Guía del usuario

AWS Organizations

AWS Organizations: Guía del usuario

Table of Contents

¿Qué es AWS Organizations? 1
Características 2
Casos de uso 3
Terminología y conceptos 4
Conjuntos de características disponibles 5
Estructura de la organización 6
Invitaciones y establecimiento de comunicación 10
Políticas de la organización 11
Cuotas y límites de servicio 12
Directrices de nomenclatura 13
Consideraciones 13
Valores mínimos y máximos 13
Tiempo de vencimiento de protocolos de enlace (handshakes) 17
Número de políticas que puede asociar a una entidad 18
Límites de limitación 19
Compatibilidad de regiones 23
Lista de regiones disponibles 24
Precios y facturación 29
Responsabilidad del pago 29
Estructura de pago 29
Soporte y comentarios 29
Otros recursos de AWS 29
Prácticas recomendadas 31
Cuenta y credenciales 31
Habilite la administración del acceso raíz para simplificar la administración de las credenciales de los usuarios raíz en las cuentas de los miembros 31
Mantener actualizado el número de teléfono de contacto 32
Utilizar una dirección de correo electrónico de grupo para todas las cuentas raíz 32
Estructura organizativa y cargas de trabajo 33
Administrar cuentas dentro de una sola organización 33
Agrupar cargas de trabajo en función del propósito empresarial y no de la estructura de informes 33
Utilizar varias cuentas para organizar cargas de trabajo 33
Administración de costos y servicio 34

Habilite AWS los servicios a nivel organizativo mediante la consola de servicios o las operaciones de API/CLI ... 34
Utilizar las herramientas de facturación para realizar un seguimiento de los costos y optimizar el uso de los recursos ... 34
Planificar la estrategia de etiquetado y la aplicación de las etiquetas en todos los recursos de la organización ... 34
Introducción ... 35
Registrarse en AWS ... 35
Inscríbase en una Cuenta de AWS ... 36
Creación de un usuario con acceso administrativo ... 36
Accediendo AWS Organizations ... 37
Tutorial: Creación y configuración de una organización ... 39
Requisitos previos ... 40
Paso 1: Crear la organización ... 41
Paso 2: Crear las unidades organizativas ... 44
Paso 3: Crear las políticas de control de servicios ... 46
Paso 4: Probar las políticas de la organización ... 51
Tutorial: Supervisa una organización con Amazon EventBridge ... 52
Requisitos previos ... 53
Paso 1: Configuración de un registro de seguimiento y un selector de eventos ... 54
Paso 2: Configuración de la función Lambda ... 55
Paso 3: Creación de un tema de Amazon SNS que envía correos electrónicos a los suscriptores ... 56
Paso 4: Crea una EventBridge regla de Amazon ... 57
Paso 5: Pon a prueba tu EventBridge regla de Amazon ... 57
Limpieza: Elimine los recursos que ya no necesite ... 59
Trabajando con AWS SDKs ... 60
Administración de una organización entera ... 62
Creación de una organización ... 62
Crear una organización ... 63
Verificación de dirección de correo electrónico ... 67
Verificar su dirección de correo electrónico ... 67
Reenvío del correo electrónico de verificación ... 68
Cambio de dirección de correo electrónico ... 68
Habilitar todas las características ... 69
Consideraciones ... 70

Proceso de migración estándar ... 71
Proceso de migración asistida ... 81
Visualización de los detalles de una organización ... 82
Eliminar una organización ... 83
Consideraciones ... 84
Eliminar una organización ... 85
Administración de cuentas en una organización ... 89
Cuenta de administración ... 89
Prácticas recomendadas para la cuenta de administración ... 90
Cierre de una cuenta de administración ... 91
Cuentas de miembros ... 93
Prácticas recomendadas para cuentas de miembros ... 93
Creación de una cuenta de miembro ... 96
Acceso a las cuentas de miembro ... 103
Cerrar una cuenta de miembro ... 110
Protección de cuentas miembro contra el cierre ... 112
Eliminación de una cuenta miembro ... 113
Abandono de una organización desde una cuenta de miembro ... 119
Actualización de la dirección de correo electrónico del usuario raíz de una cuenta de miembro ... 123
Invitaciones de cuentas ... 127
Consideraciones ... 128
Envío de invitaciones ... 130
Administración de invitaciones pendientes ... 133
Aceptar o rechazar invitaciones ... 138
Migración de una cuenta ... 142
Antes de la migración ... 143
Migración ... 146
Después de la migración ... 147
Consultar detalles de una cuenta ... 148
Exportación de los detalles de las cuentas ... 149
Exportación de una lista de todas las Cuentas de AWS de su organización ... 150
Actualización de contactos alternativos de cuentas ... 151
Actualización de la información de contacto principal ... 151
Actualización de las Regiones de AWS habilitadas para cuentas ... 152
Unidades organizativas (OUs) ... 153

Mejores prácticas para OUs 154
Comprensión AWS Organizations 155
Fundamental recomendado OUs 155
Se recomienda una adición OUs 157
Conclusión 158
Navegación por la raíz y el árbol 159
Consultar los detalles de una unidad organizativa 160
Crear una unidad organizativa 163
Cambiar el nombre de una unidad organizativa 166
Etiquetado de una unidad organizativa 168
Mover cuentas entre unidades organizativas 170
Visualización de los detalles del nodo raíz 172
Eliminar una unidad organizativa 173
Políticas de la organización 177
Tipos de políticas 177
Políticas de autorización 178
Políticas de administración 178
Políticas de autorización 180
Diferencias entre SCPs y RCPs 181
Uso y SCPs RCPs 181
Políticas de control de servicios 183
Políticas de control de recursos 237
Políticas de administración 254
Requisitos previos y permisos 255
Descripción de la herencia de políticas 257
Visualización de políticas en vigor 274
Políticas declarativas 277
Políticas de copia de seguridad 299
Políticas de etiquetas 343
Políticas de chatbot 388
Políticas de exclusión de servicios de IA 403
Administrador delegado para AWS Organizations 413
Creación de una política de delegación basada en recursos 414
Actualización de una política de delegación basada en recursos 419
Ver una política de delegación basada en recursos 424
Eliminar una política de delegación basada en recursos 425

Habilitar un tipo de política ... 426
Deshabilitar un tipo de política ... 428
Consideraciones ... 428
Desactivación de un tipo de política ... 428
Creación de políticas de ... 430
Creación de una política de control de servicios (SCP) ... 430
Cree una política de control de recursos (RCP) ... 436
Cree una política declarativa ... 441
Creación de una política de copia de seguridad ... 443
Creación de una política de etiquetas ... 448
Creación de una política de chatbot ... 453
Creación de una política de exclusión de servicios de IA ... 457
Actualización de políticas ... 460
Actualización de una política de control de servicio (SCP) ... 460
Actualice una política de control de recursos (RCP) ... 463
Actualice una política declarativa ... 466
Actualización de una política de copias de seguridad ... 468
Actualización de una política de etiquetas ... 472
Actualización de una política de chatbot ... 475
Actualización de una política de exclusión de servicios de IA ... 476
Edición de etiquetas vinculadas a políticas ... 479
Edición de etiquetas vinculadas a una política de control de servicio (SCP) ... 480
Edite las etiquetas adjuntas a una política de control de recursos (RCP) ... 481
Edite las etiquetas adjuntas a una política declarativa ... 483
Edición de etiquetas vinculadas a una política de copia de seguridad ... 484
Edición de etiquetas vinculadas a una política de etiquetas ... 486
Edición de etiquetas vinculadas a una política de chatbot ... 487
Edición de etiquetas vinculadas a una política de exclusión de servicios de IA ... 488
Vinculación de políticas ... 490
Vinculación de políticas ... 490
Desvinculación de políticas ... 501
Desvinculación de políticas ... 501
Obtener detalles de la política ... 514
Enumeración de todas las políticas ... 514
Listado de políticas adjuntas ... 519
Listado de todos los adjuntos ... 520

Obtener información sobre una política ... 522
Eliminación de políticas ... 525
Eliminación de políticas ... 525
Etiquetado de recursos ... 532
Consideraciones ... 532
Uso de etiquetas ... 533
Agregar, actualizar y quitar etiquetas ... 534
Adición de etiquetas a un recurso cuando lo crea ... 534
Adición o actualización de etiquetas en un recurso existente ... 535
Usando otro Servicios de AWS ... 537
Permisos necesarios para habilitar el acceso de confianza ... 538
Permisos necesarios para deshabilitar el acceso de confianza ... 539
Cómo habilitar o deshabilitar el acceso de confianza ... 541
AWS Organizations y funciones vinculadas al servicio ... 543
Uso del rol AWSServiceRoleForDeclarativePoliciesEC2Report vinculado al servicio ... 544
Servicios que funcionan con Organizations ... 544
AWS Account Management ... 608
AWS Application Migration Service ... 612
AWS Artifact ... 618
AWS Audit Manager ... 621
AWS Backup ... 625
AWS Billing and Cost Management ... 628
AWS CloudFormation StackSets ... 630
AWS CloudTrail ... 634
Amazon CloudWatch ... 639
AWS Compute Optimizer ... 644
AWS Config ... 649
Centro de optimización de costes de AWS ... 652
AWS Control Tower ... 656
Amazon Detective ... 658
El DevOps gurú de Amazon ... 662
AWS Directory Service ... 666
Amazon Elastic Compute Cloud ... 669
AWS Firewall Manager ... 672
Amazon GuardDuty ... 676
AWS Health ... 679

AWS Identity and Access Management 683
Amazon Inspector 686
AWS License Manager 690
AWS Managed Services (AMS) Informes de autoservicio (SSR) 693
Amazon Macie 695
AWS Marketplace 698
AWS Marketplace Marketplace privado 702
AWS Marketplace panel de información sobre adquisiciones 706
Administrador de red de AWS 710
Amazon Q Developer 713
AWS Resource Access Manager 715
Explorador de recursos de AWS 719
AWS Security Hub 723
Amazon S3 Storage Lens 726
AWS Respuesta a incidentes de seguridad 729
Amazon Security Lake 735
AWS Service Catalog 740
Service Quotas 744
AWS IAM Identity Center 746
AWS Systems Manager 750
AWS User Notifications 755
Políticas de etiquetas 758
AWS Trusted Advisor 760
AWS Well-Architected Tool 763
Administrador de direcciones VPC IP de Amazon (IPAM) 767
Analizador de accesibilidad de Amazon VPC 770
Administrador delegado para los Servicios de AWS integrados 775
Permisos concedidos a cuentas de administrador delegado 775
Seguridad 778
AWS PrivateLink 779
Limitaciones y restricciones de la forma AWS PrivateLinkAWS Organizations 779
Creación de un punto de conexión de VPC 780
Creación de una política de punto de conexión de VPC 780
Identity and Access Management 781
Público 781
Autenticación con identidades 782

Administración de acceso mediante políticas ... 786
¿Cómo AWS Organizations funciona con IAM ... 789
Administración de permisos en una organización ... 796
Ejemplos de políticas basadas en identidades ... 805
Ejemplos de políticas basadas en recursos ... 812
AWS políticas gestionadas ... 821
Control de acceso basado en atributos con etiquetas ... 826
Solución de problemas ... 831
Registro y supervisión ... 833
AWS CloudTrail ... 833
Amazon EventBridge ... 844
Validación de conformidad ... 844
Resiliencia ... 846
Seguridad de la infraestructura ... 846
Solución de problemas ... 848
Solución de problemas generales ... 848
Recibo un mensaje de «acceso denegado» cuando hago una solicitud a AWS Organizations ... 848
Aparece un mensaje de “acceso denegado” al realizar una solicitud con credenciales de seguridad temporales ... 849
Obtengo un mensaje de "acceso denegado" cuando intento dejar una organización como cuenta de miembro o eliminar una cuenta de miembro como cuenta de administración. ... 849
Obtengo un mensaje de "cuota superada" cuando intento agregar una cuenta a mi organización ... 850
Aparece un mensaje que indica que "esta operación requiere un periodo de espera" al añadir o eliminar cuentas ... 850
Obtengo un mensaje de "organización todavía inicializando" cuando intento añadir una cuenta a mi organización ... 850
Aparece el mensaje "Invitations are disabled" cuando intento invitar a una cuenta a mi organización. ... 851
Los cambios que realizo no están siempre visibles inmediatamente ... 851
Realizar solicitudes de consulta HTTP ... 852
puntos de conexión ... 853
HTTPS obligatorio ... 853
Firmar solicitudes de API AWS Organizations ... 853
Ejemplos de código ... 854

Conceptos básicos 855
Acciones 855
Historial de documentos 893
..... cmxi

¿Qué es AWS Organizations?

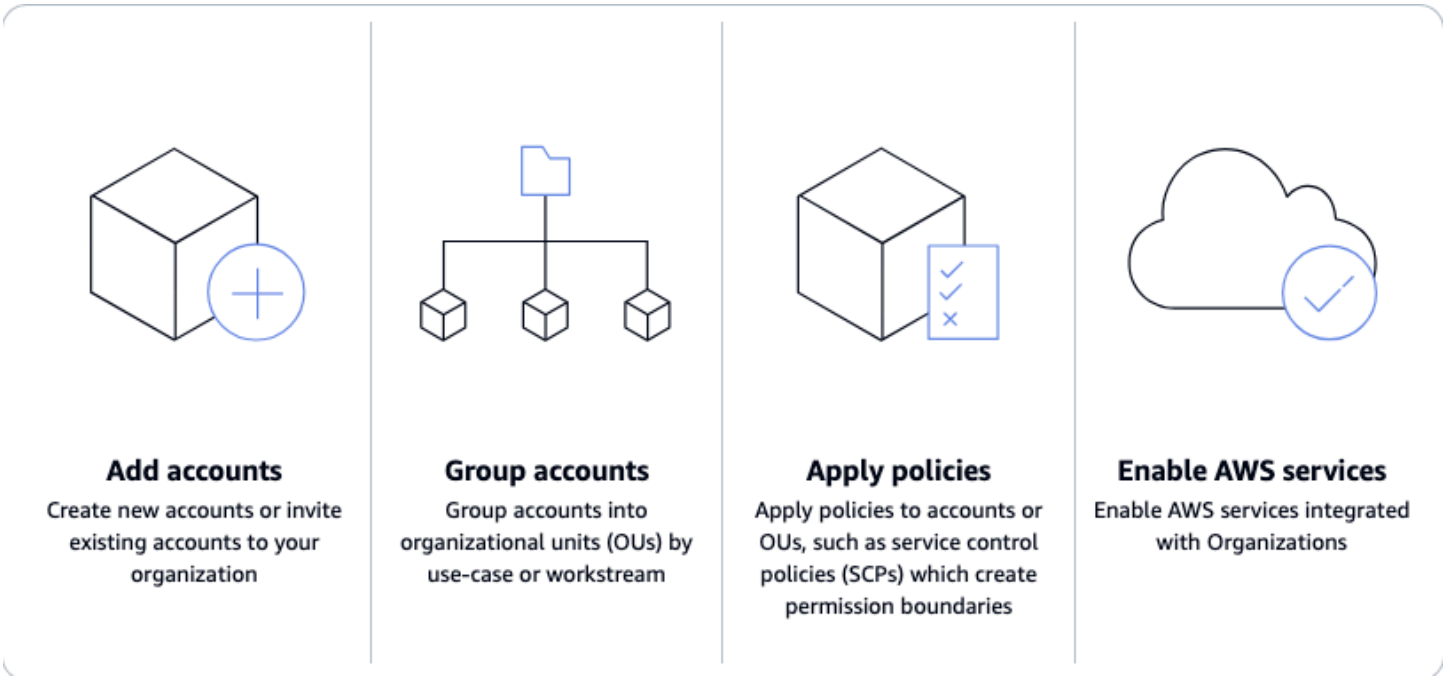
Administre su entorno de forma centralizada a medida que amplía sus AWS recursos

AWS Organizations le ayuda a administrar y gobernar su entorno de forma centralizada a medida que crece y escala sus AWS recursos. Con Organizations, puede crear nuevas cuentas y asignar recursos, agrupar cuentas para organizar sus flujos de trabajo, aplicar políticas con fines de gobernanza y simplificar la facturación mediante un único método de pago para todas sus cuentas.

Organizations se integra con otras Servicios de AWS para que pueda definir configuraciones centrales, mecanismos de seguridad, requisitos de auditoría y uso compartido de recursos entre las cuentas de su organización. Para obtener más información, consulte Uso AWS Organizations con otros Servicios de AWS.

En el siguiente diagrama puede ver una explicación avanzada sobre cómo se puede utilizar AWS Organizations:

- Agregar cuentas
- Agrupar cuentas
- Aplicar políticas
- Habilitar Servicios de AWS.



Temas

- Funciones para AWS Organizations
- Casos de uso para AWS Organizations
- Terminología y conceptos para AWS Organizations
- Cuotas y límites de servicio para AWS Organizations
- Soporte regional para AWS Organizations
- Precios y facturación de AWS Organizations
- Soporte y comentarios de AWS Organizations

Funciones para AWS Organizations

AWS Organizations ofrece las siguientes funciones:

Administre sus Cuentas de AWS

Cuentas de AWS son límites naturales para los permisos, la seguridad, los costos y las cargas de trabajo. El uso de un entorno de varias cuentas es una práctica recomendada a la hora de escalar un entorno en la nube. Puedes simplificar la creación de cuentas creando nuevas cuentas mediante programación mediante AWS Command Line Interface (AWS CLI), o SDKs APIs, y aprovisionar de forma centralizada los recursos y permisos recomendados para esas cuentas. AWS CloudFormation StackSets

Defina y administre su organización

A medida que creas cuentas nuevas, puedes agruparlas en unidades organizativas (OUs) o grupos de cuentas que sirvan a una sola aplicación o servicio. Aplique políticas de etiquetas para clasificar o hacer un seguimiento de los recursos de su organización y ofrezca un control de acceso basado en atributos a los usuarios o las aplicaciones. Además, puedes delegar la responsabilidad del soporte en las cuentas Servicios de AWS para que los usuarios puedan administrarlas en nombre de tu organización.

Proteja y supervise sus cuentas

Puede proporcionar herramientas y acceso de forma centralizada para que su equipo de seguridad administre las necesidades de seguridad en nombre de la organización. Por ejemplo, puede proporcionar acceso de seguridad de solo lectura a todas las cuentas, detectar y mitigar las amenazas con Amazon GuardDuty, revisar el acceso no deseado a los recursos con IAM Access Analyzer y proteger los datos confidenciales con Amazon Macie.

Controle el acceso y los permisos

Configure AWS IAM Identity Center para proporcionar acceso a los recursos y las Cuentas de AWS mediante su Active Directory, y personalice los permisos en función de los distintos roles de trabajo. También puede aplicar las políticas de la organización a los usuarios, las cuentas o. OUs Por ejemplo, las políticas de control de servicios (SCPs) le permiten controlar el acceso a AWS los recursos, los servicios y las regiones de su organización. Las políticas de control de recursos (RCPs) le permiten evitar de forma centralizada el uso no deseado de sus AWS recursos. Las políticas de chatbot le permiten controlar el acceso a las cuentas de su organización desde aplicaciones de chat como Slack y Microsoft Teams.

Comparta recursos entre cuentas

Puede compartir AWS recursos dentro de su organización mediante AWS Resource Access Manager (AWS RAM). Por ejemplo, puede crear sus subredes de Amazon Virtual Private Cloud (Amazon VPC) una vez y compartirlas en su organización. También puede acordar licencias de software de forma centralizada con AWS License Manager y compartir un catálogo de servicios de TI y productos personalizados entre cuentas con AWS Service Catalog.

Audite su entorno para comprobar el nivel de cumplimiento

Puede activar AWS CloudTrail en todas las cuentas, lo que crea un registro de toda la actividad de su entorno en la nube que las cuentas de miembro no pueden desactivar ni modificar. Además, puede establecer políticas para hacer cumplir las copias de seguridad según el ritmo que especifique o definir los ajustes de configuración recomendados para los recursos en todas las cuentas y Regiones de AWS con AWS Config. AWS Backup

Administre de forma centralizada la facturación y los costos

Organizations le proporciona una única factura unificada. Además, puede ver el uso de los recursos en todas las cuentas, hacer un seguimiento de los costos con AWS Cost Explorer y optimizar el uso de los recursos de computación mediante AWS Compute Optimizer.

Casos de uso para AWS Organizations

A continuación se muestran algunos casos de uso para AWS Organizations:

Automatice la creación Cuentas de AWS y categorización de las cargas de trabajo

Puede automatizar la creación de nuevas cargas de trabajo Cuentas de AWS para lanzar rápidamente nuevas cargas de trabajo. Agregue las cuentas a los grupos definidos por el usuario

para aplicar las políticas de seguridad al instante, implementar infraestructuras sin intervención y llevar a cabo auditorías. Cree grupos separados para clasificar las cuentas de desarrollo y producción y utilícelos AWS CloudFormation StackSetspara aprovisionar servicios y permisos a cada grupo.

Defina y aplique las políticas de auditoría y cumplimiento

Puede aplicar políticas de control de servicios (SCPs) para garantizar que sus usuarios realicen únicamente las acciones que cumplan con sus requisitos de seguridad y conformidad. Cree un registro central de todas las acciones hechas en su organización con AWS CloudTrail. Vea y aplique las configuraciones de recursos estándar en todas las cuentas y en las que las Regiones de AWS utilice AWS Config. Aplique automáticamente copias de seguridad periódicas con AWS Backup. Úselo AWS Control Towerpara aplicar reglas de gobierno preconfiguradas para la seguridad, las operaciones y el cumplimiento de sus cargas de AWS trabajo.

Proporcione herramientas y acceso a sus equipos de seguridad y, al mismo tiempo, fomente el desarrollo

Cree un grupo de seguridad y bríndele acceso de solo lectura a todos sus recursos para identificar y mitigar los problemas de seguridad. Puede permitir que ese grupo gestione Amazon para GuardDuty que supervise y mitigue activamente las amenazas a sus cargas de trabajo, y que IAM Access Analyzer identifique rápidamente el acceso no deseado a sus recursos.

Comparta recursos comunes entre cuentas

Organizations le facilita el uso compartido de recursos centrales críticos en sus cuentas. Por ejemplo, puede compartir su AWS Directory Service for Microsoft Active Directory central para que las aplicaciones puedan acceder a su almacén de identidades central.

Comparta los recursos centrales fundamentales entre sus cuentas

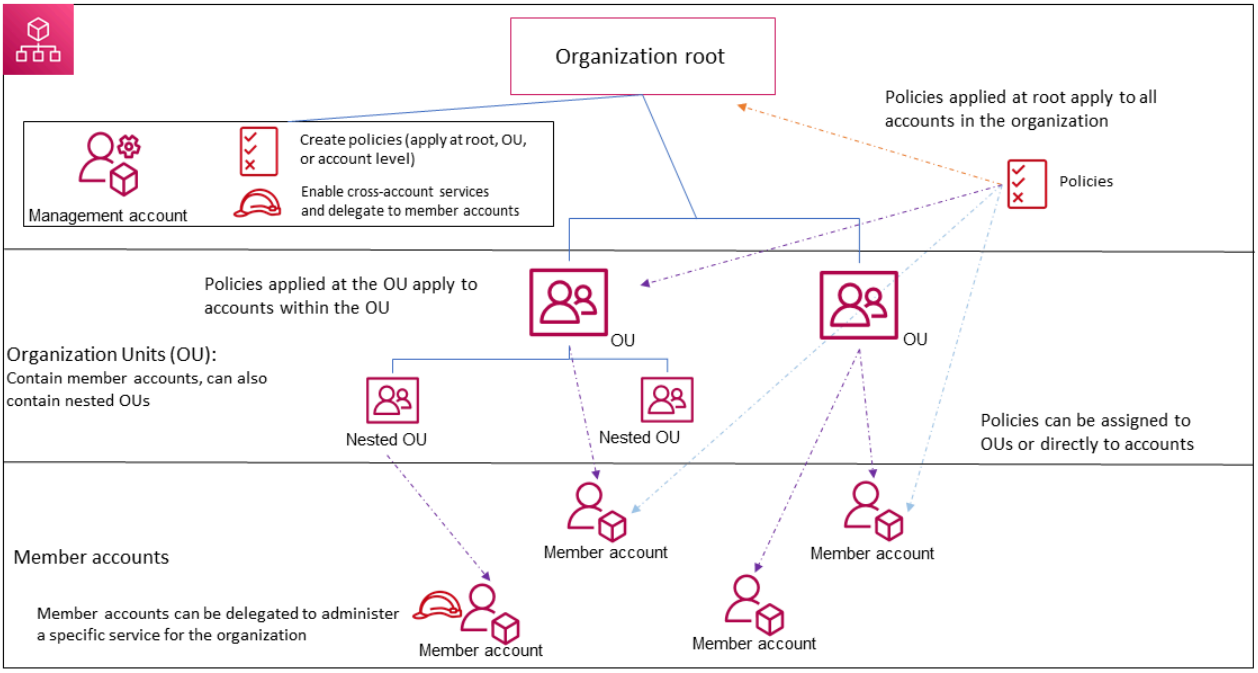
Comparta su AWS Directory Service for Microsoft Active Directory como almacén de identidades central para sus aplicaciones. Use AWS Service Catalog para compartir servicios de TI en cuentas designadas para que los usuarios puedan descubrir e implementar rápidamente los servicios aprobados. Asegúrese de que los recursos de la aplicación se creen en las subredes de Amazon Virtual Private Cloud (Amazon VPC) definiéndolos de forma centralizada una vez y compartiéndolos en toda la organización mediante AWS Resource Access Manager (AWS RAM).

Terminología y conceptos para AWS Organizations

En este tema se explican algunos de los conceptos clave de AWS Organizations.

En el siguiente diagrama se muestra una organización que consta de cinco cuentas que se organizan en cuatro unidades organizativas (OUs) bajo la raíz. La organización también tiene varias políticas que se adjuntan a algunas de las cuentas OUs o directamente a ellas.

Para obtener una descripción de cada uno de estos elementos, consulte las definiciones incluidas en este tema.



Temas

- Conjuntos de características disponibles
- Estructura de la organización
- Invitaciones y establecimiento de comunicación
- Políticas de la organización

Conjuntos de características disponibles

Todas las características (recomendado)

Todas las funciones son el conjunto de funciones predeterminado disponible en AWS Organizations. Puede establecer políticas centrales y requisitos de configuración para toda

la organización, crear capacidades o permisos personalizados dentro de la organización, administrar y organizar sus cuentas en una sola factura y delegar responsabilidades a otras cuentas en nombre de la organización. También puede utilizar las integraciones con otros Servicios de AWS para definir las configuraciones centrales, los mecanismos de seguridad, los requisitos de auditoría y el uso compartido de recursos entre todas las cuentas de miembro de su organización. Para obtener más información, consulte Uso AWS Organizations con otros Servicios de AWS.

El modo Todas las características proporciona todas las capacidades de facturación unificada junto con las capacidades administrativas.

Consolidated billing

La facturación unificada es el conjunto de funciones que proporciona la funcionalidad de facturación compartida, pero no incluye las funciones más avanzadas de AWS Organizations. Por ejemplo, no puedes permitir que otros AWS servicios se integren con tu organización para que funcionen en todas sus cuentas, ni usar políticas para restringir lo que pueden hacer los usuarios y los roles de las distintas cuentas.

Puede habilitar todas las características de una organización que originalmente solo admitía las características de facturación unificada. Para habilitar todas las características, todas las cuentas de miembro invitadas deben aprobar el cambio aceptando la invitación que se envía cuando la cuenta de administración inicia el proceso. Para obtener más información, consulte Habilitar todas las funciones de una organización con AWS Organizations.

Estructura de la organización

Organización

Una organización es un conjunto de Cuentas de AWS que puede administrar de forma centralizada y organizar en una estructura jerárquica similar a un árbol, con un nodo raíz en la parte superior y unidades organizativas anidadas debajo de la raíz. Cada cuenta puede estar directamente en la raíz o colocarse en una de las OUs siguientes jerarquías.

Cada organización se compone de los siguientes elementos:

- Una cuenta de administración
- Cero o más cuentas de miembro
- Cero o más unidades organizativas (OUs)

- Cero o más políticas.

Una organización tiene la funcionalidad determinada por el conjunto de características habilitadas.

Raíz

Hay un nodo raíz administrativo (raíz) en la cuenta de administración que actúa como el punto de partida para organizar Cuentas de AWS. El nodo raíz es el contenedor que corona la jerarquía de la organización. En esta raíz, puedes crear unidades organizativas (OUs) para agrupar tus cuentas de forma lógica y organizarlas OUs en la jerarquía que mejor se adapte a tus necesidades.

Si aplicas una política de administración a la raíz, se aplica a todas las unidades organizativas (OUs) y cuentas, incluida la cuenta de administración de la organización.

Si aplicas una política de autorización (por ejemplo, una política de control de servicios (SCP)) a la raíz, se aplicará a todas las unidades organizativas (OUs) y a las cuentas de los miembros de la organización. No se aplica a la cuenta de administración de la organización.

> **Note**
>
> Solo puedes tener una raíz. AWS Organizations crea automáticamente la raíz al crear una organización.

Unidad organizativa (OU)

Una unidad organizativa (OU) es un grupo de Cuentas de AWS dentro de una organización. Una OU también puede contener otras OUs que le permitan crear una jerarquía. Por ejemplo, puede agrupar todas las cuentas que pertenezcan al mismo departamento en una OU departamental. Del mismo modo, puede agrupar todas las cuentas que ponen en marcha servicios de seguridad en una OU de seguridad.

OUs son útiles cuando necesita aplicar los mismos controles a un subconjunto de cuentas de su organización. El anidamiento OUs permite unidades de administración más pequeñas. Por ejemplo, puede crear OUs para cada carga de trabajo y, a continuación, crear dos anidadas OUs en cada unidad organizativa de carga de trabajo para dividir las cargas de trabajo de producción de las de preproducción. Estas OUs heredan las políticas de la unidad organizativa principal,

además de cualquier control asignado directamente a la unidad organizativa a nivel de equipo. Si se incluye la raíz y Cuentas de AWS se crea en el nivel más bajo OUs, la jerarquía puede tener cinco niveles de profundidad.

Cuenta de AWS

An Cuenta de AWSes un contenedor para tus AWS recursos. Usted crea y administra sus AWS recursos en un Cuenta de AWS, y esto Cuenta de AWS proporciona capacidades administrativas de acceso y facturación.

El uso de varios Cuentas de AWS es una práctica recomendada para escalar su entorno, ya que proporciona un límite de facturación para los costos, aísla los recursos por motivos de seguridad, brinda flexibilidad a las personas y los equipos, además de poder adaptarse a los nuevos procesos.

> **Note**
>
> Una AWS cuenta es diferente de un usuario. Un usuario es una identidad que se crea usando AWS Identity and Access Management (IAM) y toma la forma de usuario de IAM con credenciales a largo plazo o un rol de IAM con credenciales a corto plazo. Una sola AWS cuenta puede contener, y normalmente lo hace, muchos usuarios y roles.

Hay dos tipos de cuentas en una organización: una cuenta única que se denomina la cuenta de administración y una o más cuentas de miembro.

Cuenta de administración

Una cuenta de administración es la Cuenta de AWS que se utiliza para crear la organización. Desde la cuenta de administración, puede hacer lo siguiente:

- Crear otras cuentas en su organización
- Invitar y administrar las invitaciones para que otras cuentas se unan a su organización
- Designar cuentas de administrador delegado
- Eliminar cuentas de la organización
- Adjunta políticas a entidades como las raíces, las unidades organizativas (OUs) o las cuentas de tu organización
- Habilite la integración con AWS los servicios compatibles para proporcionar funcionalidad de servicio en todas las cuentas de la organización.

La cuenta de administración es el propietario final de la organización y tiene el control final de las políticas de seguridad, infraestructura y finanzas. Esta cuenta tiene el rol de cuenta pagadora y es responsable de todos los cargos acumulados por las cuentas de su organización.

> **Note**
>
> No puede cambiar qué cuenta de su organización es la cuenta de administración.

Cuenta de miembro

Una cuenta de miembro es una Cuenta de AWS, distinta de la cuenta de administración, que forma parte de una organización. Si es un administrador de una organización, puede crear cuentas de miembro e invitar a cuentas existentes a unirse a la organización. También puede aplicar políticas a las cuentas de miembro.

> **Note**
>
> Una cuenta de miembro no puede pertenecer a más de una organización a la vez. Puede designar algunas cuentas de miembro para que sean cuentas de administrador delegado.

Administrador delegado

Le recomendamos que utilice la cuenta de administración de y sus usuarios y roles únicamente para las tareas que deba realizar dicha cuenta. Almacene todos sus recursos de AWS en otras cuentas de miembros de la organización y manténgalos fuera de la cuenta de administración. Esto se debe a que las funciones de seguridad, como las políticas de control de servicios de Organizations (SCPs), no restringen ningún usuario o función en la cuenta de administración. Separar los recursos de su cuenta de administración también lo ayudará a comprender los cargos de sus facturas. Desde la cuenta de administración de la organización, puede designar una o más cuentas de miembros como cuentas de administrador delegado para ayudarlo a implementar esta recomendación. Hay dos tipos de administradores delegados:

- Administrador delegado para Organizations: desde estas cuentas, puede administrar las políticas de la organización y adjuntar políticas a las entidades (raíces o cuentas) de la organización. OUs La cuenta de administración puede controlar los permisos de delegación en niveles detallados. Para obtener más información, consulte Administrador delegado para AWS Organizations.

- Administrador delegado de un AWS servicio: desde estas cuentas, puede administrar los AWS servicios que se integran con Organizations. La cuenta de administración puede registrar diferentes cuentas de miembros como administradores delegados para diferentes servicios, según sea necesario. Estas cuentas tienen permisos administrativos para un servicio específico, así como permisos para las acciones de solo lectura de las organizaciones. Para obtener más información, consulte Administrador delegado de los Servicios de AWS que funcionan con Organizations

Invitaciones y establecimiento de comunicación

Invitación

Una invitación es el proceso de pedir a otra cuenta que se una a su organización. Únicamente la cuenta de administración de la organización puede emitir una invitación. La invitación se amplía al ID de la cuenta o a la dirección de correo electrónico asociada a la cuenta invitada. Una vez que la cuenta invitada acepta una invitación, pasa a ser una cuenta de miembro de la organización. También se pueden enviar invitaciones a todas las cuentas de miembro actuales cuando la organización necesita que todos los miembros aprueben el cambio de admitir únicamente las características de la facturación unificada a admitir todas las características de la organización. Las invitaciones funcionan mediante el intercambio de protocolos de enlace (handshakes) entre cuentas. Es posible que no vea protocolos de enlace cuando trabaja en la consola de AWS Organizations . Pero si utilizas la AWS Organizations API AWS CLI o, debes trabajar directamente con handshakes.

Protocolo de enlace

Un establecimiento de comunicación es un proceso de varios pasos para intercambiar información entre dos partes. Uno de sus usos principales AWS Organizations es servir como implementación subyacente para las invitaciones. Los mensajes de protocolos de enlace se transfieren entre el iniciador del protocolo de enlace y el destinatario y los responden ellos mismos. Los mensajes se transfieren de una forma que ayuda a garantizar que ambas partes sepan cuál es el estado actual. Los protocolos de enlace se usan también cuando la organización cambia de admitir solo las características de facturación unificada a admitir todas las características que ofrece AWS Organizations . Por lo general, solo necesitas interactuar directamente con handshakes si trabajas con la AWS Organizations API o con herramientas de línea de comandos como la. AWS CLI

Políticas de la organización

Una política es un «documento» con una o más declaraciones que definen los controles que se desean aplicar a un grupo de ellos. Cuentas de AWS AWS Organizations admite políticas de autorización y políticas de administración.

Políticas de autorización

Las políticas de autorización le ayudan a gestionar de forma centralizada la seguridad de Cuentas de AWS toda la organización.

Política de control de servicios (SCP)

: Una política de control de servicios es un tipo de política que ofrece un control central sobre los permisos máximos disponibles para los usuarios de IAM y las funciones de IAM en una organización.

  Esto significa que hay que SCPs especificar los controles centrados en el principal. SCPs cree una barrera de permisos o establezca límites a los permisos máximos disponibles para los directores en sus cuentas de miembros. Utiliza un SCP cuando quiere aplicar de forma centralizada controles de acceso coherentes a los directores de su organización.

  Esto puede incluir especificar a qué servicios pueden acceder sus usuarios y funciones de IAM, a qué recursos pueden acceder o las condiciones en las que pueden realizar solicitudes (por ejemplo, desde regiones o redes específicas). Para obtener más información, consulte SCPs.

Política de control de recursos (RCP)

: Una política de control de recursos es un tipo de política que ofrece un control central sobre el máximo de permisos disponibles para los recursos de una organización.

  Esto significa que hay que RCPs especificar los controles centrados en los recursos. RCPs cree una barrera de permisos o establezca límites a los permisos máximos disponibles para los recursos en sus cuentas de miembros. Utilice un RCP cuando desee aplicar de forma centralizada controles de acceso coherentes en todos los recursos de su organización.

  Esto puede incluir restringir el acceso a sus recursos para que solo puedan acceder a ellos las identidades que pertenezcan a su organización, o especificar las condiciones en las que las identidades externas a su organización pueden acceder a sus recursos. Para obtener más información, consulte RCPs.

Políticas de administración

Las políticas de administración le ayudan a configurar Servicios de AWS y gestionar de forma centralizada sus funciones en toda la organización.

Política declarativa

Una política declarativa es un tipo de política que permite declarar y aplicar de forma centralizada las configuraciones deseadas para una determinada escala Servicio de AWS en toda la organización. Una vez adjunta, la configuración siempre se mantiene cuando el servicio agrega nuevas funciones o, para obtener más información, consulte la política declarativa APIs.

Política de copia de seguridad

Una política de respaldo es un tipo de política que le permite administrar y aplicar planes de respaldo de manera centralizada a los AWS recursos de las cuentas de una organización. Para obtener más información, consulte la política de copias de seguridad.

Política de etiquetas

Una política de etiquetas es un tipo de política que permite estandarizar las etiquetas adjuntas a los AWS recursos de las cuentas de una organización. Para obtener más información, consulte la política de etiquetas.

Política de chatbot

Una política de chatbot es un tipo de política que te permite controlar el acceso a las cuentas de una organización desde aplicaciones de chat como Slack y Microsoft Teams. Para obtener más información, consulta la política de Chatbot.

Política de exclusión de servicios de IA

Una política de exclusión de los servicios de IA es un tipo de política que permite controlar la recopilación de datos para los servicios de AWS IA en todas las cuentas de una organización. Para obtener más información, consulta la política de exclusión de los servicios de IA.

Cuotas y límites de servicio para AWS Organizations

En este tema se describen las cuotas y los límites de servicio para AWS Organizations.

