuración.
tipo_regla	Tipo de regla	Indica si la regla está predefinida o personalizada.

Nombre del campo	Nombre del campo del conjunto de datos	Definición
exception_flag	Bandera de excepción	El indicador de excepción del recurso muestra la aceptación del riesgo en relación con un recurso que no cumple con las normas. Si el indicador de excepción del recurso es VERDADERO para un recurso, entonces el recurso está exento. Si el indicador de excepción es NULL, el recurso no está exento.
cal_dt	Date	La fecha de evaluación de la regla.
descripción_de_remediación	Descripción de la remediación	Una descripción de cómo corregir el cumplimiento de las normas.
severity	Gravedad	La gravedad de la regla de configuración indica el impacto del incumplimiento.
customs_action	Acción del cliente	Debe tomar las medidas necesarias para corregir esta regla.
recomendación	Recomendación	Una descripción de lo que comprueba la regla de configuración.
categoría_remediación	Categoría de remediación	Las acciones predeterminadas que adopta AMS cuando esta regla deja de ser compatible.

Política de conservación de los datos

AMS SSR tiene una política de retención de datos por informe después del período reportado, cuando los datos se borran y dejan de estar disponibles.

Nombre del informe	Consola SSR de retención de datos	Cubeta SSR S3 de retención de datos
Resumen de los detalles de la instancia (Patch Orchestrator)	2 meses	2 años
Detalles del parche	2 meses	2 años
Instancias en las que se omitieron parches durante la ejecución del período de mantenimiento	2 meses	2 años
Detalles de los cargos de facturación de AMS	2 años	2 años
Informe de Backup Diario	1 mes	2 años
Informe semanal de incidentes	2 meses	2 años
Panel de reglas de configuración de seguridad	3 meses	2 años
Panel de control de Resource Tagger	1 año	2 años

Fuera de SSR

Para desconectarse del servicio SSR, cree una solicitud de servicio (SR) a través de la consola AMS. Tras enviar la SR, un ingeniero de operaciones de AMS le ayudará a abandonar el SSR. En el SR, indique el motivo por el que desea dejar el servicio.

Para eliminar una cuenta y limpiar los recursos, crea una SR a través de la consola AMS. Tras enviar el SR, un ingeniero de operaciones de AMS le ayudará a eliminar el bucket de Amazon S3 del SSR.

Si se desconecta de AMS, se desconectará automáticamente de la consola AMS SSR. AMS deja de enviar datos a tu cuenta automáticamente. AMS borra tu bucket de SSR S3 como parte del proceso de desconexión.

Informes de incidentes, solicitudes de servicio y preguntas sobre facturación en AMS

Temas

- [Administración de incidentes](#)
- [Gestión de solicitudes de servicio](#)
- [Preguntas sobre facturación](#)

Con AWS Managed Services (AMS), puede solicitar ayuda con problemas operativos y solicitudes en cualquier momento a través de la consola AMS. Los ingenieros de operaciones de AMS están disponibles para responder a sus incidentes y solicitudes de servicio las 24 horas del día, los 7 días de la semana, con acuerdos de nivel de servicio (SLAs) y objetivos de nivel de servicio (SLOs) con plazos de respuesta, según el nivel de servicio de la cuenta que haya seleccionado (Plus, Premium). Los ingenieros de operaciones de AMS le notifican de forma proactiva las alertas y preguntas importantes mediante los mismos mecanismos.

Administración de incidentes

Temas

- [¿Qué es la gestión de incidentes?](#)
- [Compromisos del servicio de gestión de incidentes](#)
- [Ejemplos de gestión de incidentes](#)

Los incidentes son problemas de Servicio de AWS rendimiento que afectan a su entorno gestionado, según lo determine AWS Managed Services (AMS) o usted. Los incidentes identificados por el equipo de AMS se reciben primero como «eventos»: un cambio en el estado del sistema que se captura mediante la supervisión. Si se supera un umbral configurado, el evento activa una alarma, también denominada alerta. El equipo de operaciones de AMS determina si el evento no tiene ningún impacto, si se trata de un incidente (una interrupción o degradación del servicio) o de un problema (la causa raíz subyacente de uno o más incidentes resueltos).

El equipo de AMS también recibe los incidentes identificados por usted a través del Soporte centro o mediante programación mediante la [API de AWS Support](#) con el código de servicio. `sentinel-report-incident`

Una vez que el equipo de operaciones de AMS recibe el incidente, lo revisa para garantizar que no se clasifique mejor como una solicitud de servicio. Si debe clasificarse como una solicitud de servicio, se reclasifica inmediatamente y el equipo de solicitudes de servicio de AMS asume el control y se le notifica. Si el operador receptor puede resolver el incidente, se toman medidas para resolverlo de inmediato. Los operadores de AMS consultan la documentación interna para encontrar una solución y, si es necesario, trasladan el incidente a otros recursos de apoyo hasta que se resuelva. Para mantenerse informado en cada paso del proceso de resolución de incidentes, asegúrese de rellenar la opción Correos electrónicos de CC y, si va a conectarse por federación, inicie sesión antes de seguir el enlace del correo electrónico que envía AMS. Una vez resuelto, el equipo de operaciones de AMS documenta el incidente y la resolución para su uso futuro.

Si la resolución de un incidente requiere cambios en la infraestructura, es posible que sea necesario realizar una revisión de seguridad. Los cambios en la infraestructura que pueden requerir una revisión de seguridad incluyen los relacionados con la IAM, la política basada en los recursos o la aprobación de riesgos. Este tipo de incidentes requieren que un ingeniero de operaciones de AMS cree una RFC antes de realizar el cambio, y se requiere su aprobación para dicha RFC. Por ejemplo, si la resolución del incidente requiriera la actualización de una política de IAM, se realizaría una revisión de seguridad de AMS y, a continuación, un ingeniero de operaciones de AMS crearía una RFC con Management | Advanced stack components | Identity and Access Management (IAM) | Actualizar el tipo de cambio de entidad o política (ct-27tuth19k52b4) y esperaría a que usted aprobara la RFC antes de continuar.

Note

El AMS ahora permite la resolución de incidentes que requieren que se realicen cambios en la infraestructura sin el paso adicional de la aprobación de la RFC. Si los cambios necesarios para resolver el incidente NO requieren una revisión de seguridad (el cambio no está relacionado con la IAM, ni con una política basada en los recursos, ni con la aprobación de riesgos), AMS puede realizar los cambios en función de su aprobación recibida en el incidente, sin necesidad de una aprobación independiente en una RFC.

[Para ver las definiciones de los términos de gestión de incidentes, consulte los términos clave de AMS.](#)

Para entender la evolución de los incidentes, consulta [Cómo obtener ayuda](#).

Para obtener una descripción de la respuesta de AMS a los incidentes, consulte [Respuesta a los incidentes de AMS](#).

¿Qué es la gestión de incidentes?

La gestión de incidentes es el proceso que utiliza AMS para registrar los incidentes activos, actuar en consecuencia, comunicar el progreso y notificar los incidentes activos.

El objetivo del proceso de gestión de incidentes es garantizar que el funcionamiento normal del servicio gestionado se restablezca lo antes posible, que se minimice el impacto empresarial y que todas las partes interesadas estén informadas.

Algunos ejemplos de incidentes incluyen (pero no se limitan a) la pérdida o la degradación de la conectividad de la red, un proceso o API que no responde o una tarea programada que no se está realizando (por ejemplo, una copia de seguridad fallida).

El siguiente gráfico muestra el flujo de trabajo de un incidente que usted notifique a AMS.

Este gráfico muestra el flujo de trabajo de un incidente que AMS le notifica.

Prioridad de incidentes

Los incidentes creados en el centro de soporte de AWS, la consola o la API de soporte (SAPI) tienen clasificaciones diferentes a las de los incidentes creados en la consola AMS.

- Bajo: las funciones no críticas de su servicio o aplicación empresarial relacionadas con los recursos de AWS o AMS se ven afectadas.
- Medio: un servicio o una aplicación empresarial relacionados con los recursos de AWS and/or AMS se ve afectado moderadamente y funciona en un estado degradado.
- Alto: su empresa se ve afectada de forma significativa. Las funciones esenciales de su aplicación relacionadas con los recursos de AWS and/or AMS no están disponibles. Reservado para las interrupciones más críticas que afectan a los sistemas de producción.

Note

La consola de AWS Support ofrece cinco niveles de prioridad de incidentes que traducimos a los tres niveles de AMS.

¿Problema o incidente

Cuando AMS considera que un incidente revela un defecto mayor o una mala configuración y que podría repetirse, se considera un problema y no solo un incidente. En estos casos, AMS analiza el problema y ofrece sugerencias para resolverlo.

Compromisos del servicio de gestión de incidentes

Compromisos del servicio de gestión de incidentes

Evento o acción	Medición del compromiso de servicio
Caso 1: Se genera un evento con un impacto conocido. AMS abre un incidente y le informa. Caso 2: AMS se pone en contacto con usted para confirmar el impacto del evento. Usted confirma que el evento es un incidente. Caso 3: detectas un problema y envías un informe del incidente.	El reloj de respuesta y resolución de incidentes comienza cuando: Caso 1: AMS crea un incidente. Caso 2: Usted confirma que la alerta es un incidente. Caso 3: Usted envía un incidente. Los compromisos de servicio dependen de la prioridad del incidente creado.
Si envía el incidente, AMS envía una respuesta para confirmarlo. Si AMS crea el incidente en su nombre, no se envía una respuesta al incidente por separado.	El tiempo para la resolución de incidentes sigue corriendo. El tiempo de respuesta al incidente se detiene cuando AMS envía el acuse de recibo del incidente.  Note El tiempo dedicado a esperar sus comentarios no se incluye en los cálculos del tiempo de resolución de incidentes. En el caso de los incidentes que crea AMS, el tiempo de respuesta inicial es el momento en que se crea la

Evento o acción	Medición del compromiso de servicio
	notificación de incidente inicial que se le envía.
En el caso de los recursos o servicios en cuestión, AMS comprueba el estado de los recursos o servicios en cuestión para comprobar si: - El evento detectado por AMS o el incidente enviado por el cliente se considera incidente , y - el incidente tiene la prioridad correcta, y Si un incidente que envíe no tiene la prioridad correcta, AMS volverá a priorizarlo. Si AMS cambia la prioridad de un incidente, se le enviará una notificación con las razones que justifican el cambio de prioridad. En algunos casos, es posible que un problema que haya presentado no califique como incidente, según la causa. En esos casos, AMS cierra el incidente y te envía una notificación en la que se explica el motivo. Independientemente de la categorización del evento, AMS trabaja con usted para ayudarlo cuando sea necesario. Para entender las reglas de categorización de incidentes, consulte. Prioridad de incidentes	En caso de que la prioridad del incidente cambie, se aplicará el compromiso de servicio para la nueva prioridad; el tiempo sigue corriendo. En los casos en que un incidente se cierra porque no cumple con la definición de incidente, no se aplican los compromisos de servicio; el reloj se detiene.

Evento o acción	Medición del compromiso de servicio
AMS trabaja en el incidente para resolverlo dentro del compromiso de servicio. En algunos casos, si AMS determina que las pilas o los recursos no disponibles no se pueden resolver a tiempo, AMS ofrecerá la restauración de la infraestructura como una opción de resolución. La restauración de la infraestructura implica 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 (instantánea de EBS/RDS), a menos que especifique lo contrario. Se perderán los datos efímeros de las instancias individuales. EC2 Si no autoriza la restauración de la infraestructura según lo recomendado por AWS, no podrá optar a un crédito de servicio por el compromiso de servicio de tiempo de resolución de incidentes asociado.	El reloj se detiene cuando: - AMS ha restablecido todos los servicios o recursos no disponibles relacionados con ese incidente a un estado disponible, o - se inicia una restauración de la infraestructura.
Ocasionalmente, AMS necesita que usted aclare o tome medidas para que sus esfuerzos de resolución de incidentes sigan avanzando, a menos que cuente con una acción predefinida y aprobada. Como resultado, existe una comunicación entre AMS y usted para resolver los incidentes	El reloj se detiene cuando: AMS espera una respuesta o una acción por su parte. El reloj se reinicia cuando: AMS recibe tu respuesta o se completa la acción que AMS requiere de ti.

 Note

Para obtener una lista completa de los compromisos de servicio, descargue el [acuerdo de nivel de servicio de AMS](#).

Ejemplos de gestión de incidentes

Ejemplos de gestión de incidentes.

Temas

- [Pruebas de incidentes](#)
- [Denunciar incidentes](#)
- [Supervisión y actualización de incidentes](#)
- [Gestión de incidentes con la API AWS Support](#)
- [Responder a los incidentes generados por AMS](#)

Los siguientes ejemplos describen el uso de la consola AMS para enviar un incidente. Una vez enviado, el equipo de AMS trabajará con usted para resolver el incidente según su acuerdo de nivel de servicio (SLA).