Directrices de nomenclatura

Las siguientes son pautas para los nombres que se crean AWS Organizations, incluidos los nombres de las cuentas, las unidades organizativas (OUs), las raíces y las políticas:

- Los nombres deben estar compuestos por caracteres Unicode.
- La longitud máxima de cadena para los nombres varía según el objeto. Para obtener información sobre el límite real de cada objeto, consulte la Referencia de la API de AWS Organizations, busque la operación de API que crea el objeto y consulte los detalles del parámetro `Name` de esa operación. Por ejemplo :Nombre de cuenta, o bien Nombre de OU.

Consideraciones

Los códigos de cuota de servicio pueden cambiar con el tiempo debido a las actualizaciones. Esto no afecta a los valores ni a los nombres de las cuotas. Para encontrar el código de cuota de una cuota específica, utilice la ListServiceQuotasoperación y busque la `QuotaCode` respuesta de la cuota que desee en el resultado.

Valores mínimos y máximos

Los siguientes son los máximos predeterminados para las entidades de AWS Organizations.

> **Note**
>
> Puede solicitar aumentos de algunos de estos valores mediante la Consola Service Quotas. Organizations es un servicio global alojado físicamente en la región EE. UU. Este (Norte de Virginia) (`us-east-1`). Por lo tanto, debe `us-east-1` utilizarlas para acceder a las cuotas de Organizations cuando utilice la consola Service Quotas AWS CLI, el o un AWS SDK.

Descripción	Límite
Número de Cuentas de AWS en una organización	El número máximo de cuentas permitidas en una organización de forma predeterminada es 10. Si necesita más cuentas, puede solicitar las contactándose con la consola de Service Quotas. Nota: Solo la cuenta de administración de una organización puede enviar esta solicitud de aumento de cuota. Se pueden conceder

Descripción	Límite
	aumentos de límite de hasta 10 000 cuentas en función de las cualificaciones y requisitos de los clientes. Las cuentas y organizaciones recién creadas pueden tener una cuota inferior a la predeterminada de 10 cuentas. Una invitación enviada a una cuenta computa para esta cuota. La cuenta se devuelve si la cuenta invitada rechaza la invitación, la cuenta de administración cancela la invitación o la invitación caduca. Cuando una cuenta se cierra, sigue contabilizándose en la cuota hasta que se cierra de forma permanente. Para obtener más información sobre cuándo una cuenta se cierra permanentemente, consulte Periodo posterior al cierre en la Guía de referencia de AWS Account Management . En algunos servicios se establecen límites de cuentas distintos de la cantidad máxima de cuentas permitidas en una organización. Para obtener más información, consulta Límites por AWS servicio.
Número de nodos raíz en una organización	1
Número de miembros OUs de una organización	1 000
Número de políticas de cada tipo en una organización	Políticas de control de servicios: 2000 Políticas de control de recursos: 1000 Políticas declarativas: 1000 Políticas de copia de seguridad: 1000 Políticas de etiquetas: 1000 Políticas de chatbot: 1000 Políticas de exclusión de servicios de IA: 1000

Descripción	Límite
Tamaño máximo de un documento de política	Políticas de control de servicios: 5120 caracteres Políticas de control de recursos: 5120 caracteres Políticas declarativas: 10 000 caracteres Políticas de copia de seguridad: 10 000 caracteres Políticas de chatbot: 10 000 caracteres Políticas de exclusión de servicios de IA: 2500 caracteres Políticas de etiquetas: 10 000 caracteres Nota: Si guardas la política mediante el uso de AWS Managemen t Console, los espacios en blanco adicionales (como espacios y saltos de línea) entre los elementos JSON y fuera de las comillas se eliminan y no se cuentan. Si guardas la política mediante una operación del SDK o la AWS CLI, la política se guardará exactamen te como la proporcionaste y no se eliminarán caracteres automátic amente.
Anidación máxima de OU en un nodo raíz	Cinco niveles de OUs profundidad bajo una raíz.
Número máximo de intentos de invitación que puede realizar en un periodo de 24 horas	Ya sea 20 o el número máximo de cuentas permitidas en su organización, la que sea mayor. Las invitaciones aceptadas no se contabilizan en esta cuota. Tan pronto como se acepta una invitación, puede enviar otra invitación ese mismo día. Si el número máximo de cuentas permitidas en su organización es inferior a 20, obtendrá una excepción de “límite de cuenta superado” si intenta invitar a más cuentas de las que puede contener su organización. Sin embargo, puede cancelar invitaciones y enviar nuevas hasta un máximo de 20 intentos en un día.

Descripción	Límite
Número de cuentas de miembro que se pueden crear de forma simultánea	5 - Tan pronto como una finaliza se puede iniciar otra, pero solo puede haber cinco en curso a la vez.
Número de cuentas de miembro que se pueden cerrar en un plazo de 30 días	10 % de las cuentas de miembro de una organización, con un máximo de 1000. • Menos de 100 cuentas: puede cerrar hasta 10 cuentas de miembro • Entre 100 y 10 000 cuentas: puede cerrar hasta el 10 % de las cuentas de miembro. • Menos de 10 000 cuentas: puede cerrar hasta 1000 cuentas de miembro. Una vez alcanzado este límite, puede cerrar cuentas adicionales o esperar hasta que se restablezca la cuota. Para obtener más información, consulta Cerrar una AWS cuenta en la Guía de administración de AWS cuentas.
Número de cuentas de miembro que se pueden cerrar de forma simultánea	3: solo se pueden realizar tres cierres de cuentas al mismo tiempo. Tan pronto como termine uno, puede cerrar otra cuenta.
Número de entidades a las que puede asociar una política	Sin límite
Número de etiquetas que puede asociar a un nodo raíz, OU o cuenta	50
Tamaño máximo de la política de delegación basada en recursos	40 000 caracteres

Límites por AWS servicio

La mayoría Servicios de AWS admite el número máximo de cuentas indicado que puede tener en una organización. Sin embargo, algunos servicios establecen límites de cuentas distintos de la cantidad máxima de cuentas permitidas en una organización.

En las siguientes tablas se muestran los servicios con límites de cuentas distintos.

AWS servicio	Límite	Se puede aumentar
AWS IAM Identity Center	3 000	Sí
AWS Application Migration Service	5000	No
AWS Directory Service	250	Sí

Para obtener más información, consulte AWS IAM Identity Center quotas en la Guía del usuario de IAM Identity Center y AWS MGN service quota limits en la Guía del usuario de Application Migration Service.

Tiempo de vencimiento de protocolos de enlace (handshakes)

Los siguientes son los tiempos de espera para los apretones de manos. AWS Organizations

Descripción	Límite
Invitación para unirse a una organización	15 días
Solicitud de habilitar todas las funciones de una organización	90 días
El protocolo de enlace se elimina y ya no aparece en las listas	30 días después de que se complete el protocolo de enlace

Número de políticas que puede asociar a una entidad

El mínimo y máximo depende del tipo de política y de la entidad a la que asocia la política. En la siguiente tabla se muestra cada tipo de política y el número de entidades a la se puede asociar cada tipo.

> **Note**
>
> Estos números solo se aplican a las políticas que están directamente adjuntas a una unidad organizativa o a una cuenta. Las políticas que afectan a una unidad organizativa o a una cuenta por herencia no cuentan contra estos límites. Los límites de las políticas no se pueden superar.

Tipo de política	Mínimo que se puede asociar a una entidad	Máximo adjunto al nodo raíz	Máximo adjunto por OU	Máximo adjunto por cuenta
Política de control de servicios	1 — Cada entidad debe tener al menos un SCP adjunto en todo momento cuando se habilite. SCPs No puede eliminar la última política SCP de una entidad.	5	5	5
Política de control de recursos	1 — La `RCPFullAWSAccess` política se adjunta automáticamente a la raíz, a todas las unidades organizativas y a todas las cuentas de la organización cuando se activa RCPs. Esta política no se puede separar	5	5	5

Tipo de política	Mínimo que se puede asociar a una entidad	Máximo adjunto al nodo raíz	Máximo adjunto por OU	Máximo adjunto por cuenta
	y se tiene en cuenta para la cuota de 5 políticas.			
Política declarativa	0	10	10	10
Política de copia de seguridad	0	10	10	10
Política de etiquetas	0	10	10	10
Política de chatbot	0	5	5	5
Política de exclusión de servicios de IA	0	5	5	5

> **Note**
>
> Solo puede tener un nodo raíz en una organización.

Límites de limitación

En las siguientes tablas se enumeran AWS Organizations APIs las categorías de gestión y se muestran sus respectivas tasas de aceleración a nivel de cuenta y organización.

AWS Organizations utiliza el algoritmo token bucket para implementar la regulación de las API. Con este algoritmo, su cuenta tiene un bucket que contiene un número específico de tokens. El número de tokens del bucket representa su cuota de limitación en un segundo determinado.

La velocidad es el ritmo fijo al que se añaden los tokens al depósito de fichas por segundo.

La ráfaga es la cantidad máxima de fichas que se pueden añadir y la cantidad máxima de fichas que se pueden utilizar por segundo.

Por ejemplo, la `DescribeAccount` API está limitada Cuenta de AWS a 20 solicitudes por segundo como velocidad de referencia y a 30 solicitudes por segundo como velocidad de ráfaga. La velocidad de ráfaga de 30 solicitudes por segundo te permite superar temporalmente la velocidad de referencia de 20 solicitudes por segundo.

Puede realizar 20 solicitudes en el primer segundo, que es la velocidad de referencia. En el segundo siguiente, puedes realizar 30 solicitudes, superando la línea base pero manteniéndote dentro de la velocidad de ráfaga de 30. Sin embargo, en el tercer segundo, si intenta realizar más de 20 solicitudes, se verá limitado, ya que ha superado la velocidad de referencia y se ha utilizado la capacidad de ráfaga.

La velocidad de ráfaga te permite gestionar los picos de tráfico temporales sin que te limites, siempre y cuando el promedio de solicitudes por segundo se mantenga dentro del límite de referencia a lo largo del tiempo.

Límites de administración de cuentas

En la siguiente tabla se enumeran las correspondientes a la administración AWS Organizations APIs de cuentas.

AWS Organizations API	Límite por cuenta (tasa, ampliación)	Límite por organización (tasa, ampliación)
CloseAccount	.05, 1	
CreateAccount, CreateGov CloudAccount	0,1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10

Límites de administración del protocolo de enlace

En la siguiente tabla se muestra el apretón AWS Organizations APIs de manos de la cuenta.

AWS Organizations API	Límite por cuenta (tasa, ampliación)	Límite por organización (tasa, ampliación)
AcceptHandshake	1, 2	5, 5
DescribeHandshake	1, 2	6, 10
CancelHandshake	2, 3	
DeclineHandshake	1, 1	5, 5
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10

Límites de administración de organizaciones

La siguiente tabla muestra la gestión AWS Organizations APIs de la organización.

AWS Organizations API	Límite por cuenta (tasa, ampliación)	Límite por organización (tasa, ampliación)
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2, 3	

AWS Organizations API	Límite por cuenta (tasa, ampliación)	Límite por organización (tasa, ampliación)
DescribeOrganizationalUnit	2, 2	2, 3
ListAccounts	8, 12	9, 15
ListChildren	6, 10	7, 12
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5, 8	6, 10
ListRoots	1, 2	1, 3
ListTagsForResource	10, 15	12, 18
RemoveAccountFromOrganization	2, 2	
TagResource, UntagResource	4, 6	

Límites de administración de políticas

En la siguiente tabla se enumeran las políticas AWS Organizations APIs para la gestión.

AWS Organizations API	Límite por cuenta (tasa, ampliación)	Límite por organización (tasa, ampliación)
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2, 3	
DescribePolicy	2, 2	2, 3
DisablePolicyType, EnablePolicyType	1, 1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5, 8	6, 10

AWS Organizations API	Límite por cuenta (tasa, ampliación)	Límite por organización (tasa, ampliación)
UpdatePolicy	2, 3	

Límites de administración de servicios

En la siguiente tabla se muestra la AWS Organizations APIs para la administración de servicios.

AWS Organizations API	Límite por cuenta (tasa, ampliación)	Límite por organización (tasa, ampliación)
Habilitar el AWSServic e acceso, deshabilitar el AWSService acceso	1, 2	
Lista AWSServiceAccessFo rOrganization, ListDeleg atedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministra tor, DeregisterDelegate dAdministrator	1, 2	

Soporte regional para AWS Organizations

AWS Organizations está disponible en todas las regiones AWS comerciales y en las regiones de China. AWS GovCloud (US) Regions

Para obtener una lista de las diferencias de funcionalidad en AWS GovCloud (US) Regions, consulte AWS Organizations en AWS GovCloud (US).

Para obtener una lista de las diferencias de funcionalidad en las regiones de China, consulte AWS Organizations en China.

Los puntos de conexión de servicio de Organizations se encuentran en las siguientes regiones:

- En Este de EE. UU. (Norte de Virginia) para organizaciones comerciales
- En AWS GovCloud (EE. UU. al oeste) para organizaciones AWS GovCloud (US)
- En China (Ningxia) para organizaciones de China, operado por Ningxia Western Cloud Data Technology Co. Ltd (NWCD).

Todas las entidades de la organización son accesibles a nivel mundial, excepto las organizaciones administradas en China, de forma similar a como funciona AWS Identity and Access Management (IAM) en la actualidad. No es necesario que especifique una Región de AWS cuando cree y administre su organización, pero tendrá que crear una organización independiente para las cuentas utilizadas en China. Sus usuarios Cuentas de AWS pueden utilizarla Servicios de AWS en cualquier región geográfica en la que esté disponible ese servicio.

> **Note**
>
> Las políticas de etiquetas solo se admiten en un subconjunto de regiones
> Las políticas de etiquetas son un tipo de política que le puede ayudar a estandarizar las etiquetas en todos los recursos en las cuentas de su organización. Las políticas de etiquetas solo se admiten en un subconjunto de regiones en las que se admita Organizations. Para obtener una lista de las regiones en las que se admiten las políticas de etiquetas, consulte Tag policies | Support Regions.

Lista de disponibles Regiones de AWS

En la tabla siguiente, se muestran las Regiones de AWS disponibles.

Nombre de la región	Región	Punto de conexión	Protocolo	
Este de EE. UU. (Ohio)	us-east-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Este de EE. UU.	us-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	

Nombre de la región	Región	Punto de conexión	Protocolo
(Norte de Virginia)			
Oeste de EE. UU. (Norte de California)	us-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
África (Ciudad del Cabo)	af-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Melbourne)	ap-southeast-4	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Bombay)	ap-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Tailandia)	ap-southeast-7	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Canadá (centro)	ca-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Oeste de Canadá (Calgary)	ca-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Fráncfort)	eu-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Irlanda)	eu-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Londres)	eu-west-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Milán)	eu-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (París)	eu-west-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (España)	eu-south-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Estocolmo)	eu-north-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Zúrich)	eu-central-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Israel (Tel Aviv)	il-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
México (central)	mx-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Medio Oriente (Baréin)	me-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Medio Oriente (EAU)	me-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
América del Sur (São Paulo)	sa-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
AWS GovCloud (EE. UU.-Este)	us-gov-east-1	organizations.us-gov-west-1.amazonaws.com	HTTPS
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	organizations.us-gov-west-1.amazonaws.com	HTTPS

Precios y facturación de AWS Organizations

AWS Organizations se ofrece sin cargo adicional. Solo se le cobrarán los recursos de AWS que usen los usuarios y las funciones de las cuentas miembro. Por ejemplo, se le cobrará la tarifa estándar de las instancias de Amazon EC2 que utilicen los usuarios o las funciones de las cuentas miembro. Para obtener información acerca de los precios de otros servicios de AWS, consulte los Precios AWS.

¿Quién paga por el uso en el que incurran los usuarios de una cuenta miembro de AWS de mi organización?

El propietario de la cuenta de administración es responsable de pagar todo el uso, los datos y los recursos utilizados por las cuentas de la organización.

¿Mi factura reflejará la estructura de unidades organizativas que creé en mi organización?

Su factura no reflejará la estructura que ha definido en su organización. Puede usar etiquetas de asignación de costos en Cuentas de AWS individuales para categorizar y hacer un seguimiento de sus costos de AWS. Esta asignación estará visible en la factura unificada de su organización.

Soporte y comentarios de AWS Organizations

Agradecemos sus comentarios. Puede enviar sus comentarios a feedback-awsorganizations@amazon.com. También puede publicar sus comentarios y preguntas en nuestro foro de soporte deAWS Organizations. Para obtener más información acerca de los foros de soporte de AWS, consulte la Ayuda de los foros.

Otros recursos de AWS

- Capacitación y cursos de AWS: enlaces a cursos especializados y basados en roles, así como a laboratorios autoguiados para ayudarlo a desarrollar sus conocimientos sobre AWS y obtener experiencia práctica.
- Herramientas para desarrolladores de AWS - Enlaces a herramientas y recursos para desarrolladores que incluyen documentación, ejemplos de código, notas de la versión y otra información para ayudarle a crear aplicaciones innovadoras con AWS.

- Centro AWS Support - El centro para crear y administrar sus casos de Support AWS. También incluye enlaces a otros recursos útiles como foros, preguntas técnicas frecuentes, estado de los servicios y AWS Trusted Advisor.
- Support AWS - La página web principal para obtener información acerca de Support AWS, un canal de soporte individualizado y de respuesta rápida que le ayudará a crear y ejecutar aplicaciones en la nube.
- Contacte con nosotros – Un punto central de contacto para las consultas relacionadas con la facturación AWS, cuentas, eventos, abuso y demás problemas.
- AWSTérminos del sitio de : información detallada sobre nuestros derechos de autor y marca comercial, su cuenta, licencia y acceso al sitio, entre otros temas.

Prácticas recomendadas para un entorno de varias cuentas

Siga estas recomendaciones para ayudarle a configurar y administrar un entorno de varias cuentas en AWS Organizations.

Temas

- Cuenta y credenciales
- Estructura organizativa y cargas de trabajo
- Administración de costos y servicio

Cuenta y credenciales

Habilite la administración del acceso raíz para simplificar la administración de las credenciales de los usuarios raíz en las cuentas de los miembros

Le recomendamos que habilite la administración del acceso raíz para ayudarlo a monitorear y eliminar las credenciales de los usuarios raíz de las cuentas de los miembros. La administración del acceso raíz impide la recuperación de las credenciales de los usuarios raíz, lo que mejora la seguridad de las cuentas en su organización.

- Elimine las credenciales de usuario raíz de las cuentas de los miembros para evitar que el usuario raíz inicie sesión. Esto también impide que las cuentas de los miembros se recuperen del usuario root.
- Suponga que tiene una sesión privilegiada para realizar las siguientes tareas en las cuentas de los miembros:
  - Elimine una política de bucket mal configurada que impida a todas las entidades principales acceder a un bucket de Amazon S3.
  - Elimine una política basada en recursos de Amazon Simple Queue Service que impida a todas las entidades principales acceder a una cola de Amazon SQS.
  - Permita que la cuenta de un miembro recupere sus credenciales de usuario raíz. La persona que tenga acceso a la bandeja de entrada de correo electrónico del usuario raíz de la cuenta de miembro puede restablecer la contraseña del usuario raíz e iniciar sesión como usuario raíz de la cuenta de miembro.

Una vez que se habilita la administración del acceso raíz, las cuentas de los secure-by-default miembros recién creadas no tienen credenciales de usuario raíz, lo que elimina la necesidad de seguridad adicional, como el MFA después del aprovisionamiento.

Para obtener más información, consulte Centralizar las credenciales de los usuarios raíz de las cuentas de los miembros en la Guía del AWS Identity and Access Management usuario.

Mantener actualizado el número de teléfono de contacto

Para recuperar el acceso a las Cuenta de AWS suyas, es fundamental disponer de un número de teléfono de contacto válido y activo que te permita recibir mensajes de texto o llamadas. Te recomendamos que utilices un número de teléfono específico para asegurarnos de que AWS podamos ponernos en contacto contigo con fines de asistencia y recuperación de la cuenta. Puedes ver y administrar fácilmente los números de teléfono de tu cuenta a través de la página AWS Management Console o Administración de cuentas APIs.

Hay varias formas de obtener un número de teléfono exclusivo que garantice que AWS pueda contactarlo. Se recomienda encarecidamente que consiga una tarjeta SIM dedicada y un teléfono físico. Guarde el teléfono y la tarjeta SIM de forma segura y a largo plazo para garantizar que el número de teléfono permanezca disponible para la recuperación de la cuenta. Asegúrese también de que el equipo responsable de la factura del móvil comprenda la importancia de este número, incluso si permanece inactivo durante periodos prolongados. Es esencial mantener la confidencialidad de este número de teléfono dentro de su organización para garantizar protección adicional.

Documente el número de teléfono en la página de la consola de información de AWS contacto y comparta sus detalles con los equipos específicos de su organización que deben conocerlo. Este enfoque ayuda a minimizar el riesgo asociado con la transferencia del número de teléfono a una tarjeta SIM diferente. Almacene el teléfono de acuerdo con su política de seguridad de la información existente. Sin embargo, no almacene el teléfono en la misma ubicación que la otra información de credenciales relacionada. Se debe registrar y supervisar cualquier acceso al teléfono o a su ubicación de almacenamiento. Si el número de teléfono asociado a una cuenta cambia, implemente procesos para actualizar dicho número en la documentación existente.

Utilizar una dirección de correo electrónico de grupo para todas las cuentas raíz

Utilice una dirección de correo electrónico administrada por su empresa. Utilice una dirección de correo electrónico que reenvíe los mensajes recibidos directamente a un grupo de usuarios. En el

caso de que AWS tengas que contactar con el propietario de la cuenta, por ejemplo, para confirmar el acceso, el mensaje de correo electrónico se distribuye a varias partes. Este enfoque ayuda a reducir el riesgo de retrasos en la respuesta, incluso si las personas están de vacaciones, se enferman o abandonan el negocio.

Estructura organizativa y cargas de trabajo

Administrar cuentas dentro de una sola organización

Se recomienda crear una sola organización y administrar todas las cuentas que se encuentran en ella. Una organización es una barrera de seguridad que le permite mantener la coherencia entre las cuentas de su entorno. Puede aplicar políticas o configuraciones de nivel de servicio de forma centralizada en todas las cuentas de una organización. Si desea habilitar políticas coherentes, visibilidad central y controles programáticos en su entorno de varias cuentas, lo mejor es hacerlo dentro de una sola organización.

Agrupar cargas de trabajo en función del propósito empresarial y no de la estructura de informes

Le recomendamos que aísle los entornos y los datos de las cargas de trabajo de producción en un nivel superior orientado a las cargas de trabajo OUs. OUs Debe basarse en un conjunto común de controles en lugar de reflejar la estructura de informes de su empresa. Además de los de producción OUs, le recomendamos que defina uno o varios entornos no productivos OUs que contengan cuentas y entornos de carga de trabajo que se utilicen para desarrollar y probar las cargas de trabajo. Para obtener más información, consulte Organización orientada a las cargas de trabajo. OUs

Utilizar varias cuentas para organizar cargas de trabajo

Y Cuenta de AWS proporciona límites naturales de seguridad, acceso y facturación para sus recursos. AWS El uso de varias cuentas tiene sus ventajas, ya que permite distribuir las cuotas de nivel de cuenta y los límites de tasa de solicitudes de API, además de las ventajas adicionales que se enumeran a continuación. Se recomienda utilizar varias cuentas básicas de toda la organización, como cuentas de seguridad, registro e infraestructura. En el caso de las cuentas de carga de trabajo, debe separar las cargas de trabajo de producción de las cargas de trabajo de comprobación o desarrollo en cuentas independientes.

Administración de costos y servicio

Habilite AWS los servicios a nivel organizativo mediante la consola de servicios o las operaciones de API/CLI

Como práctica recomendada, te recomendamos que habilites o deshabilites cualquier servicio con el que desees integrarte AWS Organizations mediante la consola de ese servicio o las operaciones de la API o los comandos CLI equivalentes. Con este método, el AWS servicio puede realizar todos los pasos de inicialización necesarios para su organización, como crear los recursos necesarios y limpiarlos al inhabilitar el servicio. AWS Account Management es el único servicio que requiere el uso de la AWS Organizations consola o que debe APIs habilitarse. Para revisar la lista de servicios con los que están integrados AWS Organizations, consulteServicios de AWS que puedes usar con AWS Organizations.

Utilizar las herramientas de facturación para realizar un seguimiento de los costos y optimizar el uso de los recursos

Al administrar una organización, recibe una factura consolidada que cubre todos los cargos de las cuentas de su organización. Para los usuarios empresariales que necesiten acceder a la visibilidad de los costes, puede proporcionar una función en la cuenta de administración con permisos restringidos de solo lectura para revisar las herramientas de facturación y costos. Por ejemplo, puede crear un conjunto de permisos que proporcione acceso a los informes de facturación o utilizar el AWS Cost Explorer Service (una herramienta de visualización de tendencias de los costos a lo largo del tiempo) y servicios rentables, como Lente de almacenamiento de Amazon S3 y AWS Compute Optimizer.

Planificar la estrategia de etiquetado y la aplicación de las etiquetas en todos los recursos de la organización

A medida que las cuentas y cargas de trabajo aumentan, las etiquetas pueden ser una característica útil para el seguimiento de costos, el control de acceso y la organización de los recursos. Para etiquetar las estrategias de nomenclatura, siga las instrucciones de Etiquetar sus AWS recursos. Además de los recursos, puedes crear etiquetas en la raíz, las cuentas y las políticas de la organización. OUs Consulte la sección Building your tagging strategy para obtener más información.

Empezar con AWS Organizations

Los siguientes temas le permitirán obtener información para empezar a usar AWS Organizations. También puede utilizar los siguientes tutoriales para empezar a llevar a cabo tareas con AWS Organizations.

Tutorial: Creación y configuración de una organización

Comience a trabajar con las step-by-step instrucciones para crear su organización, invitar a sus primeras cuentas de miembros, crear una jerarquía de unidades organizativas que contenga sus cuentas y aplicar algunas políticas de control de servicios (SCPs).

Tutorial: Supervisa los cambios importantes en tu organización con Amazon EventBridge

Supervisa los cambios clave en tu organización configurando Amazon EventBridge para que active una alarma en forma de correo electrónico, mensaje de texto SMS o entrada de registro cuando se produzcan en tu organización las acciones que tú designes. Por ejemplo, muchas organizaciones desean saber cuándo se crea una cuenta nueva o cuándo una cuenta intenta salir de la organización.

Temas

- Registrarse en AWS
- Accediendo AWS Organizations
- Tutorial: Creación y configuración de una organización
- Tutorial: Supervisa los cambios importantes en tu organización con Amazon EventBridge
- Se usa AWS Organizations con un SDK AWS

Registrarse en AWS

Temas

- Inscríbase en una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Accediendo AWS Organizations

Puede trabajar con él AWS Organizations de cualquiera de las siguientes maneras:

AWS Management Console

La AWS Organizations consola es una interfaz basada en un navegador que puede utilizar para administrar su organización y sus AWS recursos. Puede llevar a cabo cualquier tarea en su organización utilizando la consola.

AWS Herramientas de línea de comandos

Con las herramientas de línea de AWS comandos, puede emitir comandos en la línea de comandos de su sistema para realizar AWS Organizations cualquier AWS tarea. El uso de la línea de comandos puede ser más rápido y cómo que utilizar la consola. Las herramientas de línea de comandos también son útiles para crear scripts que realicen tareas de AWS .

AWS proporciona dos conjuntos de herramientas de línea de comandos:

- AWS Command Line Interface

  The AWS Command Line Interface (AWS CLI) es una herramienta unificada para administrar su Servicios de AWS. Con solo una herramienta para descargar y configurar, puede controlar varias Servicios de AWS desde la línea de comandos y automatizarlas mediante scripts.

  Para obtener información sobre la instalación y el uso de AWS CLI, consulte la Guía del AWS Command Line Interface usuario.

- AWS Tools for Windows PowerShell

  Las herramientas para Windows PowerShell permiten a los desarrolladores y administradores gestionar sus Servicios de AWS recursos en el entorno de PowerShell secuencias de comandos. Puede administrar sus AWS recursos con las mismas PowerShell herramientas que usa para administrar sus entornos Windows, Linux y macOS.

  Para obtener información sobre la instalación y el uso de las herramientas para Windows PowerShell, consulte la Guía del AWS Tools for Windows PowerShell usuario.

AWS SDKs

AWS SDKs Constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas (por ejemplo, Java, Python, Ruby, .NET, iOS y Android). Se SDKs encargan de tareas como la firma criptográfica de las solicitudes, la gestión de los errores y el reintento automático de las solicitudes. Para obtener más información acerca de AWS SDKs, incluida la forma de descargarlos e instalarlos, consulte Herramientas para Amazon Web Services.

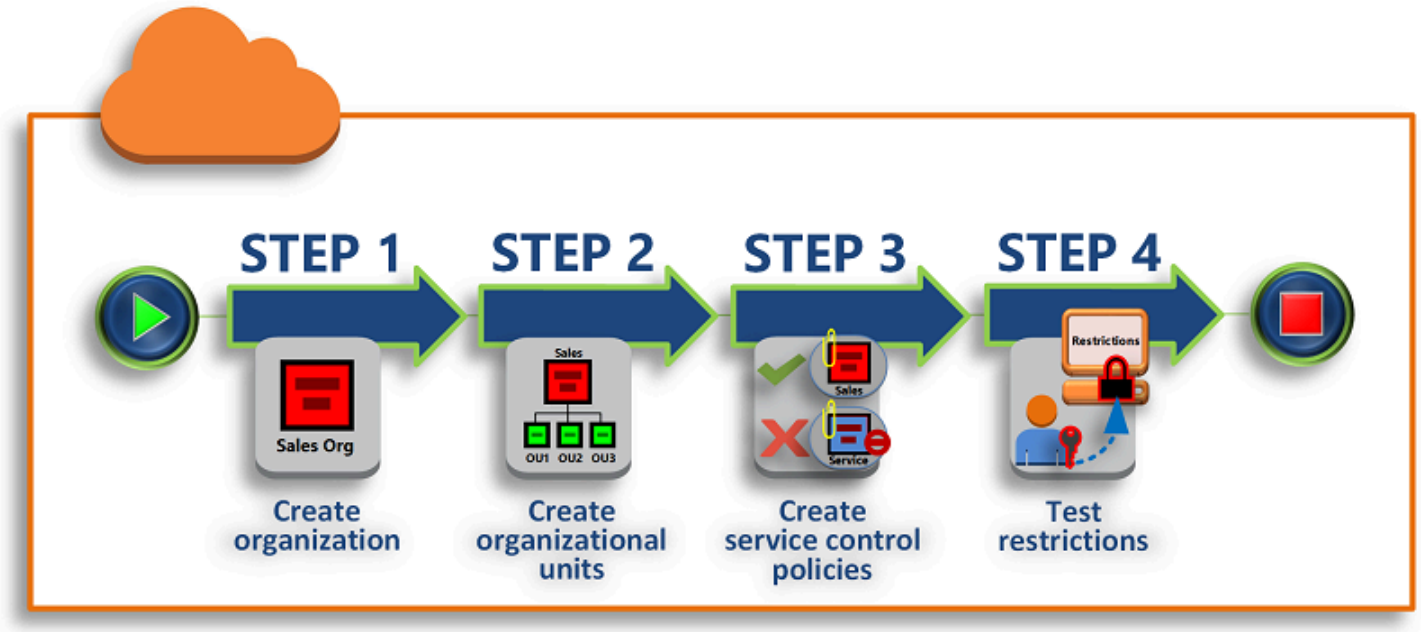
AWS Organizations API de consulta HTTPS

La API de consulta AWS Organizations HTTPS le brinda acceso programático a AWS Organizations y AWS. La API de consulta HTTPS le permite emitir solicitudes HTTPS directamente al servicio. Cuando use la API HTTPS, debe incluir código para firmar digitalmente las solicitudes utilizando sus credenciales. Para obtener más información, consulte Llamar a la API mediante solicitudes de consulta HTTP y la Referencia de API AWS Organizations.

Tutorial: Creación y configuración de una organización

En este tutorial, creará su organización y la configurará con dos cuentas de AWS miembros. Creará una de las cuentas de miembro en su organización e invitará a la otra cuenta a que se una a su organización. A continuación, usará la técnica de lista de permitidos para especificar que los administradores de cuentas pueden delegar únicamente los servicios y las acciones que se indican explícitamente. Esto permite a los administradores validar cualquier servicio nuevo que AWS introduzcan antes de permitir su uso a cualquier otra persona de la empresa. De esta forma, si AWS introduce un nuevo servicio, seguirá prohibido hasta que un administrador lo añada a la lista de permitidos de la política correspondiente. En el tutorial también se muestra cómo utilizar una lista de rechazados para garantizar que ningún usuario de la cuenta de un miembro pueda cambiar la configuración de los registros de auditoría que se AWS CloudTrail crean.

En la siguiente ilustración se muestran los principales pasos del tutorial.



[Paso 1: Crear la organización]

En este paso, creará una organización con su cuenta actual Cuenta de AWS como cuenta de administración. También invitas Cuenta de AWS a uno a unirse a tu organización y creas una segunda cuenta como cuenta de miembro.

[Paso 2: Crear las unidades organizativas]

A continuación, crea dos unidades organizativas (OUs) en la nueva organización y coloca las cuentas de los miembros en ellasOUs.

[Paso 3: Crear las políticas de control de servicios]

Puedes restringir las acciones que se pueden delegar a los usuarios y las funciones de las cuentas de los miembros mediante las políticas de control de servicios (SCPs). En este paso, debe crear dos SCPs y adjuntarlas a la OUs de su organización.

[Paso 4: Probar las políticas de la organización]

Puede iniciar sesión como usuario desde cada una de las cuentas de prueba y ver los efectos que SCPs tienen en las cuentas.

Ninguno de los pasos de este tutorial supone un coste en tu AWS factura. AWS Organizations es un servicio gratuito.

Requisitos previos

En este tutorial se presupone que tienes acceso a dos ya existentes Cuentas de AWS (crearás un tercero como parte de este tutorial) y que puedes iniciar sesión en cada uno de ellos como administrador.

El tutorial hace referencia a las cuentas de la manera siguiente:

- `111111111111`: la cuenta que usa para crear la organización. Esta cuenta pasa a ser la cuenta de administración. El propietario de esta cuenta tiene una dirección de correo electrónico de `OrgAccount111@example.com`.
- `222222222222`: una cuenta que invita a unirse a la organización como cuenta de miembro. El propietario de esta cuenta tiene una dirección de correo electrónico de `member222@example.com`.
- `333333333333`: una cuenta que crea como miembro de la organización. El propietario de esta cuenta tiene una dirección de correo electrónico de `member333@example.com`.

Sustituya los valores anteriores por los valores asociados con las cuentas de prueba. Le recomendamos que no utilice cuentas de producción para este tutorial.

Paso 1: Crear la organización

En este paso, inicia sesión en la cuenta 111111111111 como administrador, crea una organización con esa cuenta como cuenta de administración y, a continuación, invita a una cuenta existente 222222222222, a unirse como cuenta de miembro.

AWS Management Console

1. Inicie sesión AWS como administrador de la cuenta 1111 y abra la AWS Organizations consola.
2. En la página de introducción, elija Crear organización.
3. En el cuadro de diálogo de confirmación, elija Crear organización.

   > **Note**
   >
   > De forma predeterminada, la organización se crea con todas las características habilitadas. También puede crear la organización únicamente con las características de facturación unificada habilitadas.

   AWS crea la organización y muestra la Cuentas de AWSpágina. Si está en una página diferente, elija Cuentas de AWS en el panel de navegación de la izquierda.

   Si la cuenta que utiliza nunca ha tenido su dirección de correo electrónico verificada por AWS, se envía automáticamente un correo electrónico de verificación a la dirección asociada a la cuenta de administración. Puede pasar algún tiempo hasta que reciba el correo electrónico de verificación.
4. Verifique la dirección de correo electrónico en un plazo de 24 horas. Para obtener más información, consulte Verificación de dirección de correo electrónico con AWS Organizations.

Ahora tiene una organización con su cuenta como único miembro. Esta es la cuenta de administración de la organización.

Invitar a una cuenta existente a que se una a su organización

Ahora que tiene una organización, puede comenzar a rellenarla con cuentas. En los pasos de esta sección, invita a una cuenta existente a unirse como miembro de su organización.

AWS Management Console

Para invitar a una cuenta existente a unirse

1. Vaya a la página Cuentas de AWS y elija Agregar un Cuenta de AWS.
2. En la página Añadir una Cuenta de AWS página, selecciona Invitar a una existente Cuenta de AWS.
3. En el cuadro ID de cuenta o correo electrónico de un Cuenta de AWS para invitar, ingrese la dirección de correo electrónico del propietario de la cuenta a la que desea invitar, similar a lo siguiente: **`member222@example.com`**. Como alternativa, si conoces el número de Cuenta de AWS identificación, puedes ingresarlo en su lugar.
4. Escriba el texto que desee en el cuadro de texto Mensaje a incluir en el mensaje de correo electrónico de invitación. Este texto se incluirá en el correo electrónico que se envía al propietario de la cuenta.
5. Selecciona Enviar invitación. AWS Organizations envía la invitación al propietario de la cuenta.

   > **Important**
   >
   > Expanda el mensaje de error si se indica. Si el error indica que ha excedido los límites de la cuenta para la organización o que no puede añadir una cuenta porque la organización sigue inicializándose, espere a que pase una hora desde que creó la organización e inténtelo de nuevo. Si el error persiste, póngase en contacto con AWS Support.

6. A efectos de este tutorial, ahora tiene que aceptar su propia invitación. Realice alguna de las siguientes acciones para ir a la página Invitations en la consola:

   - Abre el correo electrónico AWS enviado desde la cuenta de administración y elige el enlace para aceptar la invitación. Cuando se le pida que inicie sesión, hágalo como administrador de la cuenta de miembro invitada.
   - Abra la consola de AWS Organizations y navegue hasta la página de Invitaciones.

7. En la página Cuentas de AWS , elija Aceptar y, a continuación, elija Confirmar.

> **Tip**
>
> La recepción de la invitación podría retrasarse y es posible que tenga que esperar antes de poder aceptarla.

8. Cierre la sesión de la cuenta de miembro e inicie sesión de nuevo como administrador en la cuenta de administración.

Creación de una cuenta de miembro

En los pasos de esta sección, se crea una Cuenta de AWS que se convierta automáticamente en miembro de la organización. En este tutorial, a esta cuenta la llamaremos 333333333333.

AWS Management Console

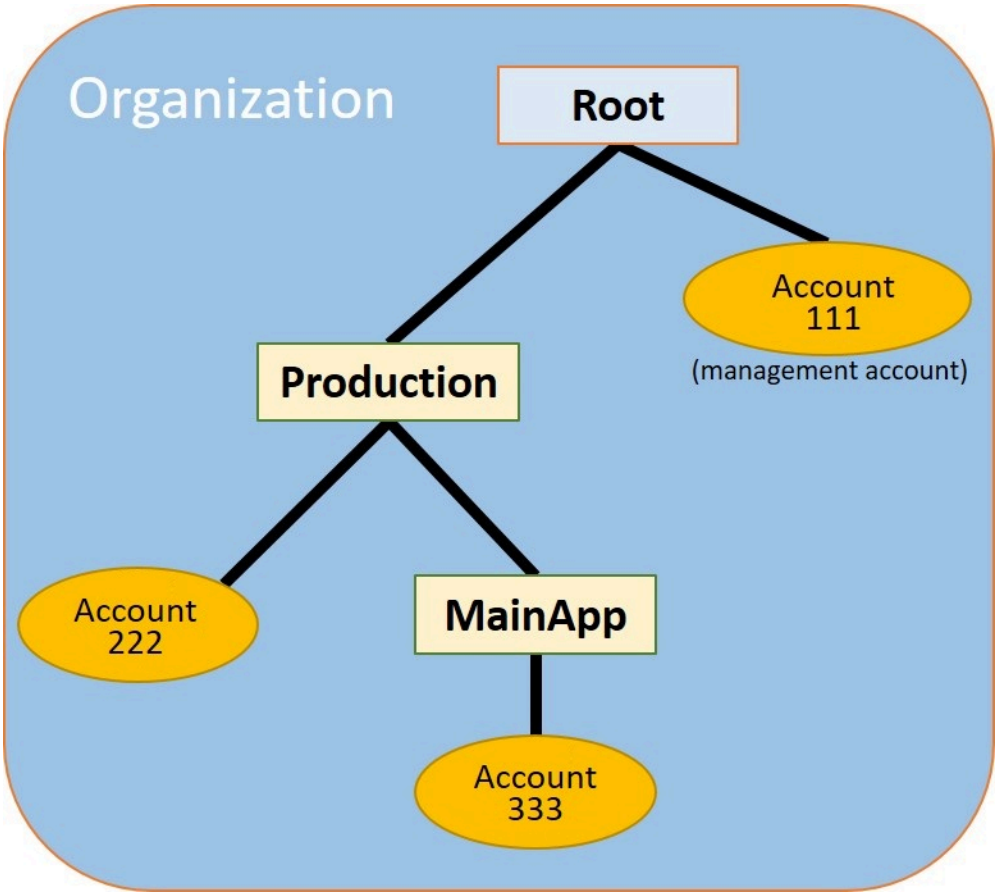
Para crear una cuenta de miembro

1. En la AWS Organizations consola, en la Cuentas de AWSpágina, selecciona Añadir Cuenta de AWS.
2. En la páginaAgregar un Cuenta de AWS, elija Crear un Cuenta de AWS.
3. En Nombre Cuenta de AWS , ingrese un nombre para la cuenta, como **`MainApp Account`**.
4. En Dirección de correo electrónico del usuario del nodo raíz de la cuenta, ingrese la dirección de correo electrónico de la persona que va a recibir las comunicaciones en nombre de la cuenta. Este valor debe ser único de forma global. Dos cuentas no pueden tener la misma dirección de correo electrónico. Por ejemplo, puede escribir un correo como **`mainapp@example.com`**.
5. En cuanto al nombre de la IAM función, puede dejar este campo en blanco para utilizar automáticamente el nombre de función predeterminado de`OrganizationAccountAccessRole`, o bien puede introducir su propio nombre. Este rol le permite acceder a la nueva cuenta de miembro al iniciar sesión como IAM usuario en la cuenta de administración. En este tutorial, déjelo en blanco para indicar a AWS Organizations que va a crear la función con el nombre predeterminado.
6. Seleccione Crear Cuenta de AWS. Es posible que tenga que esperar un rato y actualizar la página para ver la nueva cuenta en la página Cuentas de AWS.

> **Important**
>
> Si obtiene un error que indica que ha excedido los límites de la cuenta para la organización o que no puede añadir una cuenta porque la organización sigue inicializándose, espere a que pase una hora desde que creó la organización e inténtelo de nuevo. Si el error persiste, póngase en contacto con AWS Support.

Paso 2: Crear las unidades organizativas

En los pasos de esta sección, crearás unidades organizativas (OUs) y colocarás tus cuentas de miembro en ellas. Cuando haya finalizado, su jerarquía tendrá un aspecto similar al de la siguiente ilustración. La cuenta de administración permanece en el nodo raíz. Una cuenta de miembro se traslada a la OU de producción y la otra cuenta de miembro se mueve a la MainApp OU, que es una filial de Production.



AWS Management Console

Para crear y rellenar la OUs

> **Note**
>
> En los pasos siguientes, interactúa con objetos para los que puede elegir el nombre del objeto en sí o el botón de opción situado junto al objeto.
>
> - Si elige el nombre del objeto, abra una nueva página que muestre los detalles de los objetos.
> - Si elige el botón de opción situado junto al objeto, está identificando ese objeto para actuar mediante otra acción, como elegir una opción de menú.
>
> Los pasos que siguen le permiten elegir el botón de opción para que pueda actuar sobre el objeto asociado mediante la elección del menú.

1. En la consola de AWS Organizations, vaya a la página Cuentas de AWS.
2. Active la casilla de verificación
   
   junto al contenedor de Nodo raíz.
3. Seleccione el menú desplegable Acciones y, a continuación, en Unidad organizativa, elija Crear nueva.
4. En la página Crear unidad organizativa en Nodo raíz, para el Nombre de la unidad organizativa, ingrese **`Production`** y luego Crear unidad organizativa.
5. Active la casilla de verificación
   
   junto a su nueva OU de Producción.
6. Seleccionar Acciones y, a continuación, en Unidad organizativa, elija Crear nuevo.
7. En la página Crear unidad organizativa en Producción, para el nombre de la segunda OU, ingrese **`MainApp`** y luego elija Crear unidad organizativa.

   Ahora puede mover sus cuentas de miembro a estasOUs.
8. Vuelva a la página Cuentas de AWS y, a continuación, expanda el árbol bajo la unidad organizativa Production (Producción) eligiendo el triángulo

situado junto a ella. Esto muestra la MainAppOU como un elemento secundario de la producción.

9. Junto a 333333333333, elija la casilla de verificación
(no su nombre), elija Acciones y, a continuación, en Cuenta de AWS, elija Mover.
10. En la página Mover Cuenta de AWS «333333333333», elija el triángulo situado junto a Producción para expandirlo. Junto a él MainApp, selecciona el botón de radio
(no su nombre) y, a continuación, selecciona Move. Cuenta de AWS
11. Junto a 222222222222, elija la casilla de verificación
(no su nombre), elija Acciones y, a continuación, en Cuenta de AWS, elija Mover.
12. En la página Mover Cuenta de AWS «222222222222», junto a Producción, selecciona el botón de radio (no su nombre) y, a continuación, selecciona Mover. Cuenta de AWS

Paso 3: Crear las políticas de control de servicios

En los pasos de esta sección, debe crear tres políticas de control de servicios (SCPs) y adjuntarlas a la raíz y OUs a la para restringir lo que pueden hacer los usuarios de las cuentas de la organización. La primera SCP impide que cualquier usuario de las cuentas de los miembros cree o modifique AWS CloudTrail los registros que usted configure. La cuenta de administración no se ve afectada por ningunoSCP, por lo que, después de aplicarla CloudTrail SCP, debe crear todos los registros a partir de la cuenta de administración.

Habilitar el tipo de política de control de servicios para la organización

Antes de asociar una política de cualquier tipo a un nodo raíz o unidad organizativa dentro de un nodo raíz, debe habilitar el tipo de política para esa organización. Los tipos de políticas no están habilitados predeterminado. Los pasos de esta sección le muestran cómo habilitar el tipo de política de control de servicios (SCP) para su organización.

AWS Management Console

SCPsPara habilitarlo en su organización

1. Vaya a la página de Políticas y, a continuación, elija Políticas de control de servicios.

2. En la página Políticas de control de servicios, elija Habilitar políticas de control de servicios.

   Aparece un cartel verde para informarle de que ya puede crear SCPs en su organización.

Crear su SCPs.

Ahora que las políticas de control de servicios están habilitadas en su organización, puede crear las tres políticas que necesita para este tutorial.

AWS Management Console

Para crear el primero SCP que bloquee las acciones CloudTrail de configuración

1. Vaya a la página de Políticas y, a continuación, elija Políticas de control de servicios.
2. En la página Políticas de control de servicios, seleccione Crear política.
3. Para Policy name (Nombre de política), introduzca **`Block CloudTrail Configuration Actions`**.
4. En la sección Política, en la lista de servicios de la derecha, seleccione CloudTrail el servicio. A continuación, elija las siguientes acciones: AddTagsCreateTrailDeleteTrail, RemoveTags, StartLogging, StopLogging, y UpdateTrail.
5. Aún en el panel derecho, selecciona Agregar recurso y especificar CloudTraily Todos los recursos. A continuación, elija Add resource (Añadir recurso).

   La declaración de la política ubicada a la izquierda tendrá un aspecto similar a la siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
```

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

6. Elija Crear política.

La segunda política define una lista de permitidos de todos los servicios y acciones que desea permitir para los usuarios y roles de la unidad organizativa Production. Cuando haya finalizado, los usuarios de la unidad organizativa Production (Producción) podrán obtener acceso solo a los servicios y acciones enumerados.

AWS Management Console

Para crear la segunda política que permite usar los servicios aprobados para la unidad organizativa de producción

1. En la página Políticas de control de servicios, seleccione Crear política.
2. Para Policy name (Nombre de política), introduzca **`Allow List for All Approved Services`**.
3. Sitúe el cursor en el panel derecho de la sección Policy (Política) y pegue una política como la siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
```

```
}
```

4. Elija Crear política.

La política final proporciona una lista de denegación de los servicios cuyo uso está bloqueado en la MainApp OU. En este tutorial, bloqueará el acceso a Amazon DynamoDB en todas las cuentas que se encuentren en la OU. MainApp

AWS Management Console

Para crear la tercera política que deniegue el acceso a los servicios que no se pueden utilizar en la OU MainApp

1. En la página Políticas de control de servicios, seleccione Crear política.
2. Para Policy name (Nombre de política), introduzca **`Deny List for MainApp Prohibited Services`**.
3. En la sección Policy (Política) de la izquierda, seleccione el servicio Amazon DynamoDB. Para la acción, elija All actions (Todas las acciones).
4. En el panel de la izquierda, elija Add resource (Agregar recurso) y especifique DynamoDB y All Resources (Todos los recursos). A continuación, elija Add resource (Añadir recurso).

   La instrucción de la política de la derecha se actualizará y tendrá un aspecto similar al siguiente.

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

5. Elija Crear política para guardar laSCP.

Adjunte el SCPs a su OUs

Ahora que SCPs existen y están habilitados para su raíz, puede adjuntarlos a la raíz yOUs.

AWS Management Console

Para adjuntar las políticas a la raíz y al OUs

1. Vaya a la página Cuentas de AWS.
2. En la página Cuentas de AWS, elija Root (Raíz) (su nombre, no el botón de opción) para desplazarse a su página de detalles.
3. En la página de detalles de Nodo raíz, elija la pestaña Políticas y, a continuación, en Políticas de control de servicios, elija Adjuntar.
4. En la página Adjuntar una política de control de servicios, pulse el botón de radio situado junto a la SCP nombrada y`Block CloudTrail Configuration Actions`, a continuación, seleccione Adjuntar. En este tutorial, debe adjuntarla a la raíz para que afecte a todas las cuentas de los miembros y evitar que alguien modifique la configuración que ha realizado CloudTrail.

   La pestaña Políticas de la página de detalles raíz ahora muestra que SCPs hay dos asociadas a la raíz: la que acabas de adjuntar y la predeterminada `FullAWSAccess`SCP.
5. Vuelva a la página Cuentas de AWS y elija la unidad organizativa Production (Producción) (su nombre, no el botón de opción) para desplazarse a su página de detalles.
6. En la página de detalles de la OU de Producción, elija la pestaña Políticas.
7. Bajo Políticas de control de servicios, elija Adjuntar.
8. En la página Adjuntar una política de control de servicios, elija el botón de opción situado al lado de `Allow List for All Approved Services`, y luego elija Adjuntar. Esto le permite a los usuarios o roles de las cuentas de miembro en la unidad organizativa de Producción tener acceso a los servicios aprobados.
9. Vuelva a seleccionar la pestaña Políticas para comprobar que SCPs hay dos adjuntas a la unidad organizativa: la que acaba de adjuntar y la predeterminada `FullAWSAccess`SCP. Sin embargo, dado que también `FullAWSAccess` SCP hay una lista de permitidos que permite todos los servicios y acciones, ahora debe separarla SCP para asegurarse de que solo se permiten los servicios aprobados.

10. Para eliminar la política predeterminada de la unidad organizativa de producción, pulse el botón de radio que lleva a F ullAWSAccess, elija Separar y, a continuación, en el cuadro de diálogo de confirmación, elija Separar política.

    Tras eliminar esta política predeterminada, todas las cuentas de los miembros de la OU de producción pierden inmediatamente el acceso a todas las acciones y servicios que no figuran en la lista de permitidos SCP que adjuntó en los pasos anteriores. Se deniega cualquier solicitud de uso de acciones que no estén incluidas en la lista de permitidos para todos los servicios SCP aprobados. Esto es así incluso si un administrador de una cuenta concede acceso a otro servicio asociando una política de permisos de IAM a un usuario de una de las cuentas miembro.

11. Ahora puede adjuntar el SCP nombre `Deny List for MainApp Prohibited services` para evitar que cualquier persona de las cuentas de la MainApp OU utilice alguno de los servicios restringidos.

    Para ello, navegue hasta la Cuentas de AWSpágina, elija el icono triangular para expandir la rama de la OU de producción y, a continuación, elija la MainAppOU (su nombre, no el botón de radio) para navegar hasta su contenido.

12. En la página de MainAppdetalles, seleccione la pestaña Políticas.

13. En Políticas de control de servicios, selecciona Adjuntar y, a continuación, en la lista de políticas disponibles, pulsa el botón de radio situado junto a Denegar la lista de servicios MainApp prohibidos y, a continuación, selecciona Adjuntar política.

Paso 4: Probar las políticas de la organización

Ahora puede iniciar sesión como usuario en cualquiera de las cuentas de miembro e intentar realizar diversas acciones de AWS :

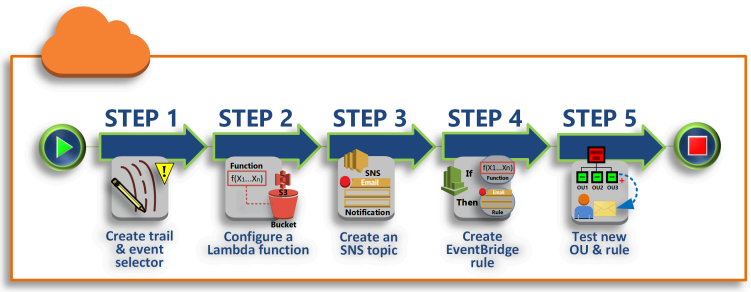
- Si inicia sesión como usuario en la cuenta de administración, puede realizar cualquier operación permitida por sus políticas de IAM permisos. SCPsNo afectan a ningún usuario o función de la cuenta de administración, independientemente de la raíz o la unidad organizativa en la que se encuentre la cuenta.
- Si inicias sesión como usuario en la cuenta 222222222222, puedes realizar cualquier acción permitida en la lista de permitidos. AWS Organizations deniega cualquier intento de realizar una acción en cualquier servicio que no esté en la lista de permitidos. Además, AWS Organizations deniega cualquier intento de realizar una de las acciones de CloudTrail configuración.

- Si inicia sesión como un usuario en la cuenta 333333333333, puede realizar cualquier acción permitida por la lista de permitidos y que no esté bloqueada por la lista de denegación. AWS Organizations deniega cualquier intento de realizar una acción en cualquier servicio que no esté en la política de la lista de permitidos y cualquier acción que esté en la de la lista de denegación. Además, AWS Organizations niega cualquier intento de realizar una de las acciones de CloudTrail configuración.

Tutorial: Supervisa los cambios importantes en tu organización con Amazon EventBridge

En este tutorial se muestra cómo configurar Amazon EventBridge, anteriormente Amazon CloudWatch Events, para que supervise su organización en busca de cambios. Para comenzar, se configura una regla que se activa cuando los usuarios invocan determinadas operaciones de AWS Organizations . A continuación, configura Amazon EventBridge para que ejecute una AWS Lambda función cuando se active la regla y configura Amazon SNS para que envíe un correo electrónico con detalles sobre el evento.

En la siguiente ilustración se muestran los principales pasos del tutorial.



[Paso 1: Configuración de un registro de seguimiento y un selector de eventos]

Cree un registro, denominado ruta, en AWS CloudTrail. Configúrelo para capturar todas las llamadas a API.

[Paso 2: Configuración de la función Lambda]

Cree una AWS Lambda función que registre los detalles del evento en un bucket de S3.

[Paso 3: Creación de un tema de Amazon SNS que envía correos electrónicos a los suscriptores]

Cree un tema de Amazon SNS que envíe correos electrónicos a sus suscriptores y, a continuación, suscríbase a ese tema.

[Paso 4: Crea una EventBridge regla de Amazon]

Cree una regla que indique EventBridge a Amazon que pase los detalles de las llamadas a la API especificadas a la función Lambda y a los suscriptores de temas de SNS.

[Paso 5: Pon a prueba tu EventBridge regla de Amazon]

Ejecute una de las operaciones monitorizadas para probar la nueva regla. En este tutorial, la operación monitorizada crea una unidad organizativa (OU). Puede ver la entrada de registro creada por la función Lambda y el correo electrónico que Amazon SNS envía a los suscriptores.

> **Sugerencia**
>
> También puede utilizar este tutorial como guía al configurar operaciones similares como, por ejemplo, el envío de notificaciones por correo electrónico cuando se haya completado la creación de la cuenta. Dado que la creación de la cuenta es una operación asíncrona, no recibirá de forma predeterminada una notificación cuando se complete. Para obtener más información sobre el uso AWS CloudTrail de Amazon EventBridge con AWS Organizations, consultaInicio de sesión y supervisión AWS Organizations.

Requisitos previos

Este tutorial se basa en los siguientes supuestos:

- Puede iniciar sesión AWS Management Console como usuario de IAM desde la cuenta de administración de su organización. El usuario de IAM debe tener permisos para crear y configurar un inicio de sesión CloudTrail, una función en Lambda, un tema en Amazon SNS y una regla en Amazon. EventBridge Para obtener más información sobre la concesión de permisos, consulte Access Management (Administración de accesos) en la guía del usuario IAM o en la guía del servicio para el que desea configurar el acceso.
- Tiene acceso a un depósito de Amazon Simple Storage Service (Amazon S3) existente (o tiene permisos para crear uno) para recibir CloudTrail el registro que configuró en el paso 1.

> **Important**
>
> Actualmente, solo AWS Organizations está alojado en la región EE.UU. Este (Virginia del Norte) (aunque está disponible en todo el mundo). Para llevar a cabo los pasos de este tutorial, debe configurar AWS Management Console para usar esa región.

Paso 1: Configuración de un registro de seguimiento y un selector de eventos

En este paso, iniciará sesión en la cuenta de administración y configurará un registro de seguimiento en AWS CloudTrail. También configuras un selector de eventos en el registro para capturar todas las llamadas a la API de lectura/escritura, de modo que Amazon EventBridge tenga llamadas que activar.

Creación de un registro de seguimiento

1. Inicie sesión AWS como administrador de la cuenta de administración de la organización y, a continuación, abra la CloudTrail consola en. https://console.aws.amazon.com/cloudtrail/
2. En la barra de navegación de la esquina superior derecha de la consola, elija la región EE. UU. Este (Norte de Virginia). Si eliges una región diferente, AWS Organizations no aparece como opción en los ajustes de EventBridge configuración de Amazon y CloudTrail no captura información sobre ella AWS Organizations.
3. En el panel de navegación, seleccione Trails.
4. Elija Create Trail (Crear registro de seguimiento).
5. En Trail name (Nombre del registro de seguimiento), escriba **`My-Test-Trail`**.
6. Realice una de las siguientes opciones para especificar dónde CloudTrail debe entregar sus registros:

   - Si necesita crear un bucket, seleccione Create new S3 bucket (Crear nuevo bucket de S3) y, a continuación, introduzca un nombre para el nuevo bucket y la carpeta de registro de seguimiento.

     > **Note**
     >
     > Los nombres de los buckets de S3 deben ser únicos de forma global.

- Si ya dispone de un bucket, seleccione Use existing S3 bucket (Usar bucket S3 existente) y, a continuación, elija el nombre del bucket en la lista de buckets S3.

7. Elija Next (Siguiente).
8. En la página Elegir eventos de registro, en la sección Eventos de administración, elija Read (Lectura) y Write (Escritura).
9. Elija Next (Siguiente).
10. Revise las selecciones y elija Create trail (Crear ruta).

Amazon te EventBridge permite elegir entre varias formas diferentes de enviar alertas cuando una regla de alarma coincide con una llamada entrante a la API. En este tutorial se muestran dos métodos: invocar una función Lambda que puede registrar la llamada a la API y enviar información a un tema de Amazon SNS que, a su vez, envía un correo electrónico o mensaje de texto a los suscriptores del tema. En los próximos dos pasos, debe crear los componentes que necesita, la función Lambda y el tema de Amazon SNS.

Paso 2: Configuración de la función Lambda

En este paso, se crea una función Lambda que registra la actividad de la API que le envía la EventBridge regla de Amazon que se configura más adelante.

Para crear una función Lambda que registre los eventos de Amazon EventBridge

1. Abra la AWS Lambda consola en. https://console.aws.amazon.com/lambda/
2. Si es nuevo en Lambda, elija Get Started Now (Comenzar ahora) en la página de bienvenida; de lo contrario, elija Create a function (Crear una función).
3. En la página Create function (Crear función), seleccione Use a blueprint (Utilizar un proyecto).
4. En el cuadro de búsqueda Blueprints (Proyectos), escriba **`hello`** para el filtro y elija el proyecto hello-world.
5. Elija Configurar.
6. En la página Basic information (Información básica), haga lo siguiente:

    a. Para el nombre de la función Lambda, ingrese **`LogOrganizationEvents`** en el cuadro desde el cuadro de texto Name (Nombre).

    b. Para Role (Rol), elija Create a new role with basic Lambda permissions (Crear un nuevo rol con permisos básicos de Lambda) Este rol concede a la función Lambda permisos para obtener acceso a los datos que requiere y para escribir en su registro de salida.

7. Edite el código de la función de Lambda tal y como se muestra en el siguiente ejemplo.

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

   Este código de muestra registra el evento con una cadena de marcador **`LogOrganizationEvents`** seguida de la cadena JSON que compone el evento.

8. Seleccione Crear función.

Paso 3: Creación de un tema de Amazon SNS que envía correos electrónicos a los suscriptores

En este paso, se crea un tema de Amazon SNS que envía información a sus suscriptores por correo electrónico. Convierte este tema en el objetivo de la EventBridge regla de Amazon que cree más adelante.

Para crear un tema de Amazon SNS con el fin de enviar un correo electrónico a los suscriptores

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/.
2. En el panel de navegación, elija Topics (Temas).
3. Elija Create new topic (Crear nuevo tema).
   a. En Topic name (Nombre del tema), escriba **`OrganizationsCloudWatchTopic`**.
   b. En Display name (Nombre visible), escriba **`OrgsCWEvnt`**.
   c. Seleccione Crear tema.
4. Ahora puede crear una suscripción para el tema. Elija el ARN del tema que acaba de crear.
5. Elija Crear una suscripción.
   a. En la página Create subscription, para Protocol, elija Email.
   b. Para punto de conexión, introduzca su dirección de correo electrónico.

c. Selecciona Crear suscripción. AWS envía un correo electrónico a la dirección de correo electrónico que especificó en el paso anterior. Espere a recibir ese correo electrónico y, a continuación, elija el enlace Confirm subscription que contiene para confirmar que lo ha recibido correctamente.

d. Vuelva a la consola y actualice la página. El mensaje Pending confirmation desaparece y se sustituye por el ID de suscripción que ha quedado validado.

Paso 4: Crea una EventBridge regla de Amazon

Ahora que la función Lambda requerida existe en su cuenta, crea una EventBridge regla de Amazon que la invoca cuando se cumplen los criterios de la regla.

Para crear una regla EventBridge

1. Abre la EventBridge consola de Amazon enhttps://console.aws.amazon.com/events/.
2. Debe configurar la consola en la región de Este de EE. UU. (Norte de Virginia) o la información acerca de Organizations no estará disponible. En la barra de navegación de la esquina superior derecha de la consola, elija la región EE. UU. Este (Norte de Virginia).
3. Para obtener instrucciones sobre cómo crear reglas, consulta Reglas en Amazon EventBridge en la guía del EventBridge usuario de Amazon.

Paso 5: Pon a prueba tu EventBridge regla de Amazon

En este paso, creas una unidad organizativa (OU) y observas la EventBridge regla de Amazon, generas una entrada de registro y te envías un correo electrónico con los detalles del evento.

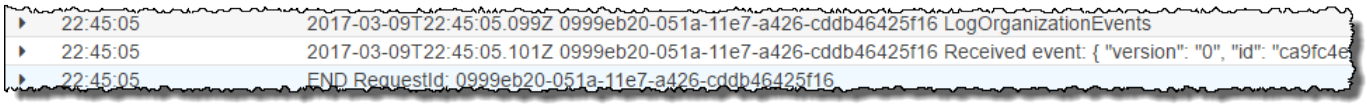
AWS Management Console

Para crear una OU

1. Abre la AWS Organizations consola en la Cuentas de AWSpágina.
2. Seleccionar la casilla de verificación
   ☑
   OU de Nodo raíz, elija Acciones y, a continuación, en Unidad organizativa, elija Crear nuevo.
3. Para el nombre de la unidad organizativa, escriba **`TestCWEOU`** y, a continuación, elija Create organizational unit (Crear unidad organizativa).

Para ver la entrada de EventBridge registro

1. Abra la CloudWatch consola enhttps://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Registros.
3. En Grupos de registros, elija el grupo que está asociado a la función Lambda:/. aws/lambda/ LogOrganizationEvents
4. Cada grupo contiene uno o más flujos; debería haber un grupo para hoy. Elíjalo.
5. Consulte el registro. Deben aparecer filas similares a las siguientes.



6. Seleccione la fila central de la entrada para ver todo el texto JSON del evento recibido. Aparecen todos los detalles de la solicitud al API en los componentes `requestParameters` y `responseElements` de la salida.

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
        },
```

```
        "responseElements": {
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
        "eventType": "AwsApiCall"
    }
}
```

7. Comprueba en tu cuenta de correo electrónico un mensaje de Orgs CWEvnt (el nombre visible de tu tema de Amazon SNS). El cuerpo del correo electrónico contiene la misma salida de texto JSON que la entrada de registro mostrada en el paso anterior.

Limpieza: Elimine los recursos que ya no necesite

Para evitar incurrir en cargos, debe eliminar todos AWS los recursos que haya creado como parte de este tutorial y que no desee conservar.

Para limpiar su entorno AWS

1. Utilice la CloudTrail consola para eliminar la ruta con el nombre **`My-Test-Trail`** que creó en el paso 1.
2. Si ha creado un bucket de Amazon S3 en el paso 1, utilice la consola de Amazon S3 para eliminarlo.
3. Utilice la consola de Lambda para eliminar la función denominada **`LogOrganizationEvents`** que se creó en el paso 2.
4. Utilice la Consola de Amazon SNS para eliminar el tema de Amazon SNS denominado **`OrganizationsCloudWatchTopic`** que creó en el paso 3.
5. Utilice la CloudWatch consola para eliminar el nombre de EventBridge regla **`OrgsMonitorRule`** que creó en el paso 4.
6. Finalmente, utilice la consola de Organizations para eliminar la OU denominada **`TestCWEOU`** que creó en el paso 5.

Y ya está. En este tutorial, configuró EventBridge para supervisar su organización en busca de cambios. Ha configurado una regla que se activa cuando los usuarios invocan determinadas operaciones de AWS Organizations . La regla ha ejecutado una función Lambda que registró el evento y envió un correo electrónico que contenía información acerca de dicho evento.

Se usa AWS Organizations con un SDK AWS

AWS Los kits de desarrollo de software (SDKs) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK for C++	AWS SDK for C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK para Go	AWS SDK para Go ejemplos de código
AWS SDK for Java	AWS SDK for Java ejemplos de código
AWS SDK for JavaScript	AWS SDK for JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código
AWS SDK for .NET	AWS SDK for .NET ejemplos de código
AWS SDK for PHP	AWS SDK for PHP ejemplos de código
AWS Tools for PowerShell	Herramientas para ejemplos PowerShell de código
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) ejemplos de código
AWS SDK for Ruby	AWS SDK for Ruby ejemplos de código
AWS SDK para Rust	AWS SDK para Rust ejemplos de código
AWS SDK para SAP ABAP	AWS SDK para SAP ABAP ejemplos de código

Documentación de SDK	Ejemplos de código
AWS SDK para Swift	AWS SDK para Swift ejemplos de código

Ejemplo de disponibilidad

¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Administrar una organización con AWS Organizations

Una organización es un conjunto de organizaciones Cuentas de AWS que se pueden administrar de forma centralizada y organizarlas en una estructura jerárquica similar a un árbol, con una raíz en la parte superior y unidades organizativas anidadas debajo de la raíz. Cada cuenta puede estar directamente en la raíz o colocarse en una de las siguientes direcciones jerárquicas. OUs

Cada organización se compone de los siguientes elementos:

- Una cuenta de administración
- Cero o más cuentas de miembro
- Cero o más unidades organizativas (OUs)
- Cero o más políticas.

Una organización tiene la funcionalidad determinada por el conjunto de características habilitadas.

Temas

- Creación de una organización con AWS Organizations
- Verificación de dirección de correo electrónico con AWS Organizations
- Reenvío del correo electrónico de verificación con AWS Organizations
- Cambio de dirección de correo electrónico de una organización con AWS Organizations
- Habilitar todas las funciones de una organización con AWS Organizations
- Visualización de los detalles de una organización desde la cuenta de administración
- Eliminar una organización con AWS Organizations

Creación de una organización con AWS Organizations

Puede crear una organización con su Cuenta de AWS como cuenta de administración. Cuando crea una organización, puede elegir si la organización admitirá todas las características (opción recomendada) o solo las de facturación unificada. De forma predeterminada, la organización que cree admite todas las características.

Crear una organización

Puede crear una organización utilizando la AWS Management Console o mediante un comando del AWS CLI o una de las API de SDK.

Permisos mínimos

Para crear una organización con su Cuenta de AWS actual, debe contar con los siguientes permisos:

- `organizations:CreateOrganization`
- `iam:CreateServiceLinkedRole`

  Puede restringir este permiso solo a la entidad principal del servicio `organizations.amazonaws.com`.

AWS Management Console

Para crear una organización de

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. De forma predeterminada, la organización se crea con todas las características habilitadas. Sin embargo, puede elegir cualquiera de los siguientes pasos:

   - Para crear una organización con todas las características habilitadas, en la página de introducción, elija Creación de una organización.
   - Para crear una organización con funciones de Facturación unificada únicamente, en la página de introducción y en Creación de una organización, elija características de facturación unificada y, a continuación, en el cuadro de diálogo de confirmación, elija Crear una organización.

   Si elige accidentalmente la opción incorrecta, puede ir inmediatamente a la página Configuración y, a continuación, elija Eliminar organización y empiece de nuevo.

3. Se crea la organización y se visualizará la página Cuentas de AWS. La única cuenta presente es su cuenta de administración, y actualmente está almacenada en la Unidad organizativa raíz (OU).

   Organizations envía automáticamente un correo electrónico de verificación a la dirección asociada a su cuenta de administración. Puede pasar algún tiempo hasta que reciba el correo electrónico de verificación. Verifique la dirección de correo electrónico en un plazo de 24 horas. Para obtener más información, consulte Verificación de dirección de correo electrónico con AWS Organizations. Puede crear cuentas a la organización sin verificar la dirección de correo electrónico de la cuenta de administración. Sin embargo, para invitar a otras cuentas existentes, primero debe completar la verificación de correo electrónico.

   > **Note**
   >
   > Si esta cuenta ha verificado previamente su dirección de correo electrónico, no volverá a ocurrir cuando utilice la cuenta para crear una organización.

AWS CLI y AWS SDK

Los siguientes ejemplos de código muestran cómo utilizar `CreateOrganization`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
```

```
   public class CreateOrganization
   {
       /// <summary>
       /// Creates an Organizations client object and then uses it to create
       /// a new organization with the default user as the administrator, and
       /// then displays information about the new organization.
       /// </summary>
       public static async Task Main()
       {
           IAmazonOrganizations client = new AmazonOrganizationsClient();

           var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
           {
               FeatureSet = "ALL",
           });

           Organization newOrg = response.Organization;

           Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
       }
   }
```

- Para obtener información sobre la API, consulte CreateOrganization en la Referencia de la API de AWS SDK for .NET.

CLI

AWS CLI

Ejemplo 1: Creación de una nueva organización

Bill quiere crear una organización con las credenciales de la cuenta 111111111111. En el siguiente ejemplo se muestra que la cuenta se convierte en la cuenta maestra de la nueva organización. Puesto que no especifica un conjunto de características, la nueva organización tiene habilitadas todas las características de forma predeterminada y las políticas de control de servicios están habilitadas en la raíz.

```
aws organizations create-organization
```

El resultado incluye un objeto de organización con detalles sobre la nueva organización:

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

Ejemplo 2: Creación de una nueva organización con solo las características de facturación consolidada habilitadas

En el siguiente ejemplo se crea una organización que solo admite las características de facturación consolidada:

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

El resultado incluye un objeto de organización con detalles sobre la nueva organización:

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
```

```
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

Para obtener más información, consulte Creación de una organización en la Guía del usuario de AWS Organizations.

- Para obtener información sobre la API, consulte CreateOrganization en la Referencia de comandos de la AWS CLI.

Una vez creada la organización, puede agregar cuentas desde la cuenta de administración tal y como se indica a continuación:

- Puede crear otras Cuentas de AWS que se incorporen automáticamente a la organización como miembros.
- Después de verificar la dirección de correo electrónico, puede invitar Cuentas de AWS existentes para que se unan a su organización como cuentas miembro.

Verificación de dirección de correo electrónico con AWS Organizations

Después de crear la organización, para poder invitar a otras cuentas a que se unan, debe verificar que es el propietario de la dirección de correo electrónico asociada a la cuenta de administración de la organización.

Al crear una organización, si la cuenta de administración no se ha verificado previamente, AWS envía automáticamente un correo electrónico de verificación a la dirección de correo electrónico especificada. Puede pasar algún tiempo hasta que reciba el correo electrónico de verificación.

Verificar su dirección de correo electrónico

En un plazo de 24 horas, siga las instrucciones del correo electrónico para verificar la dirección de correo electrónico. Si han transcurrido más de 24 horas, consulte Resending the verification email.

Reenvío del correo electrónico de verificación con AWS Organizations

Si no verifica la dirección de correo electrónico en un plazo de 24 horas, puede volver a enviar la solicitud de verificación. Después de verificar la dirección de correo electrónico, podrá invitar a otras Cuentas de AWS para que se unan a su organización. Si no recibe el correo electrónico de verificación, compruebe que la dirección de correo electrónico es correcta y, si es necesario, modifíquela.

- Para saber qué dirección de correo electrónico está asociada a la cuenta de administración, consulte Visualización de los detalles de una organización desde la cuenta de administración.
- Para cambiar la dirección de correo electrónico asociada a la cuenta de administración, consulte Administración de una Cuenta de AWS en la Guía del usuario AWS Billing.

AWS Management Console

Para volver a enviar la solicitud de verificación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página de Configuración y, a continuación, elija Solicitud de verificación de envío. La opción solo está presente si no se verifica la cuenta de administración.
3. Verifique la dirección de correo electrónico en un plazo de 24 horas.

Después de verificar la dirección de correo electrónico, podrá invitar a otras Cuentas de AWS para que se unan a su organización. Para obtener más información, consulte Administrar las invitaciones a las cuentas con AWS Organizations.

Cambio de dirección de correo electrónico de una organización con AWS Organizations

Para cambiar la dirección de correo electrónico asociada a su cuenta de administración, consulte Update the Cuenta de AWS name, email address, or password for the root user en la Guía de referencia de AWS Account Management.

Si cambia la dirección de correo electrónico de la cuenta de administración, el estado de la cuenta volverá a ser "email unverified" (correo electrónico sin verificar) y deberá completar el proceso de verificación de la nueva dirección de correo electrónico.

> **Note**
>
> Si invitó a las cuentas a unirse a su organización antes de cambiar la dirección de correo electrónico de la cuenta de administración y esas invitaciones aún no se han aceptado, no se podrán aceptar hasta que verifique la nueva dirección de correo electrónico de la cuenta de administración. Primero debe volver a enviar la solicitud de verificación. Después de completar el proceso respondiendo al correo electrónico, las cuentas invitadas pueden aceptar las invitaciones.

Habilitar todas las funciones de una organización con AWS Organizations

AWS Organizations tiene dos conjuntos de funciones disponibles:

- Todas las funciones: este conjunto de funciones es la forma preferida y predeterminada de trabajar AWS Organizations, e incluye todas las funciones de la facturación consolidada. Al crear una organización, las características se habilitan de manera predeterminada. Con todas las funciones habilitadas, puede utilizar las funciones avanzadas de administración de cuentas disponibles en Organizations, como la integración con AWS los servicios compatibles y las políticas de la organización.
- Características de facturación unificada: este conjunto de características se limita a generar una sola factura en toda la organización. No hay otras capacidades de administración disponibles con la facturación unificada.

Si crea una organización que solo tenga las características de facturación unificada, podrá habilitar posteriormente todas las características. Sin embargo, no puede migrar de todas las características a la facturación unificada una vez que todas las características estén habilitadas.

Migración estándar y migración asistida

Los dos enfoques para migrar a todas las características son la migración estándar y la migración asistida.

La migración estándar es el proceso de autoservicio disponible para todos los AWS Organizations clientes para habilitar el modo con todas las funciones.

La migración asistida es un proceso disponible para que los clientes del plan Enterprise Support soliciten la AWS migración de su organización al modo con todas las funciones en su nombre.

> **Note**
>
> Procesos unidireccionales y procesos de reversión
>
> - La migración desde las características de facturación unificada a todas las características es unidireccional. No puede revertir una organización con todas las características habilitadas a solo características de facturación unificada.
> - Una vez que haya iniciado el proceso de migración asistida, no se puede revertir. Tendrá que esperar 90 días hasta que el proceso venza si, en su lugar, desea seguir el proceso estándar.

Temas

- Consideraciones
- Proceso de migración estándar para habilitar todas las características con Organizations
- Proceso de migración asistida para habilitar todas las características con Organizations

Consideraciones

Antes de cambiar de una organización que admite solamente las características de facturación unificada a una organización que admita todas las características, tenga en cuenta lo siguiente:

Las cuentas invitadas deben aprobar la migración

Al iniciar el proceso para habilitar todas las funciones, AWS Organizations envía una solicitud a cada cuenta de miembro que haya invitado a unirse a su organización. Cada cuenta invitada debe aprobar la habilitación de todas las características aceptando la solicitud. Solo entonces podrá completar el proceso para habilitar todas las características en su organización. Si una cuenta rechaza la solicitud, debe eliminar la cuenta de su organización o volver a enviar la solicitud. Se debe aceptar la solicitud antes de que pueda completar el proceso para habilitar todas las características. Las cuentas que ha creado utilizando AWS Organizations no reciben una solicitud porque no necesitan aprobar el control adicional.