Pruebas de incidentes

Al probar los envíos de incidentes de AMS, le pedimos que incluya en el texto del asunto esta bandera: AMSTestNoOpsActionRequired. Esta bandera le permite a AMS saber que el envío del incidente es solo para pruebas. Cuando los ingenieros de operaciones de AMS vean esa bandera, no responderán de ninguna manera a la notificación del incidente.

Denunciar incidentes

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.

YouTube Vídeo: [¿Cómo puedo denunciar un incidente desde la consola de AWS Managed Services?](#)

Supervisión y actualización de incidentes

Puede actualizar, supervisar y revisar los informes de incidentes y las solicitudes de servicio, ambos denominados casos, mediante la consola AMS o mediante programación mediante la Soporte API. Para obtener información sobre el uso de la Soporte API, consulte [DescribeCases](#) operación.

Para supervisar un caso, incidente o solicitud de servicio mediante la consola AMS, sigue estos pasos.

1. En el panel de informes de incidentes o solicitudes de servicio de la consola AMS, busque un caso y elija el Asunto para abrir una página de detalles con el estado actual y las correspondencias.

Cuando el equipo de operaciones de AMS actualiza un incidente o un caso de solicitud de servicio denunciado, recibes un correo electrónico y un enlace al incidente en la consola de AMS para que puedas responder. No puedes responder a la correspondencia sobre incidentes respondiendo al correo electrónico.

 Important

Debes haber introducido una dirección de correo electrónico para recibir notificaciones de cambios de estado en caso de solicitud de servicio o incidente. Las notificaciones solo se envían a la dirección de correo electrónico que se agregó al caso cuando se creó.

El enlace del correo electrónico de notificación no funcionará a menos que utilice un servidor de correo electrónico en su red federada de AMS. Sin embargo, puede responder a la correspondencia accediendo a su consola AMS y utilizando la página de detalles del caso.

2. Si hay muchos casos en la lista, puedes usar la opción Filtrar:

- Todos abiertos (predeterminado): utilice este filtro para ver todos los casos que no se han resuelto.
- Sin asignar: utilícelo si acaba de enviar el caso y no ha recibido ningún aviso de que el estado del caso haya cambiado. Tenga en cuenta que los incidentes y los casos de solicitud de servicio se abordan con diferente rapidez según la prioridad enviada (incidentes) o el acuerdo de nivel de servicio (solicitudes de servicio).
- Abrir: utilízalo si has recibido un aviso de que el caso es una acción de «Amazon pendiente»; esto significa que el caso se ha asignado pero aún no se ha empezado a trabajar.
- Reabierto: utilícela si ha recibido una notificación de que el caso se ha vuelto a abrir después de haberse resuelto.
- Trabajo en curso: utilícelo si ha recibido un aviso de que un operador ha empezado a trabajar en el caso.
- Acción pendiente del cliente: utilícela si ha recibido una solicitud de un operador para que tome medidas por su parte.
- Acción del cliente completada: utilícela si ha recibido una notificación de que su acción en el caso se ha procesado.

- Resuelto: utilícelo para ver los casos que sabe que se han resuelto. Los casos resueltos se mantienen en el historial durante doce meses.
 - Cualquier estado: utilice este filtro para ver todos los casos, independientemente del estado.
3. Para comprobar el estado más reciente, actualiza la página.
 4. Si hay tantas correspondencias que no aparecen todas en la página, selecciona Cargar más.
 5. Para actualizar el estado del caso, selecciona Responder, introduce la nueva correspondencia y, a continuación, selecciona Enviar.
 6. Para cerrar el caso una vez que se haya resuelto satisfactoriamente, selecciona Cerrar caso.
- ¡Asegúrese de calificar el servicio con una calificación de 1 a 5 estrellas para que AMS sepa cómo lo estamos haciendo!

Gestión de incidentes con la API AWS Support

La [API de AWS Support](#) le permite crear incidentes y añadirles correspondencia durante las investigaciones de sus problemas y las interacciones con el personal de AWS Support. La API de AWS Support modela gran parte del comportamiento del [AWS Support Center](#). Para obtener más información sobre cómo puede utilizar este servicio de AWS Support, consulte [Programming an AWS Support Case](#).

Note

Cuando utilice la API de AWS Support, o SAPI, para los incidentes de AMS Advanced, utilice este código de servicio: `sentinel-report-incident`.

Responder a los incidentes generados por AMS

AMS supervisa sus recursos de forma proactiva; para obtener más información, consulte [Supervisión y gestión de eventos](#). A veces, AMS identifica y crea un caso de incidente, la mayoría de las veces para notificarle un incidente. En caso de que necesites tomar medidas para resolver un incidente, AMS envía una notificación a la información de contacto que has proporcionado para la cuenta. Usted responde a este incidente de la misma manera que respondería a cualquier otro incidente. Por lo general, respondes a los incidentes a través de la consola AMS; en algunos casos, es necesario ponerte en contacto por correo electrónico o por teléfono.

 Note

AMS envía las comunicaciones a la dirección de correo electrónico principal de su cuenta de AWS; le recomendamos añadir un alias de correo electrónico de contacto de operaciones alternativo para facilitar el proceso de gestión de incidentes. Esto se explica durante el proceso de incorporación de AMS y en la documentación de incorporación relacionada. Si ha proporcionado a AMS contactos no basados en recursos (de los que ha informado a su CSDM) durante la incorporación, se utilizarán esos contactos. Por ejemplo, puedes proporcionarte una lista de contactos llamada «SecurityContacts» para utilizarla en incidentes o notificaciones CSDMs/CAs relacionados con la seguridad. Sus etiquetas de contacto se instances/resources utilizan para los incidentes generados por AMS, si ha dado su consentimiento al CSDM para que utilice la información de las etiquetas.

[Para obtener más información sobre este servicio de notificaciones, consulte Notificaciones.](#)

Gestión de solicitudes de servicio

Temas

- [Cuándo utilizar una solicitud de servicio](#)
- [Cómo funciona la administración de solicitudes de servicio](#)
- [Probar una solicitud de servicio en AMS](#)
- [Crear una solicitud de servicio en AMS](#)
- [Supervisión y actualización de las solicitudes de servicio en AMS](#)
- [Responder a una solicitud de servicio generada por AMS](#)

Las solicitudes de servicio son comunicaciones dirigidas a AMS que usted crea para solicitar información o asesoramiento. Un buen ejemplo de solicitud de servicio estándar es solicitar orientación o ayuda para configurar un servicio AMS, como Alarm Manager, Patch Orchestrator, etc. También puede recibir solicitudes de servicio de AMS; se denominan solicitudes de servicio salientes o notificaciones de servicio. Para ver una lista de sus solicitudes de servicio y de las solicitudes de servicio salientes (notificaciones de servicio) que le ha enviado AMS, consulte la página de solicitudes de servicio de la consola de AMS.

Para obtener más información sobre las solicitudes de servicio salientes, consulte. [Responder a una solicitud de servicio generada por AMS](#)

Puede crear una solicitud de servicio de AWS Managed Services (AMS) mediante la consola AMS o, mediante programación, mediante la Soporte API. [Para obtener más información sobre el uso de la API, consulte Soporte API](#). Para AMS, elige el código `sentinel-service-request` de servicio.

Una vez que el equipo de operaciones de AMS reciba su solicitud de servicio, se le asignará prioridad de acuerdo con su acuerdo de nivel de servicio. Para mantenerse informado en cada paso del proceso de resolución de la solicitud de servicio, asegúrese de rellenar la opción Correos electrónicos de CC y, si va a conectarse por federación, inicie sesión antes de seguir el enlace incluido en el correo electrónico que envía AMS.

Utilice la página de creación de solicitudes de servicio de la consola AMS para realizar las siguientes tareas:

- Cree y actualice una solicitud de servicio
- Obtenga una lista e información detallada sobre todas sus solicitudes de servicio actuales
- Limite la búsqueda de solicitudes de servicio por fechas e identificadores de incidentes, incluidas las solicitudes que se han resuelto
- Añada comunicaciones y archivos adjuntos a sus solicitudes y añada destinatarios de correo electrónico para la correspondencia entre casos
- Resuelva las solicitudes de servicio
- Califique las comunicaciones de solicitud de servicio

Cuándo utilizar una solicitud de servicio

Los siguientes ejemplos describen una solicitud de servicio:

- AMS o guía AWS general
- Preguntas relacionadas con Patch MW
- Preguntas relacionadas con el cronograma de Backup
- Preguntas sobre la funcionalidad de los AWS servicios

Los siguientes son ejemplos de lo que no debería plantearse en una solicitud de servicio:

- Problemas de acceso
- Fallo del parche

- Fallo de Backup
- Fallo en el RFC o en el RFC que provoca la interrupción de la actividad empresarial (utilice el incidente para interrumpir la actividad empresarial)
- Preguntas sobre la RFC o información adicional o cambio del alcance de la RFC (utilice la correspondencia bidireccional de la RFC)

Cómo funciona la administración de solicitudes de servicio

Las solicitudes de servicio las gestiona el equipo de operaciones de AMS, que está de guardia.

Una vez que el equipo de operaciones de AMS recibe su solicitud de servicio, la revisa para garantizar que no se clasifique más adecuadamente como incidente. Si se debe clasificar como incidente, se reclasifica inmediatamente, el equipo de gestión de incidentes de AMS asume el control y se te notifica.

Si la solicitud de servicio se puede resolver con la presentación de una RFC, el operador encargado de la revisión le enviará un correo electrónico solicitándole que envíe la RFC correspondiente (se proporcionan los detalles).

Si el operador de AMS puede resolver la solicitud de servicio, se toman las medidas necesarias de inmediato. Por ejemplo, si la solicitud de servicio es para obtener asesoramiento sobre arquitectura u otro tipo de información, el operador le remite a los recursos adecuados o responde directamente a la pregunta.

Si el análisis de su solicitud de servicio identifica un error o una solicitud de función, AMS le envía una notificación a través de la solicitud de servicio. Como no hay una ETA para las solicitudes de funciones o las correcciones de errores, la solicitud de servicio original está cerrada. Póngase en contacto con su CSDM si tiene preguntas de seguimiento relacionadas con la solicitud de servicio original.

Si la solicitud de servicio está fuera del alcance de las operaciones de AMS, el operador la envía a su gerente de prestación de servicios en la nube para que pueda comunicarse con usted, o al equipo de AWS operaciones correspondiente, junto con un correo electrónico para informarle sobre las medidas que se van a tomar.

La solicitud de servicio no se resuelve hasta que haya indicado que está satisfecho con el resultado.

 Note

Recomendamos proporcionar un correo electrónico de contacto, un nombre y un número de teléfono en todos los casos para facilitar las comunicaciones.

Probar una solicitud de servicio en AMS

Al probar las solicitudes de servicio de AMS, le pedimos que incluya en el asunto del texto este indicador: `AMSTestNoOpsActionRequired` para que AMS sepa que la solicitud de servicio es únicamente para realizar pruebas. Cuando los ingenieros de operaciones de AMS ven esa bandera, no responden a la solicitud de servicio.

Crear una solicitud de servicio en AMS

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 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:

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, cree un caso de solicitud de servicio desde Support Center Console.

YouTube Vídeo: [¿Cómo y cuándo enviar solicitudes de servicio desde la consola de AWS y cuáles son sus objetivos de nivel de servicio?](#)

Supervisión y actualización de las solicitudes de servicio en AMS

Puede actualizar, supervisar y revisar los informes de incidentes y las solicitudes de servicio, ambos denominados casos, mediante la consola AMS o mediante programación mediante la Soporte API. Para obtener información sobre el uso de la Soporte API, consulte [DescribeCases](#) la operación.

Para supervisar un caso, incidente o solicitud de servicio mediante la consola AMS, sigue estos pasos.

1. En el panel de informes de incidentes o solicitudes de servicio de la consola AMS, busque un caso y elija el Asunto para abrir una página de detalles con el estado actual y las correspondencias.

Cuando el equipo de operaciones de AMS actualiza un incidente o un caso de solicitud de servicio denunciado, recibes un correo electrónico y un enlace al incidente en la consola de AMS para que puedas responder. No puedes responder a la correspondencia sobre incidentes respondiendo al correo electrónico.

Important

Debes haber introducido una dirección de correo electrónico para recibir notificaciones de cambios de estado en relación con una solicitud de servicio o un caso de incidente. Las notificaciones solo se envían a la dirección de correo electrónico que se agregó al caso cuando se creó.

El enlace del correo electrónico de notificación no funcionará a menos que utilice un servidor de correo electrónico en su red federada de AMS. Sin embargo, puede responder a la correspondencia accediendo a su consola AMS y utilizando la página de detalles del caso.