A las cuentas invitadas se les notifica qué conjunto de características está activado actualmente

La invitación informa al propietario de una cuenta invitada si se está uniendo a una organización con solo facturación unificada o con todas las funciones habilitadas. Puede seguir invitando cuentas a su organización mientras habilita todas las funciones.

Si invita a una cuenta durante el proceso para habilitar todas las características, la invitación indica que la organización a la que se unen tiene todas las características habilitadas. Si cancela el proceso para habilitar todas las funciones antes de que la cuenta acepte la invitación, dicha invitación se cancelará. Solo debe invitar a la cuenta para que sea miembro de una organización con características de facturación unificada.

Si invita a una cuenta y la invitación aún no está aceptada antes de que inicie el proceso para habilitar todas las características, esa invitación se cancela porque la invitación indica que la organización solo tiene funciones de facturación unificada. Debe invitar de nuevo a la cuenta para que sea miembro de una organización con todas las características habilitadas.

El proceso de creación de cuentas en una organización no se ve afectado por la migración

Puede seguir creando cuentas en la organización. Ese proceso no se ve afectado por este cambio.

El rol vinculado al servicio **`AWSServiceRoleForOrganizations`** es obligatorio

AWS Organizations verifica que cada cuenta de miembro tenga un rol vinculado al servicio denominado. `AWSServiceRoleForOrganizations` Este rol es obligatorio en todas las cuentas para habilitar todas las características. Si elimina el rol en una cuenta invitada, al aceptar la invitación para habilitar todas las características, se vuelve a crear el rol. Si eliminaste el rol de una cuenta que se creó usando AWS Organizations, esa cuenta recibirá una invitación específica para volver a crear ese rol. Todas estas invitaciones deben aceptarse para que la organización complete el procedimiento de habilitación de todas las características.

Proceso de migración estándar para habilitar todas las características con Organizations

En este tema se describe cómo habilitar todas las características con el proceso de migración estándar.

Paso 1: solicitar a las cuentas invitadas que aprueben la migración (cuenta de administración)

Puede iniciar el proceso para habilitar todas las características iniciando sesión en la cuenta de administración de la organización. Para ello, siga los pasos que se describen a continuación.

> **Permisos mínimos**
>
> Para habilitar todas las características en su organización, debe contar con el permiso siguiente:
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para pedir a las cuentas miembro invitadas que acepten la habilitación de todas las características en la organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Configuración, elija Iniciar proceso para habilitar todas las características.
3. En la página Habilitar todas las características, confirme que entiende que no puede volver a las características de facturación unificada después de cambiar seleccionando Iniciar proceso para habilitar todas las características.

   AWS Organizations envía una solicitud a cada cuenta invitada (no creada) de la organización para pedir que apruebe la habilitación de todas las características en la organización. Si tiene alguna de las cuentas que se han creado utilizando AWS Organizations y el administrador de la cuenta miembro eliminó la función vinculada al servicio denominada `AWSServiceRoleForOrganizations`, AWS Organizations envía a esa cuenta una solicitud para volver a crear la función.

   La consola muestra la lista de Estado de las solicitudes de aprobación para las cuentas invitadas.

> **Tip**
>
> Para volver a esta página más adelante, abra la página Configuración y en la sección de Solicitud enviada fecha, elija Ver estado.

4. La página Habilitar todas las características muestra el estado de la solicitud actual para cada cuenta de la organización. Las cuentas que han aceptado la solicitud muestran un estado de ACEPTADA. Las cuentas que aún no han acordado muestran un estado de ABIERTA.

AWS CLI & AWS SDKs

Para pedir a las cuentas miembro invitadas que acepten la habilitación de todas las características en la organización

Puede utilizar uno de los siguientes comandos para habilitar todas las características de una organización:

- AWS CLI: enable-all-features

  El siguiente comando inicia el proceso para habilitar todas las características en la organización.

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
```

```
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

El resultado muestra los detalles del apretón de manos que las cuentas de miembro invitadas deben aceptar.

- SDK de AWS: EnableAllFeatures

> **Notas**
>
> - Cuando se envía la solicitud a las cuentas miembro comienza una cuenta atrás de 90 días. Todas las cuentas deben aprobar la solicitud en ese período de tiempo; en caso contrario, la solicitud caducará. Si la solicitud expira, todas las solicitudes relacionadas con este intento se cancelan y tendrá que empezar con el paso 2.
> - Cuando realice la solicitud para habilitar todas las funciones, se cancelarán todas las invitaciones a cuentas existentes que no se hayan aceptado.
> - Durante el proceso de migración de todas las funciones, aún puede iniciar invitaciones nuevas a cuentas y crear cuentas nuevas.

Después de que todas las cuentas invitadas de la organización aprueben sus solicitudes, puede finalizar el proceso y habilitar todas las características. También puede finalizar inmediatamente el proceso si su organización no tiene ninguna cuenta miembro invitada. Para finalizar el proceso, continúe con Paso 3: finalizar el proceso de migración para habilitar todas las características (cuenta de administración).

Paso 2: aprobar la solicitud para habilitar todas las características o volver a crear el rol vinculado al servicio (cuenta de invitado)

Cuando inicia sesión en una de las cuentas miembro invitadas de la organización, puede aprobar una solicitud desde una cuenta de administración. Si su cuenta recibió originalmente una invitación a unirse a la organización, la invitación es para habilitar todas las características y e incluye implícitamente la aprobación para recrear el rol `AWSServiceRoleForOrganizations`, si es

necesario. Si su cuenta se ha creado en AWS Organizations y ha eliminado la función vinculada al servicio `AWSServiceRoleForOrganizations`, recibirá una invitación únicamente para volver a crear la función. Para ello, siga los pasos que se describen a continuación.

> **Important**
>
> Si habilita todas las funciones, la cuenta de administración de la organización puede aplicar controles basados en políticas a la cuenta miembro. Estos controles pueden restringir lo que los usuarios e incluso usted como administrador pueden hacer en la cuenta. Estas restricciones podrían impedir que su cuenta abandonara la organización.

> **Permisos mínimos**
>
> Para aprobar una solicitud a fin de habilitar todas las características para la cuenta miembro, debe contar con los permisos siguientes:
>
> - `organizations:AcceptHandshake`
> - `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
> - `organizations:ListHandshakesForAccount`: solo se requiere cuando se utiliza la consola de Organizations
> - `iam:CreateServiceLinkedRole`: solo es necesario si el rol `AWSServiceRoleForOrganizations` debe crearse de nuevo en la cuenta miembro.

AWS Management Console

Para aceptar la solicitud para habilitar todas las características de la organización

1. Inicie sesión en la consola de AWS Organizations en consola AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en una cuenta de miembro.
2. Lea las implicaciones de aceptar la solicitud de todas las características para su cuenta y después elija Aceptar. La página muestra el proceso como incompleto hasta que todas las cuentas de la organización aceptan las solicitudes y el administrador de la cuenta de administración finaliza el proceso.

AWS CLI & AWS SDKs

Para aceptar la solicitud para habilitar todas las características de la organización

Para aceptar la solicitud, debe aceptar el protocolo de enlace con `"Action": "APPROVE_ALL_FEATURES"`.

- AWS CLI:
  - accept-handshake
  - list-handshakes-for-account

  En el ejemplo siguiente se indica cómo enumerar los protocolo de enlace disponibles para su cuenta. El valor de `"Id"` en la cuarta línea de la salida es el valor que necesita para el siguiente comando.

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
                    "Type": "ACCOUNT"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
```

```
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
        }
    ]
}
```

En el siguiente ejemplo se utiliza el ID del protocolo de enlace del comando anterior para aceptar ese protocolo de enlace.

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
```

```
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
}
```

- SDK de AWS
  - list-handshakes-for-account
  - AcceptHandshake

Paso 3: finalizar el proceso de migración para habilitar todas las características (cuenta de administración)

Todas las cuentas miembro invitadas deben aprobar la solicitud para habilitar todas las características. Si no hay ninguna cuenta miembro invitada en la organización, la página Enable all features progress (Progreso de habilitación de todas las características) indica con un banner verde que puede finalizar el proceso.

> **Permisos mínimos**
>
> Para finalizar el proceso para habilitar todas las características de la organización, debe contar con el permiso siguiente:
>
> - `organizations:AcceptHandshake`
> - `organizations:ListHandshakesForOrganization`
> - `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para finalizar el proceso para habilitar todas las características

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Configuración, si todas las cuentas invitadas aceptan la solicitud para habilitar todas las características, aparecerá un cuadro verde situado en la parte superior de la página para informarle. En el cuadro verde, elija Ir a finalizar.
3. En la página Habilitar todas las características, elija Finalizar y, a continuación, en el cuadro de diálogo de confirmación, elija Finalizar de nuevo.
4. Ahora, la organización tiene habilitadas todas las características.

AWS CLI & AWS SDKs

Para finalizar el proceso para habilitar todas las características

Para completar el proceso, debe aceptar el protocolo de enlace con `"Action": "ENABLE_ALL_FEATURES"`.

- AWS CLI:
  - list-handshakes-for-organization
  - accept-handshake

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
```

```
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

En el ejemplo siguiente se indica cómo enumerar los protocolo de enlace disponibles para la organización. El valor de `"Id"` en la cuarta línea de la salida es el valor que necesita para el siguiente comando.

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- SDK de AWS

- ListHandshakesForOrganization
- AcceptHandshake

Proceso de migración asistida para habilitar todas las características con Organizations

Si es cliente de Enterprise, puede resultar difícil completar el proceso de migración estándar debido a la gran cantidad de cuentas que puede administrar. Por ejemplo, es posible que tenga dificultades para obtener la aprobación para migrar todas las cuentas invitadas en organizaciones grandes.

La migración asistida ofrece ayuda en este proceso, ya que permite a los clientes con un plan Enterprise Support solicitar que AWS migre su organización a todas las características en su nombre. Este proceso requiere que firme un contrato en el que se afirme que es propietario de todas las cuentas, seguido de un período de espera de 14 días. Este período de espera permite a las cuentas abandonar la organización si así lo desean antes de que se lleve a cabo la migración a todas las características.

AWS Management Console

Para migrar a todas las características con migración asistida

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Configuración, seleccione Habilitar todas las características y, a continuación, seleccione Migración asistida.
3. Lea los términos y condiciones del acuerdo, seleccione Aceptar y elija Iniciar el proceso para habilitar todas las características para iniciar la migración.

> **Note**
>
> Al iniciar el proceso de migración asistida, se anula el proceso de migración estándar Si actualmente está habilitando todas las características mediante el proceso de migración estándar, se cancelará y se iniciará el proceso de migración asistida.
> El proceso de migración asistida es unidireccional y no se puede revertir

Una vez que haya iniciado el proceso de migración asistida, no se puede revertir. Tendrá que esperar 90 días hasta que el proceso venza si, en su lugar, desea seguir el proceso estándar.

Si utiliza la migración asistida, no tiene que preocuparse por acceder a su cuenta invitada como usuario raíz para aceptar la migración a todas las características.

Puede contactar con su administrador técnico de cuentas (TAM) para obtener los detalles exactos, el progreso y los plazos de la migración asistida.

Visualización de los detalles de una organización desde la cuenta de administración

Cuando inicia sesión en la cuenta de administración de la organización en la AWS Organizationsconsola de , puede ver los detalles de la organización.

Permisos mínimos

Para ver los detalles de una organización, debe contar con el permiso siguiente:

- `organizations:DescribeOrganization`

AWS Management Console

Para ver los detalles de su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página de Configuración. En esta página se muestran detalles sobre la organización, incluido el ID de la organización, el nombre de la cuenta y la dirección de correo electrónico asignados a la cuenta de administración de la organización.

AWS CLI & AWS SDKs

Para ver los detalles de su organización

Puede utilizar uno de los siguientes comandos para ver detalles de una organización:

- AWS CLI: describe-organization

  El siguiente ejemplo muestra la información incluida en los resultados de este comando.

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
}
```

  Important

  El campo `AvailablePolicyTypes` está obsoleto y no contiene información precisa sobre las políticas habilitadas en su organización. Para ver la lista precisa y completa de los tipos de política que están realmente habilitados para la organización, utilice el comando `ListRoots`, tal y como se describe en la parte AWS CLI de la siguiente sección.

- SDK de AWS: DescribeOrganization

Eliminar una organización con AWS Organizations

Cuando ya no necesite una organización, puede eliminarla. Al eliminar una organización no se cierra la cuenta de administración, sino que se elimina, así como la propia organización.

La cuenta de administración anterior se convierte en una cuenta independiente Cuenta de AWS que ya no es administrada por AWS Organizations. Tiene tres opciones:

- Puede seguir utilizando esta cuenta como cuenta independiente.
- Puede usarla para crear una organización diferente

- Puede aceptar una invitación de otra organización para agregar la cuenta a esa organización como cuenta de miembro.

Temas

- Consideraciones
- Eliminar una organización

Consideraciones

Las organizaciones eliminadas no se pueden recuperar

Si elimina una organización, no puede recuperarla. Si creó alguna política dentro de la organización, también se eliminará y no se podrá recuperar.

Solo puede eliminar las organizaciones después de haber eliminado todas las cuentas de miembro

Solo puede eliminar una organización después de eliminar todas las cuentas de miembro de la organización. Si creó algunas de sus cuentas de miembro con ella AWS Organizations, es posible que no pueda eliminarlas. Puede eliminar una cuenta de miembro solo si esta tiene toda la información necesaria para operar como Cuenta de AWS independiente. Para obtener más información sobre cómo proporcionar dicha información y eliminar la cuenta, consulte Salir de una organización desde una cuenta de miembro con AWS Organizations.

Las cuentas de miembro en un estado “suspendido” no se pueden eliminar de una organización

Si cerró una cuenta de miembro antes de eliminarla de la organización, ésta ingresará en un estado “suspendido” durante un período de tiempo y no podrá eliminar la cuenta de la organización hasta que finalmente se cierre. Esto puede tardar hasta 90 días y puede impedir que elimine la organización hasta que todas las cuentas de miembro estén completamente cerradas.

Eliminar la cuenta de administración de una organización eliminando la propia organización puede repercutir en la cuenta de las siguientes formas:

- La cuenta es responsable de pagar únicamente sus propios cargos y ya no es responsable de los cargos generados por cualquier otra cuenta.
- La integración con otros servicios podría estar deshabilitada. Por ejemplo, AWS IAM Identity Center requiere que funcione una organización, por lo que si eliminas una cuenta de una

organización compatible con el Centro de Identidad de IAM, los usuarios de esa cuenta ya no podrán utilizar ese servicio.

La cuenta de administración de una organización nunca se ve afectada por las políticas de control de servicios (SCPs), por lo que los permisos no cambian cuando SCPs dejan de estar disponibles.

Haga copias de seguridad de todos los informes

Asegúrese de exportar o hacer copias de seguridad de los informes de la cuenta de administración, especialmente los informes de facturación. Los informes y el historial de la organización no se almacenan al eliminar una organización. Se eliminan todos los datos de costes (como el conjunto de datos de Cost Explorer). Se recomienda realizar una exportación completa de todo el historial de facturación.

Para obtener más información, consulte Cost and Usage Reports, Cost Explorer Reports, Savings Plans Reports y Reserved Instance (RI) utilization and coverage.

Eliminar una organización

Utilice el siguiente procedimiento para eliminar una organización que convierte la cuenta de administración anterior en una cuenta independiente Cuenta de AWS que ya no es administrada por él. AWS Organizations

> **Permisos mínimos**
>
> Para eliminar una organización, debe iniciar sesión como usuario o rol en la cuenta de administración y contar con los siguientes permisos:
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para eliminar una organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. Para poder eliminar la organización, primero debe eliminar todas las cuentas de la organización. Para obtener más información, consulte Eliminación de una cuenta miembro de la organización con AWS Organizations.
3. Vaya a la página Configuración y, a continuación, elija Eliminar organización.
4. En el cuadro de diálogo de confirmación Eliminar organización, ingrese el ID de la organización que se muestra en la línea situada encima del cuadro de texto. A continuación, elija Eliminar organización.

> **Important**
>
> Esta operación no cierra la cuenta de administración, pero la devuelve a una Cuenta de AWS independiente. Para cerrar la cuenta, siga los pasos que se indican en Cerrar una cuenta de miembro en una organización con AWS Organizations.

AWS CLI & AWS SDKs

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteOrganization`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más en marcha. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
```

```
    {
        /// <summary>
        /// Initializes the Organizations client and then calls
        /// DeleteOrganizationAsync to delete the organization.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- Para obtener más información sobre la API, consulta DeleteOrganizationla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Eliminación de una organización

En el siguiente ejemplo se muestra cómo eliminar una organización. Para realizar esta operación, debe ser administrador de la cuenta maestra de la organización. En el ejemplo se supone que previamente eliminaste todas las cuentas y políticas de los miembros de la organización: OUs

```
aws organizations delete-organization
```

- Para obtener más información sobre la API, consulte DeleteOrganizationla Referencia de AWS CLI comandos.

Administrar cuentas en una organización con AWS Organizations

An Cuenta de AWSes un contenedor para sus AWS recursos. Usted crea y administra sus AWS recursos en un Cuenta de AWS.

En este tema se describe cómo administrar las cuentas de AWS Organizations.

Temas

- Administrar la cuenta de administración con AWS Organizations
- Administrar las cuentas de los miembros con AWS Organizations
- Administrar las invitaciones a las cuentas con AWS Organizations
- Migración de una cuenta a otra organización con AWS Organizations
- Visualización de los detalles de una cuenta de una organización con AWS Organizations
- Exportación de detalles de una cuenta en una organización con AWS Organizations
- Actualización de contactos alternativos de una cuenta de una organización con AWS Organizations
- Actualización de la información de contacto principal de una cuenta en una organización con AWS Organizations
- Actualización de las Regiones de AWS habilitadas para una cuenta de una organización con AWS Organizations

Administrar la cuenta de administración con AWS Organizations

Una cuenta de administración es la Cuenta de AWS que se utiliza para crear la organización.

La cuenta de administración es el propietario final de la organización y tiene el control final de las políticas de seguridad, infraestructura y finanzas. Esta cuenta tiene el rol de cuenta pagadora y es responsable de todos los cargos acumulados por las cuentas de su organización.

En este tema se describe cómo administrar la cuenta de administración con AWS Organizations.

Temas

- Prácticas recomendadas para la cuenta de administración
- Cierre de una cuenta de administración de la organización

Prácticas recomendadas para la cuenta de administración

Siga estas recomendaciones para ayudar a proteger la seguridad de la cuenta de administración en AWS Organizations. Estas recomendaciones suponen que también se adhiere a las Prácticas recomendadas de utilizar el usuario raíz exclusivamente para aquellas tareas que realmente lo requieran.

Temas

- Limitar quién tiene acceso a la cuenta de administración
- Revisar quién tiene acceso y realizar un seguimiento
- Utilice la cuenta de administración solo para tareas que requieren la cuenta de administración
- Evitar la implementación de cargas de trabajo en la cuenta de administración de la organización
- Delegar responsabilidades fuera de la cuenta de administración para la descentralización

Limitar quién tiene acceso a la cuenta de administración

La cuenta de administración es clave para todas las tareas administrativas mencionadas, como la administración de cuentas, las políticas, la integración con otros AWS servicios, la facturación unificada, etc. Por lo tanto, debe restringir y limitar el acceso a la cuenta de administración solo a los usuarios administradores que necesiten derechos para realizar cambios en la organización.

Revisar quién tiene acceso y realizar un seguimiento

Para asegurarse de mantener el acceso a la cuenta de administración, revise periódicamente el personal de su empresa que tiene acceso a la dirección de correo electrónico, contraseña, MFA y número de teléfono asociados a ella. Alinee su revisión con los procedimientos comerciales existentes. Agregue una revisión mensual o trimestral de esta información para asegurarse de que solo las personas correctas tengan acceso. Asegúrese de que el proceso para recuperar o restablecer el acceso a las credenciales del usuario raíz no dependa de que se complete ninguna persona específica. Todos los procesos deben abordar la posibilidad de que las personas no estén disponibles.

Utilice la cuenta de administración solo para tareas que requieren la cuenta de administración

Se recomienda que utilice la cuenta de administración y sus usuarios y roles para tareas que solo puede realizar esa cuenta. Almacene todos sus AWS recursos Cuentas de AWS en otras partes

de la organización y manténgalos fuera de la cuenta de administración. Una razón importante para mantener los recursos en otras cuentas es que las políticas de control de servicios de SCPs Organizations () no sirven para restringir ningún usuario o rol en la cuenta de administración. Separar los recursos de la cuenta de administración también lo ayudará a comprender los cargos de sus facturas.

Para obtener una lista de las tareas a las que se debe llamar desde la cuenta de administración, consulte Operations you can call from only the organization's management account.

Evitar la implementación de cargas de trabajo en la cuenta de administración de la organización

Las operaciones privilegiadas se pueden realizar dentro de la cuenta de administración de una organización y SCPs no se aplican a la cuenta de administración. Por eso, debe limitar los recursos y datos de la nube que contenga la cuenta de administración únicamente a los que deben administrarse en esta cuenta.

Delegar responsabilidades fuera de la cuenta de administración para la descentralización

Siempre que sea posible, se recomienda delegar responsabilidades y servicios fuera de la cuenta de administración. Proporcione a sus equipos permisos en sus propias cuentas para administrar las necesidades de la organización sin necesidad de acceder a la cuenta de administración. Además, puede registrar varios administradores delegados para los servicios que admiten esta funcionalidad, por ejemplo, AWS Service Catalog para compartir software en toda la organización o AWS CloudFormation StackSets para crear e implementar paquetes.

Para obtener más información, consulte Arquitectura de referencia de seguridad, Organización del AWS entorno mediante varias cuentas y sugerencias sobre cómo registrar las cuentas de los miembros como administradores delegados Servicios de AWS que puedes usar con AWS Organizations para varios servicios. AWS

Para obtener más información sobre la configuración de administradores delegados, consulte Enabling a delegated admin account for AWS Account Management and Administrador delegado para AWS Organizations.

Cierre de una cuenta de administración de la organización

Para cerrar la cuenta de administración de la organización, primero debe quitar o eliminar todas las cuentas de miembro de la organización. Al cerrar la cuenta de administración, también se eliminan la

instancia de AWS Organizations y las políticas que haya creado dentro de esa organización una vez transcurrido el periodo posterior al cierre.

Cierre de la cuenta de administración

Utilice el siguiente procedimiento para cerrar una cuenta de administración.

> **Important**
>
> Antes de cerrar la cuenta de administración, le recomendamos encarecidamente que revise las consideraciones y comprenda el impacto de cerrar una cuenta. Para obtener más información, consulte What you need to know before closing your account y What to expect after you close your account en la Guía de administración de cuentas de AWS .

AWS Management Console

Para cerrar una cuenta de administración desde la página Cuentas

> **Note**
>
> No puede cerrar una cuenta de administración directamente desde la consola de AWS Organizations .

1. Inicie sesión AWS Management Console como usuario raíz de la cuenta de administración que desee cerrar. Si inicia sesión como un rol o usuario de IAM, no puede cerrar una cuenta.
2. Compruebe que no queden cuentas de miembro activas en su organización. Para ello, ve a la AWS Organizations consola. Si tienes una cuenta de miembro que sigue activa, tendrás que seguir las instrucciones que se proporcionan en el paso siguiente Cerrar una cuenta de miembro en una organización con AWS Organizations o Eliminación de una cuenta miembro de su organización antes de hacerlo.
3. En la barra de navegación situada en la esquina superior derecha, elija el nombre o número de cuenta y, a continuación, elija Cuenta.
4. En la página de la cuenta, seleccione el botón Cerrar cuenta. Lea y asegúrese de comprender la guía para el cierre de la cuenta.
5. Pulse el botón Cerrar cuenta para iniciar el proceso de cierre de cuenta.

6. En unos minutos, recibirá un correo electrónico de confirmación de que su cuenta se ha cerrado.

AWS CLI & AWS SDKs

Esta tarea no es compatible con una operación de API de ninguna de las AWS SDKs. AWS CLI Solo puede realizar esta tarea mediante AWS Management Console.

Administrar las cuentas de los miembros con AWS Organizations

Una cuenta de miembro es una Cuenta de AWS, distinta de la cuenta de administración, que forma parte de una organización.

En este tema se describe cómo administrar las cuentas de los miembros con AWS Organizations.

Temas

- Prácticas recomendadas para cuentas de miembros
- Crear una cuenta de miembro en una organización con AWS Organizations
- Acceder a las cuentas de los miembros de una organización con AWS Organizations
- Cerrar una cuenta de miembro en una organización con AWS Organizations
- Protección de cuentas miembro contra el cierre con AWS Organizations
- Eliminación de una cuenta miembro de la organización con AWS Organizations
- Salir de una organización desde una cuenta de miembro con AWS Organizations
- Actualizar la dirección de correo electrónico del usuario raíz de una cuenta de miembro con AWS Organizations

Prácticas recomendadas para cuentas de miembros

Siga estas recomendaciones para proteger la seguridad de las cuentas de los miembros de su organización. Estas recomendaciones suponen que también se adhiere a las Prácticas recomendadas de utilizar el usuario raíz exclusivamente para aquellas tareas que realmente lo requieran.

Temas

- Definir el nombre y los atributos de la cuenta
- Ampliar el entorno y el uso de la cuenta de manera eficiente
- Habilite la administración del acceso raíz para simplificar la administración de las credenciales de los usuarios raíz para las cuentas de los miembros

Definir el nombre y los atributos de la cuenta

En el caso de las cuentas de los miembros, utilice una estructura de nombres y una dirección de correo electrónico que reflejen el uso de la cuenta. Por ejemplo, `Workloads+fooA+dev@domain.com` para `WorkloadsFooADev`, `Workloads+fooB+dev@domain.com` para `WorkloadsFooBDev`. Si ha definido etiquetas personalizadas para su organización, se recomienda que asigne esas etiquetas a las cuentas que reflejen el uso de la cuenta, el centro de costos, el entorno y el proyecto. Esto facilita la identificación, organización y búsqueda de las cuentas.

Ampliar el entorno y el uso de la cuenta de manera eficiente

A medida que vaya escalando, antes de crear cuentas nuevas, asegúrese de que no existan ya cuentas para necesidades similares, a fin de evitar duplicaciones innecesarias. Cuentas de AWS debe basarse en requisitos de acceso comunes. Si tiene previsto volver a utilizar las cuentas, como una cuenta de entorno aislado o una cuenta equivalente, se recomienda que elimine las cargas de trabajo o los recursos innecesarios de las cuentas, pero que guarde las cuentas para utilizarlas en el futuro.

Antes de cerrar cuentas, tenga en cuenta que están sujetas a los límites de cuota de cierre de cuentas. Para obtener más información, consulte Cuotas y límites de servicio para AWS Organizations. Considere la posibilidad de implementar un proceso de limpieza para reutilizar las cuentas en lugar de cerrarlas y crear otras nuevas cuando sea posible. De esta forma, evitará incurrir en costes derivados de la gestión de los recursos y de alcanzar los límites de las CloseAccount API.

Habilite la administración del acceso raíz para simplificar la administración de las credenciales de los usuarios raíz para las cuentas de los miembros

Le recomendamos que habilite la administración del acceso raíz para ayudarlo a monitorear y eliminar las credenciales de los usuarios raíz de las cuentas de los miembros. La administración del acceso raíz impide la recuperación de las credenciales de los usuarios raíz, lo que mejora la seguridad de las cuentas en su organización.

- Elimine las credenciales de usuario raíz de las cuentas de los miembros para evitar que el usuario raíz inicie sesión. Esto también impide que las cuentas de los miembros se recuperen del usuario root.
- Suponga que tiene una sesión privilegiada para realizar las siguientes tareas en las cuentas de los miembros:
  - Elimine una política de bucket mal configurada que impida a todas las entidades principales acceder a un bucket de Amazon S3.
  - Elimine una política basada en recursos de Amazon Simple Queue Service que impida a todas las entidades principales acceder a una cola de Amazon SQS.
  - Permita que la cuenta de un miembro recupere sus credenciales de usuario raíz. La persona con acceso a la bandeja de entrada de correo electrónico del usuario raíz de la cuenta de miembro puede restablecer la contraseña del usuario raíz e iniciar sesión como usuario raíz de la cuenta de miembro.

Una vez que se habilita la administración del acceso raíz, las cuentas de los secure-by-default miembros recién creadas no tienen credenciales de usuario raíz, lo que elimina la necesidad de seguridad adicional, como el MFA después del aprovisionamiento.

Para obtener más información, consulte Centralizar las credenciales de los usuarios raíz de las cuentas de los miembros en la Guía del AWS Identity and Access Management usuario.

Utilice una SCP para restringir lo que puede hacer el usuario raíz en tus cuentas de miembro

Se recomienda crear una política de control de servicios (SCP) en la organización y adjuntarla al nodo raíz de la organización para que se aplique a todas las cuentas de miembros. Para obtener más información, consulte Proteja las credenciales de usuario raíz de su cuenta de Organizations.

Puede denegar todas las acciones raíz, excepto una acción específica exclusiva para usuarios raíz que debe realizar en su cuenta de miembro. Por ejemplo, el siguiente SCP impide que el usuario raíz de cualquier cuenta miembro realice llamadas a la API de AWS servicio, excepto «actualizar una política de bucket de S3 que estaba mal configurada y niega el acceso a todos los principales» (una de las acciones que requiere credenciales raíz). Para obtener más información, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

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

    "Statement": [
```

```
        {

            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
"StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }

        }

    ]
}
```

En la mayoría de las circunstancias, un rol de AWS Identity and Access Management (IAM) puede realizar cualquier tarea administrativa en la cuenta de miembro que tiene permisos de administrador pertinentes. Cualquiera de estos roles debe tener controles adecuados implementados que limiten, registren y supervisen la actividad.

Crear una cuenta de miembro en una organización con AWS Organizations

En este tema se describe cómo crear Cuentas de AWS dentro de su organización en AWS Organizations. Para obtener información sobre la creación de un single Cuenta de AWS, consulte el Centro de recursos de introducción.

Consideraciones antes de crear una cuenta de miembro

Organizations crea automáticamente el IAM rol **`OrganizationAccountAccessRole`** para la cuenta del miembro

Al crear una cuenta de miembro en su organización, Organizations crea automáticamente el IAM rol `OrganizationAccountAccessRole` en la cuenta de miembro que permite a los usuarios y roles de la cuenta de administración ejercer un control administrativo total sobre la cuenta de miembro. Toda cuenta adicional asociada a la misma política administrada se actualizará automáticamente cada vez que se actualice la política. Este rol está sujeto a cualquier política de control de servicios (SCPs) que se aplique a la cuenta del miembro.

Organizations crea automáticamente el rol vinculado al servicio **`AWSServiceRoleForOrganizations`** para la cuenta del miembro

Cuando crea una cuenta de miembro en su organización, Organizations crea automáticamente un rol vinculado al servicio `AWSServiceRoleForOrganizations` en la cuenta de miembro que permite la integración con servicios de AWS seleccionados. Debe configurar los demás servicios para permitir la integración. Para obtener más información, consulte AWS Organizations y funciones vinculadas al servicio.

Las cuentas de miembro pueden requerir información adicional para funcionar como una cuenta independiente

AWS no recopila automáticamente toda la información necesaria para que la cuenta de un miembro funcione como una cuenta independiente. Si alguna vez necesita eliminar la cuenta de miembro de la organización y convertirla en cuenta independiente, debe proporcionar la información solicitada para la cuenta antes de poder eliminarla. Para obtener más información, consulte Salir de una organización desde una cuenta de miembro con AWS Organizations.

Las cuentas de miembro solo se pueden crear en la raíz de una organización

Las cuentas de los miembros de una organización solo se pueden crear en la raíz de la organización y no en ninguna otra unidad organizativa (OUs). Después de crear la raíz de una cuenta de miembro de una organización, puedes moverla de una organización a otraOUs. Para obtener más información, consulte Mover cuentas a una unidad organizativa (OU) o entre la raíz y las unidades organizativas con AWS Organizations.

Las políticas asociadas al nodo raíz se aplican inmediatamente

Si tiene política asociadas al nodo raíz del árbol de la OU, dichas políticas se aplican inmediatamente a todos los usuarios y roles de la cuenta creada.

Si has activado la confianza de servicio para otro AWS servicio de tu organización, ese servicio de confianza puede crear funciones vinculadas al servicio o realizar acciones en cualquier cuenta de miembro de la organización, incluida la cuenta que hayas creado.

Las cuentas de los miembros de las organizaciones administradas por AWS Control Tower deben crearse en AWS Control Tower

Si su organización está administrada por AWS Control Tower, cree sus cuentas de miembro utilizando la fábrica de AWS Control Tower cuentas de la AWS Control Tower consola o utilizando el AWS Control Tower APIs. Si creas una cuenta de miembro en Organizations cuando la organización está gestionada por la organización AWS Control Tower, la cuenta no se inscribirá en ella AWS Control Tower. Para obtener más información, consulte Referencia del tipo de recurso fuera de AWS Control Tower en la Guía del usuario AWS Control Tower .

Las cuentas de miembro deben optar por recibir correos electrónicos de marketing

Las cuentas de miembros que crees como parte de una organización no se suscriben automáticamente a los correos electrónicos de AWS marketing. Para suscribir sus cuentas para recibir correos electrónicos de marketing, consulte https://pages.awscloud.com/communication-preferences.

Creación de una cuenta de miembro

Luego de iniciar sesión en la cuenta de administración de la organización, puede crear cuentas que se conviertan en cuentas de miembro de su organización.

Al crear una cuenta mediante el siguiente procedimiento, copia AWS Organizations automáticamente la siguiente información de contacto principal de la cuenta de administración a la nueva cuenta de miembro:

- Número de teléfono
- Nombre de la empresa
- Sitio web URL
- Dirección

Organizations también copia el idioma de comunicación y la información de Marketplace (en algunos casos, el proveedor de la cuenta Regiones de AWS) de la cuenta de administración.

> **Permisos mínimos**
>
> Para crear una cuenta de miembro en su organización, debe contar con los permisos siguientes:

- `organizations:CreateAccount`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `iam:CreateServiceLinkedRole` (concedido a la entidad principal `organizations.amazonaws.com` para permitir la creación del rol vinculado al servicio requerido en las cuentas de miembro).

AWS Management Console

Para crear una Cuenta de AWS que forme parte automáticamente de su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, elija Agregar un Cuenta de AWS.
3. En la página Agregar una Cuenta de AWS, elija Crear una Cuenta de AWS (se elige de forma predeterminada).
4. En la página Crear una Cuenta de AWS, para Nombre de Cuenta de AWS ingrese el nombre que desee asignar a la cuenta. Este nombre le ayuda a distinguir la cuenta de todas las demás de la organización y es independiente del alias de IAM o del nombre de correo electrónico del propietario.
5. Para Dirección de correo electrónico del propietario de la cuenta, ingrese la dirección de correo electrónico del propietario de la cuenta. Esta dirección de correo electrónico no puede estar asociada ya Cuenta de AWS a otra porque se convierte en la credencial del nombre de usuario del usuario raíz de la cuenta.
6. (Opcional) Especifique el nombre que va a asignar a la función de IAM que se crea automáticamente en la nueva cuenta. Este rol concede a la cuenta de administración de la organización el permiso para tener acceso a la cuenta de miembro que acaba de crear. Si no especifica un nombre, AWS Organizations asigna al rol un nombre predeterminado de`OrganizationAccountAccessRole`. Recomendamos que utilice el nombre predeterminado en todas sus cuentas para mayor coherencia.

> **Important**
>
> Recuerde este nombre de rol. Lo necesitará más adelante para conceder acceso a la nueva cuenta a los usuarios y roles de la cuenta de administración.

7. (Opcional) En la sección Etiquetas, agregue una o varias etiquetas con Agregar etiqueta y a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede asociar hasta 50 etiquetas a una cuenta.
8. Seleccione Crear Cuenta de AWS.

   - Si aparece un error que indica que ha superado la cuota de cuenta de la organización, consulte Obtengo un mensaje de "cuota superada" cuando intento agregar una cuenta a mi organización.
   - Si obtiene un error que indica que no puede añadir una cuenta porque la organización todavía se está inicializando, espere una hora y vuelva a intentarlo.
   - También puede consultar el AWS CloudTrail registro para obtener información sobre si la creación de la cuenta se ha realizado correctamente. Para obtener más información, consulte Inicio de sesión y supervisión AWS Organizations.
   - Si el error persiste, póngase en contacto con AWS Support.

   La página Cuentas de AWS aparece, con su cuenta nueva agregada a la lista.
9. Ahora que la cuenta existe y tiene un IAM rol que otorga acceso de administrador a los usuarios de la cuenta de administración, puede acceder a la cuenta siguiendo los pasos que se indicanAcceder a las cuentas de los miembros de una organización con AWS Organizations.

AWS CLI & AWS SDKs

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateAccount`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var accountName = "ExampleAccount";
        var email = "someone@example.com";

        var request = new CreateAccountRequest
        {
            AccountName = accountName,
            Email = email,
        };

        var response = await client.CreateAccountAsync(request);
        var status = response.CreateAccountStatus;

        Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
    }
```

```
    }
```

- Para API obtener más información, consulte CreateAccountla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Creación de una cuenta de miembro que forme parte automáticamente de la organización

En el siguiente ejemplo se muestra cómo crear una cuenta de miembro en una organización. La cuenta de miembro se configura con el nombre Production Account y la dirección de correo electrónico susan@example.com. Organizations crea automáticamente un IAM rol con el nombre predeterminado de OrganizationAccountAccessRole porque el roleName parámetro no está especificado. Además, la configuración que permite a IAM los usuarios o roles con permisos suficientes acceder a los datos de facturación de la cuenta se establece en el valor predeterminado de ALLOW porque el IamUserAccessToBilling parámetro no está especificado. Organizations envía automáticamente a Susan un correo electrónico de AWS bienvenida a:

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

La salida incluye un objeto de solicitud que muestra que el estado ahora es `IN_PROGRESS`:

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Más adelante, puede consultar el estado actual de la solicitud proporcionando el valor de respuesta Id al describe-create-account-status comando como valor del create-account-request-id parámetro.

Para obtener más información, consulte Crear una AWS cuenta en su organización en la Guía del AWS usuario de Organizations.

- Para API obtener más información, consulte CreateAccountla Referencia de AWS CLI comandos.

Acceder a las cuentas de los miembros de una organización con AWS Organizations

Al crear una cuenta en la organización, además del usuario raíz,AWS Organizations crea automáticamente un rol de IAM con el nombre predeterminado `OrganizationAccountAccessRole`. Puedes especificar un nombre diferente al crearla, pero te recomendamos que le pongas un nombre uniforme en todas tus cuentas. AWS Organizations no crea ningún otro usuario o rol.

Para tener acceso a las cuentas de su organización, debe utilizar uno de los siguientes métodos:

Uso del usuario raíz (no se recomienda para las tareas diarias)

Al crear una nueva cuenta de miembro en su organización, la cuenta no tiene credenciales de usuario raíz de forma predeterminada. Las cuentas de miembros no pueden iniciar sesión con su usuario raíz ni recuperar la contraseña de su usuario raíz a menos que la recuperación de cuentas esté habilitada.

Puede centralizar el acceso raíz a las cuentas de los miembros para eliminar las credenciales de los usuarios raíz de las cuentas de los miembros existentes en su organización. Al eliminar las credenciales del usuario raíz, se eliminan la contraseña del usuario raíz, las claves de acceso y los certificados de firma y se desactiva la autenticación multifactor (MFA). Estas cuentas de miembros no tienen credenciales de usuario raíz, no pueden iniciar sesión como usuarios raíz y no pueden recuperar la contraseña del usuario raíz. Las cuentas nuevas que cree en Organizations no tienen credenciales de usuario raíz de forma predeterminada.

Póngase en contacto con el administrador si necesita realizar una tarea que requiera credenciales de usuario raíz en una cuenta de miembro en la que no estén presentes las credenciales de usuario raíz.

Para acceder a su cuenta de miembro como usuario root, debe realizar el proceso de recuperación de la contraseña. Para más información, consulte He olvidado la contraseña del usuario raíz de mi cuenta de Cuenta de AWS en la Guía del usuario de Inicio de sesión en AWS .

Si debe acceder a la cuenta de un miembro con el usuario root, siga estas prácticas recomendadas:

- No utilices el usuario root para acceder a tu cuenta, excepto para crear otros usuarios y roles con permisos más limitados. A continuación, inicie sesión como uno de los usuarios o roles.
- Habilite la autenticación multifactor (MFA) en el usuario raíz. Restablezca la contraseña y asigne un dispositivo MFA al usuario raíz.

Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM. Para obtener más recomendaciones de seguridad para los usuarios root, consulte las mejores prácticas para los usuarios root Cuenta de AWS en la Guía del usuario de IAM.

Uso de un acceso de confianza para IAM Identity Center

Utilice AWS IAM Identity Centery habilite el acceso confiable al Centro de Identidad de IAM con. AWS Organizations Esto permite a los usuarios iniciar sesión en el portal de AWS acceso con sus credenciales corporativas y acceder a los recursos de la cuenta de administración o las cuentas de los miembros que tengan asignadas.

Para obtener más información, consulte Multi-account permissions (Permisos de varias cuentas) en la Guía del usuario de AWS IAM Identity Center . Para obtener más información acerca de cómo configurar el acceso de confianza para IAM Identity Center, consulte AWS IAM Identity Center y AWS Organizations.

Uso del rol de IAM **`OrganizationAccountAccessRole`**

Si crea una cuenta con las herramientas que se proporcionan como parte de ella AWS Organizations, puede acceder a la cuenta mediante el rol preconfigurado denominado `OrganizationAccountAccessRole` que existe en todas las cuentas nuevas que cree de esta manera. Para obtener más información, consulte Acceso a una cuenta miembro que tiene OrganizationAccountAccessRole con AWS Organizations.

Si invita a una cuenta existente a que se una a su organización y la cuenta acepta la invitación, puede elegir crear un rol de IAM que permita a la cuenta de administración tener acceso a la cuenta de miembro invitada. Se pretende que este rol sea idéntico al rol que se añade automáticamente a una cuenta que se crea con AWS Organizations.

Para crear esta función, consulte Creación de OrganizationAccountAccessRole en una cuenta miembro invitada con AWS Organizations.

Después de crear la función, puede tener acceso a él siguiendo los pasos de Acceso a una cuenta miembro que tiene OrganizationAccountAccessRole con AWS Organizations.

> **Permisos mínimos**
>
> Para acceder y Cuenta de AWS desde cualquier otra cuenta de su organización, debe tener el siguiente permiso:
>
> - `sts:AssumeRole` - El elemento `Resource` debe estar establecido en un asterisco (*) o en el ID de la cuenta con el número de la cuenta con la que el usuario necesita obtener acceso a la nueva cuenta de miembro.

Temas

- Creación de OrganizationAccountAccessRole en una cuenta miembro invitada con AWS Organizations
- Acceso a una cuenta miembro que tiene OrganizationAccountAccessRole con AWS Organizations

Creación de OrganizationAccountAccessRole en una cuenta miembro invitada con AWS Organizations

De forma predeterminada, si crea una cuenta miembro como parte de su organización, AWS crea automáticamente un rol en la cuenta que concede permisos de administrador a los usuarios de IAM en la cuenta maestra. De forma predeterminada, este rol se denomina `OrganizationAccountAccessRole`. Para obtener más información, consulte Acceso a una cuenta miembro que tiene OrganizationAccountAccessRole con AWS Organizations.

Sin embargo, a las cuentas miembro a las que invite a unirse a su organización no se les crea automáticamente un rol de administrador. Tiene que hacerlo manualmente, tal y como se muestra en el siguiente procedimiento. Lo que este procedimiento hace básicamente es duplicar el rol configurado de forma automática para las cuentas creadas. Le recomendamos que utilice el mismo nombre, `OrganizationAccountAccessRole`, para los roles creados manualmente en aras de la coherencia y para que sea fácil de recordar.

AWS Management Console

Para crear un rol de administrador de AWS Organizations en una cuenta miembro

1. Inicie sesión en la consola de IAM en https://console.aws.amazon.com/iam/. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de miembro. El usuario o el rol deben tener permiso para crear roles y políticas de IAM.
2. En la consola de IAM, vaya a Roles y, a continuación, seleccione Crear rol.
3. Elija Cuenta de AWS y, a continuación, seleccione Otra Cuenta de AWS.
4. Ingrese el número de ID de 12 dígitos de la cuenta maestra a la que desea conceder acceso de administrador. En Opciones, tenga en cuenta lo siguiente:
   - Para este rol, dado que las cuentas son internas a su empresa, no debe seleccionar Require external ID. Para obtener más información acerca de la opción de ID externo, consulte ¿Cuándo debería utilizar un ID externo? en la Guía del usuario de IAM.
   - Si ha habilitado y configurado MFA, puede elegir que se requiera autenticación mediante un dispositivo MFA. Para obtener más información sobre MFA, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.
5. Elija Siguiente.
6. En la página Agregar permisos, elija la política administrada por AWS denominada `AdministratorAccess` y, a continuación, seleccione Siguiente.
7. En la página Asignar nombre, revisar y crear, especifique un nombre del rol y una descripción opcional. Le recomendamos que utilice `OrganizationAccountAccessRole` para mantener la coherencia con el nombre predeterminado asignado al rol en las cuentas nuevas. Para confirmar los cambios, elija Crear rol.
8. Su nuevo rol aparecerá en la lista de roles disponibles. Seleccione el nombre del nuevo rol para ver los detalles y preste especial atención a la URL de enlace facilitada. Entregue esta URL a los usuarios de la cuenta miembro que necesitan tener acceso al rol. Además, anote el Role ARN (ARN de rol), ya que lo necesitará en el paso 15.
9. Inicie sesión en la consola de IAM en https://console.aws.amazon.com/iam/. Esta vez, inicie sesión como usuario de la cuenta de administración con permisos para crear políticas y asignarlas a los usuarios o grupos.
10. Vaya a Políticas y, a continuación, seleccione Crear política.
11. En Service, seleccione STS.

12. En Actions (Acciones), comience a escribir **`AssumeRole`** en el cuadro Filter (Filtro) y marque la casilla cuando aparezca.
13. Seleccione Recursos, asegúrese de que Específico esté seleccionado y seleccione Agregar ARN.
14. Escriba su número de ID de cuenta miembro de AWS y, a continuación, el nombre del rol que haya creado anteriormente en los pasos 1-8. Seleccione Agregar ARN.
15. Si está concediendo un permiso para asumir la función en varias cuentas miembro, repita los pasos 14 y 15 para cada cuenta.
16. Elija Siguiente.
17. En la página Revisar y crear, ingrese un nombre para la nueva política y, a continuación, seleccione Crear política para guardar los cambios.
18. Elija Grupos de usuarios en el panel de navegación y, a continuación, elija el nombre del grupo (no la casilla) que desea utilizar para delegar la administración de la cuenta miembro.
19. Elija la pestaña Permisos.
20. Elija Agregar permisos, luego Asociar políticas y, a continuación, seleccione la política que creó en los pasos 11-18.

Los usuarios que sean miembros del grupo seleccionado ahora pueden utilizar las direcciones URL que anotó en el paso 9 para obtener acceso al rol de cada cuenta miembro. Pueden obtener acceso a estas cuentas miembro de la misma forma que lo harían si tuvieran acceso a una cuenta que usted haya creado en la organización. Para obtener más información sobre el uso del rol para administrar una cuenta miembro, consulte Acceso a una cuenta miembro que tiene OrganizationAccountAccessRole con AWS Organizations.

Acceso a una cuenta miembro que tiene OrganizationAccountAccessRole con AWS Organizations

Cuando crea una cuenta miembro con la consola de AWS Organizations, AWS Organizations crea automáticamente un rol de IAM denominado `OrganizationAccountAccessRole` en la cuenta. Este rol tiene permisos administrativos completos en la cuenta miembro. El ámbito de acceso de este rol incluye todas las entidades principales de la cuenta de administración, de modo que el rol esté configurado para conceder ese acceso a la cuenta de administración de la organización.

Puede crear un rol idéntico para una cuenta miembro invitada siguiendo los pasos que se indican en Creación de OrganizationAccountAccessRole en una cuenta miembro invitada con AWS Organizations.

Para utilizar este rol para tener acceso a la cuenta miembro, debe iniciar sesión como usuario de la cuenta de administración con permisos para asumir el rol. Para configurar estos permisos, siga este procedimiento. Le recomendamos que conceda permisos a los grupos en lugar de a los usuarios para simplificar el mantenimiento.

AWS Management Console

Para conceder permisos a los miembros de un grupo de IAM en la cuenta de administración para tener acceso al rol

1. Inicie sesión en la consola de IAM en https://console.aws.amazon.com/iam/ con un usuario que tenga permisos de administrador en la cuenta de administración. Esto es necesario para delegar permisos al grupo de IAM cuyos usuarios vayan a tener acceso al rol en la cuenta miembro.
2. Comience creando la política administrada que necesitará más tarde en ???.

   En el panel de navegación, elija Policies (Políticas) y, a continuación, seleccione Create policy (Crear política).
3. En la pestaña Editor visual, elija Elegir un servicio, ingrese **`STS`** en el cuadro de búsqueda para filtrar la lista y, a continuación, elija la opción STS.
4. En la sección Acciones, ingrese **`assume`** en el cuadro de búsqueda para filtrar la lista y, a continuación, elija la opción AssumeRole.
5. En la sección Recursos, elija Específico y, a continuación, seleccione Agregar ARN
6. En la sección Especificar ARN, elija Otra cuenta para Recurso en.
7. Ingrese el ID de la cuenta miembro que acaba de crear
8. En el campo Nombre del rol de recurso con ruta, ingrese el nombre del rol que creó en la sección anterior (se recomienda asignarle el nombre `OrganizationAccountAccessRole`).
9. Elija Agregar ARN cuando el cuadro de diálogo muestre el ARN correcto.
10. (Opcional) Si desea requerir Multi-Factor Authentication (MFA) o restringir el acceso al rol desde un intervalo de direcciones IP especificado, expanda la sección Condiciones de solicitud y seleccione las opciones que desee aplicar.
11. Elija Siguiente.
12. En la página Revisar y crear, ingrese un nombre para la nueva política. Por ejemplo: **`GrantAccessToOrganizationAccountAccessRole`**. También puede agregar una descripción opcional.

13. Elija Crear política para guardar la nueva política administrada.
14. Ahora que tiene la política disponible, puede asociarla a un grupo.

    En el panel de navegación, elija Gropos de usuarios y, a continuación, elija el nombre del grupo (no la casilla) cuyos miembros desea que asuman el rol en la cuenta miembro. Si es necesario, puede crear un grupo nuevo.
15. Elija la pestaña Permisos, elija Agregar permisos y luego, Asociar políticas.
16. (Opcional) En el cuadro Buscar puede comenzar a escribir el nombre de la política para filtrar la lista hasta que pueda ver el nombre de la política que acaba de crear en Step 2 mediante Step 13. También puede filtrar todas las políticas administradas de AWS eligiendo Todos los tipos y, a continuación, eligiendo Administrada por cliente.
17. Marque la casilla situada junto a la política y, a continuación, elija Asociar políticas.

Los usuarios de IAM que sean miembros del grupo ahora tendrán permisos para cambiar el nuevo rol en la consola de AWS Organizations siguiendo el procedimiento que se detalla a continuación.

AWS Management Console

Para cambiar al rol de la cuenta miembro

Cuando se utilice el rol, el usuario tendrá permisos de administrador en la nueva cuenta miembro. Indique a los usuarios de IAM que sean miembros del grupo que hagan lo siguiente para cambiar al nuevo rol.

1. En la esquina superior derecha de la consola de AWS Organizations, elija el enlace que contiene el nombre de inicio de sesión y, a continuación, elija Switch Role (Cambiar rol).
2. Escriba el número de ID de la cuenta y el nombre del rol proporcionados por el administrador.
3. En Display Name (Nombre de visualización), escriba el texto que desee mostrar en la barra de navegación en la esquina superior derecha en lugar de su nombre de usuario mientras utiliza la función. Si lo desea, puede elegir un color.
4. Elija Switch Role. Ahora, todas las acciones que realice se harán con los permisos concedidos a la función a la que ha cambiado. Ya no tendrá los permisos asociados a su usuario de IAM original hasta que cambie otra vez a este rol.
5. Cuando haya terminado de realizar acciones que requieran los permisos del rol, puede volver a su usuario de IAM normal. Elija el nombre de la función en la esquina superior

derecha, independientemente de lo que haya especificado como Display Name (Nombre de visualización). A continuación, elija Back to ***UserName*** (Volver a UserName).

Cerrar una cuenta de miembro en una organización con AWS Organizations

Si ya no necesita una cuenta de miembro en su organización, puede cerrarla desde la consola de AWS Organizations con las instrucciones de este tema. Solo puedes cerrar la cuenta de un miembro mediante la AWS Organizations consola si tu organización está en el modo Todas las funciones.

También puedes cerrar una Cuenta de AWS directamente desde la página de la cuenta AWS Management Console después de iniciar sesión como usuario root. Para step-by-step obtener instrucciones, consulta Cerrar un Cuenta de AWS en la Guía de administración de AWS cuentas.

Para cerrar una cuenta de administración, consulte Cierre de una cuenta de administración de la organización.

Cierre de una cuenta de miembro

Cuando inicia sesión en la cuenta de administración de la organización, puede cerrar las cuentas de miembro que pertenecen a su organización. Para ello, siga los pasos que se describen a continuación.

> **Important**
>
> Antes de cerrar su cuenta de miembro, le recomendamos encarecidamente que revise las consideraciones y comprenda el impacto de cerrar una cuenta. Para obtener más información, consulte What you need to know before closing your account y What to expect after you close your account en la Guía de administración de cuentas de AWS .

AWS Management Console

Para cerrar la cuenta de un miembro desde la AWS Organizations consola

1. Inicie sesión en la consola de AWS Organizations.
2. En la página Cuentas de AWS, busque y elija el nombre de la cuenta de miembro que desea cerrar. Puede navegar por la jerarquía de unidades organizativas o ver una lista plana de cuentas sin la estructura de unidad organizativa.

3. Elija Close (Cerrar) junto al nombre de la cuenta en la parte superior de la página. Esta opción solo está disponible cuando una AWS organización está en el modo Todas las funciones.

> **Note**
>
> Si su organización utiliza el modo de facturación unificada, no podrá ver el botón Cerrar en la consola. Para cerrar una cuenta en el modo de facturación unificada, inicie sesión en la cuenta que desee cerrar como usuario raíz. En la página Cuentas, pulsa el botón Cerrar cuenta, introduce tu ID de cuenta y, a continuación, pulsa el botón Cerrar cuenta.

4. Lea y asegúrese de comprender la guía para el cierre de la cuenta.
5. Ingrese el ID de la cuenta de miembro y, a continuación, elija Cerrar cuenta.

> **Note**
>
> Cualquier cuenta de miembro que cierre mostrará una etiqueta `SUSPENDED` junto al nombre de la cuenta en la consola de AWS Organizations hasta 90 días después de la fecha de cierre original. Transcurridos 90 días, la cuenta de miembro dejará de mostrarse en AWS Organizations.

Para cerrar una cuenta de miembro desde la página Cuentas

Si lo desea, puede cerrar la cuenta de un AWS miembro directamente desde la página Cuentas del AWS Management Console. Para obtener step-by-step orientación, sigue las instrucciones de Cerrar y de Cuenta de AWS la Guía de administración de AWS cuentas.

AWS CLI & AWS SDKs

Para cerrar una Cuenta de AWS

Puede utilizar uno de los siguientes comandos para cerrar una cuenta de AWS :

- AWS CLI: close-account

```
$ aws organizations close-account \
    --account-id 123456789012
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS SDKs: CloseAccount

Protección de cuentas miembro contra el cierre con AWS Organizations

Si desea proteger una cuenta miembro de un cierre accidental, puede crear una política de IAM para especificar qué cuentas están exentas de cierre. No se puede cerrar ninguna cuenta de miembro que esté protegida con estas políticas. Esto no se puede lograr con una SCP, porque no afecta a las entidades principales en la cuenta de administración.

Puede crear una política de IAM que niegue el cierre de cuentas de dos formas:

- Haga una lista explícita de cada cuenta que desea proteger en la política mediante la inclusión del `arn` en el elemento `Resource`. Para ver un ejemplo, consulte Evitar que las cuentas miembro enumeradas en esta política se cierren.
- Etiquete cuentas individuales para evitar que se cierren. Utilice la clave de condición global de etiqueta `aws:ResourceTag` en la política para evitar que se cierre cualquier cuenta con esta etiqueta. Para obtener información sobre cómo etiquetar una cuenta, consulte Etiquetado de los recursos de Organizations. Para ver un ejemplo, consulte Evitar que las cuentas miembro con etiquetas se cierren .

Ejemplos de políticas de IAM que impiden los cierres de las cuentas miembro

Los siguientes ejemplos de código muestran dos métodos diferentes que puede utilizar para impedir que las cuentas miembro cierren sus cuentas.

Evitar que las cuentas miembro con etiquetas se cierren

Puede adjuntar la siguiente política a una identidad en su cuenta de administración. Esta política impide que las entidades principales de la cuenta de administración cierren cualquier cuenta de miembro etiquetada con la clave de condición global de etiqueta `aws:ResourceTag`, la clave `AccountType` y el valor de etiqueta `Critical`.

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

```
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

Evitar que las cuentas miembro enumeradas en esta política se cierren

Puede adjuntar la siguiente política a una identidad en su cuenta de administración. Esta política impide que las entidades principales de la cuenta de administración cierren las cuentas miembro especificadas de forma explícita en el elemento `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

Eliminación de una cuenta miembro de la organización con AWS Organizations

Al eliminar una cuenta de miembro, no se cierra la cuenta, sino que se elimina la cuenta de miembro de la organización. La cuenta de miembro anterior pasa a ser una Cuenta de AWS independiente que AWS Organizations ya no administra.

Posteriormente, la cuenta ya no estará sujeta a ninguna política y será responsable del pago de sus propias facturas. A la cuenta de administración de la organización ya no se le cobrará ningún gasto acumulado en la cuenta una vez que se haya retirado de la organización.

Consideraciones

Los roles de acceso de IAM creados por la cuenta de administración no se eliminan automáticamente

Cuando elimina una cuenta miembro de la organización, no se eliminan automáticamente los roles de IAM que se hayan creado para permitir el acceso de la cuenta de administración de la organización. Si desea eliminar este acceso desde la cuenta de administración anterior de la organización, debe eliminar manualmente el rol de IAM. Para obtener información acerca de cómo eliminar un rol, consulte Eliminación de roles o perfiles de instancia en la Guía del usuario de IAM.

Puede eliminar una cuenta de la organización solo si la cuenta tiene la información que necesita para funcionar como cuenta independiente

Puede eliminar una cuenta de la organización solo si la cuenta tiene la información que necesita para funcionar como cuenta independiente. Cuando se crea una cuenta en una organización con la consola AWS Organizations , la API o los comandos de AWS CLI, no se recopila automáticamente toda la información necesaria para las cuentas independientes.

Por cada cuenta que desee convertir en independiente, deberá elegir un plan de soporte, proporcionar y verificar la información de contacto necesaria y proporcionar un método de pago. AWS utiliza el método de pago para cobrar cualquier actividad de AWS facturable (no AWS del nivel gratuito) que se produzca mientras la cuenta no esté asociada a una organización. Para eliminar una cuenta que aún no cuenta con esta información, siga los pasos que se indican enSalir de una organización desde una cuenta de miembro con AWS Organizations.

Debe esperar al menos siete días después de que se creara la cuenta

Para eliminar una cuenta que creó en la organización, debe esperar al menos siete días después de que se creó la cuenta. Las cuentas invitadas no están sujetas a este período de espera.

El propietario de la cuenta que abandona la organización pasa a ser responsable de todos los nuevos costos acumulados

En el momento en que la cuenta abandona con éxito la organización, el propietario de la Cuenta de AWS se hace responsable de todos los nuevos costos AWS acumulados, y se utiliza el método de pago de la cuenta. La cuenta de gestión de la organización ya no es responsable.

La cuenta no puede ser una cuenta de administrador delegado para cualquier servicio de AWS habilitado para la organización

La cuenta que desea eliminar no debe ser una cuenta de administrador delegada para cualquier servicio AWS habilitado para su organización. Si la cuenta es un administrador delegado, primero debe cambiar la cuenta de administrador delegada a otra cuenta que quede en la organización. Para obtener más información acerca de cómo deshabilitar o cambiar la cuenta de administrador delegado para un servicio de AWS, consulte la documentación correspondiente a dicho servicio.

La cuenta ya no tiene acceso a los datos de costo y uso

Si una cuenta miembro deja una organización, esa cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización. Sin embargo, la cuenta de administración de la organización puede seguir obteniendo acceso a los datos. Si la cuenta se vuelve a unir a la organización, la cuenta puede obtener de nuevo acceso a esos datos.

Se eliminan las etiquetas adjuntas a la cuenta

Cuando una cuenta de miembro abandona una organización, se eliminan todas las etiquetas asociadas a la cuenta.

Las entidades principales de la cuenta ya no se verán afectadas por ninguna política de la organización

Las entidades principales de la cuenta ya no se verán afectadas por ninguna política que se aplique en la organización. Esto significa que las restricciones impuestas por esas SCP ya no existen, y que los usuarios y los roles de la cuenta podrían tener más permisos que antes. Otros tipos de políticas de organización ya no se pueden aplicar ni procesar.

La cuenta ya no está cubierta por los acuerdos de la organización

Si una cuenta miembro se elimina de una organización, dicha cuenta miembro ya no estará cubierta por los acuerdos de la organización. Los administradores de cuentas de administración deben comunicar esto a las cuentas miembro antes de eliminar las cuentas miembro de la organización, para que dichas cuentas miembro puedan formalizar nuevos acuerdos si es necesario. Puede consultar una lista de los acuerdos activos de la organización en la consola AWS Artifact en la página Acuerdos de Organization AWS Artifact.

La integración con otros servicios podría estar deshabilitada

La integración con otros servicios podría estar deshabilitada. Si elimina una cuenta de una organización que tiene integración con una AWS, los usuarios de esa cuenta ya no podrán utilizar dicho servicio.

Eliminación de una cuenta miembro de su organización

Cuando inicie sesión en la cuenta de administración de la organización, puede quitar las cuentas miembro de la organización que ya no necesite. Para ello, complete el procedimiento siguiente. Este procedimiento se aplica únicamente a las cuentas de miembro. Para eliminar la cuenta de administración, debe eliminar la organización.

Permisos mínimos

Para eliminar una o varias cuentas de miembro de la organización, debe iniciar sesión como usuario o rol en la cuenta de administración con los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:RemoveAccountFromOrganization`

Si decidió iniciar sesión como usuario o rol en una cuenta de miembro en el paso 5, ese usuario o rol debe tener los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:LeaveOrganization`; tenga en cuenta que el administrador de la organización puede aplicar una política a la cuenta que elimine este permiso, lo que le impedirá eliminar la cuenta de la organización.
- Si inicia sesión como un usuario de IAM y la cuenta tiene información de pago faltante, el usuario debe tener permisos de `aws-portal:ModifyBilling` y de `aws-portal:ModifyPaymentMethods` (si la cuenta aún no ha migrado a permisos específicos) O permisos de `payments:CreatePaymentInstrument` y de `payments:UpdatePaymentPreferences` (si la cuenta ha migrado a permisos específicos). Además, la cuenta miembro debe tener habilitado el acceso del usuario de IAM a la facturación. Si no está habilitado, consulte Activación del acceso a la consola Billing and Cost Management en la Guía del usuario de AWS Billing.

AWS Management Console

Para eliminar una cuenta miembro de su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la pestaña Cuentas de AWS, busque y marque la casilla
   
   junto a cada cuenta miembro que desea eliminar de su organización. Puede navegar por la jerarquía de unidades organizativas o habilitar Ver solo Cuentas de AWS para ver una lista plana de cuentas sin la estructura de unidad organizativa. Si tiene muchas cuentas, puede que tenga que elegir Cargar más cuentas en 'Nombre de OU' en la parte inferior de la lista para encontrar todas las que desea mover.

   En la página Cuentas de AWS, busque y elija el nombre de la cuenta miembro que desea eliminar de su organización. Es posible que tenga que expandir las unidades organizativas (elija la opción
   
)
   para encontrar la cuenta que desea.
3. Seleccionar Acciones y, a continuación, en Cuenta de AWS, elija Eliminar de la organización.
4. En el navegador ¿Eliminar cuenta 'Nombre de la cuenta' (#account-id) de la organización?, elija Eliminar la cuenta.
5. Si AWS Organizations no consigue eliminar una o más de las cuentas, normalmente se debe a que no ha proporcionado toda la información necesaria para que la cuenta funcione como cuenta independiente. Siga estos pasos:

   a. Inicie sesión en la cuenta con errores. Le recomendamos que inicie sesión en la cuenta miembro seleccionando Copy link y, a continuación, pegándolo en la barra de direcciones en una nueva ventana del navegador de incógnito. Si no ve el enlace Copiar, use este enlace para ir a la página Registrarse en AWS y complete los pasos de registro que faltan. Si no utiliza una ventana de incógnito, se cerrará la sesión de la cuenta de administración y no podrá navegar para volver a este cuadro de diálogo.

   b. El navegador le lleva directamente al proceso de registro para completar los pasos que falten para esta cuenta. Complete todos los pasos indicados. Esto podría incluir lo siguiente:

- Proporcionar información de contacto
- Proporcionar un método de pago válido
- Verificar el número de teléfono
- Seleccionar una opción de plan de soporte

c. Al completar el último paso del registro, AWS redirige automáticamente su navegador a la consola de AWS Organizations de la cuenta miembro. Seleccione Leave organization y confirme su selección en el cuadro de diálogo de confirmación. Se le redirigirá a la página Introducción de la consola de AWS Organizations, donde podrá ver las invitaciones pendientes de su cuenta para unirse a otras organizaciones.

d. Elimine de la organización los roles de IAM que conceden acceso a su cuenta.

> **Important**
>
> Si la cuenta se creó en la organización, Organizations creó automáticamente un rol de IAM en la cuenta que habilitó el acceso de la cuenta de administración de la organización. Si la cuenta fue invitada a unirse, entonces Organizations no creó automáticamente dicho rol, pero usted u otro administrador podría haber creado uno para obtener los mismos beneficios. En cualquier caso, cuando quita la cuenta de la organización, dicho rol no se elimina automáticamente. Si desea terminar este acceso desde la cuenta de administración de la organización anterior, debe eliminar manualmente este rol de IAM. Para obtener información acerca de cómo eliminar un rol, consulte Eliminación de roles o perfiles de instancia en la Guía del usuario de IAM.

AWS CLI & AWS SDKs

Para eliminar una cuenta miembro de su organización

Puede utilizar uno de los siguientes comandos para quitar una cuenta de miembro:

- AWS CLI: remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

Este comando no genera ninguna salida si se realiza correctamente.

- SDK de AWS: RemoveAccountFromOrganization

Una vez que se haya eliminado de la organización la cuenta de miembro, asegúrese de eliminar de la organización los roles de IAM que dan acceso a su cuenta.

> **Important**
>
> Si la cuenta se creó en la organización, Organizations creó automáticamente un rol de IAM en la cuenta que habilitó el acceso de la cuenta de administración de la organización. Si la cuenta fue invitada a unirse, entonces Organizations no creó automáticamente dicho rol, pero usted u otro administrador podría haber creado uno para obtener los mismos beneficios. En cualquier caso, cuando quita la cuenta de la organización, dicho rol no se elimina automáticamente. Si desea terminar este acceso desde la cuenta de administración de la organización anterior, debe eliminar manualmente este rol de IAM. Para obtener información acerca de cómo eliminar un rol, consulte Eliminación de roles o perfiles de instancia en la Guía del usuario de IAM.

En su lugar, las cuentas de los miembros pueden eliminarse a sí mismas con el comando leave-organization. Para obtener más información, consulte Salir de una organización desde una cuenta de miembro con AWS Organizations.

Salir de una organización desde una cuenta de miembro con AWS Organizations

Cuando inicia sesión en una cuenta de miembro, puede abandonar una organización. La cuenta de administración no puede abandonar la organización mediante esta técnica. Para eliminar la cuenta de administración, debe eliminar la organización.

Consideraciones

El estado de una cuenta con una organización afecta a los datos de costo y uso visibles

Si una cuenta de miembro deja una organización y pasa a ser una cuenta independiente, la cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización. La cuenta tiene acceso únicamente a los datos que se generan como cuenta independiente.

Si una cuenta de miembro deja una organización A para unirse a una organización B, la cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización A. La cuenta tiene acceso únicamente a los datos que se generan como miembro de la organización B.

Si una cuenta vuelve a unirse a una organización a la que pertenecía anteriormente, la cuenta vuelve a recuperar el acceso a sus datos históricos de costos y uso.

La cuenta ya no estará cubierta por los acuerdos de la organización que la organización aceptó en su nombre

Si abandona una organización, ya no estará cubierto por los acuerdos de la organización que la cuenta de administración de la organización aceptó en su nombre. Puedes ver una lista de estos acuerdos organizativos en la AWS Artifact consola de la página Acuerdos AWS Artifact organizativos. Antes de abandonar la organización, debe determinar (con la ayuda de los equipos jurídicos, de privacidad o de conformidad, si procede) si es necesario formalizar nuevos acuerdos.

Abandono de una organización desde una cuenta de miembro

Para abandonar una organización, complete el procedimiento siguiente.

Permisos mínimos

Para abandonar una organización, debe disponer de los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:LeaveOrganization`; tenga en cuenta que el administrador de la organización puede aplicar una política a la cuenta que elimine este permiso, lo que le impedirá eliminar la cuenta de la organización.
- Si inicias sesión como IAM usuario y falta información de pago en la cuenta, el usuario debe tener `aws-portal:ModifyPaymentMethods` permisos (si la cuenta aún no ha migrado a permisos específicos) o `payments:CreatePaymentInstrument` `payments:UpdatePaymentPreferences` permisos (si la cuenta ha migrado a permisos específicos). `aws-portal:ModifyBilling` Además, la cuenta miembro debe tener habilitado el acceso del usuario de IAM a la facturación. Si no está habilitado, consulte Activación del acceso a la consola Billing and Cost Management en la Guía del usuario de AWS Billing .

AWS Management Console

Para abandonar una organización desde su cuenta de miembro

1. Inicia sesión en la consola desde la consola. AWS OrganizationsAWS Organizations Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario root (no se recomienda) en una cuenta de miembro.

   De forma predeterminada, no tienes acceso a la contraseña del usuario raíz de una cuenta de miembro que se creó con AWS Organizations. Si es necesario, recupera la contraseña del usuario root siguiendo los pasos que se indican en Cómo usar el usuario root (no se recomienda para las tareas diarias) enAcceder a las cuentas de los miembros de una organización con AWS Organizations.
2. En la página Panel de Organizations, seleccione Abandonar esta organización.
3. En el cuadro de diálogo ¿Confirmar el abandono de la organización?, elija Abandonar organización. Cuando se le indique, confirme su elección para eliminar la cuenta. Tras confirmarlo, se te redirigirá a la página de introducción de la AWS Organizations consola, donde podrás ver las invitaciones pendientes de tu cuenta para unirte a otras organizaciones.

   Si aparece el mensaje Todavía no puede abandonar la organización, significa que su cuenta no tiene toda la información necesaria para funcionar como una cuenta independiente. En tal caso, continúe en el paso siguiente.
4. Si el cuadro de diálogo ¿Confirmar el abandono de la organización? muestra el mensaje Todavía no puede abandonar la organización, seleccione el enlace Completar los pasos de inscripción de la cuenta.

   Si no ve el enlace Completar los pasos de inscripción de la cuenta, utilice este enlace para ir a la página Registrarse en AWS y completar los pasos de registro que faltan.
5. En la página Inscribirse a AWS, introduzca toda la información solicitada para que la cuenta se convierta en una cuenta independiente. Puede incluir los siguientes tipos de información:

   - Nombre y dirección de contacto
   - Método de pago válido
   - Verificación de número de teléfono
   - Opciones de planes de soporte
6. Cuando vea el cuadro de diálogo que le avisa de que el proceso de inscripción se ha completado, seleccione Leave organization.

Aparece un cuadro de diálogo de confirmación. Confirme su elección para eliminar la cuenta. Se te redirigirá a la página de introducción de la AWS Organizations consola, donde podrás ver las invitaciones pendientes de tu cuenta para unirte a otras organizaciones.

7. Elimine de la organización los roles de IAM que conceden acceso a su cuenta.

> **Important**
>
> Si su cuenta se creó en la organización, Organizations creó automáticamente un IAM rol en la cuenta que permitió el acceso de la cuenta de administración de la organización. Si la cuenta fue invitada a unirse, entonces Organizations no creó automáticamente dicho rol, pero usted u otro administrador podría haber creado uno para obtener los mismos beneficios. En cualquier caso, cuando quita la cuenta de la organización, dicho rol no se elimina automáticamente. Si desea cancelar este acceso desde la cuenta de administración de la organización anterior, debe eliminar este IAM rol manualmente. Para obtener información sobre cómo eliminar un rol, consulte Eliminar roles o perfiles de instancia en la Guía del IAM usuario.

AWS CLI & AWS SDKs

Para abandonar una organización como cuenta de miembro

Puede utilizar uno de los siguientes comandos para abandonar una organización:

- AWS CLI: leave-organization

  El siguiente ejemplo hace que la cuenta cuyas credenciales se utilizan para ejecutar el comando abandone la organización.

  ```
  $ aws organizations leave-organization
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS SDKs: LeaveOrganization

Una vez que la cuenta de miembro haya abandonado la organización, asegúrate de eliminar de la organización IAM los roles que permiten el acceso a tu cuenta.

> **Important**
>
> Si su cuenta se creó en la organización, Organizations creó automáticamente un IAM rol en la cuenta que permitió el acceso de la cuenta de administración de la organización. Si la cuenta fue invitada a unirse, entonces Organizations no creó automáticamente dicho rol, pero usted u otro administrador podría haber creado uno para obtener los mismos beneficios. En cualquier caso, cuando quita la cuenta de la organización, dicho rol no se elimina automáticamente. Si desea cancelar este acceso desde la cuenta de administración de la organización anterior, debe eliminar este IAM rol manualmente. Para obtener información sobre cómo eliminar un rol, consulte Eliminar roles o perfiles de instancia en la Guía del IAM usuario.

En su remove-account-from-organizationlugar, un usuario de la cuenta de administración también puede eliminar las cuentas de los miembros. Para obtener más información, consulte Eliminación de una cuenta miembro de su organización.

Actualizar la dirección de correo electrónico del usuario raíz de una cuenta de miembro con AWS Organizations

Para aumentar la seguridad y la flexibilidad administrativa, IAM los directores de la cuenta de administración (que tienen los IAM permisos necesarios) pueden actualizar de forma centralizada la dirección de correo electrónico de un usuario raíz (también denominada dirección de correo electrónico principal) de cualquiera de sus cuentas de miembros sin tener que iniciar sesión en cada cuenta de forma individual. De este modo, los administradores de la cuenta de administración (o de una cuenta de administrador delegado) tienen más control sobre las cuentas de miembro. También garantiza que las direcciones de correo electrónico de los usuarios raíz de todas tus AWS Organizations cuentas de miembros estén actualizadas, incluso si has perdido el acceso a la dirección de correo electrónico o las credenciales administrativas originales del usuario raíz.

Cuando un administrador de la cuenta de administración cambie de forma centralizada la dirección de correo electrónico del usuario raíz, tanto la contraseña como la MFA configuración seguirán siendo las mismas que antes del cambio. Tenga en cuenta que un usuario MFA puede omitirla si controla la dirección de correo electrónico y el número de teléfono de contacto principal del usuario raíz de una cuenta.

Para actualizar la dirección de correo electrónico del usuario raíz de la cuenta de un miembro de su organización, esta debe haber activado previamente el modo de todas las funciones. AWS Organizations en el modo de facturación unificada o en las cuentas que no forman parte de una organización, no pueden actualizar la dirección de correo electrónico del usuario raíz de forma centralizada. Los usuarios que deseen cambiar la dirección de correo electrónico del usuario raíz de las cuentas que no son compatibles con ella API deben seguir utilizando la Consola de facturación para administrar la dirección de correo electrónico del usuario raíz.

Uso de una dirección de correo electrónico de grupo para todos los usuarios raíz de cuentas de miembro

Utilice el siguiente procedimiento para actualizar la dirección de correo electrónico del usuario raíz.

AWS Management Console

> **Notas**
>
> - Para llevar a cabo este procedimiento desde la cuenta de administración o desde una cuenta de administrador delegado de una organización y compararla con las cuentas de miembro, debe habilitar el acceso de confianza al servicio de administración de cuentas.
> - No puede usar este procedimiento para acceder a una cuenta de una organización diferente a la que utiliza para llamar a la operación.

Para actualizar la dirección de correo electrónico del usuario raíz de una cuenta de miembro mediante la consola de AWS Organizations

1. Inicie sesión en la AWS Organizations consola como usuario raíz de la cuenta de administración (o IAM permisos equivalentes) de su organización.
2. En la página Cuentas de AWS, elija la cuenta de miembro para la que desee actualizar la dirección de correo electrónico del usuario raíz.
3. En la sección Detalles de la cuenta, seleccione el botón Acciones y, a continuación, seleccione Actualizar dirección de correo electrónico.
4. En Correo electrónico, ingrese la nueva dirección de correo electrónico del usuario raíz y, a continuación, seleccione Guardar. Esto envía una contraseña de un solo uso (OTP) a la nueva dirección de correo electrónico.