2. Si hay muchos casos en la lista, puedes usar la opción Filtrar:

- Todos abiertos (predeterminado): utilice este filtro para ver todos los casos que no se han resuelto.
 - Sin asignar: utilícelo si acaba de enviar el caso y no ha recibido ningún aviso de que el estado del caso haya cambiado. Tenga en cuenta que los incidentes y los casos de solicitud de servicio se abordan con diferente rapidez en función de la prioridad enviada (incidentes) o del acuerdo de nivel de servicio (solicitudes de servicio).
 - Abrir: utilízalo si has recibido un aviso de que el caso es una acción de «Amazon pendiente»; esto significa que el caso se ha asignado pero aún no se ha empezado a trabajar.
 - Reabierto: utilícela si ha recibido una notificación de que el caso se ha vuelto a abrir después de haberse resuelto.
 - Trabajo en curso: utilícelo si ha recibido un aviso de que un operador ha empezado a trabajar en el caso.
 - Acción pendiente del cliente: utilícela si ha recibido una solicitud de un operador para que tome medidas por su parte.
 - Acción del cliente completada: utilícela si ha recibido una notificación de que su acción en el caso se ha procesado.
 - Resuelto: utilícelo para ver los casos que sabe que se han resuelto. Los casos resueltos se mantienen en el historial durante doce meses.
 - Cualquier estado: utilice este filtro para ver todos los casos, independientemente del estado.
3. Para comprobar el estado más reciente, actualiza la página.
 4. Si hay tantas correspondencias que no aparecen todas en la página, selecciona Cargar más.
 5. Para actualizar el estado del caso, selecciona Responder, introduce la nueva correspondencia y, a continuación, selecciona Enviar.
 6. Para cerrar el caso una vez que se haya resuelto satisfactoriamente, selecciona Cerrar caso.
- ¡Asegúrese de calificar el servicio con una calificación de 1 a 5 estrellas para que AMS sepa cómo lo estamos haciendo!

Responder a una solicitud de servicio generada por AMS

La administración de parches de AMS le envía las solicitudes de servicio (también conocidas como notificaciones de servicio) antes de que finalice el período de mantenimiento establecido; para obtener más información, consulte el período de [mantenimiento de AMS](#). AMS también le envía notificaciones de servicio cuando existe la posibilidad de que un AWS servicio afecte a su

infraestructura o cuando sea necesario reiniciar una EC2 instancia de su cuenta; para obtener más información, consulte Notificaciones de [servicio](#).

 Note

AMS envía las comunicaciones a la dirección de correo electrónico principal de su AWS cuenta que usted haya indicado; le recomendamos añadir un alias de correo electrónico de contacto de operaciones alternativo para facilitar el proceso de gestión de las solicitudes o notificaciones de servicio. La adición de estos correos electrónicos se explica durante el proceso de incorporación de AMS y la documentación de incorporación relacionada.

Preguntas sobre facturación

Para enviar una pregunta relacionada con la facturación, complete los siguientes pasos:

1. Abre el [AWS Support Centro en casa#](https://console.aws.amazon.com/support/). <https://console.aws.amazon.com/support/>
2. Selecciona Cuenta y facturación.
3. Seleccione Crear caso.
4. Selecciona Cuenta y facturación y, a continuación, sigue las instrucciones para enviar tu caso.

Operaciones bajo demanda

Operations on Demand (OOD) es una función de AWS Managed Services (AMS) que amplía el alcance estándar de su plan de operaciones de AMS al proporcionar servicios operativos que actualmente no ofrecen de forma nativa los [planes de operaciones de AMS](#) o AWS. Una vez seleccionada, la oferta del catálogo se ofrece mediante una combinación de automatización y recursos de AMS altamente cualificados. No hay compromisos a largo plazo ni contratos adicionales, lo que le permite ampliar su AMS, sus AWS operaciones y capacidades actuales según sea necesario. Aceptas comprar bloques de horas (bloques OOD), 20 horas por bloque, mensualmente.

Puede seleccionar una oferta del catálogo estandarizada e iniciar una nueva contratación de OOD mediante una solicitud de servicio. Algunos ejemplos de ofertas de OOD incluyen la asistencia con el mantenimiento de Amazon EKS, las operaciones y la AWS Control Tower administración de los clústeres de SAP. Las nuevas ofertas de catálogo se añaden periódicamente en función de la demanda y de los casos de uso operativo que vemos con más frecuencia.

El OOD está disponible para los planes de operaciones AMS Advanced y AMS Accelerate y está disponible en todos los [Regiones de AWS](#) lugares donde AMS esté disponible.

AMS gestiona los riesgos de seguridad del cliente (CSRM) mientras implementa los cambios solicitados. Para obtener más información sobre el proceso de CSRM, consulte las revisiones de seguridad de las solicitudes de [cambio](#).

Catálogo de ofertas de Operations on Demand

Operations on Demand (OOD) le ofrece los servicios que se describen en la siguiente tabla.

Note

Para obtener las definiciones de los términos clave, consulte los [términos clave](#) de la documentación de AWS Managed Services.

Plan de operaciones	Title (Título)	Descripción	Resultados esperados

AMS Accelerate	Mantenimiento del clúster de Amazon EKS	AMS libera a sus desarrolladores de contenedores al encargarse del mantenimiento continuo de las implementaciones de Amazon Elastic Kubernetes Service (Amazon EKS). AMS lleva a cabo los end-to-end procedimientos necesarios para actualizar un clúster abordando los componentes del plano de control, los complementos y los nodos. AMS realiza la actualización de los tipos de nodos gestionados, así como de un conjunto seleccionado de complementos de Amazon EKS y Kubernetes.	Los equipos de clientes ayudaron con las operaciones subyacentes de actualización de los clústeres de Amazon EKS.

AMS Accelerate	Edificio AMI y máquinas expendedoras	AMS proporciona una gestión continua de la construcción y venta de AMI para los clientes. Nuestros ingenieros publican mensualmente los datos suscritos AMIs, los publican bajo demanda AMIs para las actividades de aplicación de parches emergentes, gestionan los cambios mediante manuales de ejecución y supervisan las compilaciones de AMI mediante la supervisión. CloudWatch También ofrecemos asistencia para la solución de problemas e informes detallados para todas las cuentas designadas AMIs . Esta oferta requiere que las canalizaciones de compilación de AMI se implementen mediante EC2 Image Builder. AMS no admite ningún otro servicio o automatización que interactúe con EC2 Image Builder.	La postura de seguridad de los clientes mejoró y se redujo el tiempo que los clientes dedicaban a construir y vender. AMIs

AMS Accelerate	Ejecución de cambios selecta	Trabaje con nuestros expertos ingenieros de operaciones para traducir los requisitos de su empresa en solicitudes de cambio validadas que puedan ejecutarse de forma segura en su AWS entorno. Aproveche nuestro enfoque único de automatización y nuestro conocimiento de las mejores prácticas operativas (por ejemplo, la evaluación del impacto, las anulaciones o la regla de dos personas), tanto si se trata de un simple cambio a gran escala como de una acción compleja con repercusiones posteriores.	Los clientes ayudaron a definir, crear y ejecutar solicitudes de cambio personalizadas. Los cambios pueden ser manuales o automáticos (CloudFormation, SSM). Incluye consultas con nosotros Soporte para obtener orientación sobre la configuración cuando sea necesario. No está diseñado para cambios en el código de la aplicación, la instalación o implementación de la aplicación, la migración de datos o los cambios en la configuración del sistema operativo.

AMS Accelerate	AWS Network Firewall Operaciones	AMS colabora con usted para integrar su firewall e implementar y administrar las políticas y reglas para las operaciones continuas del firewall. Para ello, nuestros ingenieros aprovechan nuestras mejores prácticas operativas y la automatización para configurar políticas y reglas estandarizadas, y permiten la supervisión para detectar los cambios realizados fuera del proceso de automatización. AMS le notifica rápidamente los cambios no deseados y le ofrece opciones para incluirlos, si así lo solicita, o restaurar la cuenta a una configuración anterior para garantizar la estabilidad general de sus sistemas.	Los equipos de clientes ayudaron a reducir la sobrecarga de administración al detectar rápidamente los cambios involuntarios en el firewall de la red, lo que mejoró la resolución de incidentes y redujo el tiempo de análisis de la causa raíz de los problemas esperados e inesperados.
AMS Accelerate	AWS Control Tower operaciones	Operaciones y administración continuas de su zona de AWS Control Tower aterrizaje, incluida AWS Transit Gateway, que proporciona una solución integral de zona de aterrizaje. AWS Organizations Nos encargamos de la venta de cuentas, la gestión de los SCP y las unidades organizativas, la corrección de los errores de tráfico, la gestión de los usuarios del SSO y AWS Control Tower las actualizaciones con nuestra biblioteca de controles y banderas personalizadas.	Los equipos de clientes ayudaron con algunas de las operaciones subyacentes de administración AWS Control Tower de AWS Transit Gateway y AWS Organizations.

AMS Accelerate	AWS landing zone Acelera las operaciones	AMS ofrece operaciones continuas en las zonas de AWS aterrizaje desplegadas a través del AWS Landing Zone Accelerator (LZA). Nuestros ingenieros se encargan de los cambios en los archivos de configuración, AWS Control Tower de la gestión del entorno (venta de cuentas, creación de unidades organizativas, barreras de control de los sistemas de control de servicios (SCP), de la detección y corrección de desviaciones de los sistemas de TC, de la gestión de la configuración de la red y de las actualizaciones de CT y del marco LZA. AWS LZA proporciona un medio para configurar y gobernar un AWS entorno seguro y multicuenta utilizando las mejores prácticas y servicios operativos, como: AWS Control Tower	Los equipos de clientes ayudaron con las operaciones continuas y la administración de la solución AWS Landing Zone Accelerator.

AMS Accelerate	SAP Cluster Assist	Alarmas, monitorización, parches de clústeres, copias de seguridad y solución de incidentes dedicados a sus clústeres de SAP. Este elemento del catálogo le permite delegar parte del trabajo operativo continuo de su equipo de operaciones de SAP para que pueda centrarse en la gestión de la capacidad y el ajuste del rendimiento.	Los equipos de SAP, clientes o socios, ayudaron con algunas de las operaciones subyacentes. Aún así, requiere que el cliente proporcione otras capacidades de SAP, como la administración de la capacidad, el ajuste del rendimiento, la administración de bases de datos y la administración de bases de SAP.

AMS Accelerate	SQL Server sobre operaciones EC2	AMS colabora con usted para incorporar, implementar y administrar las operaciones continuas de sus bases de datos de SQL Server implementadas en las EC2 instancias. Nuestros ingenieros aprovechan nuestras mejores prácticas operativas y la automatización para liberar a sus equipos de bases de datos realizando tareas como la creación de copias de seguridad y la aplicación de parches, ampliando el soporte operativo de AMS a los parches de SQL Server para incluir actualizaciones continuas con reconocimiento de clústeres, servicios de copia de seguridad y restauración alineados con nuestra estrategia de defensa contra el ransomware y supervisando el cumplimiento de los controles de copia de seguridad y parches proporcionados por el cliente.	Los clientes de SQL Server ayudaron a reducir las operaciones de parches y copias de seguridad de las bases de datos para mejorar la resiliencia y la postura de seguridad de sus cargas de trabajo, además de optimizar los costos de las licencias al incorporar sus propias licencias (BYOL) a EC2.

AMS Advanced	Mantenimiento de clústeres de Amazon EKS	AMS libera a sus desarrolladores de contenedores al gestionar el mantenimiento y el estado continuos de las implementaciones de Amazon Elastic Kubernetes Service (Amazon EKS). AMS lleva a cabo los end-to-end procedimientos necesarios para actualizar un clúster abordando los componentes del plano de control, los complementos y los nodos. AMS realiza la actualización de los tipos de nodos gestionados, así como de un conjunto seleccionado de complementos de Amazon EKS y Kubernetes.	Los equipos de clientes ayudaron con las operaciones subyacentes de actualización de los clústeres de Amazon EKS.
AMS Advanced	Ejecución prioritaria de RFC	Capacidad de ingeniero de operaciones designada por AMS para priorizar la ejecución de sus solicitudes de cambio (RFC). Todos los envíos reciben un mayor nivel de respuesta y el orden de prioridad se puede ajustar interactuando directamente con los ingenieros a través de una sala de reuniones de Amazon Chime.	Los clientes reciben un SLO de respuesta de 8 horas durante RFCs

AMS Advanced y AMS Accelerate	Actualización del sistema operativo anterior	Evite la migración de instancias actualizándolas a una versión de sistema operativo compatible. Podemos realizar una actualización in situ en las instancias seleccionadas aprovechando la automatización y las capacidades de actualización de los proveedores de software (por ejemplo, Microsoft Windows 2008 R2 a Microsoft Windows 2012 R2). Este enfoque es ideal para las aplicaciones heredadas que no se pueden volver a instalar fácilmente en una nueva instancia y proporciona protección adicional contra las amenazas de seguridad conocidas y sin paliativos en las versiones anteriores del sistema operativo. Se admiten los siguientes sistemas operativos para las actualizaciones locales: • Microsoft Windows 2012 R2 a Microsoft Windows 2016 y versiones posteriores • Microsoft Windows 2016 a Microsoft Windows 2022 y versiones posteriores • De Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8 • De Red Hat Enterprise Linux 8 a Red Hat Enterprise Linux 9 • De Oracle Linux 7 a Oracle Linux 8	Esta solución se proporciona para aplicaciones que ya no se pueden volver a instalar en una instancia nueva (por ejemplo, si se pierde el código fuente, si el ISV deja de funcionar, etc.). Puede devolver las actualizaciones fallidas a su estado original. Desde un punto de vista operativo, se prefiere la reversión, ya que permite que la instancia quede en un estado más compatible con los últimos parches de seguridad.