> **Note**
>
> Si necesitas cerrar esta página en la consola de Organizations mientras esperas el código, puedes volver y finalizar el OTP proceso en un plazo de 24 horas a partir del envío del código. Para ello, en la página Detalles de la cuenta, seleccione el botón Acciones y, a continuación, seleccione Completar la actualización del correo electrónico.

5. En Código de verificación, ingrese el código que se envió a la nueva dirección de correo electrónico en el paso anterior y, a continuación, seleccione Confirmar. Esto confirma la actualización para el usuario raíz de la cuenta.

AWS CLI & AWS SDKs

Puede recuperar o actualizar la dirección de correo electrónico del usuario raíz (también denominada dirección de correo electrónico principal) mediante los siguientes AWS CLI comandos o sus operaciones AWS SDK equivalentes:

- GetPrimaryEmail
- StartPrimaryEmailUpdate
- AcceptPrimaryEmailUpdate

> **Notas**
>
> - Para llevar a cabo estas operaciones desde la cuenta de administración o desde una cuenta de administrador delegado de una organización y compararlas con las cuentas de miembro, debe habilitar el acceso de confianza para el servicio de administración de cuentas.
> - No puede acceder a una cuenta de una organización diferente a la que utiliza para llamar a la operación.

> **Permisos mínimos**
>
> Para cada operación, debe tener el permiso que se asigna a esa operación:

- `account:GetPrimaryEmail`
- `account:StartPrimaryEmailUpdate`
- `account:AcceptPrimaryEmailUpdate`

Si utiliza estos permisos individuales, puede conceder a algunos usuarios la capacidad de leer únicamente la información de la dirección de correo electrónico del usuario raíz y conceder a otros la capacidad de leer y escribir.

Para completar el proceso de actualización del correo electrónico del usuario raíz, debe utilizar el correo principal en APIs conjunto en el orden en que se muestran en los ejemplos siguientes.

Example **`GetPrimaryEmail`**

En el siguiente ejemplo se recupera la dirección de correo electrónico del usuario raíz de la cuenta de miembro especificada de una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de Account Management.

```
$ aws account get-primary-email --account-id 123456789012
```

Example **`StartPrimaryEmailUpdate`**

En el siguiente ejemplo, se inicia el proceso de actualización de la dirección de correo electrónico del usuario raíz, se identifica la nueva dirección de correo electrónico y se envía una contraseña de un solo uso (OTP) a la nueva dirección de correo electrónico de la cuenta de miembro especificada en una organización. Las credenciales utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de Account Management.

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email
 john@examplecorp.com
```

Example **`AcceptPrimaryEmailUpdate`**

En el siguiente ejemplo, se acepta el OTP código y se establece la nueva dirección de correo electrónico en la cuenta de miembro especificada en una organización. Las credenciales

utilizadas deben provenir de la cuenta de administración de la organización o de la cuenta de administrador delegado de la administración de la cuenta.

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678
 --primary-email john@examplecorp.com
```

Administrar las invitaciones a las cuentas con AWS Organizations

Después de crear una organización y comprobar que eres el propietario de la dirección de correo electrónico asociada a la cuenta de administración, puedes invitar a una persona existente Cuentas de AWS a unirse a tu organización. Usa la AWS Organizations consola para iniciar y administrar las invitaciones que envíes a otras cuentas. Solo puede enviar una invitación a otras cuentas desde la cuenta de administración de su organización.

Cuando invitas a una cuenta, AWS Organizations envía una invitación al propietario de la cuenta, quien puede decidir aceptarla o rechazarla.

Si eres el administrador de una organización Cuenta de AWS, también puedes aceptar o rechazar una invitación de una organización. Si la acepta, su cuenta se convierte en miembro de esa organización.

Para crear una cuenta que forme parte automáticamente de su organización, consulte Crear una cuenta de miembro en una organización con AWS Organizations.

> **Important**
>
> Todas las cuentas de una organización deben provenir de la misma AWS partición que la cuenta de administración. Las cuentas de la Regiones de AWS partición comercial no pueden estar en una organización con cuentas de la partición Regiones de China o cuentas de la partición AWS GovCloud (US) Regiones.

Temas

- Consideraciones
- Enviar invitaciones a cuentas con AWS Organizations
- Gestiona las invitaciones de cuentas pendientes con AWS Organizations
- Aceptar o rechazar invitaciones a cuentas con AWS Organizations

Consideraciones

Limitaciones en la cantidad de invitaciones que puede enviar por día

Para ver el número de invitaciones que puede enviar por día, consulte Valores mínimos y máximos. Las invitaciones aceptadas no se contabilizan en esta cuota. Tan pronto como se acepta una invitación, puede enviar otra invitación ese mismo día. Todas las invitaciones deben responderse en un plazo de 15 días o caducarán.

Una invitación enviada a una cuenta se contabiliza para la cuota de cuentas de la organización. La cuenta se restaura si la cuenta invitada rechaza la invitación, la cuenta de administración cancela la invitación o la invitación vence.

Una cuenta solo puede unirse a una organización

Una cuenta solo puede unirse a una organización. Si recibe varias invitaciones, solo puede aceptar una.

El historial y los informes de facturación permanecen en la cuenta de administración

El historial y los informes de facturación de todas las cuentas permanecen en la cuenta del pagador de una organización. Antes de trasladar la cuenta a una nueva organización, exporte o haga una copia de seguridad de los historiales e informes de facturación de cualquier cuenta de miembro que desee conservar. Esto puede incluir informes de costos y usos, informes de Explorador de costos, informes de Savings Plans y cobertura y uso de instancias reservadas.

La cuenta de administración es responsable de pagar los cargos acumulados de todas las cuentas de miembro

En el momento en que una cuenta acepta la invitación para unirse a una organización, la cuenta de administración de la organización se hace responsable de todos los cargos acumulados por la nueva cuenta de miembro. El método de pago asociado a la cuenta de miembro ya no se utiliza. En su lugar, el método de pago adjunto a la cuenta de gestión de la organización paga todos los cargos acumulados por la cuenta de miembro.

Organizations crea automáticamente el rol vinculado al servicio **`AWSServiceRoleForOrganizations`**

AWS Organizations crea un rol vinculado a un servicio llamado `AWSServiceRoleForOrganizations` para respaldar las integraciones entre AWS Organizations

y otros servicios. AWS Para obtener más información, consulte AWS Organizations y funciones vinculadas al servicio. La cuenta invitada debe tener este rol si su organización admite todas las características. Puede eliminar este rol si la organización únicamente admite el conjunto de características de facturación unificada. Si elimina este rol y, posteriormente, habilita todas las funciones de su organización, AWS Organizations vuelve a crear este rol para la cuenta.

Organizations no crea automáticamente el rol de IAM **`OrganizationAccountAccessRole`**

En el caso de las cuentas de miembros invitados, AWS Organizations no crea automáticamente el rol de IAM. `OrganizationAccountAccessRole` Este rol otorga a los usuarios de la cuenta de administración acceso administrativo a la cuenta de miembro. Si desea habilitar ese nivel de control administrativo a la cuenta invitada, puede agregar manualmente el rol. Para obtener más información, consulte Creación de OrganizationAccountAccessRole en una cuenta miembro invitada con AWS Organizations.

> **Note**
>
> Cuando creas una cuenta en tu organización, en lugar de invitar a una cuenta existente a unirse, crea AWS Organizations automáticamente la función de IAM de forma `OrganizationAccountAccessRole` predeterminada.

Las políticas asociadas al nodo raíz o a la OU que contienen la cuenta se aplican inmediatamente

Si tiene política asociadas al nodo raíz o a la unidad organizativa (OU) que contiene la cuenta invitada, dichas políticas se aplican inmediatamente a todos los usuarios y roles de la cuenta invitada.

Puede habilitar la confianza en el servicio para otro AWS servicio de su organización. Tras ello, ese servicio de confianza puede crear roles vinculados a servicios o realizar acciones en cualquier cuenta de miembro de la organización, incluida una cuenta invitada.

Las organizaciones que solo tienen el conjunto de características de facturación unificada pueden seguir invitando cuentas

Puede invitar a una cuenta a unirse a una organización que solo tenga habilitadas las características de facturación unificada. Si posteriormente desea habilitar todas las características para la organización, las cuentas invitadas deben aprobar el cambio.

Enviar invitaciones a cuentas con AWS Organizations

Para poder invitar a cuentas a su organización, primero debe verificar que es el propietario de la dirección de correo electrónico asociada a la cuenta de administración. Para obtener más información, consulte Verificación de dirección de correo electrónico con AWS Organizations. Una vez que haya verificado la dirección de correo electrónico, siga los pasos que se describen a continuación para invitar a otras cuentas a que se unan a su organización.

Permisos mínimos

Para invitar a una Cuenta de AWS persona a unirse a tu organización, debes tener los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola)
- `organizations:InviteAccountToOrganization`

AWS Management Console

Para invitar a otra cuenta a que se una a su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Si ya has verificado tu dirección de correo electrónico con AWS, omite este paso.

   Si la dirección de correo electrónico aún no se ha verificado, siga las instrucciones del correo electrónico de verificación en un plazo de 24 horas después de crear la organización. Puede pasar algún tiempo hasta que reciba el correo electrónico de verificación. No puede invitar a una cuenta a unirse a su organización hasta que no verifique su dirección de correo electrónico.
3. Vaya a la página Cuentas de AWS y elija Agregar una cuenta AWS .
4. En la página Agregar un Cuenta de AWS, elija Invitar una cuenta AWS existente.
5. En la AWS página Invitar a una cuenta existente, en la dirección de correo electrónico o ID de cuenta de la persona Cuenta de AWS a la que se va a invitar, introduce la dirección de correo electrónico asociada a la cuenta a la que se va a invitar o su número de ID de cuenta.

6. (Opcional) Para Mensaje a incluir en el mensaje de correo electrónico de invitación, ingrese el texto que desee incluir en la invitación por correo electrónico al propietario de la cuenta invitada.
7. (Opcional) En la sección Agregar etiquetas, especifique una o más etiquetas que se apliquen automáticamente a la cuenta después de que su administrador acepte la invitación. Para ello, elija Agregar etiqueta y, a continuación, ingrese una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede adjuntar hasta 50 etiquetas a una Cuenta de AWS.
8. Seleccione Send invitation (Enviar invitación).

   > **Important**
   >
   > Si obtiene un mensaje en el que se indica que ha superado las cuotas de la organización o que no puede agregar una cuenta porque la organización aún se está inicializando, póngase en contacto con AWS Support.

9. La consola le redirige a la página de Invitaciones donde puede ver todas las invitaciones abiertas y aceptadas aquí. La invitación que acaba de crear aparece en la parte superior de la lista con el estado establecido en OPEN.

   AWS Organizations envía una invitación a la dirección de correo electrónico del propietario de la cuenta que has invitado a la organización. Este mensaje de correo electrónico incluye un enlace a la AWS Organizations consola, donde el propietario de la cuenta puede ver los detalles y elegir si acepta o rechaza la invitación. Como alternativa, el propietario de la cuenta invitada puede omitir el mensaje de correo electrónico, ir directamente a la AWS Organizations consola, ver la invitación y aceptarla o rechazarla.

   La invitación a esta cuenta se contabiliza de inmediato para el número máximo de cuentas que puede tener en su organización. AWS Organizations no espera hasta que la cuenta acepta la invitación. Si la cuenta invitada la rechaza, la cuenta de administración cancela la invitación. Si la cuenta invitada no responde en el periodo de tiempo especificado, la invitación caducará. En cualquier caso, la invitación ya no se contabiliza para la cuota.

AWS CLI & AWS SDKs

Para invitar a otra cuenta a que se una a su organización

Puede utilizar uno de los siguientes comandos para invitar a otra cuenta a unirse a su organización:

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
```

```
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
    }
}
```

- AWS SDKs: InviteAccountToOrganization

Gestiona las invitaciones de cuentas pendientes con AWS Organizations

Tras iniciar sesión en su cuenta de administración, puede ver todas las cuentas vinculadas de Cuentas de AWS de su organización y cancelar cualquier invitación pendiente (abierta). Para ello, siga los pasos que se describen a continuación.

> **Permisos mínimos**
>
> Para administrar las invitaciones pendientes de su organización, debe contar con los siguientes permisos:
>
> - `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
> - `organizations:ListHandshakesForOrganization`
> - `organizations:CancelHandshake`

AWS Management Console

Para ver o cancelar las invitaciones que se envían desde su organización a otras cuentas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página Invitaciones.

Esta página muestra todas las invitaciones que se envían desde su organización y su estado actual.

Si no puedes ver una invitación, comprueba si la cuenta invitada es la cuenta de administración de otra organización. Solo las cuentas de los miembros y las cuentas independientes pueden recibir invitaciones. Las cuentas de administración no pueden recibir invitaciones.

Si desea invitar a una cuenta que sea una cuenta de administración de otra organización, se recomienda convertir esa cuenta en una cuenta independiente.

> **Note**
>
> Las invitaciones aceptadas, canceladas y rechazadas siguen apareciendo en la lista durante 30 días. Posteriormente, se eliminan y ya no aparecen en la lista.

3. Elija el botón de opción

   junto a la invitación que desee cancelar y luego elija Cancelar invitación. Si el botón de opción está atenuado, entonces esa invitación no se puede cancelar.

   El estado de la invitación cambia de OPEN a CANCELED.

   AWS envía un mensaje de correo electrónico al propietario de la cuenta indicándole que has cancelado la invitación. La cuenta ya no puede unirse a la organización a menos que envíe una nueva invitación.

AWS CLI & AWS SDKs

Para ver o cancelar las invitaciones que se envían desde su organización a otras cuentas

Puede utilizar los siguientes comandos para ver o cancelar invitaciones:

- AWS CLI: list-handshakes-for-organization, cancel-apretón de manos
- En el ejemplo siguiente se muestran las invitaciones enviadas por esta organización a otras cuentas.

```
$ aws organizations list-handshakes-for-organization
{
```

```
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
```

```
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
```

```
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
            ]
        }
    ]
}
```

En el ejemplo siguiente se muestra cómo cancelar una invitación a una cuenta.

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
```

```
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS SDKs: ListHandshakesForOrganization, CancelHandshake

Aceptar o rechazar invitaciones a cuentas con AWS Organizations

Si le invitan a unirse a una organización en, puede aceptar o rechazar la invitación.

Consideraciones

El estado de una cuenta con una organización afecta a los datos de costo y uso visibles

Si una cuenta de miembro deja una organización y pasa a ser una cuenta independiente, la cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización. La cuenta tiene acceso únicamente a los datos que se generan como cuenta independiente.

Si una cuenta de miembro deja una organización A para unirse a una organización B, la cuenta ya no tiene acceso a los datos de costo y uso del intervalo de tiempo en el que la cuenta era miembro de la organización A. La cuenta tiene acceso únicamente a los datos que se generan como miembro de la organización B.

Si una cuenta vuelve a unirse a una organización a la que pertenecía anteriormente, la cuenta vuelve a recuperar el acceso a sus datos históricos de costos y uso.

Solo las cuentas de miembro y las cuentas independientes pueden aceptar o rechazar una invitación

Solo las cuentas de miembros y las cuentas independientes pueden aceptar o rechazar una invitación para unirse a una organización. Si se envía una invitación a la cuenta de un miembro, dicha cuenta debe abandonar la organización actual antes de aceptar la invitación. Si se envía una invitación a una cuenta de administración que ya forma parte de una organización, esa cuenta no podrá ver la invitación hasta que elimine todas las cuentas de los miembros de su organización y elimine la organización.

Aceptar o rechazar una invitación

Para aceptar o rechazar la invitación, complete los pasos siguientes.

> **Permisos mínimos**
>
> Para aceptar o rechazar una invitación para unirse a una organización de , debe disponer de los siguientes permisos:
>
> - `organizations:ListHandshakesForAccount`— Necesario para ver la lista de invitaciones en la AWS Organizations consola.
> - `organizations:AcceptHandshake`.
> - `organizations:DeclineHandshake`.
> - `iam:CreateServiceLinkedRole`: necesario solo cuando aceptamos la invitación; requiere crear un rol vinculado al servicio en la cuenta de miembro para facilitar la integración con otros Servicios de AWS. Para obtener más información, consulte AWS Organizations y funciones vinculadas al servicio.

AWS Management Console

Para aceptar o rechazar una invitación

1. Una invitación para unirse a una organización se envía a la dirección de correo electrónico del propietario de la cuenta. Si es el propietario de la cuenta y recibe un correo electrónico de invitación, siga las instrucciones indicadas en el correo electrónico de invitación o vaya a la consola AWS Organizations con el navegador y luego elija Invitations (Invitaciones), o vaya directo a la página de member account's Invitation (Invitación de la cuenta de miembro).

2. Si se le solicita, inicie sesión en la cuenta invitada como usuario de IAM, asuma un rol de IAM o inicie sesión como usuario raíz de la cuenta (no se recomienda).
3. La página de Invitación de la cuenta de miembro muestra las invitaciones abiertas de su cuenta para unirse a organizaciones.

   Elija Aceptar o Rechazar invitación según corresponda.

   - Si selecciona Aceptar invitación en el paso anterior, la consola le redirige a la página de Información general de la organización con detalles sobre la organización de la que su cuenta es ahora miembro. Puede ver el ID de organización y la dirección de correo electrónico del propietario.

     > **Note**
     >
     > Las invitaciones aceptadas siguen apareciendo en la lista durante 30 días. Posteriormente, se eliminan y ya no aparecen en la lista.

     AWS Organizations crea automáticamente un rol vinculado al servicio en la cuenta del nuevo miembro para facilitar la integración entre otros AWS Organizations . Servicios de AWS Para obtener más información, consulte AWS Organizations y funciones vinculadas al servicio.

     AWS envía un mensaje de correo electrónico al propietario de la cuenta de administración de la organización en el que se indica que has aceptado la invitación. También envía un correo electrónico al propietario de la cuenta de miembro para indicarle que la cuenta ahora es miembro de la organización.
   - Si elige Rechazar en el paso anterior, la cuenta permanece en la página Invitación de la cuenta de miembro, que muestra todas las demás invitaciones pendientes.

     AWS envía un mensaje de correo electrónico al propietario de la cuenta de administración de la organización en el que se indica que has rechazado la invitación.

     > **Note**
     >
     > Las invitaciones rechazadas siguen apareciendo en la lista durante 30 días. Posteriormente, se eliminan y ya no aparecen en la lista.

AWS CLI & AWS SDKs

Para aceptar o rechazar una invitación

Puede utilizar los siguientes comandos para aceptar o rechazar invitaciones:

- AWS CLI: accept-handshake, decline-handshake

  El siguiente ejemplo muestra cómo aceptar una invitación para unirse a una organización.

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
```

```
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
}
```

El siguiente ejemplo muestra cómo rechazar una invitación para unirse a una organización.

- AWS SDKs: AcceptHandshake, DeclineHandshake

Migración de una cuenta a otra organización con AWS Organizations

Puedes migrar y Cuenta de AWS de otra organización a otra en cualquier momento. Por ejemplo, la migración de una cuenta puede resultar útil en el caso de una fusión o adquisición cuando se necesita consolidar una o más Cuentas de AWS de varias organizaciones en una sola.

Sea cual sea su caso, para migrar una cuenta entre organizaciones es necesario eliminar la cuenta de la organización anterior, convertirla en una cuenta independiente y que la cuenta acepte la invitación para unirse a la nueva organización. Sus cargas de trabajo y servicios seguirán funcionando según sus especificaciones durante la migración. Sin embargo, es importante que esté al tanto de las dependencias que pueda tener en su organización.

> **Note**
>
> Las cuentas cerradas o suspendidas no se pueden migrar
> No puede migrar una cuenta cerrada o suspendida. Para reactivar una cuenta, contacte con Soporte.
> Requisito de antigüedad de siete días
> Para migrar una cuenta que creó en una organización, debe esperar al menos siete días después de que se creó la cuenta. Las cuentas invitadas no están sujetas a este período de espera.

Replicación de datos entre cuentas
La siguiente guía AWS prescriptiva proporciona información sobre las estrategias para replicar datos entre Cuentas de AWS: la replicación de recursos o la migración entre ellas. Cuentas de AWS

Lo que debe hacer antes de migrar una cuenta

Antes de migrar Cuenta de AWS de una organización a otra, asegúrese de haber completado los siguientes pasos.

Paso 1: Comprueba que tienes los IAM permisos necesarios para migrar una cuenta

Paso 1

Asegúrese de haber aplicado los permisos necesarios para migrar una cuenta a las organizaciones respectivas.

Para abandonar una organización, debe disponer de los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola)
- `organizations:LeaveOrganization`

Para obtener más información, consulte Leave an organization from your member account.

Para invitar a un usuario Cuenta de AWS a unirse a una organización, debes tener los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola)
- `organizations:InviteAccountToOrganization`

Para obtener más información, consulte Invitar a un Cuenta de AWS hombre a unirse a su organización.

Para migrar una cuenta, no puede tener IAM políticas o políticas de control de servicios que impidan la migración

Si eres la cuenta de administración o un administrador delegado, puedes controlar el acceso a AWS los recursos adjuntando políticas de permisos a las IAM identidades (usuarios, grupos y roles) de una organización. Para obtener más información, consulte IAMlas políticas de. AWS Organizations

Antes de migrar una cuenta:

- Comprueba que no haya IAM políticas o políticas de control de servicios (SCPs) que te impidan migrar la cuenta.
- Identifique IAM las políticas y las políticas de control de servicios existentes (SCPs) que necesita replicar en la organización a la que va a migrar la cuenta.
- Identifique IAM las políticas existentes que especifican el ID de su organización. Por ejemplo, `aws:PrincipalOrgID`.

Para obtener más información, consulte Administración de IAM políticas en la Guía del IAM usuario y Políticas de control de servicios (SCPs).

Paso 2: compruebe que ha eliminado IAM los permisos que permitían el acceso a la cuenta de administración anterior

Paso 2

Asegúrese de haber eliminado IAM los permisos que permitían el acceso a la cuenta de administración anterior, por ejemplo`OrganizationAccountAccessRole`.

Cuando eliminas una cuenta de miembro de una organización, cualquier IAM rol que se haya creado para permitir el acceso a la cuenta de administración de la organización no se elimina automáticamente. Si desea cancelar este acceso desde la cuenta de administración de la organización anterior, debe eliminar el IAM rol manualmente.

Para obtener información sobre cómo eliminar un rol, consulte Eliminar roles o perfiles de instancia en la Guía del IAM usuario.

Paso 3: compruebe la verificación de su teléfono y el método de pago

Paso 3

La cuenta migrada debe funcionar como una cuenta independiente durante un tiempo antes de migrarse a la nueva organización.

Para permitir que una cuenta funcione como una cuenta independiente, compruebe lo siguiente:

- Asegúrese de que la verificación de su teléfono sea up-to-date.
- Asegúrese de haber agregado un método de pago válido para la cuenta a fin de poder pagar cualquier cargo en el que se incurra durante la migración de la cuenta.
- Si utilizas la facturación como método de pago, asegúrate de que la factura lo sea up-to-date.

Paso 4: haga una copia de seguridad de todos los informes

Paso 4

Asegúrese de exportar o hacer copias de seguridad de los informes de la cuenta de administración, especialmente los informes de facturación. Los informes y el historial de la organización no se almacenan al migrar una cuenta. Se recomienda realizar una exportación completa de todo el historial de facturación. Puedes seguir accediendo a los informes de las cuentas de los miembros, como el historial de AWS CloudTrail eventos y el historial de facturación de la cuenta.

> **Important**
>
> Todos los informes y el historial de la organización, como la información de facturación de la organización en la cuenta de administración, se eliminarán una vez que se elimine una cuenta de la organización.

Para obtener más información, consulte Cost and Usage Reports, Cost Explorer Reports, Savings Plans Reports y Reserved Instance (RI) utilization and coverage.

Paso 5: compruebe las dependencias de la organización

Paso 5

Asegúrese de que la cuenta que se va a migrar no tenga ninguna dependencia relacionada con la organización.

Dependencias que hay que comprobar:

- Si la cuenta es de un administrador delegado, debe anular los permisos de administrador delegado antes de migrar la cuenta. Para obtener más información, consulta los servicios con los que puedes utilizarlos AWS Organizations.

- Si la cuenta es la cuenta de administración, debe eliminar todas las cuentas de miembro de la organización y eliminar la organización antes de llevar a cabo la migración. Una vez que haya eliminado la organización, su cuenta de administración funcionará como una cuenta independiente. Tras la migración, la cuenta de administración será una cuenta de miembro de la nueva organización. Para obtener más información, consulte Deleting an organization.
- Si algún IAM permiso depende de la cuenta, tendrás que ajustar los permisos de la organización anterior después de migrar la cuenta a la nueva organización para que la antigua funcione como antes. Para obtener más información, consulte Managing access permissions for your organization.
- Si utiliza alguna etiqueta de cuenta o unidad organizativa (OU), tendrá que volver a crear las etiquetas en la nueva organización.

(Opcional) Paso 6: Revisa la guía si utilizas AWS Control Tower

(Opcional) Paso 6

Si va a migrar una cuenta hacia o desde una organización gestionada por AWS Control Tower, consulte la siguiente AWS guía normativa: Migre una cuenta de AWS miembro de a AWS Organizations. AWS Control Tower

Lo que debe hacer para migrar una cuenta

El proceso de migración requiere que la nueva organización envíe una invitación a la cuenta de migración, que la organización anterior elimine la cuenta de migración y que la cuenta que migra acepte la invitación para unirse a la nueva organización.

Para migrar una cuenta

1. Envíe una invitación desde la cuenta de administración de la nueva organización a la cuenta de migración. Debe enviar la invitación a la cuenta antes de que abandone la organización anterior. Esto ayuda a minimizar los costos incurridos cuando la cuenta que se migra funciona temporalmente como una cuenta independiente. Para obtener información sobre cómo invitar a cuentas, consulte Invitar a un hombre a unirse Cuenta de AWS a su organización.
2. Elimine la cuenta que va a migrar de la organización anterior. Puede eliminar una cuenta de miembro de su organización con la cuenta de administración o abandonar una organización como cuenta de miembro.
3. Acepte la invitación para unirse a la nueva organización. Para obtener más información, consulte Accepting an invitation from an organization. Las cuentas que se migren de una organización a

otra se agregarán automáticamente a la raíz de la nueva organización. Antes de trasladar una cuenta a una unidad organizativa (OU) de la nueva organización, se recomienda comprobar que la cuenta que se está migrando tenga las políticas organizativas y los permisos de la OU adecuados.

4. Si desea migrar la cuenta de administración, debe eliminar todas las cuentas de miembro de la organización y eliminar la organización antes de migrar la cuenta de administración a la nueva organización. Una vez que haya eliminado la organización anterior, su cuenta de administración funcionará como una cuenta independiente y podrá aceptar la invitación para unirse a la nueva organización. Si acepta la invitación, la cuenta de administración se convertirá en una cuenta de miembro de la nueva organización.

Lo que debe hacer después de migrar una cuenta

Tras migrar su cuenta de una organización a otra, asegúrese de haber completado los siguientes pasos.

Revisión posterior a la migración

1. Evalúe todas las configuraciones de las herramientas de facturación de la cuenta migrada, como las categorías de costos, los presupuestos y las alarmas de facturación.
2. Revise y actualice la siguiente información monetaria de cualquier cuenta que haya migrado de una organización a otra:
   a. Si es necesario, actualice la configuración fiscal de la cuenta.
   b. Asegúrese de que el plan de Soporte de la cuenta que va a migrar coincida con la cuenta del pagador de la nueva organización.
   c. Revise las posibles exenciones fiscales que quiera aplicar a la cuenta que migró.
3. Valide y confirme IAM las políticas y políticas de control de servicios existentes (SCPs) para la cuenta migrada. Por ejemplo, es posible que tengas que actualizar el identificador de la organización de algunas IAM políticas para que reflejen la nueva organización.
4. Actualice las etiquetas de asignación de costos de la nueva organización a la que migró la cuenta. Deberá actualizar todas las etiquetas de asignación de costos anteriores recopiladas por la cuenta que ha migrado.
5. Todas las instancias reservadas y Saving Plans se migrarán junto con la cuenta. Estos no se conservan en la organización anterior. Ponte en contacto con nosotros Soporte si es necesario transferirlas a la organización anterior.

Visualización de los detalles de una cuenta de una organización con AWS Organizations

Cuando inicia sesión en la cuenta de administración de la organización en la consola de AWS Organizations, puede ver los detalles de las cuentas.

Permisos mínimos

Para ver los detalles de una Cuenta de AWS, debe disponer de los siguientes permisos:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:ListAccounts`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para ver los detalles de una Cuenta de AWS

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página Cuentas de AWS y elija el nombre del nombre de la cuenta (no el botón de opción) que desea examinar. Si la cuenta que desea es secundaria de una OU, es posible que tenga que elegir el icono del triángulo  junto a una unidad organizativa para expandirla y ver a sus secundarias. Repetir hasta que encuentre la cuenta.

   El cuadro Detalles de la cuenta muestra la información sobre la cuenta.

AWS CLI & AWS SDKs

Para ver los detalles de una Cuenta de AWS

Puede utilizar los siguientes comandos para ver detalles de una cuenta:

- AWS CLI:
  - list-accounts — enumera los detalles de todas las cuentas de la organización
  - describe-account — muestra los detalles de solo la cuenta especificada

  Ambos comandos devuelven los mismos detalles para cada cuenta incluida en la respuesta.

  El siguiente ejemplo muestra cómo recuperar los detalles sobre una cuenta especificada.