Temas

- [Solicitar AMS Operations On Demand](#)
- [Realizar cambios en las ofertas de Operations on Demand](#)

Solicitar AMS Operations On Demand

Las operaciones bajo demanda (OOD) de AWS Managed Services (AMS) están disponibles para todos los Cuentas de AWS usuarios que se hayan incorporado a AMS. Para aprovechar las ventajas de Operations on Demand, solicite información adicional a su administrador de prestación de servicios en la nube (CSDM), arquitecto de soluciones (SA), administrador de cuentas o arquitecto de nube (CA). Las ofertas de OOD disponibles figuran en la tabla anterior del [catálogo de ofertas de Operations on Demand](#). Una vez finalizado el análisis del alcance de la contratación, envíe una solicitud de servicio a AMS Operations para iniciar la contratación de OOD.

Cada solicitud de servicio de OOD debe contener la siguiente información detallada relativa a la contratación:

- Las ofertas de OOD específicas solicitadas y para cada oferta de OOD específica:
 - El número de bloques (un bloque equivale a 20 horas de recursos operativos en un mes natural determinado, que se cobrarán según la tarifa estándar vigente en AWS ese momento para la oferta de operaciones bajo demanda aplicable) que se van a asignar a la oferta de OOD específica.
 - El ID de cuenta de cada cuenta de AWS Managed Services para la que se solicita la oferta de OOD específica.

Debe enviar las solicitudes de servicio de OOD a través de uno de los siguientes medios:

- La cuenta de AWS Managed Services que recibe las ofertas de Operations on Demand correspondientes, o
- Una cuenta de AWS Managed Services que es una cuenta AWS Organizations de administración en el modo de todas las funciones, en nombre de cualquiera de sus cuentas de miembros que sean cuentas de AWS Managed Services.

Una vez recibida la solicitud de servicio OOD, AMS Operations revisa y actualiza las cuentas con su aprobación, aprobación parcial o denegación.

Una vez aprobada la solicitud de servicio que ofrece OOD, AMS y usted se coordinan para iniciar la contratación. No se inicia ninguna oferta de OOD hasta que se apruebe la solicitud de servicio y se acuerde una fecha de inicio de la contratación.

AMS utiliza una asignación de suscripción mensual de bloques de OOD. Asignamos mensualmente el número aprobado de bloques, a partir de la fecha de inicio de la contratación, hasta que solicite la exclusión mediante una nueva solicitud de servicio. Los bloques OOD son válidos durante un mes natural. Los bloques no utilizados, o las partes de bloques, no se acumulan ni se trasladan a futuros meses.

Se le facturará un mínimo de un bloque de OOD cada mes, independientemente de la cantidad de horas realmente utilizadas. No se facturará ningún bloque de OOD adicional asignado en el que no se hayan utilizado horas.

Realizar cambios en las ofertas de Operations on Demand

Para solicitar cambios en las contrataciones continuas de las ofertas de Operations on Demand (OOD), envíe una solicitud de servicio que contenga la siguiente información:

- La (s) modificación (es) solicitada (s) y
- La fecha solicitada para que las modificaciones entren en vigor.

Tras recibir la solicitud de servicio OOD, AMS Operations la revisa y la actualiza con su aprobación, o bien solicita al CSDM asignado que colabore con usted para determinar el alcance y las implicaciones de la modificación. Si se determina que la modificación requiere un esfuerzo de análisis con el CSDM, debe enviar una segunda solicitud de servicio de OOD para iniciar la contratación modificada una vez finalizado el ejercicio de análisis.

Una vez aprobada, la asignación de bloques modificada más recientemente pasará a estar activa y permanecerá activa, sustituyendo cualquier asignación de bloques anterior, a menos que usted y usted acuerden lo contrario. AWS

Historial de documentos

En la siguiente tabla se describen los cambios importantes de cada versión de la Guía del usuario avanzada de AMS. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

- Versión de la API: 21 de mayo de 2019
- Nuevos o actualizados CTs y tutoriales: historial de documentos de referencia de [AMS Advanced Change Type](#).
- Nuevo AMS AMIs: [Imágenes de máquinas AMS Amazon \(AMIs\)](#)

Cambio	Descripción	Fecha
Tabla actualizada para AWS Identity and Access Management (IAM) en los controles estándar de la sección avanzada de AMS	Información actualizada de la tabla sobre las políticas de IAM y el acceso a los buckets de Amazon S3.	25 de septiembre de 2025
Paso actualizado para consultas relacionadas con la facturación	Se actualizó el paso para crear solicitudes de servicio para consultas relacionadas con la facturación en la sección Crear una solicitud de servicio en AMS.	25 de septiembre de 2025
Información actualizada sobre las notificaciones por correo electrónico para los tipos de cambios	Información actualizada y un ejemplo para agregar notificaciones por correo electrónico para los tipos de cambios en la sección Configurar las notificaciones por correo electrónico de RFC (consola).	25 de septiembre de 2025
Tipo de cambio actualizado	Se actualizó la sección de etiquetado automático de la	25 de septiembre de 2025

infraestructura de AMS con un tipo de cambio para etiquetar los recursos creados por AMS.

[Preguntas frecuentes sobre máquinas virtuales actualizadas Import/Export en AWS Managed Services](#)

Se actualizó el RFC utilizado para solicitar un perfil de instancia para permitir que las herramientas ejecuten comandos desde la instancia.

24 de septiembre de 2025

[Se actualizó la solicitud de cambio \(RFC\) para lanzar una instancia de SUSE Linux Enterprise Server for SAP Applications 15 SP6](#)

Se actualizó el paso 2, sobre cómo lanzar una nueva SP6 instancia de SUSE Linux Enterprise Server para SAP Applications 15 con la RFC correcta.

22 de septiembre de 2025

[Solicitud de cambio \(RFC\) actualizada](#)

Se actualizó AWS Elastic Disaster Recovery en la sección de preguntas frecuentes de AWS Managed Services con el RFC correcto para crear las funciones de IAM necesarias en su cuenta.

22 de septiembre de 2025

[Se agregaron 4 nuevas comprobaciones de optimización de Trusted Advisor costos compatibles con Trusted Remediator](#)

Se agregaron las siguientes comprobaciones de optimización de costos:

22 de septiembre de 2025

- c1z7kmr00n - Recomendaciones de optimización de costes de Amazon para instancias EC2
- c1z7kmr02n - Recomendaciones de optimización de costes de Amazon EBS para volúmenes
- c1z7kmr03n - Recomendaciones de optimización de costes de Amazon RDS para instancias de base de datos
- c1z7kmr05n AWS Lambda : recomendaciones de optimización de costos para las funciones

[Nota actualizada para las zonas de disponibilidad \(AZs\)](#)

Información actualizada sobre los grupos de seguridad en AMS.

5 de septiembre de 2025

[Tipo de cambio actualizado](#)

Se actualizó la sección de preguntas frecuentes sobre Amazon FSx en AWS Managed Services con un tipo de cambio para compartir el AD gestionado con la cuenta de la aplicación.

5 de septiembre de 2025

Tipo de cambio actualizado

Se actualizó Amazon DocumentDB en la sección de preguntas frecuentes de AWS Managed Services con un cambio de tipo para utilizar la eliminación. APIs

5 de septiembre de 2025

Tipo de cambio actualizado

Se actualizó la sección de preguntas frecuentes sobre Alexa for Business en AWS Managed Services con el cambio de tipo a dos usuarios de IAM de acceso limitado para instalar y operar su puerta de enlace Alexa for Business.

5 de septiembre de 2025

Tipo de cambio actualizado

Se actualizó la AppStream versión 2.0 en la sección de preguntas frecuentes de AWS Managed Services con un tipo de cambio para crear y elegir un rol de IAM que estará disponible en todas las instancias de streaming de flotas

5 de septiembre de 2025

Tipo de cambio actualizado

Se actualizó EventBridge en la sección de preguntas frecuentes de AWS Managed Services con un tipo de cambio para solicitar un rol de EventBridge servicio antes de usarlo EventBridge para activar otros AWS recursos.

5 de septiembre de 2025

Trusted Trusted Advisor Remediator ha actualizado la compatibilidad con las comprobaciones de seguridad	Se actualizaron los parámetros y restricciones preconfigurados compatibles para comprobar Hs4Ma3G108: las rutas CloudTrail deberían integrarse con Amazon Logs CloudWatch	5 de septiembre de 2025
Trusted Remediator ha actualizado Trusted Advisor la compatibilidad con las comprobaciones de seguridad	Se actualizó Trusted Advisor la comprobación de seguridad para añadir la versión 2 de Hs4Ma3G184: se debe habilitar el registro de los balanceadores de carga de aplicaciones y los balanceadores de carga clásicos	5 de septiembre de 2025
Las comprobaciones de excelencia Trusted Advisor operativa actualizadas son compatibles con la sección Trusted Remediator	Se actualizaron las comprobaciones de excelencia Trusted Advisor operativa compatibles con la sección Trusted Remediator para añadir una nueva comprobación compatible c1fd6b96l4 Amazon S3 Access Logs Enabled.	28 de agosto de 2025
Tipo de cambio actualizado	Cambie el tipo de función de IAM personalizada.	25 de agosto de 2025
Se actualizó con CloudWatch Application Insights para .Net y SQL Server en la sección AMS	Se revisó el tipo de cambio para usar CloudWatch Application Insights.	25 de agosto de 2025

Solicitud de cambio (RFC) actualizada	Solicitud de cambio (RFC) para añadir más etiquetas al bucket de Amazon S3.	25 de agosto de 2025
Solicitud de cambio (RFC) actualizada	Solicitud de cambio (RFC) para etiquetar todos los recursos creados por AMS con fines de administración.	25 de agosto de 2025
Lambda actualizada en la sección de preguntas frecuentes sobre AWS Managed Services	Se revisó el tipo de cambio para acceder a otros AWS servicios a fin de crear fuentes de eventos.	25 de agosto de 2025
Lambda actualizada en la sección de preguntas frecuentes sobre AWS Managed Services	Se revisó el tipo de cambio para aprovisionar funciones Lambda.	25 de agosto de 2025
Se actualizó la sección de creación, cambio o eliminación de grupos de seguridad	Se revisó el tipo de cambio para crear un grupo de seguridad fuera de las pilas y VPCs.	25 de agosto de 2025
Se actualizó la sección Trusted Remediator para incluir contenido nuevo para Compute Optimizer	Se actualizó la sección Trusted Remediator para incluir contenido nuevo para las recomendaciones compatibles. AWS Compute Optimizer	18 de agosto de 2025
Se ha eliminado el enlace al glosario TOC	AWS Glosario.	8 de agosto de 2025

[Recomendación precisa del tipo de cambio](#)

Para integrar la métrica de sus clientes en su sistema de supervisión de aplicaciones, solicite a AMS que cree un tema de Amazon SNS para la métrica enviando una RFC junto con Deployment | Monitoring and notification | SNS | Create CT (ct-3dfnglm4ombbs).

8 de agosto de 2025

[Recomendación precisa sobre el tipo de cambio](#)

Para eliminar los volúmenes de instancias de marcadores de posición, envíe un archivo Management | Advanced stack components | EBS Volume | Delete change type (ct-3e3h8u0sp5z80).

8 de agosto de 2025

[Nuevas SecureChannelFailure alertas de monitoreo: y Broken Secure Channel](#)

[Las alertas de la supervisión básica en AMS](#) [AMS corrigen automáticamente las alertas.](#)

8 de agosto de 2025

Nuevas comprobaciones de Trusted Remediator	Trusted Advisor comprobaciones de optimización de costes compatibles con las comprobaciones de Trusted Advisor seguridad de Trusted Remediator compatibles con Trusted Remediator Hs4Ma3G120— AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime, Hs4Ma3G230— 2 y c18d2gz150— 2. AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingVAWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime	8 de agosto de 2025
Actualización del estándar de IAM en el punto 3.2	Se ha aclarado el lenguaje y se ha eliminado la mención del etiquetado.	25 de julio de 2025
Actualización de las opciones de exclusión de alertas	La adición de una etiqueta le permite optar por no recibir otras dos alertas.	25 de julio de 2025
Obsolescencia del servicio de aprovisionamiento de autoservicio	El servicio de aprovisionamiento CloudEndure de autoservicio está en desuso en favor de. AWS Application Migration Service	25 de julio de 2025
Nueva función para las copias de seguridad	Personalice las notificaciones en las bóvedas de respaldo con una nueva etiqueta.	25 de julio de 2025

Tabla de controles actualizada	Se eliminaron algunos controles duplicados en la sección de la tabla AMS-STD-002 - AWS Identity and Access Management (IAM).	26 de junio de 2025
Se AWS Transfer Family actualizaron los requisitos previos del servicio SSP	Se agregó información a la sección de requisitos previos.	26 de junio de 2025
Ejemplo de política de IAM actualizada	Ejemplo de política de IAM actualizado con más restricciones, según lo recomendado.	26 de junio de 2025
Compatible con AML actualizada OSes	Se agregó Ubuntu Linux 24.04 a Ubuntu Linux 22.04 y se cambiaron todas las referencias a SP5 . SP6	26 de junio de 2025
Servicio de aprovisionamiento de autoservicio, obsoleto MediaStore	Se agregó una nota de obsolescencia para. AWS Elemental MediaStore	26 de junio de 2025
Servicio de aprovisionamiento de autoservicio, Amazon Inspector Classic, obsoleto	Se ha añadido una nota de obsolescencia para Amazon Inspector Classic.	26 de junio de 2025
Servicio de aprovisionamiento de autoservicio, Amazon Connect está en desuso	Se ha añadido una nota de obsolescencia para Amazon Connect.	26 de junio de 2025
Se ha actualizado la sección sobre las configuraciones compatibles en AMS	Configuraciones compatibles actualizadas para los sistemas operativos compatibles y los sistemas operativos de fin de soporte (EOS) compatibles en AMS.	25 de junio de 2025

Servicio de aprovisionamiento de autoservicio, obsoleto WorkDocs	Se ha eliminado la página y las referencias a una página obsoleta. WorkDocs	19 de junio de 2025
Nota de seguridad importante sobre la administración de parches para repositorios de parches alternativos	Nota de seguridad importante y mejores prácticas para el uso de repositorios de parches alternativos en AMS.	10 de junio de 2025
Actualizaciones de sistemas operativos compatibles	Los sistemas operativos compatibles con AMS Advanced se actualizan, algunos se añaden y otros se eliminan.	22 de mayo de 2025
Solo para uso interno APIs	Solo internos APIs que aparecen en algunos registros . CloudWatch	22 de mayo de 2025
Actualizaciones de AMS Trusted Remediator	Cómo utilizar un parámetro nuevo, <code>preconfigured-parameters</code> , para personalizar las Trusted Advisor comprobaciones en Trusted Remediator.	22 de mayo de 2025
Actualizaciones de SSP Amazon Elastic Container Registry	Al incorporar el servicio Amazon ECR, se aprovisionan automáticamente más funciones.	8 de mayo de 2025

[Preguntas frecuentes y actualizaciones sobre AMS Advanced Trusted Remediator.](#)

Varias actualizaciones de las Trusted Advisor comprobaciones compatibles y las preguntas frecuentes sobre Trusted Remediator (se agregó: «¿Qué recursos utiliza Trusted Remediator en sus cuentas?») y mucho más. Consulte también las [Trusted Advisor comprobaciones compatibles con Trusted Remediator.](#)

8 de mayo de 2025

[Actualización de los controles de seguridad del estándar avanzado de AMS.](#)

Se agregaron los controles de «uso compartido de grupos de seguridad».

8 de mayo de 2025

[Espacios de nombres protegidos por AMS Advanced.](#)

AMS protegió los espacios de nombres EPSMarketplaceSubscriptionRole y los agregó. EPS

24 de abril de 2025

[Ubicaciones de registro de AMS Advanced.](#)

Se agregaron ubicaciones de registro adicionales.

24 de abril de 2025

[Actualización de los requisitos previos del modo AMS Advanced Self-SERVICE Provisioning para la AppStream versión 2.0.](#)

Se ha añadido un requisito previo para la AppStream versión 2.0: debe incluir un nombre de bucket de Amazon S3 al enviar la RFC de aprovisionamiento para el servicio.

24 de abril de 2025

<u>Alerta de corrección automática de AMS Advanced New Amazon RDS.</u>	ID de alerta: - 0224, se activa cuando el almacenamiento asignado solicitado alcanza o supera el umbral de almacenamiento máximo configurado.	27 de marzo de 2025
<u>AMS Advanced AWS ha cerrado el acceso de nuevos clientes a Amazon CloudSearch a partir del 25 de julio de 2024.</u>	Los clientes actuales pueden seguir utilizando el servicio, pero no habrá nuevas funciones.	27 de marzo de 2025
<u>AMS Advanced AWS ha cerrado el acceso de nuevos clientes a AWS CodeCommit partir del 25 de julio de 2024.</u>	Los clientes actuales pueden seguir utilizando el servicio, pero no habrá nuevas funciones.	27 de marzo de 2025
<u>Trusted Remediator ya está disponible.</u>	Ya está disponible Trusted Remediator, una solución de AWS Managed Services que automatiza la corrección de las AWS Trusted Advisor comprobaciones.	19 de marzo de 2025
<u>AMS Advanced: nueva alerta RDS de autorremediaciones.</u>	Se agregó el RDS-EVENT -0224.	17 de marzo de 2025
<u>Nueva función avanzada de AMS: notificaciones de incidentes.</u>	Se puede utilizar AppRegistry para crear aplicaciones y personalizar las notificaciones de incidentes para esas aplicaciones.	13 de marzo de 2025
<u>Actualización del AMS al umbral de monitorización de alarmas del RDS.</u>	El umbral de alarma de uso medio de la CPU del RDS se ha cambiado del 75% al 90%.	20 de febrero de 2025

[Informes de autoservicio actualizados con nuevas opciones de datos para la visualización de informes agregados](#)

Se agregaron opciones de datos para incluir un nuevo nombre de campo: Admin Account ID, nombre de campo del conjunto de datos: aws_admin_account_id y definición: Trusted AWS Organization account enabled by the customer para los siguientes informes de autoservicio:

- Informe de parches (diario)
- Informe de Backup (diario)
- Informe de incidentes (semanal)

28 de enero de 2025

[Actualización del AWS Batch SSP](#)

Puede utilizar el siguiente RFC para aprovisionar AWS Batch en su cuenta de AMS: Administración | Servicio de AWS | Servicio de autoaprovisionamiento | Añadir (ct-1w8z66n899dct).

28 de enero de 2025

[Nueva función de AMS: informes agregados de autoservicio](#)

Los informes de autoservicio agregados (SSR) le proporcionan una vista de los informes de autoservicio existentes agregados a nivel de la organización y de forma transversal.

21 de enero de 2025

[Actualización de la sección
Forecast SSP](#)

Nota adicional: 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.

10 de enero de 2025

[Actualización de la sección
de espacios de nombres
protegidos por AMS](#)

Se agregó un espacio de nombres protegido que faltaba (*mc, *MC y *Mc) a la lista de espacios de nombres protegidos por AMS.

9 de enero de 2025

[Actualización de la sección
Cómo funciona la supervisión](#)

Se agregó información sobre una nueva función, que permite configurar las notificaciones de alerta por recurso o ID de instancia, en lugar de por incidente.

8 de enero de 2025

[Actualizado: contenido de
actualización basado en
etiquetas](#)

Se corrigió un error tipográfico en el nombre de la clave y se corrigió la ruta incorrecta del archivo de configuración.

6 de enero de 2025

[Actualizado: Notas AMI de
AMS](#)

El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.

21 de noviembre de 2024

[Tabla actualizada de ofertas de Operations On Demand](#)

Se admiten los siguientes sistemas operativos para las actualizaciones locales:

11 de noviembre de 2024

- Microsoft Windows 2016 a Microsoft Windows 2022 y versiones posteriores

[Tabla de ofertas de Operations On Demand actualizada](#)

Se admiten los siguientes sistemas operativos para las actualizaciones locales:

1 de noviembre de 2024

- Microsoft Windows 2012 R2 a Microsoft Windows 2016 y versiones posteriores
- De Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8
- De Red Hat Enterprise Linux 8 a Red Hat Enterprise Linux 9
- De Oracle Linux 7 a Oracle Linux 8

[Configuraciones compatibles actualizadas](#)

Se actualizaron los sistemas operativos Oracle Linux compatibles a 9.0-9.3, 8.0-8.9 y 7.5-7.9.

24 de octubre de 2024

[Imágenes actualizadas de AMS Amazon Machine \(AMIs\)](#)

Basado en Windows actualiza do AMIs para eliminar Windows 2012 y 2012 R2. Se actualizó la versión basada en Linux AMIs para eliminar varias AMIS que ya no son compatibles y añadir las siguientes:

24 de octubre de 2024

- Amazon Linux (2ARM64)
- RHEL 9
- Servidor SUSE Linux Enterprise 15 SP5

[Ahora puede incluir varias direcciones de correo electrónico en las alertas basadas en etiquetas.](#)

Ahora se admiten varias direcciones de correo electrónico en las alertas basadas en etiquetas.

20 de septiembre de 2024

[Se agregó la sección de revisiones de seguridad de las solicitudes de cambio.](#)

Se ha agregado una nueva sección que proporciona detalles sobre el proceso de revisión de seguridad de las solicitudes de cambio.

17 de septiembre de 2024

[Se ha agregado una nueva sección.](#)

Ya está disponible una nueva sección que describe cómo se realizan las revisiones de seguridad de las solicitudes de cambio en AMS Advanced.

12 de septiembre de 2024

[Nuevo servicio compatible con AMS Advanced.](#)

AWS Resilience Hub ahora es compatible con AMS Advanced.

30 de agosto de 2024

[AMS Advanced admite nuevos servicios.](#)

AMS Advanced ahora admite cinco nuevos servicios:

21 de agosto de 2024

- Amazon Bedrock
- Amazon Kendra
- Amazon Quantum Ledger Database (Amazon QLDB)
- AWS Service Catalog AppRegistry
- Servicio administrado por Amazon para Prometheus

[Ya está disponible una nueva configuración predeterminada de la red de seguridad de terminales.](#)

La fuente de actualización ahora está incluida en la configuración de red predeterminada del EPS.

21 de agosto de 2024

[Actualizado: Notas AMI de AMS](#)

El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.

30 de julio de 2024

[AMS ahora es compatible con el firewall DNS Amazon Route 53 Resolver.](#)

AMS ahora es compatible con el firewall DNS Amazon Route 53 Resolver

30 de julio de 2024

[AWS DataSync Actualización de SSPS](#)

AWS DataSync ya no requiere el prefijo «datasync-» en los nombres de los buckets de Amazon S3.

30 de julio de 2024

[Panel de reglas de configuración de seguridad](#)

El panel de reglas de Security Config ahora está disponible en los informes de autoservicio.

24 de julio de 2024

AMS ahora es compatible con Oracle Linux 8.9, RHEL 8.10 y RHEL 9.4.	AMS ahora es compatible con Oracle Linux 8.9, RHEL 8.10 y RHEL 9.4.	5 de julio de 2024
Amazon Bedrock ahora está disponible en modo de aprovisionamiento de autoservicio	Ahora puede solicitar Amazon Bedrock en modo AMS SSP.	27 de junio de 2024
Eventos de firewall de DNS de Amazon Route 53 Resolver en Security Incident Response	AMS ahora monitorea los eventos del firewall de DNS de Amazon Route 53 Resolver en Security Incident Response	21 de junio de 2024
Se agregó información adicional sobre cómo activar la función BYOEPS (BYOEPS) de AMS.	Se ha añadido información adicional sobre cómo activar la función AMS bring your own EPS (BYOEPS).	5 de junio de 2024
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	23 de mayo de 2024
Se agregó información sobre el uso de un rol personalizado AWS Amplify en el modo de aprovisionamiento de autoservicio (solo en entornos MALZ).	Se agregaron instrucciones sobre cómo los entornos MALZ pueden usar un rol personalizado AWS Amplify en el modo de aprovisionamiento de autoservicio.	23 de mayo de 2024
Amazon Kendra ya está disponible en el modo de aprovisionamiento de autoservicio.	Amazon Kendra ya está disponible en el modo de aprovisionamiento de autoservicio.	23 de mayo de 2024

<u>AMS Advanced es compatible con otros sistemas operativos.</u>	AMS Advanced es compatible con Red Hat Enterprise Linux (RHEL) 9.x y Ubuntu 20.04 y 22.04.	25 de abril de 2024
<u>AMS Advanced admite ARM64 la arquitectura de Amazon Linux 2.</u>	AMS Advanced admite ARM64 la arquitectura de Amazon Linux 2.	25 de abril de 2024
<u>Se ha actualizado la sección de cuentas de Landing Zone (MALZ) que se descargan de las zonas de landing zone con múltiples cuentas.</u>	Se agregó información detallada sobre cómo desvincular las cuentas principales y de aplicación de la landing zone multicuenta.	11 de abril de 2024
<u>Actualización: descripción de la gestión de las solicitudes de servicio.</u>	Se actualizó la descripción de la gestión de solicitudes de servicio en el tema Descripción del servicio.	21 de marzo de 2024
<u>Actualizado: sección de compromisos del servicio de gestión de incidentes.</u>	Se agregó un enlace al acuerdo de nivel de servicio de AMS.	21 de marzo de 2024
<u>Actualizado: sección sobre cómo funciona la gestión de las solicitudes de servicio.</u>	Se ha añadido una aclaración sobre cómo AMS gestiona las solicitudes de servicio que contienen una solicitud de función o un error.	21 de marzo de 2024
<u>Actualizado: obtenga la sección de soporte.</u>	Se actualizó la sección Obtenga asistencia para incluir una nueva sección de preguntas sobre facturación.	21 de marzo de 2024

Actualizado: aprovisionamiento automatizado de IAM por AMS	Se actualizó el aprovisionamiento automatizado de IAM de AMS con información personalizada sobre listas de denegación	21 de marzo de 2024

Actualizaciones anteriores

En la siguiente tabla se describen los cambios importantes en la documentación de la guía avanzada de AMS antes de marzo de 2024.

Cambio	Descripción	Enlace
Febrero de 2024		
Sistemas operativos compatibles actualizados	Se actualizaron los sistemas operativos compatibles para incluir SUSE Linux Enterprise Server 15 SP5.	Consulte Configuraciones admitidas
Se ha añadido una nota a las alertas sobre la supervisión básica en AMS.	Se agregó una nota que indica que la alarma para el uso de volúmenes EC2 no raíz está desactivada de forma predeterminada.	Consulte Alertas del monitoreo de referencia en AMS
Se ha añadido una nueva sección, AMS Event Router, a la supervisión y la gestión de eventos.	Se agregó una nueva sección sobre el AMS Advanced Event Router.	Consulte Uso de Amazon EventBridge Managed Rules en AMS
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	Consulte AMIs. csv-and-notes.02.2024

Cambio	Descripción	Enlace
Febrero de 2024		
Se ha añadido una nueva sección para el rol vinculado al servicio de EventBridge reglas de Amazon para AMS Advanced	Se ha añadido una nueva sección para la función vinculada al servicio de EventBridge reglas de Amazon para AMS Advanced en la sección Seguridad de la infraestructura.	Consulte el rol vinculado al servicio de EventBridge reglas de Amazon para AMS Advanced
Se actualizó la sección sobre el modo de aprovisionamiento de	Se ha añadido una nueva sección para el nuevo Amazon Inspector en el modo de aprovisionamiento de autoservicio.	Consulte Amazon Inspector Classic (AMS SSPS)
Enero de 2024		
Se actualizó la sección de gestión de eventos planificados (PEM)	Se han añadido detalles adicionales y una sección de preguntas frecuentes a la gestión de eventos planificados (PEM).	Consulte Administración de eventos planificados en AWS Managed Services
Se agregó una nueva sección para la instalación automática de SSM Agent	Se agregó una nueva sección para la instalación automática del agente SSM en la configuración de EC2 instancias automatizada.	Consulte Instalación automática de SSM Agent
Se agregó AWS Resilience Hub (AMS SSPS)	Se agregó un nuevo servicio SSPS.	Consulte Utilice AMS SSP para aprovisionar AWS Resilience Hub en su cuenta AMS

Cambio	Descripción	Enlace
Actualizado: Notas AML de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	Consulte AMIs. csv-and-notes.01.2024
Diciembre de 2023		
Se actualizó el modo Direct Change en AMS	Se ha añadido una nueva subsección, denominada Casos de uso del modo de cambio directo, al modo de cambio directo de AMS.	Consulte Modo de cambio directo en AMS
Actualizado AWS Amplify (AMS SSPS)	Se actualizaron las preguntas frecuentes para aclarar que se requiere una aceptación del riesgo para solicitar Amplify.	Consulte Utilice AMS SSP para aprovisionar AWS Amplify en su cuenta de AMS
Nuevo AWS Elastic Disaster Recovery (AMS SSPS)	Se agregó un nuevo servicio SSPS	Consulte Utilice AMS SSP para aprovisionar AWS Elastic Disaster Recovery en su cuenta AMS
Nuevo Amazon Managed Service para Prometheus (AMS SSPS)	Se agregó un nuevo servicio SSPS	Consulte Utiliza AMS SSP para aprovisionar Amazon Managed Service para Prometheus en tu cuenta de AMS
Se actualizó la sección Cómo funciona la administración de la continuidad.	Se agregó una nueva subsección, monitoreo e informes de respaldo de AMS.	Consulte Cómo funciona la gestión de la continuidad

Cambio	Descripción	Enlace
Nuevo Amazon DevOps Guru (AMS SSPS)	Se agregó un nuevo servicio SSPS	Consulte Utilice AMS SSP para aprovisionar Amazon DocumentDB (compatible con MongoDB) en su cuenta de AMS
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	Consulte AMIs. csv-and-notes.12.2023
Noviembre de 2023		
Amazon CloudWatch Synthetics (AMS SSPS) actualizado	Se actualizó FAQs para usar los nombres de rol correctos.	Consulte Utilice AMS SSP para aprovisionar Amazon CloudWatch Synthetics en su cuenta de AMS
Modo de aprovisionamiento de autoservicio de Amazon API Gateway actualizado	Se agregó un rol adicional ,customer_apigateway_cloudwatch_role , a la sección API Gateway.	Consulte Utilice AMS SSP para aprovisionar Amazon API Gateway en su cuenta de AMS
Se agregó un nuevo servicio al modo de aprovisionamiento de autoservicio	Se agregó AWS Service Catalog AppRegistry a la sección del modo de aprovisionamiento de autoservicio	Consulte Utilice AMS SSP para aprovisionar AWS Service Catalog AppRegistry en su cuenta AMS
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	Consulte AMIs. csv-and-notes1.11.2023
Septiembre de 2023		

Cambio	Descripción	Enlace
Se agregó una nota a Using Patch Orchestrator	Se agregó la siguiente nota a la sección Uso de Patch Orchestrator: «Las alertas de error de los parches no se crean para las instancias que tienen sistemas operativos no compatibles o que se detienen durante el período de mantenimiento»	Consulte Administración de parches en AMS
Cifrado de datos actualizado con servicios adicionales	Se agregaron servicios al cifrado de datos en AMS.	Consulte Protección de datos en AMS
Se agregó un nuevo párrafo a los mensajes de error del RFC.	Se agregó un nuevo párrafo para agregar el enlace Crear una solicitud de servicio.	Consulte Solución de problemas de errores de RFC en AMS
Se corrigieron los nombres de las funciones de IAM.	Se corrigió el nombre de rol de IAM customer_emr_cluster_autoscaling_role.	Consulte Modo de aprovisionamiento de autoservicio en AMS
Se actualizó la información de supervisión básica	Se eliminó la referencia a dos alarmas obsoletas y. RDSRead LatencyAlarm RDSWrite LatencyAlarm	Consulte Alertas del monitoreo de referencia en AMS
Agosto de 2023		
Se agregó: Respuesta a incidentes de seguridad de AMS	Se agregó documentación para usar la respuesta a incidentes de seguridad de AMS.	Consulte Respuesta a incidentes de seguridad en AMS
Julio de 2023		

Cambio	Descripción	Enlace
Se agregó: aprovisionamiento automatizado de IAM	Se agregó documentación para usar el aprovisionamiento automatizado de IAM.	Consulte Aprovisionamiento automatizado de IAM (AMS)
Actualizado: tabla de roles de acceso	Se agregaron las funciones que faltaban en AMS Access.	Consulte Funciones de IAM para el acceso a la cuenta de los clientes de AMS
Junio de 2023		
Actualizado: Lista de alertas de RDS monitoreadas.	Se actualizó la lista de alertas de RDS para el monitoreo de referencia de AMS. Se agregaron 9 nuevos tipos de alertas de RDS y se eliminaron 3 tipos de alertas de RDS existentes.	Consulte Alertas del monitoreo de referencia en AMS .
Actualización: tabla de funciones de acceso	Nuevas funciones para AMS Security.	Consulte Funciones de IAM para el acceso a la cuenta de los clientes de AMS
Mayo de 2023		
Actualizado: Política de fecha de inicio de facturación del servicio.	Definiciones actualizadas de la fecha de inicio de la facturación.	Consulte Términos clave de AMS .
Abril de 2023		

Cambio	Descripción	Enlace
Actualizado: informe mensual de autoservicio de facturación.	Nota adicional: Los informes de facturación mensual solo están disponibles en una cuenta de Management Payer (AMS Advanced multi-account landing zone), pero están disponibles para todas las cuentas gestionadas por AMS Accelerate vinculadas.	Consulte Informe de facturación (mensual) .
Actualizado: se ha eliminado el contenido de «parches estándar»	AMS usa Patch Orchestrator.	Administración de parches en AMS
Actualizado: ¿Qué es AMS?	Hemos trasladado algunos temas anteriormente a ¿Qué es AMS? para formar parte de la descripción del servicio AMS.	Descripción del servicio
Actualizado: Desactivación de la landing zone multicuenta	Hizo varias aclaraciones.	Olvídense de las cuentas multicuenta de AMS en las zonas de landing zone
Actualización: AWS Transfer Family (AMS SSPS)	Se agregó un enlace al tutorial de configuración de la transferencia.	Utilice AMS SSP para aprovisionar AWS Transfer Family en su cuenta AMS
Contenido actualizado: aprovisionamiento de autoservicio	Se reemplazó CodeSuite «» por «Servicios de código» según las normas legales de AWS.	Utilice AMS SSP para proporcionar servicios de código AMS en su cuenta AMS
Contenido actualizado: CloudWatch métricas y alarmas	Se agregó un enlace al ejemplo: contar las apariciones de un término .	Creación de CloudWatch métricas y alarmas personalizadas en AMS

Cambio	Descripción	Enlace
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	AMIs. csv-and-notes.04.2023
Marzo de 2023		
Contenido actualizado: desconexión de AMS	Se aclaró qué recursos se eliminan al cerrar cuentas multicuenta de landing zone	Olvídese de las cuentas multicuenta de AMS en las zonas de landing zone
Actualizado: AMS AMIs	Se agregó un enlace al archivo ZIP AMI para cada mes en la sección Historial de documentos.	Historial de documentos
Actualizado: corrección automática	Se ha eliminado el soporte de LVM para la automatización de EC2 volúmenes.	Remediación automática de alertas por parte de AMS
Actualizado: parche RACI	Varias actualizaciones y aclaraciones de la RACI para la aplicación de parches.	Matriz de responsabilidad de AMS (RACI)
Contenido actualizado: aprovisionamiento de autoservicio	Se ha añadido una bullet de preguntas frecuentes. Para lanzar un nuevo agente de AWS Datasync, no es necesario utilizar WIGS.	Modo de aprovisionamiento de autoservicio en AMS
Contenido actualizado: aprovisionamiento de autoservicio	Se ha añadido una bullet de preguntas frecuentes. Para lanzar un nuevo agente de AWS Datasync, no es necesario utilizar WIGS.	Modo de aprovisionamiento de autoservicio en AMS

Cambio	Descripción	Enlace
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	AMIs. csv-and-notes.03.2023
Febrero de 2023		
Contenido actualizado: desconexión de AMS	Se aclaró cómo eliminar los entornos de zonas de landing zone con múltiples cuentas y las cuentas de VPCs aplicaciones.	Cuentas AMS externas
Contenido actualizado: ¿Descubrimiento ARNs	Se agregó la CLI de <code>describe-table</code> DynamoDB para buscar el ARN de una tabla de DynamoDB	Encuentra nombres de recursos de Amazon (ARNs) en AMS

Cambio	Descripción	Enlace
Contenido actualizado: Autoservicio de aprovisionamiento	Se ha eliminado la opción AMS «CodeSuite», ya que no es un SSPS propiamente dicho. Puede seguir utilizando la opción Administración AWS Servicio Servicio autoaprovisionado Añadir (es necesario revisar) (ct-3qe6io8t6jtny), cambiar el tipo y solicitar los tres servicios: y. CodeBuild CodeDeploy CodePipeline A continuación, AMS asignará las siguientes funciones de IAM a su cuenta: y. customer_codebuild_service_role customer_codedeploy_service_role aws_code_pipeline_service_role Una vez aprovisionado en su cuenta, debe incorporar el rol a su solución de federación.	Modo de aprovisionamiento de autoservicio en AMS
Contenido actualizado: actualización de Secrets Manager	Se corrigieron los roles necesarios para la zona de aterrizaje multicuenta (MALZ) frente a la zona de aterrizaje con una sola cuenta (SALZ).	Preguntas frecuentes sobre cómo compartir claves mediante Secrets Manager
Contenido actualizado: AMS corrige automáticamente las alertas	Se agregó soporte para los volúmenes de Logical Volume Manager (LVM).	EC2 automatización de la corrección del uso del volumen

Cambio	Descripción	Enlace
Contenido actualizado: AMS Amazon Machine Images (AMIs)	Se agregó la sección Offboarding AMS AMIs con un código de muestra para eliminarlo AMIs de tu cuenta.	Imágenes de máquinas AMS Amazon (AMIs)
Contenido actualizado: rol de usuario de IAM	Se actualizó la política de IAM: AMSBilling Política.	Función de usuario de IAM en AMS
Contenido nuevo: no compatible OSes	Se agregó información sobre los servicios que ofrece AMS para sistemas operativos no compatibles ()OSes.	Capacidades para sistemas operativos no compatibles en AMS
Contenido actualizado: informes a pedido	Algunos informes bajo demanda no están disponibles en AMS Advanced y se mostraron erróneamente como disponibles.	Informes a petición
Contenido actualizado: cierre de cuentas de AMS	Instrucciones aclaradas para desvincular las cuentas de aplicaciones de MALZ.	Extraiga las cuentas de la aplicación AMS
Contenido actualizado: Secrets Manager	Se corrigieron los nombres de las funciones de IAM necesarias para usar Secrets Manager.	Preguntas frecuentes sobre Secrets Manager in AWS Managed Services
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	AMIs. csv-and-notes.02.2023

Enero de 2023

Cambio	Descripción	Enlace
Contenido nuevo: AWS Device Farm (AMS SSPS)	Se agregó un nuevo servicio de SSPS: AWS Device Farm.	Utilice AMS SSP para aprovisionar AWS Device Farm en su cuenta AMS
Actualizado: versiones de Windows compatibles	Se agregó soporte para Windows Server 2022.	Imágenes de máquinas AMS Amazon (AMIs), Configuraciones admitidas, y Notificaciones AMI de AMS con SNS
Actualizado: administración de continuidad	Se actualizaron las reglas del plan de respaldo predeterminado de AMS.	Planes de respaldo predeterminados, landing zone multicuenta
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	AMIs. csv-and-notes.01.2023
Diciembre de 2022		
Actualizado: Uso de bastiones	Se ha corregido un enlace incorrecto.	Acceso a las instancias mediante bastiones
Actualizado: Programador de recursos	Se realizaron varias mejoras y se agregaron enlaces al Programador de AWS instancias para obtener más contexto.	Programador de recursos de AWS Managed Services

Cambio	Descripción	Enlace
Actualizado: Windows AMIs y configuraciones compatibles (para Windows AMIs nuevo)	Se actualizó el contenido AMI de AMS agregado desde EC2 Launch (Windows Server 2016 y versiones posteriores) a EC2 Launch (Windows Server 2016 y Windows Server 2019) y se agregó EC2 LaunchV2 (Windows Server 2022 y versiones posteriores). Basado en Windows actualizado AMIs de Microsoft Windows Server (2012, 2012 R2, 2016 y 2019) a Microsoft Windows Server (2012, 2012 R2, 2016, 2019 y 2022).	Imágenes de máquinas AMS Amazon (AMIs) y Descripción del servicio
Actualizado: sección Programador de recursos	Métodos mejorados para implementar y personalizar el AMS Resource Scheduler.	Programador de recursos de AWS Managed Services
Actualizado: configuración de AMS: DNS público y privado	Se actualizó el diagrama de arquitectura del DNS.	Configuración de DNS públicos y privados
Actualizado: arquitectura de red MALZ	Se actualizó el diagrama y se agregaron directrices para las cuentas de aplicaciones de Accelerate.	Arquitectura de red MALZ
Actualizado: Configuración: uso de etiquetas	Nota nueva: el etiquetado o personalizado solo es compatible con las cuentas de la aplicación MALZ, no con las cuentas principales.	Etiquetado automático de infraestructuras AMS

Cambio	Descripción	Enlace
Actualizado: Gestión de acceso: uso de bastiones	Introducción actualizada para incluir bastiones RDP.	Ahorro de costes en los bastiones de las zonas de landing zone con una sola cuenta (SALZ)
Actualizado: configuración predeterminada de AMS: alertas	EC2 Instancia añadida: uso de volúmenes no raíz a la tabla de alertas.	Alertas del monitoreo de referencia en AMS
Actualizado: Gestión de la continuidad	Se agregó una guía sobre las copias de seguridad continuas .	Cómo funciona la gestión de la continuidad
Actualizado: configuración de EC2 instancias automatizada	Se agregó soporte para PowerBroker Identity Service (PBIS) y On Instance Code (OIC).	Actualice automáticamente PBIS en instancias de Linux y Actualice automáticamente el código en las instancias de Linux
Actualizado: aprovisionamiento de autoservicio para Secrets Manager	Se actualizó el CT para añadir Secrets Manager a tu cuenta (en FAQs).	Utilice AMS SSP para aprovisionar AWS Secrets Manager en su cuenta AMS
Actualizado: administración de registros	Se actualizó la lista de registros a EC2 nivel del sistema.	Amazon Elastic Compute Cloud (Amazon EC2): registros a nivel de sistema
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	AMIs. csv-and-notes.12.2022
Noviembre de 2022		
Actualizado: AMS Amazon Machine Images (AMIs)	Se actualizaron las versiones compatibles de SUSE Linux.	Imágenes de máquinas AMS Amazon (AMIs)

Cambio	Descripción	Enlace
Actualizado: cuentas MALZ	Se ha añadido una guía para eliminar una cuenta de aplicación gestionada por el cliente.	Cuentas de aplicaciones administradas por el cliente
Actualizado: configuración de AMS	Se ha agregado <code>customer-ams-amazon2-security-enhanced</code> .	Notificaciones AMI de AMS con SNS
Actualizado: ¿Cómo funciona el monitoreo	Explicación actualizada de las notificaciones de servicio y los informes de incidentes.	Cómo funciona la supervisión
Actualizado: tipos de cuentas de la aplicación MALZ	Se ha mejorado la explicación de los tipos de cuentas.	Tipos de cuentas de aplicaciones
Actualizado: modo desarrollador	Se agregó una advertencia sobre el modo Desarrollador.	Antes de empezar con el modo AMS Developer
Actualizado: gestión de eventos planificados	Se agregó la sección: Tipos de PEM	Administración de eventos planificados en AWS Managed Services
Actualizado: Amazon Machine Images (AMIs)	Se actualizaron las versiones compatibles de SUSE Linux	Imágenes de máquinas AMS Amazon (AMIs)
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	AMIs. csv-and-notes1.11.2022
Octubre de 2022		
Nuevo: configuración de instancias automatizada	La nueva sección describe el proceso de configuración automatizada de instancias.	Configuración automatizada de instancias en AMS Advanced

Cambio	Descripción	Enlace
Nuevo: solo se acepta la tomografía computarizada manual en algunos SSPS	Se actualizaron más de 50 servicios de aprovisionamiento de autoservicio FAQs para utilizar el CT manual y no el CT automatizado para añadir el SSPS.	Modo de aprovisionamiento de autoservicio en AMS
Actualización: configuración de AMS	Se han añadido dos políticas a los perfiles de instancia de Amazon EC2 IAM para MALZ.	EC2 Perfil de instancia de IAM
Nuevo: biblioteca de reglas preventivas y de detección personalizadas.	Se agregó un conjunto de ejemplos de políticas de control de servicios (SCPs) y controles de reglas de Config preventivos basados en lo aprendido de varios clientes.	Reglas seleccionadas SCPs y Config
Actualización: advertencia AWS Backup	Se agregó una advertencia: «No edite los planes de respaldo de AMS, ya que los cambios podrían perderse. En su lugar, cree nuevos planes de respaldo utilizando ct-2hyozbpa0sx0m para sus configuraciones personalizadas».	Cómo funciona la gestión de la continuidad
AWS Backup Actualización: precaución	Se ha añadido una nota sobre la adición de nuevas funciones de IAM a su federación.	Implementación de recursos de IAM en AMS Advanced
Actualización: gestión de la supervisión	Las alertas generan informes de incidentes, no solicitudes de servicio.	Cómo funciona la supervisión

Cambio	Descripción	Enlace
Actualización: traiga su propio EPS	Se aplica tanto a SALZ como a MALZ.	AMS trae tu propio EPS
Actualización: cuenta de Accelerate Application	Se ha aclarado que su cuenta de Accelerate es una cuenta de aplicación.	Tipos de cuentas de aplicaciones
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	AMIs. csv-and-notes.10.2022
Septiembre de 2022		
Actualizado: ejemplos de comandos CLI para encontrar recursos	Se agregó un nuevo ejemplo y esa --region opción podría ser necesaria.	Búsqueda de los datos que necesita (SKMS), AMS
Actualizado: aprovisionamiento de funciones de IAM	Los roles de IAM ahora se pueden crear y administrar con. <code>AWSManagedServicesCloudFormationAdminRole</code>	Creación de pilas mediante el modo de cambio directo
Actualizado: Normas técnicas de AMS	Registro AMS-STD-007: (#20) Se aclararon los requisitos de reenvío.	Seguridad y conformidad
Actualizado: ¿Cómo funciona la gestión de la continuidad	Se revisó la redacción de Start Backup Job a «bajo demanda» en lugar de «existente».	Cómo funciona la gestión de la continuidad

Cambio	Descripción	Enlace
Actualizado: seguridad y conformidad	Descripción y guía actualizadas para el estándar AMS-STD-007 número 20: reenvío de registros entre cuentas.	Seguridad y conformidad
Actualizado: casos de uso de la gestión de cambios	Se ha eliminado un enlace roto a la antigua Guía del usuario sobre la gestión de cambios.	Casos de uso de la gestión de cambios
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	AMIs. csv-and-notes09.09.2022
11 de agosto de 2022		

Cambio	Descripción	Enlace
Actualizado: los encabezados de los capítulos han sido trasladados a secciones más apropiadas para garantizar una mayor coherencia y legibilidad	Tanto la «arquitectura de red MALZ» como la «arquitectura de red SALZ» son ahora subsecciones de la sección de nivel superior «Arquitectura de red», anteriormente la sección «Arquitectura de red AMS» «Modos de gestión de cambios» es el nuevo título de «Gestión de cambios» La «Configuración predeterminada» es ahora una subsección de la sección «Configuración de AMS» «Configuración de SAML y regla de notificación de ADFS» (anteriormente «regla de notificación y configuración de SAML de los Servicios de ActiveDirectory Federación (ADFS)») es ahora una subsección de «Configuración de AMS» «Gestión del acceso» es el nuevo título de «Acceso en AMS» y ha pasado a ocupar un lugar destacado en la tabla de contenido «Encontrar los datos que necesita» es el nuevo título de	¿Qué es AWS Managed Services?

Cambio	Descripción	Enlace
	«Gestión del conocimiento de los servicios» «Informes y opciones» es el nuevo título de «Informes de AMS» y aparece más abajo en el índice «Operaciones bajo demanda» es ahora el último tema del TOC	
Actualizado: Búsqueda y ARN, Nuevo: Búsqueda de un recurso con un ARN	Ambos procedimientos se reescribieron por completo para mayor utilidad.	Encuentra nombres de recursos de Amazon (ARNs) en AMS y Encuentre recursos por ARN en AMS .
Actualizado: Cómo conectar tu CMA con Transit Gateway	La automatización no permite añadir rutas a los dominios de rutas principales y era necesario actualizar el procedimiento.	Cómo conectar tu CMA con Transit Gateway
Actualización: precios de los componentes básicos de MALZ	Todos los precios están en dólares estadounidenses, formateados con signos de dólar.	Componentes básicos del entorno AMS
Actualizado: Notas AMI de AMS	El archivo zip incluye notas sobre las últimas imágenes de máquinas AMS Amazon (AMIs) y un archivo CSV con las últimas AMIs.	AMIs. csv-and-notes.08.2022
14 de julio de 2022		

Cambio	Descripción	Enlace
Actualizado: Informes de autoservicio	Se agregaron instrucciones para cifrar los AWS Glue metadatos con claves KMS.	Informes de autoservicio
Actualizado: monitoreo de referencia de AMS	Se agregó DeleteRec overyPoint una alerta de respaldo.	Alertas del monitoreo de referencia en AMS
Actualizado: sistemas operativos compatibles	Se agregó la fecha de fin de soporte para Amazon Linux 2.	Configuraciones admitidas
Actualizado: aprovisionamiento de autoservicio	Se agregó un requisito previo para el SSPS de AWS transferencia.	Utilice AMS SSP para aprovisionar AWS Transfer Family en su cuenta AMS
Actualizado: informes de AMS	Se agregó una nota sobre las regiones de suscripción.	Informes y opciones
Actualizado: correspondencia y archivos adjuntos a la RFC	Se aclararon los tipos de archivos de texto permitidos; en particular, los archivos YAML deben terminar en .yaml (no en .yml).	Agregue la correspondencia y los archivos adjuntos del RFC (consola)
21 de junio de 2022		
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.	Descripción general de los modos.
Nueva alarma	Se ha añadido una AWS Backup alarma.	Alertas del monitoreo de referencia en AMS

Cambio	Descripción	Enlace
16 de junio de 2022		
Contenido nuevo	Gestión de incidentes. AMS ahora puede resolver los incidentes que no supongan un riesgo para la seguridad con su aprobación en el informe del incidente y no necesitan una RFC ni una aprobación independientes.	Administración de incidentes
Contenido actualizado	MALZ: Diagrama de arquitectura de red actualizado. Actualizaciones: se debe eliminar el emparejamiento de VPC de la cuenta maestra con la vpc de servicios compartidos, ya que no existe.	Arquitectura de cuentas de red
	Servicio aprovisionado de autoservicio (SSPS) de Sagemaker. Se actualizó con una nueva función de IAM añadida al incorporarse para que Sagemaker la utilizara.	Utilice AMS SSP para aprovisionar Amazon SageMaker AI en su cuenta de AMS

Cambio	Descripción	Enlace
	A la lista de notificaciones de SNS AMIs compatibles: se agregaron customer-ams-sles 12, customer-ams-sles 15, customer-ams-amazon 1 con seguridad mejorada, 8, customer-ams-rhel 8 con seguridad mejorada, 18, 2012, 2019 y customer-ams-rhel 2019 con seguridad mejorada. customer-ams-ubuntu customer-ams-windows customer-ams-windows customer-ams-windows Se eliminaron customer-ams-rhel en AMIs las versiones 6 y 6 de seguridad mejorada. customer-ams-rhel	Notificaciones AMI de AMS con SNS
	Se eliminaron los correos electrónicos de escalada.	Obtener ayuda en AWS Managed Services
	Se ha movido la lista de temas a la parte inferior de los párrafos iniciales.	¿Qué es AWS Managed Services?
	Registros de servicio actualizados con mejores enlaces para los registros de equilibrio de carga, también reformateados.	Registros de servicios agregados de AMS

Cambio	Descripción	Enlace
Servicio de aprovisionamiento de autoservicio (SSPS) de EKS. Se agregó información sobre cómo habilitar el cifrado de secretos de sobres en su clúster.	Utilice AMS SSP para aprovisionar Amazon EKS AWS Fargate en su cuenta de AMS	
09 de junio de 2022		
Contenido actualizado, ¿Cómo obtener ayuda	Se eliminaron los correos electrónicos de rutas de escalamiento AMS proporciona métodos de comunicación a través de informes de incidentes, solicitudes de servicio y RFCs.	Obtener ayuda en AWS Managed Services
12 de mayo de 2022		
Nuevo contenido, modelo de suscripción a Operations on Demand (OOD)	AMS ha cambiado la incorporación de Operations on Demand del modelo actual de registro y renovación a un modelo predeterminado de asignación de suscripciones y suscripción voluntaria. Al crear una cuenta de AMS, ahora se inscribe automáticamente en Operations on Demand.	Operaciones bajo demanda
14 de abril de 2022		
Contenido nuevo, optimización de costes	AMS proporciona recomendaciones para la optimización de costos.	Optimización de costos en AWS Managed Services

Cambio	Descripción	Enlace
Contenido actualizado, cuenta Accelerate en MALZ	Se actualizó un nombre de función incorrecto (CustomerDefaultAdminRole) por el nombre de función correcto (AccelerateDefaultAdminRole).	Cuentas AMS Accelerate Sección «Acceder a su cuenta de Accelerate».
Contenido actualizado, AMS accede a las funciones de IAM	Se agregaron otras funciones de IAM de AMS que se utilizan para acceder a sus cuentas.	Por qué y cuándo AMS accede a tu cuenta Sección «Funciones de IAM para el acceso a las cuentas de los clientes de AMS».
Contenido actualizado, planes de respaldo de AMS	Se agregaron planes de respaldo administrados por AMS.	Planes de respaldo de AMS y Bóvedas de respaldo de AMS
Contenido actualizado, AWS Secrets Manager	Se actualizaron las preguntas frecuentes.	Utilice AMS SSP para aprovisionar AWS Secrets Manager en su cuenta AMS
Contenido actualizado, incorporación del modo de cambio directo (DCM)	AMS no permite la incorporación de clientes de Service Catalog a DCM.	Cómo empezar con el modo Direct Change

Cambio	Descripción	Enlace
Contenido actualizado, descripción del servicio	Se ha aclarado la sección de servicios compatibles: • Amazon EKS en AWS Fargate -> Amazon Elastic Kubernetes Service en Fargate • Amazon ECS para Fargate -> Amazon Elastic Container Service en Fargate AWS • Amazon Kinesis -> Amazon Kinesis Data Streams	AWS Servicios compatibles
Contenido actualizado, excluyendo las cuentas de MALZ	Se actualizó para hacer referencia a los nuevos tipos de cambios en las cuentas de aplicaciones que se están excluyendo.	Extraiga las cuentas de la aplicación AMS
Contenido actualizado, modo desarrollador, gestión de incidentes	Se actualizó la descripción del SLA para incidentes a: El SLA de AMS no se aplica a los recursos creados o actualizados fuera de AMS Change Management (incluido el modo de desarrollador), por lo que los recursos actualizados o creados en el modo de desarrollador se degradan automáticamente a P3 y el soporte es todo lo que se puede hacer.	Gestión de incidentes en el modo AMS Developer

Cambio	Descripción	Enlace
Contenido actualizado, incorporación de DCM	La plantilla de RFC para el nuevo DCM ahora incluye un campo para el ARN de su proveedor de SAML.	Cómo empezar con el modo Direct Change
Contenido actualizado, DCM para AWS CloudFormation	Las instrucciones para crear y actualizar AWS CloudFormation pilas ahora incluyen ejemplos de YAML.	Transformación AMS
Contenido actualizado, cuenta MALZ Tools	Hay una nueva función de IAM para las migraciones: <code>AWSManagedServicesMigrationRole</code>	AWS Servicio de migración de aplicaciones (AWS MGN) y Habilitar el acceso a la nueva cuenta de AMS Tools
Contenido nuevo, cuentas de landing zone multicuenta	Puedes crear una cuenta de Accelerate en tu cuenta de AMS Management multicuenta de landing zone.	Cuentas AMS Accelerate
Contenido actualizado, instalación API/CLI del SDK	Las instrucciones de instalación indicaban un nombre de archivo incorrecto para Mac/Linux las instalaciones y un comando incorrecto. Se ha corregido este error.	Uso de la API y la CLI de AMS
Contenido actualizado, cuenta Accelerate en MALZ	El nombre de la regla era incorrecto (<code>CustomerDefaultAdminRole</code>), pero se actualizó por el correcto (<code>AccelerateDefaultAdminRole</code>).	Cuentas AMS Accelerate , sección «Acceso a su cuenta de Accelerate»
Contenido actualizado, monitoreo	La supervisión del uso de root se revisó del 85% al 95%.	Alertas del monitoreo de referencia en AMS

Cambio	Descripción	Enlace
Contenido actualizado, notificaciones de AMI	Puede crear muchos tipos de notificaciones de SNS para los nuevos AMS AMIs. Hemos añadido información sobre la creación de varios tipos.	Notificaciones AMI de AMS con SNS
Contenido actualizado, configuración predeterminada de AMS	Se eliminaron las referencias a Macie Classic y se sustituyeron por Macie.	Alertas del monitoreo de referencia en AMS
Contenido actualizado, prefijos reservados de AMS	Ordenó alfabéticamente la lista de prefijos reservados.	Prefijos reservados AMS
Contenido actualizado, descripción del servicio	Las secciones de funciones sobre la gestión de cambios y el aprovisionamiento de autoservicio se actualizaron con más información sobre los modos AMS.	Características del plan operativo avanzado de AWS Managed Services (AMS) AMS
Contenido actualizado, AWS Secrets Manager	Compartir claves mediante Secrets Manager.	10 de febrero de 2022
Contenido nuevo, aprovisionamiento de autoservicio, Amazon Connect	Se agregó una sección de preguntas frecuentes sobre cómo solicitar la adición de una lista de países para las llamadas entrantes o salientes.	10 de febrero de 2022

Cambio	Descripción	Enlace
Contenido nuevo, aprovisionamiento de autoservicio, Amazon EKS en Fargate	Se agregó una restricción en las preguntas frecuentes según la cual AMS no admite la implementación de clústeres de EKS mediante el kit de desarrollo en la AWS nube (CDK) o CloudFormation Ingest.	10 de febrero de 2022
Contenido modificado, modo desarrollador	Corrección: no utiliza una RFC o una solicitud de servicio para asignar usuarios a su solución de federación, sino que lo hace usted mismo según la solución.	10 de febrero de 2022
	Tenga en cuenta que el IAM no es compatible con DCM.	10 de febrero de 2022
Contenido modificado, modo de cambio directo (DCM)	DCM, tome nota de las validaciones que realizamos.	10 de febrero de 2022
	DCM, aclare las restricciones de las diferentes funciones.	10 de febrero de 2022
Contenido modificado, monitoreo de las alertas de referencia	Se han modificado las alertas de recursos del clúster de Redshift.	10 de febrero de 2022
Contenido modificado, informes de autoservicio	Se agregó el nombre exacto del bucket s3, (ams-reporting-data-a<Account_ID>), para que los clientes lo usen para buscar los informes.	10 de febrero de 2022

Cambio	Descripción	Enlace
Se ha modificado el contenido, se ha actualizado el contenido para hacer referencia a los tipos de cambios automatizados en lugar de a los manuales Gestión Otros Otros (MOO)	Se actualizó el contenido de la cuenta de la aplicación de zonas de aterrizaje multicuenta (MALZ) para hacer referencia a los tipos de cambios automatizados (tres: «Asociar el adjunto de TGW a una tabla de rutas», «Crear rutas en las tablas de rutas de TGW para conectarse a esta VPC» y «Configurar las tablas de rutas de la VPC para que apunten a la pasarela de tránsito de la zona de aterrizaje multicuenta de AMS»). Recibir alertas generadas por AMS Notificaciones de alertas basadas en etiquetas	10 de febrero de 2022
Contenido modificado: AMS. AMIs	Se agregó nueva información sobre la seguridad mejorada AMIs. Consulte Configuraciones admitidas Imágenes de máquinas AMS Amazon (AMIs) , y. Seguridad mejorada AMIs	27 de enero de 2022
Contenido nuevo: aprovisionamiento de autoservicio.	Se agregó Amazon Fax para OpenZFS. Consulte Usa AMS SSP para aprovisionar Amazon FSx para OpenZFS en tu cuenta de AMS.	27 de enero de 2022

Cambio	Descripción	Enlace
Contenido modificado: servicio de aprovisionamiento de autoservicio (SSPS) de CodeDeploy.	Nombre de función adicional y nota de restricción adicional . Consulte Utilice AMS SSP para aprovisionar AWS CodeDeploy en su cuenta AMS	27 de enero de 2022
Contenido modificado: enlaces actualizados.	Se corrigieron los enlaces rotos: AMS-AMIs, Búsqueda de su configuración, Búsqueda de un ID de pila, Búsqueda de un ID de VPC, ListVpcSummaries ListStack Summaries, y. GetStack APIs Por ejemplo, consulte Encuentra una pila IDs en AMS .	13 de enero de 2022
Contenido modificado: EKS Support for Fargate	Se agregó una limitación a FAQs: EC2 No se admite la creación o administración de grupos de nodos con EKS. Consulte Utilice AMS SSP para aprovisionar Amazon EKS AWS Fargate en su cuenta de AMS .	13 de enero de 2022
Contenido modificado: modo CloudFormation de cambio directo (DCM)	Se agregaron instrucciones para crear o actualizar pilas de CF utilizando. AmsStackT ransform Consulte Creación de pilas mediante el modo de cambio directo .	13 de enero de 2022

Cambio	Descripción	Enlace
Contenido modificado: uniformidad en los nombres de los servicios AWS	Las referencias a AMS Servicios de AWS deben coincidir exactamente con los AWS títulos o metadatos oficiales. Anteriormente, había pequeñas variaciones que complicaban la coincidencia de patrones. Por ejemplo, consulte Usa AMS SSP para aprovisionar Alexa for Business en tu cuenta de AMS.	13 de enero de 2022
Contenido modificado: aprovisionamiento de autoservicio de Elastic Container Registry (ECR)	Se agregó un elemento de preguntas frecuentes sobre el uso del ECR para administrar los permisos de los usuarios. Consulte Utilice AMS SSP para aprovisionar Amazon Elastic Container Registry en su cuenta de AMS.	13 de enero 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.