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
}
```

- SDK de AWS
  - ListAccounts
  - DescribeAccount

Exportación de detalles de una cuenta en una organización con AWS Organizations

Con AWS Organizations, los usuarios de cuentas de administración y los administradores delegados de una organización pueden exportar un archivo .csv con los detalles de todas las cuentas de una organización. Como resultado, los administradores de la organización pueden ver las cuentas fácilmente y filtrar por estado: `ACTIVE`, `SUSPENDED` o `PENDING`. Si su organización tiene muchas cuentas, la opción de descargar el archivo .csv ofrece una forma sencilla de ver y ordenar los detalles de las cuentas en una hoja de cálculo.

> **Note**
>
> Solo las entidades principales de la cuenta de administración pueden descargar la lista de cuentas.

Exportación de una lista de todas las Cuentas de AWS de su organización

Cuando se inicia sesión en la cuenta de administración de la organización, se puede obtener una lista de todas las cuentas que forman parte de la organización en forma de archivo .csv. La lista contiene los detalles de las cuentas individuales; no obstante, no especifica a qué unidad organizativa (OU) pertenece cada cuenta.

El archivo .csv contiene la siguiente información sobre cada cuenta:

- Account ID (ID de cuenta): identificador de cuenta numérico. Por ejemplo: 123456789012
- ARN (ARN): nombre de recurso de Amazon de la cuenta. Por ejemplo: `arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`.
- Email (Correo electrónico): dirección de correo electrónico asociada a la cuenta. Por ejemplo: marymajor@example.com
- Name (Nombre): nombre de la cuenta proporcionado por el creador de la cuenta. Por ejemplo: cuenta de pruebas de fase
- Status (Estado): estado de la cuenta dentro de la organización. El valor puede ser `PENDING`, `ACTIVE` o `SUSPENDED`.
- Joined method (Método de unión): especifica cómo se creó la cuenta. El valor puede ser `INVITED`, o `CREATED`.
- Joined timestamp (Marca de tiempo de unión): fecha y hora en que la cuenta se unió a la organización.

> **Permisos mínimos**
>
> Para exportar un archivo .csv con todas las cuentas miembro de su organización, debe contar con los permisos siguientes:
>
> - `organizations:DescribeOrganization`

- `organizations:ListAccounts`

AWS Management Console

Para exportar un archivo .csv de todas las Cuentas de AWS de su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Actions (Accciones), y luego, para Cuenta de AWS, elija Export account list (Exportar lista de cuentas). El banner azul de la parte superior de la página indica "Export is in progress!" (La exportación está en curso)
3. Cuando el archivo esté listo, el banner se vuelve verde e indica "Download is ready!" (La descarga está lista) Elija Download CSV (Descargar CSV). El archivo `Organization_accounts_information.csv` se descarga en su dispositivo.

AWS CLI & AWS SDKs

La única forma de exportar el archivo .csv con los detalles de las cuenta es mediante la AWS Management Console. No se puede exportar el archivo .csv de la lista de cuentas mediante la AWS CLI.

Actualización de contactos alternativos de una cuenta de una organización con AWS Organizations

Puede actualizar contactos alternativos para cuentas de su organización mediante la Consola de AWS Organizations o mediante programación utilizando AWS CLI o AWS SDK. Para obtener información sobre cómo actualizar contactos alternativos, consulte Acceso o actualización de los contactos alternativos en la AWS Referencia de administración de cuentas de.

Actualización de la información de contacto principal de una cuenta en una organización con AWS Organizations

Puede actualizar la información de contacto principal de las cuentas de su organización mediante la consola de AWS Organizations o mediante programación con la AWS CLI o los AWS SDK. Para

obtener información sobre cómo actualizar la información de contacto principal, consulte Acceso o actualización del contacto principal de la cuenta en la Referencia de administración de cuentas de AWS.

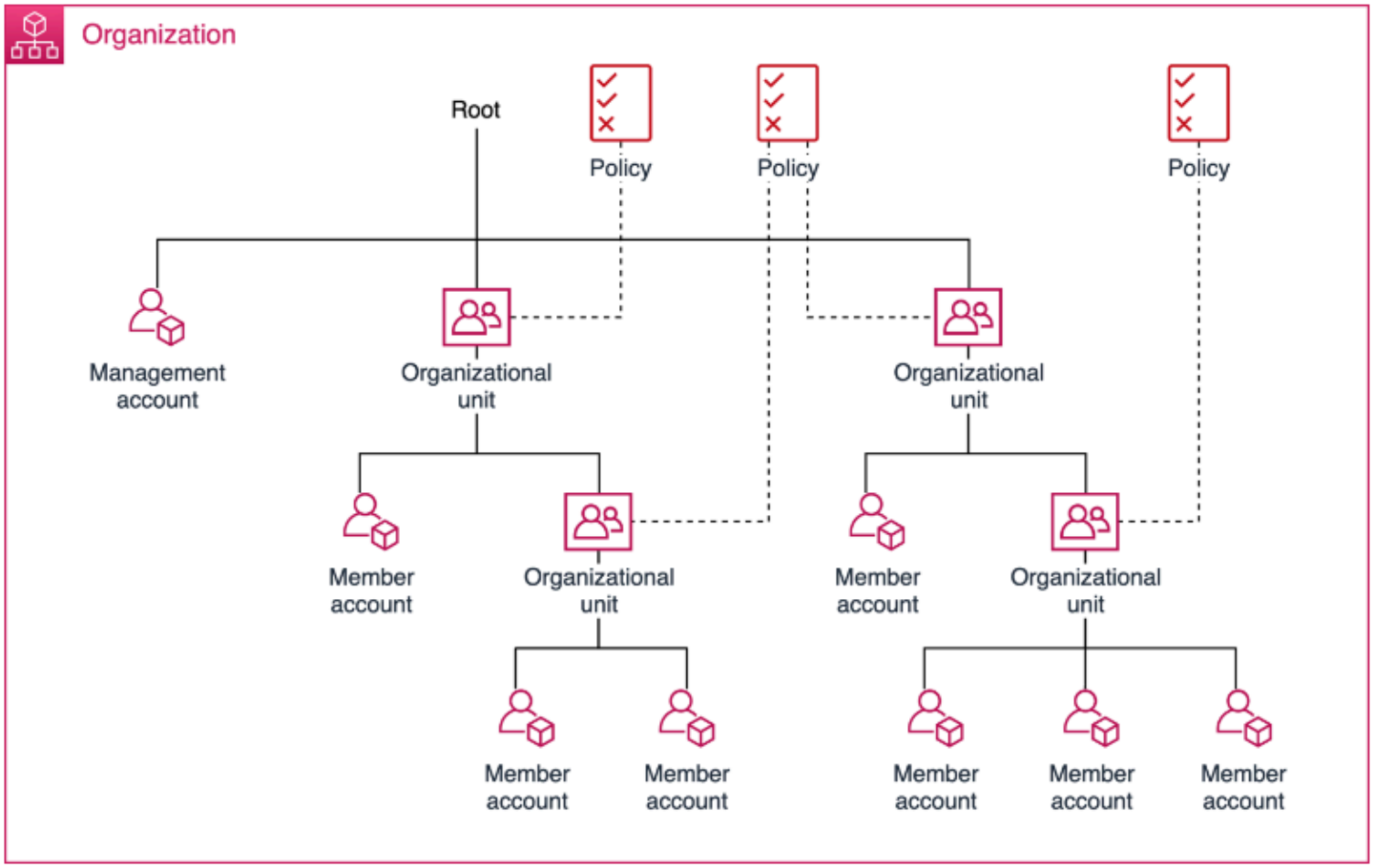
Actualización de las Regiones de AWS habilitadas para una cuenta de una organización con AWS Organizations

Puede actualizar las Regiones de AWS habilitadas para las cuentas de su organización mediante la consola de AWS Organizations. Para saber cómo actualizar las Regiones de AWS habilitadas, consulte Specifying which Regiones de AWS your account can use en la Referencia de administración de cuentas de AWS.

Gestión de unidades organizativas (OUs) con AWS Organizations

Puedes usar las unidades organizativas (OUs) para agrupar cuentas y administrarlas como una sola unidad. Esto simplifica enormemente la administración de sus cuentas. Por ejemplo, puede asociar un control basado en políticas a una unidad organizativa para que todas las cuentas de la unidad organizativa hereden automáticamente la política. Puedes crear varias OUs dentro de una sola organización y puedes crearlas OUs dentro de otra OUs. Cada unidad organizativa puede contener varias cuentas, y puede mover cuentas de una unidad organizativa a otra. Sin embargo, los nombres de las unidades organizativas deben ser únicos dentro de una unidad organizativa o nodo raíz.

El siguiente diagrama muestra una organización que consta de siete cuentas que se organizan en cuatro OUs en la raíz. La organización también tiene algunas políticas a las que se aplican OUs.



> **Note**
>
> Hay una raíz en la organización, que se AWS Organizations crea automáticamente cuando la configuras por primera vez.

Temas

- Mejores prácticas para gestionar unidades organizativas (OUs) con AWS Organizations
- Navegación por la raíz y la jerarquía de unidades organizativas (OU) con AWS Organizations
- Visualización de los detalles de una unidad organizativa (OU) con AWS Organizations
- Creación de una unidad organizativa (OU) con AWS Organizations
- Cambio de nombre de una unidad organizativa (OU) con AWS Organizations
- Etiquetado de una unidad organizativa (OU) con AWS Organizations
- Mover cuentas a una unidad organizativa (OU) o entre la raíz y las unidades organizativas con AWS Organizations
- Visualización de los detalles del nodo raíz con AWS Organizations
- Eliminación de una unidad organizativa (OU) con AWS Organizations

Mejores prácticas para gestionar unidades organizativas (OUs) con AWS Organizations

Sigue estas recomendaciones para ayudarte a gestionar un entorno de varias cuentas mediante el AWS Organizations uso de unidades organizativas (OUs).

Temas

- Comprensión AWS Organizations
- Unidad organizativa fundamental recomendada () OUs
- Unidad organizativa adicional recomendada () OUs
- Conclusión

Comprensión AWS Organizations

La base de un AWS entorno de múltiples cuentas bien diseñado es AWS Organizations que le permita administrar y gobernar varias cuentas de forma centralizada. Una unidad organizativa (OU) es una agrupación lógica de cuentas en una organización. OUs le permiten organizar sus cuentas en una jerarquía y le ayudan a aplicar los controles de gestión. Las políticas de Organizations definen los controles que puede aplicar a un grupo de Cuentas de AWS. Por ejemplo, una política de control de servicios (SCP) es una política que define las Servicio de AWS acciones, como Amazon EC2 Run Instance, que pueden realizar las cuentas de su organización.

Si bien puede comenzar su AWS viaje con una sola cuenta, le AWS recomienda configurar varias cuentas a medida que sus cargas de trabajo aumenten de tamaño y complejidad. El uso de un entorno de varias cuentas es una práctica AWS recomendada que puede ofrecer varios beneficios:

- Innovación rápida con diferentes requisitos: puede asignarlos Cuentas de AWS a diferentes equipos, proyectos o productos de su empresa para garantizar que cada uno de ellos pueda innovar rápidamente y, al mismo tiempo, tener en cuenta sus propios requisitos de seguridad.
- Facturación simplificada: el uso de varios Cuentas de AWS puede simplificar la forma de asignar los AWS costes, ya que ayuda a identificar qué línea de productos o servicios es responsable de un AWS cargo.
- Controles de seguridad flexibles: puede utilizar varios Cuentas de AWS para aislar cargas de trabajo o aplicaciones que tengan requisitos de seguridad específicos o que deban cumplir normas estrictas de conformidad, como la HIPAA o la PCI.
- Adáptese a los procesos empresariales: puede organizar varios de Cuentas de AWS ellos de la forma que mejor refleje las diversas necesidades de los procesos empresariales de su empresa, que tienen diferentes requisitos operativos, normativos y presupuestarios.

Unidad organizativa fundamental recomendada () OUs

Tu unidad organizativa (OUs) debe basarse en una función o en un conjunto común de controles, en lugar de reflejar la estructura jerárquica de la empresa. AWS recomienda empezar teniendo en cuenta la seguridad y la infraestructura. La mayoría de las empresas tienen equipos centralizados que abordan las necesidades de toda la organización. Recomendamos crear un conjunto de bases OUs para estas funciones específicas:

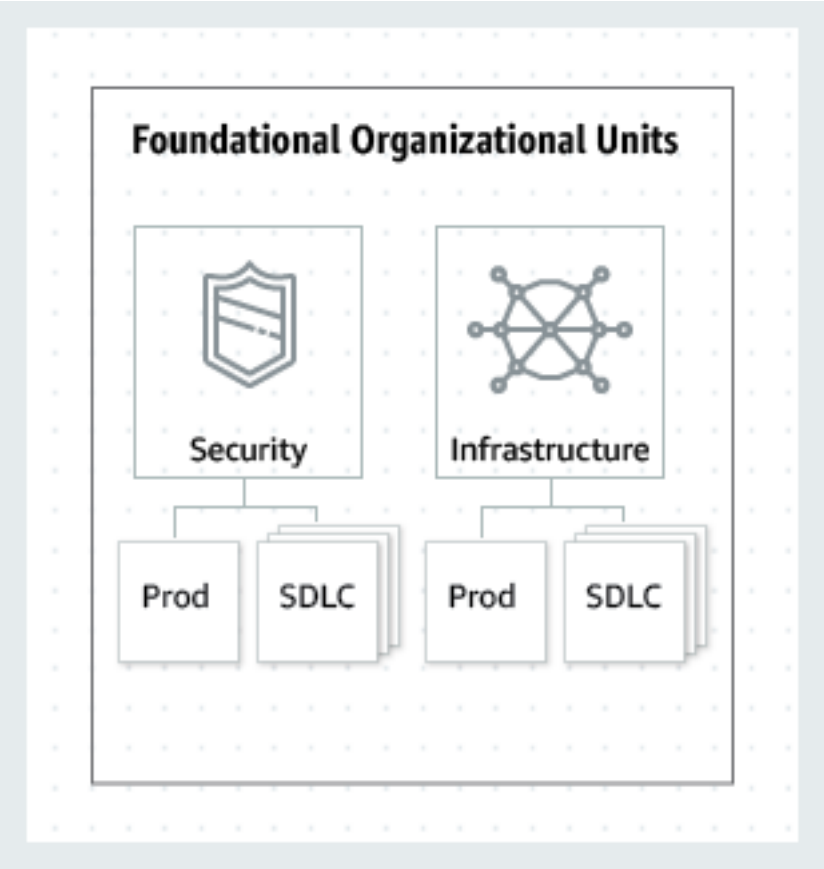
- Seguridad: se utiliza para los servicios de seguridad. Cree cuentas para los archivos de registro, el acceso de seguridad de solo lectura, las herramientas de seguridad y el acceso de emergencia.

- Infraestructura: se utiliza para servicios de infraestructura compartida, como servicios de redes y de TI. Cree cuentas para cada tipo de servicio de infraestructura que necesite.

Dado que la mayoría de las empresas tienen diferentes requisitos de política para las cargas de trabajo de producción, la infraestructura y la seguridad pueden haber estado centradas en las áreas OUs de no producción (SDLC) y de producción (Prod). Las cuentas de la unidad organizativa del entorno SDLC alojan cargas de trabajo que no son de producción y no deberían tener dependencias de producción con otras cuentas. Si hay variaciones en las políticas de unidades organizativas entre las distintas etapas del ciclo de vida, el SDLC se puede dividir en varias OUs (por ejemplo, de desarrollo y preproducción). Las cuentas de la unidad organizativa de Prod alojan las cargas de trabajo de producción.

Aplique políticas de OU para regular el entorno de Prod y SDLC de acuerdo con sus requisitos. En general, aplicar políticas a una OU es una práctica más recomendada que aplicarlas a cuentas individuales, ya que simplifica la gestión de las políticas y cualquier posible solución de problemas.

El siguiente diagrama muestra los fundamentos OUs (Prod y SDLC) de la seguridad y la infraestructura:



Unidad organizativa adicional recomendada () OUs

Una vez implementados los servicios centrales, recomendamos crearlos directamente relacionados con la creación OUs o el funcionamiento de sus productos o servicios. Muchos AWS clientes crean lo siguiente OUs después de establecer una base:

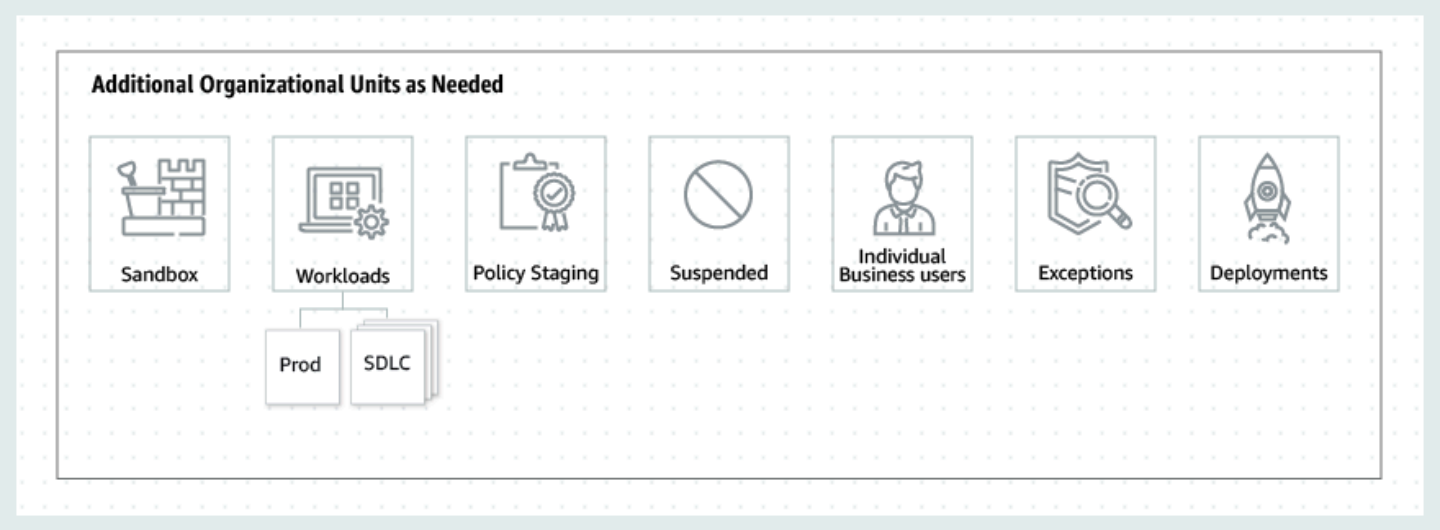
- Caja de arena: contiene Cuentas de AWS elementos que los desarrolladores individuales pueden utilizar para experimentar Servicios de AWS. Asegúrese de que estas cuentas se puedan separar de las redes internas.
- Cargas de trabajo: contiene los servicios de aplicaciones externos Cuentas de AWS que alojan. Debe estructurarse OUs en entornos SDLC y Prod (similares a los básicos OUs) para aislar y controlar estrictamente las cargas de trabajo de producción.

También recomendamos añadir más OUs para el mantenimiento y la expansión continua, en función de sus necesidades específicas. Los siguientes son algunos temas comunes basados en las prácticas de AWS los clientes actuales:

- Programación de políticas: mantiene AWS cuentas en las que puede probar los cambios de política propuestos antes de aplicarlos ampliamente a la organización. Comience por implementar los cambios a nivel de cuenta en la OU prevista y vaya avanzando poco a poco en otras cuentas y en el resto de la organización. OUs
- Suspendido: contiene contenido Cuentas de AWS que se ha cerrado y está pendiente de ser eliminado de la organización. Adjunte una SCP a esta OU que deniegue todas las acciones. Asegúrese de que las cuentas estén etiquetadas con detalles para garantizar su trazabilidad en caso de que sea necesario restaurarlas.
- Usuarios empresariales individuales: unidad organizativa de acceso limitado Cuentas de AWS destinada a usuarios empresariales (no desarrolladores) que puedan necesitar crear aplicaciones relacionadas con la productividad empresarial, por ejemplo, configurar un bucket de S3 para compartir informes o archivos con un socio.
- Excepciones: las Cuentas de AWS suspensiones se utilizan para casos de uso empresarial que tienen requisitos de seguridad o auditoría altamente personalizados, distintos de los definidos en la OU sobre cargas de trabajo. Por ejemplo, configurar una nueva aplicación o Cuenta de AWS función específica para una nueva función confidencial. SCPs Úselo a nivel de cuenta para satisfacer necesidades personalizadas. Considera configurar un sistema de detección y reacción con Amazon EventBridge y sus AWS Config reglas.

- Implementaciones: contiene contenido Cuentas de AWS pensado para una integración continua y continuo delivery/deployment (CI/CD deployments). You can create this OU if you have a different governance and operational model for CI/CD deployments as compared to accounts in the Workloads OUs (Prod and SDLC). Distribution of CI/CD helps reduce the organizational dependency on a shared CI/CD environment operated by a central team. For each set of SDLC/Prod Cuentas de AWS para una aplicación en la OU Workloads. Cree una cuenta para CI/CD en la OU Deployments.
- Transitorio: se utiliza como área de almacenamiento temporal para las cuentas y cargas de trabajo existentes antes de trasladarlas a las áreas estándar de la organización. Esto puede deberse a que las cuentas forman parte de una adquisición, fueron administradas anteriormente por un tercero, o a cuentas heredadas de una estructura organizativa antigua.

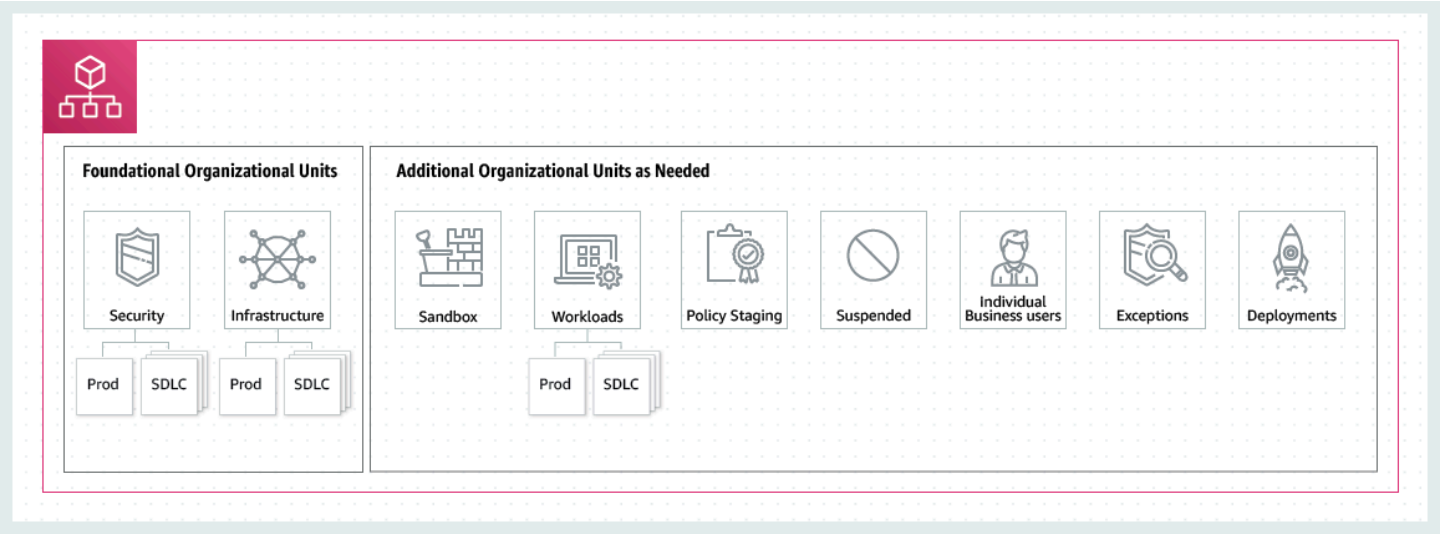
El siguiente diagrama muestra información adicional OUs para entornos aislados, cargas de trabajo, implementación de políticas, usuarios empresariales individuales o suspendidos, excepciones, despliegues y cuentas transitorias:



Conclusión

Una estrategia multicuenta bien diseñada puede ayudarle a innovar y, al mismo tiempo AWS, a garantizar que cumple sus necesidades de seguridad y escalabilidad. El marco descrito en este tema representa las AWS mejores prácticas que debe utilizar como punto de partida para su viaje. AWS

En el siguiente diagrama se muestran las recomendaciones básicas OUs y adicionales OUs:



Navegación por la raíz y la jerarquía de unidades organizativas (OU) con AWS Organizations

Para navegar por distintas unidades organizativas (OU) o al nodo raíz al desplazar cuentas o adjuntar políticas, puede utilizar la vista de “árbol” predeterminado.

AWS Management Console

Para navegar por la organización como un “árbol”

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, en la parte superior de la sección Organization (Organización), seleccione la opción de alternancia Hierarchy (Jerarquía) (en lugar de List [Lista]).
3. El árbol aparece inicialmente mostrando el nodo raíz y solo muestra el primer nivel de unidad organizativa secundaria y cuentas. Para ampliar el árbol para que muestre niveles más profundos, elija el icono de expandir ( ) junto a cualquier entidad principal. Para reducir el desorden y contraer una rama del árbol, elija el icono para colapsar ( ) junto a alguna de las entidades principales ampliadas.

4. Elija el nombre de una unidad organizativa o raíz para ver sus detalles y realizar determinadas operaciones. Como alternativa, puede elegir el botón de radio situado junto al nombre y realizar ciertas operaciones en esa entidad en el menú de Acciones.

También puede ver la lista de solo las cuentas de su organización en forma tabular, sin tener que desplazarse primero a una unidad organizativa para encontrarlas. En esta vista, no puede ver ninguna de las unidades organizativas ni manipular las políticas adjuntas a ellas.

AWS Management Console

Para ver la organización como una lista plana de cuentas sin jerarquía

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la páginaCuentas de AWS, en la parte superior de la sección Organización, elija la opción Ver solo Cuentas de AWSpara activarlo.
3. La lista de cuentas se muestra sin ninguna jerarquía.

Visualización de los detalles de una unidad organizativa (OU) con AWS Organizations

Cuando inicia sesión en la cuenta de administración de la organización en la consola de AWS Organizations, puede ver los detalles de las OU en su organización.

Permisos mínimos

Para ver los detalles de una unidad organizativa, debe contar con los permisos siguientes:

- `organizations:DescribeOrganizationalUnit`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:ListOrganizationsUnitsForParent`: solo se requiere cuando se utiliza la consola de Organizations

- `organizations:ListRoots`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para ver los detalles de una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, elija el nombre de la unidad organizativa (no su botón de opción) que desea examinar. Si la unidad organizativa es una unidad secundaria de otra OU, elija el icono del triángulo situado junto a su unidad organizativa principal para expandirla y verlos en el siguiente nivel de la jerarquía. Repita la operación hasta que encuentre la OU que desea.

   El cuadro de Detalles de la unidad organizativa muestra la información sobre la OU.

AWS CLI & AWS SDKs

Para ver los detalles de una unidad organizativa

Puede utilizar los siguientes comandos para ver detalles de una unidad organizativa:

- AWS CLI, SDK de AWS
  - list-roots
  - list-children
  - describe-organizational-unit

El siguiente ejemplo muestra cómo buscar el ID de una OU utilizando AWS CLI. Encontrará el ID de unidad organizativa atravesando la jerarquía comenzando por el comando `list-roots` y, a continuación, realizar `list-children` en el nodo raíz e iterativamente en cada uno de las secundarias hasta que encuentre la que desee.

```
$ aws organizations list-roots
{
    "Roots": [
```

```
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

Después de tener el ID de la unidad organizativa, el siguiente ejemplo muestra cómo recuperar los detalles sobre la OU.

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- SDK de AWS
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

Creación de una unidad organizativa (OU) con AWS Organizations

Cuando inicia sesión en la cuenta de administración de su organización, puede crear una unidad organizativa en el nodo raíz de su organización. Las unidades organizativas se pueden anidar hasta un máximo de cinco niveles de profundidad. Para crear una unidad organizativa, siga los pasos que se describen a continuación.

Important

Si esta organización se administra con AWS Control Tower, a continuación, cree sus unidades organizativas con la consola AWS Control Tower o API. Si crea la unidad organizativa en Organizations, esa unidad organizativa no está registrada conAWS Control Tower. Para obtener más información, consulte Referencia del tipo de recurso fuera deAWS Control Tower en la Guía del usuarioAWS Control Tower.

Permisos mínimos

Para crear una unidad organizativa dentro de un nodo raíz de su organización, debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:CreateOrganizationalUnit`

AWS Management Console

Para crear una unidad organizativa (OU)

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página Cuentas de AWS.

   La consola muestra el contenido del nodo raíz OU y sus contenidos. La primera vez que visite un nodo raíz, la consola mostrará todas las Cuentas de AWS en esa vista de nivel superior. Si previamente ha creado unidades organizativas y ha movido cuentas a ellas, la consola muestra

únicamente las unidades organizativas de nivel superior y todas las cuentas que aún no ha movido a una unidad organizativa.

3. (Opcional) Si desea crear una unidad organizativa dentro de una OU existente, vaya a la unidad organizativa secundaria eligiendo el nombre (no la casilla) de dicha unidad organizativa o eligiendo la ▶ al lado de las OU en la vista de árbol hasta que vea la que quiere, y luego elija su nombre.
4. Cuando haya seleccionado la unidad organizativa principal correcta en la jerarquía, en el menú Aciones, bajo Unidad organizacional, elija Crear nuevo
5. En el cuadro de diálogo Crear unidad organizacional, ingrese el nombre de la unidad organizativa que desee crear.
6. (Opcional) Agregue una o varias etiquetas seleccionando Agregar etiqueta y a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede asociar hasta 50 etiquetas a una unidad organizativa.
7. Por último, elija Crear unidad organizativa.

La nueva unidad organizativa aparecerá dentro de la principal. Ahora puede mover cuentas a esta unidad organizativa o asociarle políticas.

AWS CLI y AWS SDK

Para crear una OU

Los siguientes ejemplos de código muestran cómo utilizar `CreateOrganizationalUnit`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
```

```
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
            Name = orgUnitName,
            ParentId = "r-0000",
        };

        var response = await client.CreateOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
            Console.WriteLine($"Organizational unit {orgUnitName} Details");
            Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
        }
        else
        {
            Console.WriteLine("Could not create new organizational unit.");
        }
    }
}
```

- Para obtener información sobre la API, consulte CreateOrganizationalUnit en la Referencia de la API de AWS SDK for .NET.

CLI

AWS CLI

Creación de una unidad organizativa en raíz o UO principal

En el siguiente ejemplo se muestra cómo crear una unidad organizativa que se denomina AccountingOU:

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

El resultado incluye un objeto organizationalUnit con detalles sobre la nueva unidad organizativa:

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- Para obtener información sobre la API, consulte CreateOrganizationalUnit en la Referencia de comandos de la AWS CLI.

Cambio de nombre de una unidad organizativa (OU) con AWS Organizations

Cuando inicia sesión en la cuenta de administración de su organización, puede cambiar el nombre de una unidad organizativa. Para ello, siga los pasos que se describen a continuación.

Permisos mínimos

Para cambiar el nombre de una unidad organizativa dentro de un nodo raíz de su organización de , debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:UpdateOrganizationalUnit`

AWS Management Console

Para cambiar el nombre de una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, vaya a la unidad organizativa a la que le quiera cambiar el nombre y, a continuación, lleve a cabo uno de los siguientes pasos:
   - Seleccione el botón de opción
     
     situado junto a OU cuyo nombre desea cambiar. A continuación, en el menú de Acciones, en Unidad organizativa, elija Cambio de nombre.
   - Elija el nombre de la unidad organizativa para acceder a la página de detalles de la unidad organizativa. Luego, en la parte superior de la página, elija Renombrar.
3. En el cuadro de diálogo Cambiar el nombre de unidad organizativa, ingrese un nuevo nombre y, a continuación, elija Guardar cambios.

AWS CLI & AWS SDKs

Para cambiar el nombre de una unidad organizativa

Puede utilizar uno de los siguientes comandos para cambiar el nombre de una unidad organizativa:

- AWS CLI: update-organizational-unit

En el ejemplo siguiente se muestra cómo renombrar una OU.

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
}
```

- SDK de AWS: UpdateOrganizationalUnit

Etiquetado de una unidad organizativa (OU) con AWS Organizations

Cuando inicia sesión en la cuenta de administración de su organización, puede agregar o quitar las etiquetas adjuntas a una unidad organizativa. Para ello, siga los pasos que se describen a continuación.

Permisos mínimos

Para editar las etiquetas asociadas a una unidad organizativa dentro de un nodo raíz de su organización de , debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:DescribeOrganizationalUnit`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas asociadas a una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, vaya a la unidad organizativa cuyas etiquetas desee editar y elíjala.
3. En la página de detalles de la unidad organizativa, elija la opción Etiquetas y, a continuación, elija Administrar etiquetas.
4. Puede realizar cualquiera de estas acciones en esta pestaña:
   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No se puede modificar la clave de etiqueta. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente seleccionando Eliminar junto a la etiqueta que desea eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
5. Seleccione Guardar los cambios después de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas asociadas a una unidad organizativa

Puede utilizar uno de los siguientes comandos para cambiar las etiquetas asociadas a una unidad organizativa:

- AWS CLI:etiquetar recurso y desetiquetar recurso

  En el siguiente ejemplo se asocia la etiqueta `"Department"="12345"` a una unidad organizativa. Tenga en cuenta que `Key` y `Value` distinguen entre mayúsculas y minúsculas.

```
$ aws organizations tag-resource \
    --resource-id ou-a1b2-f6g7h222 \
```

```
    --tags Key=Department,Value=12345
```

Este comando no genera ninguna salida si se realiza correctamente.

En el ejemplo siguiente se quita la etiqueta `Department` de una OU.

```
$ aws organizations untag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tag-keys Department
```

Este comando no genera ninguna salida si se realiza correctamente.

- SDK de AWS:TagResource y UntagResource

Mover cuentas a una unidad organizativa (OU) o entre la raíz y las unidades organizativas con AWS Organizations

Cuando inicia sesión en la cuenta de administración de su organización, puede mover las cuentas de su organización desde el nodo raíz a una unidad organizativa, de una unidad organizativa a otra, o de vuelta al nodo raíz desde una unidad organizativa. Al colocar una cuenta dentro de una unidad organizativa, esta obtiene todas las políticas que se han asociado a la unidad organizativa principal y a todas las demás unidades organizativas que van desde la principal hasta el nodo raíz. Si una cuenta no está en una unidad organizativa, solo obtendrá las políticas que se han asociado directamente al nodo raíz y las políticas que se han asociado directamente a la cuenta. Para mover cuentas, siga los pasos que se describen a continuación.

Permisos mínimos

Para mover cuentas a una nueva ubicación en la jerarquía de unidades organizativas, debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:MoveAccount`

AWS Management Console

Para mover cuentas a una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la páginaCuentas de AWS, busque la cuenta o cuentas que desea mover. Puede navegar por la jerarquía de unidades organizativas o habilitar Ver solo Cuentas de AWS para ver una lista plana de cuentas sin la estructura de unidad organizativa. Si tiene muchas cuentas, puede que tenga que elegir Cargar más cuentas en 'Nombre de OU' en la parte inferior de la lista para encontrar todas las que desea mover.
3. Elija la casilla de verificación
   ☑
   junto al nombre de cada cuenta que desea mover.
4. En menú Acciones, enCuenta de AWS, elija Mover.
5. En el cuadro de diálogo MoverCuenta de AWS elija la unidad organizativa o el nodo raíz al que desea mover la cuenta y después elija MoverCuenta de AWS.

AWS CLI & AWS SDKs

Para mover cuentas a una unidad organizativa

Puede utilizar uno de los siguientes comandos para mover una cuenta:

- AWS CLI: move-account

  En el ejemplo siguiente se mueve un Cuenta de AWS de un nodo raíz a una OU. Tenga en cuenta que debe especificar los ID de los contenedores de origen y de destino.

  ```
  $ aws organizations move-account \
      --account-id 111122223333 \
      --source-parent-id r-a1b2 \
      --destination-parent-id ou-a1b2-f6g7h111
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- SDK de AWS: MoveAccount

Visualización de los detalles del nodo raíz con AWS Organizations

Cuando inicia sesión en la cuenta de administración de la organización en la consola de AWS Organizations, puede ver los detalles del nodo raíz administrativo.

> **Permisos mínimos**
>
> Para ver los detalles de un nodo raíz, debe contar con los siguientes permisos:
>
> - `organizations:DescribeOrganization` (solo consola)
> - `organizations:ListRoots`

El nodo raíz es el contenedor superior de la jerarquía de unidades organizativas (OU) y generalmente se comporta como una unidad organizativa. Sin embargo, como el contenedor en la parte superior de la jerarquía, los cambios en el nodo raíz afectan a todas las demás OU y cada Cuenta de AWS en la organización.

AWS Management Console

Para ver los detalles del nodo raíz

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página Cuentas de AWS y elija la opción Nodo raíz OU (su nombre, no el botón de opción).
3. La página de detalles del Nodo raíz aparece y muestra los detalles del nodo raíz.

AWS CLI & AWS SDKs

Para ver los detalles del nodo raíz

Puede utilizar uno de los siguientes comandos para ver detalles de un nodo raíz:

- AWS CLI: list-roots

  El siguiente ejemplo muestra cómo recuperar los detalles del nodo raíz, incluidos los tipos de política que están habilitados actualmente en la organización:

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- SDK de AWS: ListRoots

Eliminación de una unidad organizativa (OU) con AWS Organizations

Cuando inicia sesión en la cuenta de administración de su organización, puede eliminar las unidades organizativas que ya no necesite.

En primer lugar, debe mover todas las cuentas fuera de la unidad organizativa y de todas las unidades organizativas secundarias, y después puede eliminar las unidades organizativas secundarias.

Permisos mínimos

Para eliminar una unidad organizativa, debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:DeleteOrganizationalUnit`

AWS Management Console

Para eliminar una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la páginaCuentas de AWS, busque las unidades organizativas que desea eliminar y elija la casilla de verificación
   ☑
   junto al nombre de cada unidad organizativa.
3. Seleccionar Acciones y, a continuación, en Unidad organizativa, elija Eliminar.
4. Para confirmar que desea eliminar las unidades organizativas, ingrese el nombre de la unidad organizativa (si eligió eliminar solo una) o la palabra «eliminar» (si eligió más de una) y, a continuación, elija Eliminar.

   AWS Organizations elimina las unidades organizativas y las quita de la lista.

AWS CLI y AWS SDK

Eliminación de una unidad organizativa

Los siguientes ejemplos de código muestran cómo utilizar `DeleteOrganizationalUnit`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;
```

```
    /// <summary>
    /// Shows how to delete an existing AWS Organizations organizational unit.
    /// </summary>
    public class DeleteOrganizationalUnit
    {
        /// <summary>
        /// Initializes the Organizations client object and calls
        /// DeleteOrganizationalUnitAsync to delete the organizational unit
        /// with the selected ID.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitId = "ou-0000-00000000";

            var request = new DeleteOrganizationalUnitRequest
            {
                OrganizationalUnitId = orgUnitId,
            };

            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- Para obtener información sobre la API, consulte DeleteOrganizationalUnit en la Referencia de la API de AWS SDK for .NET.

CLI

AWS CLI

Eliminación de una unidad organizativa

En el ejemplo siguiente se muestra cómo se elimina una OU. En el ejemplo se supone que anteriormente se eliminaron todas las cuentas y demás unidades organizativas de la unidad organizativa:

```
aws organizations delete-organizational-unit --organizational-unit-id ou-examplerootid111-exampleouid111
```

- Para obtener información sobre la API, consulte DeleteOrganizationalUnit en la Referencia de comandos de la AWS CLI.

Administrar las políticas de la organización con AWS Organizations

Las políticas le AWS Organizations permiten aplicar tipos adicionales de administración Cuentas de AWS a su organización. Puede utilizar políticas cuando todas las características están habilitadas en su organización.

La AWS Organizations consola muestra el estado de activación o desactivación de cada tipo de política. En la pestaña Organize accounts (Organizar cuentas), elija `Root` en el panel de navegación izquierdo. El panel de detalles del lado derecho de la pantalla muestra todos los tipos de políticas disponibles. La lista indica cuáles están habilitados y cuáles están deshabilitados en la raíz de esa organización. Si está disponible la opción Enable (Habilitar) para un tipo, significa que ese tipo está deshabilitado actualmente. Si está disponible la opción Disable (Deshabilitar) para un tipo, significa que ese tipo está habilitado actualmente.

Temas

- Tipos de políticas
- Políticas de autorización en AWS Organizations
- Políticas de gestión en AWS Organizations
- Administrador delegado para AWS Organizations
- Habilitar un tipo de política
- Deshabilitar un tipo de política
- Crear políticas de la organización con AWS Organizations
- Actualización de las políticas de la organización con AWS Organizations
- Edición de etiquetas adjuntas a las políticas de la organización con AWS Organizations
- Adjuntar las políticas de la organización con AWS Organizations
- Separar las políticas de la organización con AWS Organizations
- Obtener información sobre las políticas de su organización
- Eliminar políticas de la organización con AWS Organizations

Tipos de políticas

Organizations ofrece tipos de política en las dos categorías generales siguientes:

Políticas de autorización

Las políticas de autorización le ayudan a gestionar de forma centralizada la seguridad de Cuentas de AWS toda la organización.

- Las políticas de control de servicios (SCPs) ofrecen un control central sobre los permisos máximos disponibles para los usuarios de IAM y las funciones de IAM en una organización.
- Las políticas de control de recursos (RCPs) ofrecen un control central sobre los permisos máximos disponibles para los recursos de una organización.

Políticas de administración

Las políticas de administración le ayudan a configurar Servicios de AWS y gestionar de forma centralizada sus funciones en toda la organización.

- Las políticas declarativas le permiten declarar y aplicar de forma centralizada las configuraciones deseadas para una determinada escala Servicio de AWS en toda la organización. Una vez conectada, la configuración siempre se mantiene cuando el servicio agrega nuevas funciones o APIs.
- Las políticas de respaldo le permiten administrar y aplicar planes de respaldo de manera centralizada a los AWS recursos de las cuentas de una organización.
- Las políticas de etiquetas le permiten estandarizar las etiquetas adjuntas a los AWS recursos en las cuentas de una organización.
- Las políticas de Chatbot te permiten controlar el acceso a las cuentas de una organización desde aplicaciones de chat como Slack y Microsoft Teams.
- Las políticas de exclusión de los servicios de IA te permiten controlar la recopilación de datos para los servicios de AWS IA en todas las cuentas de una organización.

En la siguiente tabla se resumen algunas características de cada tipo de política. Para conocer las características adicionales de estos tipos de políticas, consulte Cuotas y límites de servicio para AWS Organizations.

Tipo de política	Categoría de política	Afecta a la administración de la cuenta	Número máximo que se puede asociar a un nodo raíz, unidad organizativa o cuenta	Tamaño máximo	Admite la visualización efectiva de la política para la unidad organizativa o cuenta
SCP	Autorización	 No	5	5120 caracteres	 No
RCP	Autorización	 No	5	5120 caracteres	 No
Política declarativa	Administración	 Sí	10	10,000 caracteres	 Sí
Política de copia de seguridad	Administración	 Sí	10	10,000 caracteres	 Sí
Política de etiquetas	Administración	 Sí	10	10,000 caracteres	 Sí

Tipo de política	Categoría de política	Afecta a la administración de la cuenta	Número máximo que se puede asociar a un nodo raíz, unidad organizativa o cuenta	Tamaño máximo	Admite la visualización efectiva de la política para la unidad organizativa o cuenta
Política de chatbot	Administración	 Sí	5	10,000 caracteres	 Sí
Política de exclusión de servicios de IA	Administración	 Sí	5	2500 caracteres	 Sí

Políticas de autorización en AWS Organizations

Las políticas de autorización le AWS Organizations permiten configurar y administrar de forma centralizada el acceso de los principales y los recursos de sus cuentas de miembros. La forma en que esas políticas afectan a las unidades organizativas (OUs) y a las cuentas a las que se aplican depende del tipo de política de autorización que se aplique.

Existen dos tipos diferentes de políticas de autorización AWS Organizations: políticas de control de servicios (SCPs) y políticas de control de recursos (RCPs).

Temas

- Diferencias entre SCPs y RCPs
- Uso y SCPs RCPs
- Políticas de control de servicios (SCPs)
- Políticas de control de recursos (RCPs)

Diferencias entre SCPs y RCPs

SCPs son controles centrados en el principal. SCPs cree una barrera de permisos o establezca límites a los permisos máximos disponibles para los directores en sus cuentas de miembros. Puede usar un SCP cuando desee aplicar de forma centralizada controles de acceso consistentes a los directores de su organización. Esto puede incluir especificar a qué servicios pueden acceder sus usuarios y roles de IAM, a qué recursos pueden acceder o las condiciones en las que pueden realizar solicitudes (por ejemplo, desde regiones o redes específicas).

RCPs son controles centrados en los recursos. RCPs cree una barrera de permisos o establezca límites a los permisos máximos disponibles para los recursos en sus cuentas de miembros. Puede utilizar un RCP cuando desee aplicar de forma centralizada controles de acceso coherentes en todos los recursos de su organización. Esto puede restringir el acceso a sus recursos para que solo puedan acceder a ellos las identidades que pertenecen a su organización, o especificar las condiciones en las que las identidades externas a su organización pueden acceder a sus recursos.

Algunos controles se pueden aplicar de forma similar mediante SCPs y RCPs. Por ejemplo, es posible que desee impedir que sus usuarios carguen objetos no cifrados en S3, que puede escribirse como un SCP para controlar las acciones que sus directores pueden realizar en sus depósitos de S3. Este control también se puede escribir como un RCP para requerir el cifrado siempre que un responsable cargue objetos en el bucket de S3. Es posible que prefiera la segunda opción si su bucket permite que entidades ajenas a su organización, como proveedores externos, carguen objetos a su bucket de S3. Sin embargo, algunos controles solo se pueden implementar en un RCP y otros solo se pueden implementar en un SCP. Para obtener más información, consulte Casos de uso generales para y SCPs RCPs.

Uso y SCPs RCPs

SCPs y RCPs son controles independientes. Puede optar por habilitar solo SCPs o RCPs usar ambos tipos de políticas a la vez. Al usar ambas SCPs y RCPs, puede crear un perímetro de datos en torno a sus identidades y sus recursos.

SCPs proporcionan la capacidad de controlar a qué recursos pueden acceder sus identidades. Por ejemplo, es posible que desee permitir que sus identidades accedan a los recursos de su AWS organización. Sin embargo, es posible que desee impedir que sus identidades accedan a recursos ajenos a su organización. Puede hacer cumplir este control mediante SCPs.

RCPs proporcionan la posibilidad de controlar qué identidades pueden acceder a sus recursos. Por ejemplo, es posible que desee permitir que las identidades de su organización puedan acceder a los

recursos de su organización. Sin embargo, es posible que desee impedir que identidades externas a su organización accedan a sus recursos. Puede hacer cumplir este control mediante RCPs. RCPs permiten influir en los permisos efectivos de los directores externos a su organización que acceden a sus recursos. SCPs solo puede afectar a los permisos efectivos de los directores de su AWS organización.

Casos de uso generales para y SCPs RCPs

La siguiente tabla detalla los casos de uso generales para usar un SCP y RCPs

		Impactos			
Caso de uso	Tipo de política	Sus identidades	Identidades externas	Sus recursos	Recursos externos (objetivo de la solicitud)
Restrinja los servicios o acciones que pueden utilizar sus identidades	SCP	X		X	X
Restrinja a qué recursos pueden acceder sus identidades	SCP	X		X	X
Haga cumplir los requisitos sobre cómo sus identidades pueden acceder a los recursos	SCP	X		X	X

		Impactos		
Restrinja qué identidad es pueden acceder a sus recursos	RCP	X	X	X
Proteja los recursos confidenc iales de su organización	RCP	X	X	X
Haga cumplir los requisito s sobre cómo se puede acceder a sus recursos	RCP	X	X	X

Políticas de control de servicios (SCPs)

Las políticas de control de servicios (SCPs) son un tipo de política organizacional que puede usar para administrar los permisos en su organización. SCPsofrecen un control central sobre el máximo de permisos disponibles para los IAM usuarios y IAM las funciones de su organización. SCPsle ayudan a garantizar que sus cuentas se ajusten a las directrices de control de acceso de su organización. SCPsestán disponibles solo en una organización que tenga todas las funciones habilitadas. SCPsno están disponibles si su organización ha activado únicamente las funciones de facturación unificada. Para obtener instrucciones sobre cómo habilitar SCPs, consulte Habilitar un tipo de política.

SCPsno conceda permisos a los IAM usuarios y IAM roles de su organización. UnSCP. An SCP define una barrera de permisos, o establece límites, a las acciones que pueden realizar los IAM usuarios y los IAM roles de su organización. Para conceder permisos, el administrador debe adjuntar políticas para controlar el acceso, como las políticas basadas en la identidad que se asocian a IAM los usuarios y las IAM funciones, y las políticas basadas en los recursos que se adjuntan a

los recursos de sus cuentas. Para obtener más información, consulte las políticas basadas en la identidad y las políticas basadas en recursos en la Guía del usuario. IAM

Los permisos efectivos son la intersección lógica entre lo que permiten las políticas de control de recursos (RCPs) SCP y lo que permiten las políticas basadas en la identidad y en los recursos.

> ⚠ SCPsno afectan a los usuarios ni a las funciones de la cuenta de administración
>
> SCPsno afectan a los usuarios ni a las funciones de la cuenta de administración. Afectan solo a las cuentas de miembro de su organización. Esto también significa que SCPs se aplican a las cuentas de los miembros designadas como administradores delegados.

Temas en esta página

- Probando los efectos de SCPs
- Tamaño máximo de SCPs
- Adscribirse SCPs a diferentes niveles de la organización
- SCPefectos en los permisos
- Utilizar los datos de acceso para mejorar SCPs
- Las tareas y entidades no están restringidas por SCPs
- Evaluación de SCP
- Sintaxis de SCP
- Ejemplos de políticas de control de servicios
- Solución de problemas de políticas de control de servicio (SCP) con AWS Organizations

Probando los efectos de SCPs

AWS le recomienda encarecidamente que no se fije SCPs en la raíz de su organización sin comprobar exhaustivamente el impacto que la política tiene en las cuentas. En lugar de ello, cree una unidad organizativa en la que pueda mover sus cuentas de una en una, o al menos en incrementos pequeños, a fin de garantizar que no bloquee inadvertidamente a los usuarios de servicios clave. Una forma de determinar si una cuenta utilizará un servicio es examinar los datos a los que tuvo acceso el servicio por última vez en IAM. Otra forma consiste en AWS CloudTrail registrar el uso del servicio a API nivel.

> **Note**
>
> No debes eliminar la ullAWSAccess política F a menos que la modifiques o la sustituyas por una política independiente que prevea las acciones permitidas; de lo contrario, todas AWS las acciones de las cuentas de los miembros fallarán.

Tamaño máximo de SCPs

Todos los caracteres de tu lista se SCP tienen en cuenta para su tamaño máximo. Los ejemplos de esta guía muestran los objetos SCPs formateados con espacios en blanco adicionales para mejorar su legibilidad. Sin embargo, para ahorrar espacio si el tamaño de la política se aproxima al tamaño máximo, puede eliminar todos los espacios en blanco, como espacios y saltos de línea, que estén fuera de las comillas.

> **Tip**
>
> Usa el editor visual para crear tu. SCP Este elimina automáticamente el espacio en blanco adicional.

Adscribirse SCPs a diferentes niveles de la organización

Para obtener una explicación detallada de cómo SCPs funciona, consulteEvaluación de SCP.

SCPefectos en los permisos

SCPsson similares a las políticas de AWS Identity and Access Management permisos y utilizan prácticamente la misma sintaxis. Sin embargo, SCP Dan nunca concede permisos. En cambio, SCPs son controles de acceso que especifican el máximo de permisos disponibles para los IAM usuarios y IAM roles de su organización. Para obtener más información, consulte la lógica de evaluación de políticas en la Guía del IAM usuario.

- SCPsafectan únicamente a IAM los usuarios y roles gestionados por las cuentas que forman parte de la organización. SCPsno afectan directamente a las políticas basadas en recursos. Tampoco afectan a los usuarios ni a los roles de cuentas que no pertenecen a la organización. Por ejemplo, tomemos el caso de un bucket de Amazon S3 que es propiedad de la cuenta A de una organización. La política de bucket (basada en recursos) concede acceso a los usuarios de la cuenta B que no pertenecen a la organización. La cuenta A tiene un adjuntoSCP. Esto SCP no se

aplica a los usuarios externos de la cuenta B. Solo SCP se aplica a los usuarios administrados por la cuenta A de la organización.

- A SCP restringe los permisos de los IAM usuarios y los roles en las cuentas de los miembros, incluido el usuario raíz de la cuenta de miembro. Cada cuenta tiene únicamente los permisos concedidos por cada elemento principal situado por encima de ella. Si un permiso está bloqueado en cualquier nivel superior a la cuenta, ya sea de forma implícita (al no incluirse en una declaración de `Allow` política) o de forma explícita (al incluirse en una declaración de `Deny` política), un usuario o rol de la cuenta afectada no podrá usar ese permiso, incluso si el administrador de la cuenta asocia la `AdministratorAccess` IAM política con los permisos */* al usuario.
- SCPsafectan únicamente a las cuentas de los miembros de la organización. No tienen ningún efecto en los usuarios ni en los roles de la cuenta de administración. Esto también significa que SCPs se aplican a las cuentas de los miembros designadas como administradores delegados. Para obtener más información, consulte Prácticas recomendadas para la cuenta de administración.
- A los usuarios y las funciones se les deben seguir concediendo permisos con las políticas de permisos de IAM adecuadas. Un usuario sin políticas de IAM permisos no tiene acceso, incluso si las correspondientes SCPs permiten todos los servicios y todas las acciones.
- Si un usuario o rol tiene una política de IAM permisos que otorga acceso a una acción que también está permitida por la autoridad correspondienteSCPs, el usuario o rol puede realizar esa acción.
- Si un usuario o rol tiene una política de IAM permisos que otorga acceso a una acción que no está permitida o denegada explícitamente por la autoridad correspondienteSCPs, el usuario o rol no podrá realizar esa acción.
- SCPsafectan a todos los usuarios y roles de las cuentas asociadas, incluido el usuario raíz. Las únicas excepciones son las descritas en Las tareas y entidades no están restringidas por SCPs.
- SCPsno afectan a ningún rol vinculado a un servicio. Los roles vinculados al servicio permiten que otros se Servicios de AWS integren AWS Organizations y no se pueden restringir mediante ellos. SCPs
- Al deshabilitar el tipo SCP de política en una raíz, todas SCPs se separan automáticamente de todas AWS Organizations las entidades de esa raíz. AWS Organizations las entidades incluyen unidades organizativas, organizaciones y cuentas. Si se vuelve a habilitar SCPs en una raíz, esa raíz solo volverá a ser la `FullAWSAccess` política predeterminada que se adjunta automáticamente a todas las entidades de la raíz. Todos los archivos adjuntos SCPs a AWS Organizations entidades que antes SCPs estaban deshabilitados se pierden y no se pueden recuperar automáticamente, aunque puede volver a adjuntarlos manualmente.
- Si SCP hay un límite de permisos (una IAM función avanzada) y un límite, entonces el límite, la política basada en la identidad y la SCP política basada en la identidad deben permitir la acción.

Utilizar los datos de acceso para mejorar SCPs

Al iniciar sesión con las credenciales de la cuenta de administración, puede ver los datos de una AWS Organizations entidad o política a los que se accedió por última vez en la AWS Organizationssección de la IAM consola. También puede usar AWS Command Line Interface (AWS CLI) o AWS API in IAM para recuperar los datos del servicio al que se accedió por última vez. Estos datos incluyen información sobre los servicios permitidos a los que los IAM usuarios y los roles de una AWS Organizations cuenta intentaron acceder por última vez y cuándo. Puede utilizar esta información para identificar los permisos no utilizados, de forma que pueda ajustarlos mejor SCPs a fin de cumplir mejor con el principio de privilegios mínimos.

Por ejemplo, es posible que tenga una lista de denegaciones SCP que prohíba el acceso a tres Servicios de AWS. Se permiten todos los servicios que no figuran en SCP la `Deny` declaración. Los datos del servicio al que se accedió por última vez indican cuáles Servicios de AWS están permitidos SCP pero nunca se utilizan. IAM Con esa información, puede actualizarla SCP para denegar el acceso a los servicios que no necesita.

Para obtener más información, consulte los siguientes temas en la Guía del usuario de IAM:

- Visualización de los datos del último acceso al servicio de Organizations
- Uso de datos para ajustar los permisos de una unidad organizativa

Las tareas y entidades no están restringidas por SCPs

No se pueden utilizar SCPs para restringir las siguientes tareas:

- Cualquier acción realizada por la cuenta de administración
- Cualquier acción realizada mediante permisos que adjuntos a un rol vinculado al servicio
- Registrarse en el plan Enterprise Support como usuario raíz
- Proporcione una funcionalidad de firmante confiable para el contenido CloudFront privado
- Configurar reverse DNS para un servidor de correo electrónico de Amazon Lightsail y una instancia de EC2 Amazon como usuario root
- Tareas en algunos servicios AWS relacionados:
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk

- Marketing de productos de Amazon API

Evaluación de SCP

> **Note**
>
> La información de esta sección no se aplica a los tipos de políticas de administración, incluidas las políticas de copia de seguridad, las políticas de etiquetas, las políticas de chatbot o las políticas de exclusión de servicios de IA. Para obtener más información, consulte Descripción de la herencia de políticas de administración.

Como puede adjuntar varias políticas de control de servicios (SCPs) en diferentes niveles AWS Organizations, comprender cómo SCPs se evalúan puede ayudarle a redactar las SCPs que arrojen el resultado correcto.

Temas

- ¿Cómo SCPs trabajar con Allow
- ¿Cómo SCPs trabajar con Deny
- Estrategia de uso SCPs

¿Cómo SCPs trabajar con Allow

Para que se conceda un permiso a una cuenta específica, debe haber una declaración **`Allow`** explícita en cada nivel, desde la raíz hasta cada unidad organizativa situada en la ruta directa a la cuenta (incluida la propia cuenta de destino). Por eso, cuando lo habilita SCPs, AWS Organizations adjunta una política SCP AWS administrada llamada Full AWSAccess que permite todos los servicios y acciones. Si esta política se elimina y no se reemplaza en ningún nivel de la organización, todas OUs las cuentas que estén por debajo de ese nivel quedarán bloqueadas para que no puedan realizar ninguna acción.

Por ejemplo, veamos la situación que se muestra en las figuras 1 y 2. Para permitir un permiso o un servicio en la cuenta B, la SCP que permita el permiso o el servicio debe estar vinculada a la raíz, a la unidad organizativa de producción y a la propia cuenta B.

La evaluación del SCP sigue un deny-by-default modelo, lo que significa que se deniegan todos los permisos que no SCPs estén explícitamente permitidos en el sistema. Si no hay una declaración de

autorización en ninguno de los SCPs niveles, como raíz, unidad organizativa de producción o cuenta B, se deniega el acceso.

> **Notas**
>
> - Una declaración de `Allow` en un SCP permite al elemento `Resource` para tener solo una entrada de `"*"`.
> - Un registro `Allow` en una SCP no puede tener un elemento `Condition` en absoluto.

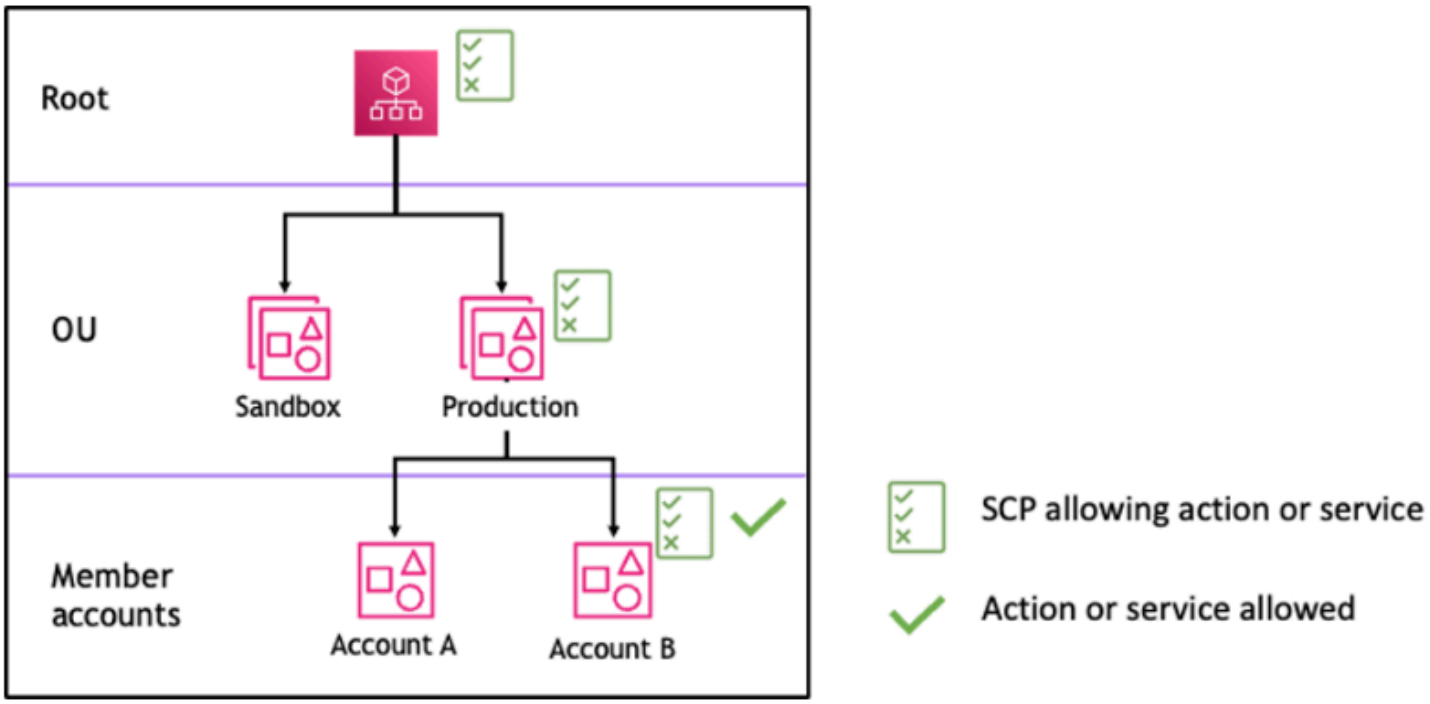


Figura 1: Ejemplo de estructura organizativa con una declaración *`Allow`* adjunta en la raíz, la OU de producción y la cuenta B

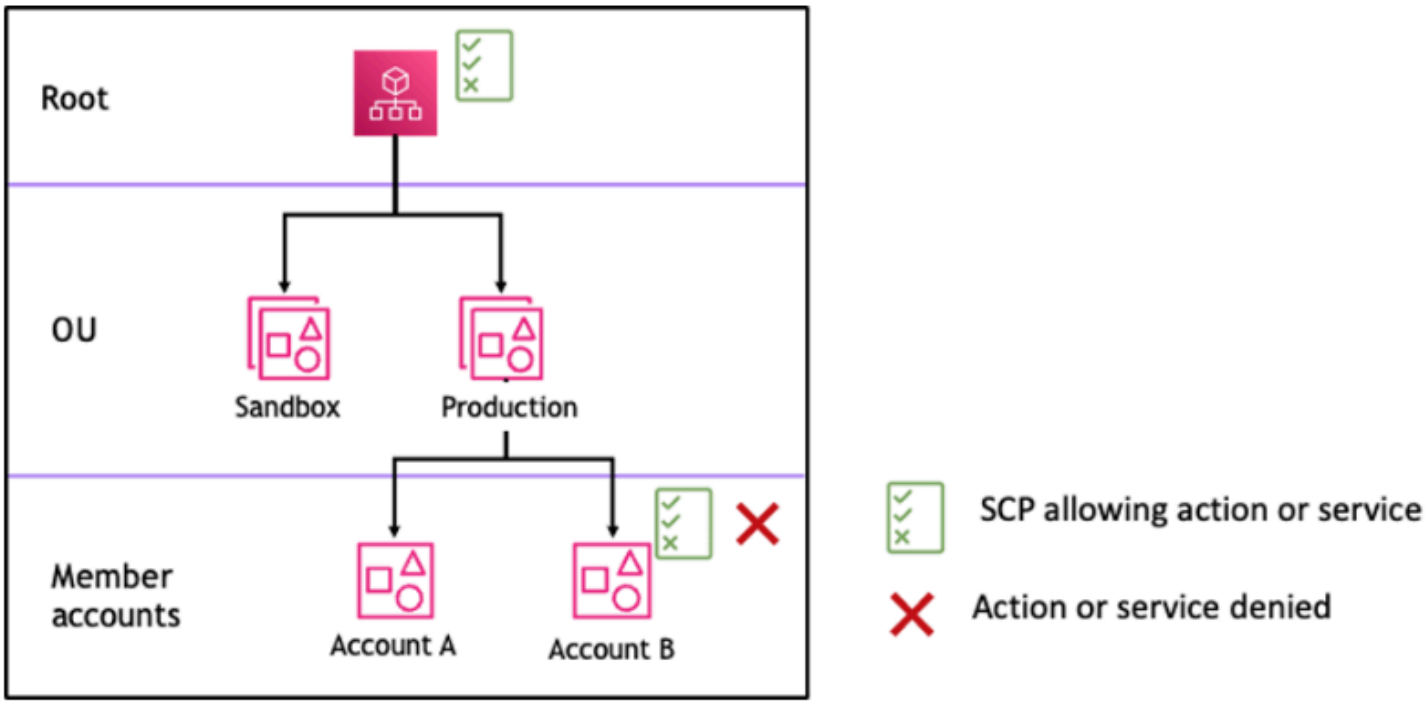


Figura 2: Ejemplo de estructura organizativa con una declaración *`Allow`* faltante en la OU de producción y su impacto en la cuenta B

¿Cómo SCPs trabajar con Deny

Si se niega un permiso para una cuenta específica, cualquier SCP desde la raíz hasta cada unidad organizativa situada en la ruta directa a la cuenta (incluida la propia cuenta de destino) puede denegar ese permiso.

Por ejemplo, supongamos que hay una SCP adjunta a la OU de producción que tiene una declaración `Deny` explícita especificada para un servicio determinado. Resulta que también hay otra SCP conectada a la raíz y a la cuenta B que permite explícitamente el acceso a ese mismo servicio, como se muestra en la figura 3. Como resultado, se negará el acceso al servicio tanto a la cuenta A como a la cuenta B, ya que se aplica una política de denegación a cualquier nivel de la organización para todas las cuentas OUs y las cuentas de los miembros que dependen de él.

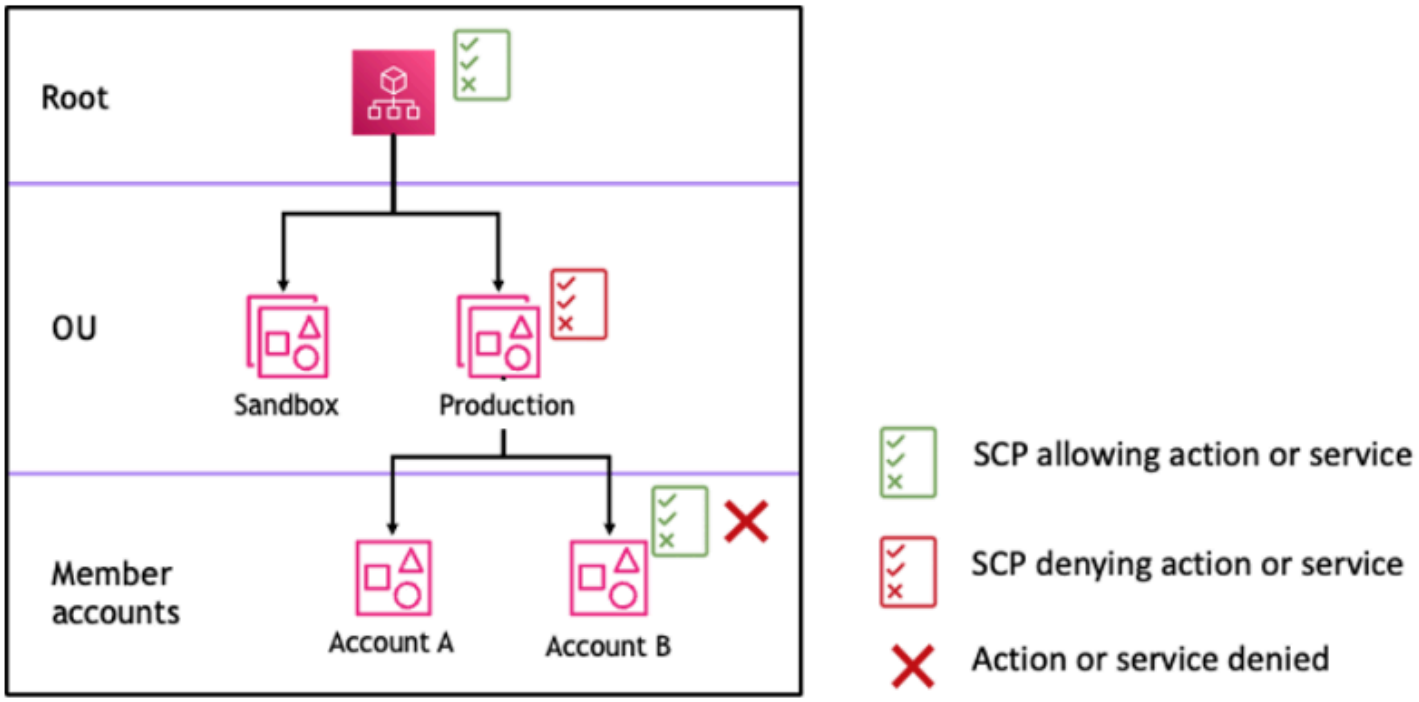


Figura 3: Ejemplo de estructura organizativa con una declaración *Deny* adjunta en la OU de producción y su impacto en la cuenta B

Estrategia de uso SCPs

Al escribir SCPs , puede utilizar una combinación de `Deny` declaraciones `Allow` y declaraciones para permitir las acciones y servicios previstos en su organización. `Deny`Las declaraciones son una forma eficaz de implementar restricciones que deberían aplicarse a una parte más amplia de la organización o OUs porque, cuando se aplican a nivel raíz o de la unidad organizativa, afectan a todas las cuentas que dependen de ella.

Por ejemplo, puede implementar una política con declaraciones `Deny` en Evitar que las cuentas de miembros dejen la organización. en la raíz, que será efectiva para todas las cuentas de la organización. Las declaraciones de denegación también admiten un elemento de condición que puede ser útil para crear excepciones.

> **Tip**
>
> Puede utilizar los datos del servicio al que se accedió por última vez en IAM SCPs para actualizarlos y restringir el acceso únicamente a los Servicios de AWS que necesite. Para obtener más información, consulte Visualización de los datos del último acceso al servicio de Organizations en la Guía del usuario IAM.

AWS Organizations Cuando se crea, adjunta un SCP AWS gestionado denominado Full AWSAccess a cada raíz, unidad organizativa y cuenta. Esta política permite todos los servicios y acciones. Puede sustituir el Full AWSAccess por una política que permita solo un conjunto de servicios, de modo que no Servicios de AWS se permitan los nuevos, a menos que se autoricen explícitamente mediante una actualización. SCPs Por ejemplo, si su organización solo quiere permitir el uso de un subconjunto de servicios en su entorno, puede usar una declaración `Allow` para permitir solo servicios específicos.

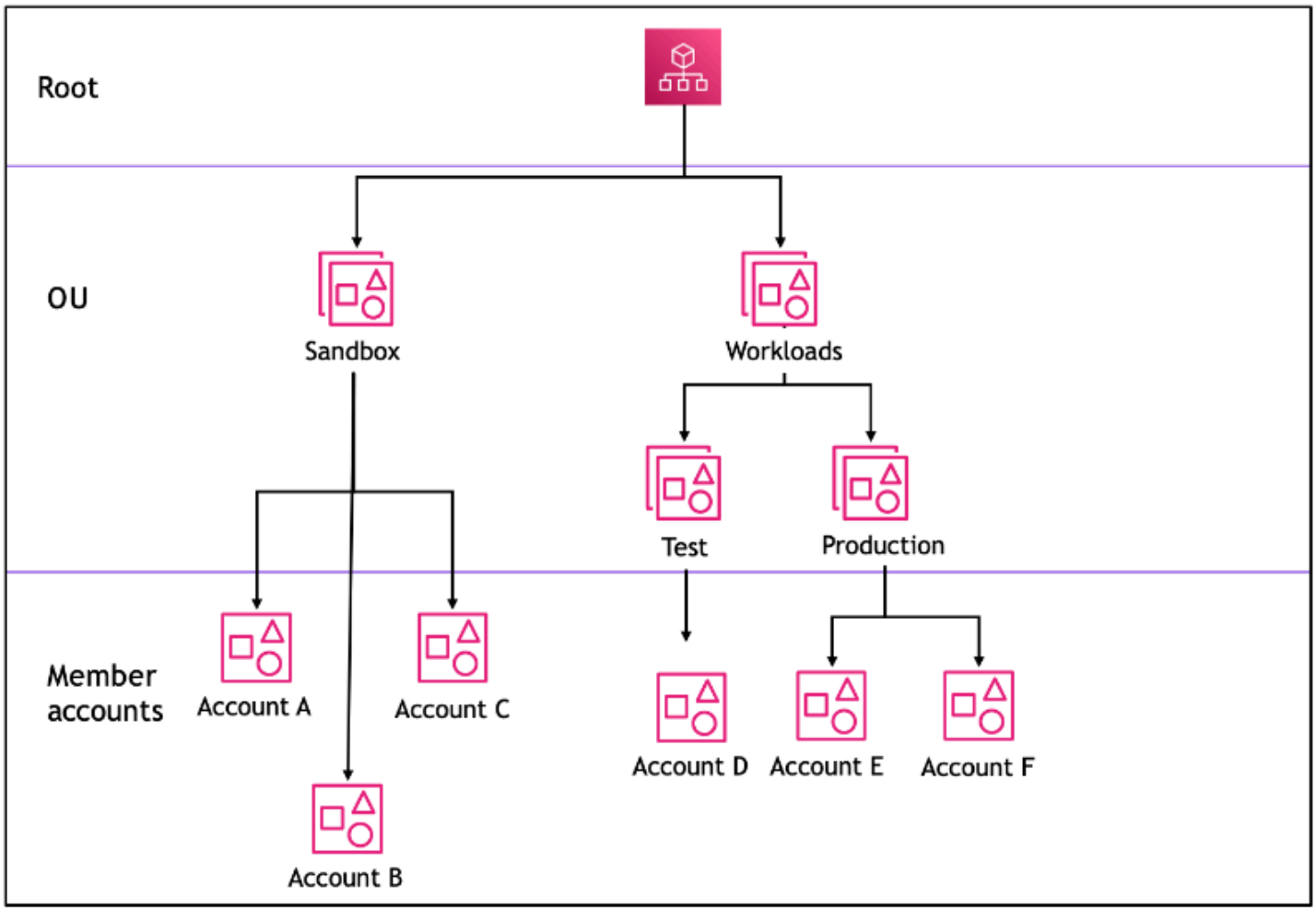
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Una política que combine las dos declaraciones podría ser como la del ejemplo siguiente, que impide que las cuentas de los miembros salgan de la organización y permite el uso de los servicios AWS deseados. El administrador de la organización puede separar la AWSAccess política completa y adjuntar esta en su lugar.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Ahora, considere el siguiente ejemplo de estructura organizativa para comprender cómo puede aplicar varios tipos de organización SCPs en distintos niveles de una organización.



En la tabla siguiente se muestran las políticas efectivas de la OU de un entorno aislado.

Escenario	SCP en la raíz	SCP en la OU de un entorno aislado	SCP en la cuenta A	Política resultante en la cuenta A	Política resultante en la cuenta B y la cuenta C
1	AWS Acceso completo	AWS Acceso total + denegar el acceso a S3	AWS Acceso total + denegar el EC2 acceso	Sin S3, sin EC2 acceso	Sin acceso a S3
2	AWS Acceso completo	Permitir el EC2 acceso	Permitir el EC2 acceso	Permitir el EC2 acceso	Permitir el EC2 acceso
3	Denegar el acceso a S3	Permitir el acceso a S3	AWS Acceso completo	Sin acceso a los servicios	Sin acceso a los servicios

En la tabla siguiente se muestran las políticas efectivas de la OU de cargas de trabajo.

Escenario	SCP en la raíz	SCP en OU de cargas de trabajo	SCP en OU de pruebas	Política resultante en la cuenta D	Políticas resultantes en OU de producción, cuenta E y cuenta F
1	AWS Acceso completo	AWS Acceso completo	AWS Acceso total + denegar el EC2 acceso	Sin EC2 acceso	AWS Acceso completo
2	AWS Acceso completo	AWS Acceso completo	Permitir el EC2 acceso	Permitir el EC2 acceso	AWS Acceso completo
3	Denegar el acceso a S3	AWS Acceso completo	Permitir el acceso a S3	Sin acceso a los servicios	Sin acceso a S3

Sintaxis de SCP

Las políticas de control de servicios (SCPs) utilizan una sintaxis similar a la que utilizan las políticas de permisos AWS Identity and Access Management (IAM) y las políticas basadas en recursos (como las políticas de bucket de Amazon S3). Para obtener más información sobre las políticas del IAM y su sintaxis, consulte Información general de las políticas del AM en la Guía del usuario IAM.

Una política SCP es un archivo de texto sin formato estructurado de acuerdo con las reglas JSON. Utiliza los elementos que se describen en este tema.

> **Note**
>
> Todos los caracteres de la SCP se contabilizan para calcular su tamaño máximo. Los ejemplos de esta guía muestran las imágenes SCPs formateadas con espacios en blanco adicionales para mejorar su legibilidad. Sin embargo, para ahorrar espacio si el tamaño de la política se aproxima al tamaño máximo, puede eliminar todos los espacios en blanco, como espacios y saltos de línea, que estén fuera de las comillas.

Para obtener información general sobre SCPs, consulte. Políticas de control de servicios (SCPs)

Resumen de elementos

En la siguiente tabla se resumen los elementos de política que puede utilizar. SCPs Algunos elementos de política solo están disponibles para denegar acciones. SCPs En la columna Efectos admitidos se muestra el tipo de efecto que se puede utilizar con cada elemento de política SCPs.

Elemento	Finalidad	Efectos admitidos
Action	Especifica el AWS servicio y las acciones que el SCP permite o deniega.	`Allow`, `Deny`

Elemento	Finalidad	Efectos admitidos
Effect	Define si la instrucción SCP permite o deniega el acceso a los usuarios y roles IAM en una cuenta.	`Allow`, `Deny`
Instrucción	Sirve como contenedor de elementos de política. Puede incluir varias declaraciones. SCPs	`Allow`, `Deny`

Elemento	Finalidad	Efectos admitidos
Statement ID (Sid) (ID de instrucción)	(Opcional) Proporciona un nombre fácil de recordar para la instrucción.	`Allow`, `Deny`
Versión	Especifica las reglas de sintaxis del lenguaje que se utilizarán para procesar la política.	`Allow`, `Deny`
Condición	Especifica las condiciones que determinan cuándo se aplica la instrucción.	`Deny`

Elemento	Finalidad	Efectos admitidos
NotAction	Especifica los AWS servicios y las acciones que están exentos del SCP. Se utiliza en lugar del elemento `Action`.	`Deny`
Resource	Especifica los AWS recursos a los que se aplica el SCP.	`Deny`

En las siguientes secciones se proporciona más información y ejemplos de cómo se utilizan los elementos de política. SCPs

Temas

- Elementos Action y NotAction
- Elemento Condition
- Elemento Effect
- Elemento Resource
- Elemento Statement
- Elemento de ID de instrucción (Sid)
- Elemento Version
- Elementos no compatibles

Elementos **`Action`** y **`NotAction`**

Cada instrucción debe contener uno de los elementos siguientes:

- En las instrucciones de permiso o denegación, un elemento `Action`.
- En las instrucciones de denegación solo (cuando el valor del elemento `Effect` sea `Deny`), un elemento `Action` o `NotAction`.

El valor del `NotAction` elemento `Action` o es una lista (una matriz JSON) de cadenas que identifican AWS los servicios y las acciones que la sentencia permite o deniega.

Cada cadena consta de la abreviatura del servicio (como "s3", "ec2", "iam" u "organizaciones"), en letras minúsculas, seguida de un carácter de punto y coma y una acción de ese servicio. Las acciones y las acciones excluidas no distinguen entre mayúsculas y minúsculas. Por lo general, todas se escriben y cada palabra comienza con una letra mayúscula y el resto en minúscula. Por ejemplo: `"s3:ListAllMyBuckets"`.

También puede utilizar caracteres comodín tales como el asterisco (*) o el signo de interrogación de cierre (?) en una SCP:

- Utilice un asterisco (*) como carácter comodín como representación de varias acciones que comparten parte de un nombre. El valor `"s3:*"` significa todas las acciones del servicio Amazon S3. El valor solo `"ec2:Describe*"` coincide con las EC2 acciones que comienzan por «Describir».
- Utilice el carácter comodín del signo de interrogación de cierre (?) como representación de un carácter único.

> **Note**
>
> En una política SCP, el carácter comodín (*) o (?) de un elemento `Action` o `NotAction` únicamente puede aparecer solo o al final de la cadena. No puede aparecer al principio o en el medio de la cadena. Por lo tanto, `"servicename:action*"` es válido, pero `"servicename:*action"` ambos no `"servicename:some*action"` son válidos en SCPs.

Para obtener una lista de todos los servicios y las acciones que admiten tanto en las políticas de permisos de IAM como AWS Organizations SCPs en las políticas de permisos de IAM, consulte las acciones, los recursos y las claves de condición de AWS los servicios en la Guía del usuario de IAM.

Para obtener más información, consulte Elementos de la política JSON de IAM: acción y Elementos de la política JSON de IAM: NotAction en la Guía del usuario de IAM.

Ejemplo de elemento **`Action`**

En el siguiente ejemplo, se muestra un SCP con una declaración que permite a los administradores de cuentas delegar los permisos de descripción, inicio, detención y finalización de las EC2 instancias de la cuenta. Este es un ejemplo de una lista de permitidos, y es útil cuando las políticas `Allow *` predeterminadas no se adjuntan para que, de forma predeterminada, los permisos sean denegados implícitamente. Si la política `Allow *` predeterminada sigue estando asociada al nodo raíz, unidad organizativa o cuenta a la que la siguiente política está asociada, entonces la política no tiene ningún efecto.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

El siguiente ejemplo muestra cómo puede denegar el acceso a servicios que no desea usar en cuentas asociadas. Se supone que los valores predeterminados `"Allow *"` SCPs siguen asociados a todas OUs y a la raíz. Este ejemplo de política impide que los administradores de cuentas asociadas deleguen permisos para los servicios de IAM EC2, Amazon y Amazon RDS. Cualquier acción desde otros servicios se puede delegar siempre y cuando no exista otra política asociada que la deniegue.

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

```
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

Ejemplo de elemento **`NotAction`**

En el siguiente ejemplo, se muestra cómo se puede utilizar un `NotAction` elemento para excluir AWS los servicios del efecto de la política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
         }
       }
     }
   ]
}
```

Con esta declaración, las cuentas afectadas se limitan a realizar las acciones especificadas Región de AWS, excepto cuando utilizan acciones de IAM.

Elemento **`Condition`**

Puede especificar un elemento `Condition` en las instrucciones de denegación de una SCP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
```

```
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

Esta SCP deniega el acceso a todas las operaciones fuera de las regiones `eu-central-1` y `eu-west-1`, excepto para las acciones de los servicios enumerados.

Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Elemento **`Effect`**

Cada instrucción debe contener un elemento `Effect`. El valor puede ser `Allow` o `Deny`. Afecta a las acciones enumeradas en la misma instrucción.

Para obtener más información, consulte Elemento de la política de JSON de IAM: Efecto en la Guía del usuario IAM.

`"Effect": "Allow"`

En el siguiente ejemplo se muestra una SCP con una instrucción que contiene un elemento `Effect` con un valor de `Allow` que permite a los usuarios de la cuenta realizar acciones para el servicio Amazon S3. Este ejemplo es útil en una organización que usa la estrategia de permitidos (donde las políticas `FullAWSAccess` predeterminadas estén desasociadas y, por tanto, los permisos se deniegan implícitamente de forma predeterminada). El resultado es que la instrucción permite los permisos de Amazon S3 en cualquier cuenta asociada:

```
{
```

```
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

Tenga en cuenta que aunque esta instrucción utiliza la misma palabra clave con el valor `Allow` que en una política de permisos de IAM, las SCP no conceden en realidad permisos de usuario. En su lugar, SCPs actúan como filtros que especifican los permisos máximos para las cuentas de una organización, unidad organizativa (OU) o cuenta. En el ejemplo anterior, aunque un usuario de la cuenta tuviera la política `AdministratorAccess` administrada asociada, esta SCP limita las acciones de todos los usuarios de la cuenta afectada a solo las acciones de Amazon S3.

`"Effect": "Deny"`

En una declaración en la que el `Effect` elemento tenga un valor de`Deny`, también puedes restringir el acceso a recursos específicos o definir las condiciones para cuando SCPs estén en vigor.

A continuación, se muestra un ejemplo de cómo utilizar una clave de condición en una instrucción de denegación.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

Esta declaración en un SCP establece una barrera de protección para evitar que las cuentas afectadas (donde el SCP está adjunto a la propia cuenta o a la raíz de la organización o unidad organizativa que contiene la cuenta) lancen instancias de Amazon EC2 si la EC2 instancia de Amazon no está configurada para ello. `t2.micro` Aunque se adjunte a la cuenta una política de IAM que permita esta acción, la medida de seguridad creada por la SCP la impedirá.

Elemento **`Resource`**

En las instrucciones cuyo elemento `Effect` tiene el valor `Allow`, puede especificar solamente "*" en el elemento `Resource` de una SCP. No puede especificar los nombres de recursos de Amazon (ARNs) de recursos individuales.

También puede utilizar caracteres comodín tales como el asterisco (*) o el signo de interrogación de cierre (?) en el elemento de recurso:

- Utilice un asterisco (*) como carácter comodín como representación de varias acciones que comparten parte de un nombre.
- Utilice el carácter comodín del signo de interrogación de cierre (?) como representación de un carácter único.

En las declaraciones en las que el `Effect` elemento tiene un valor de`Deny`, puede especificar un individuo ARNs, como se muestra en el siguiente ejemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

Esta SCP restringe a las cuentas de usuarios y roles IAM para que no puedan realizar cambios en un rol de IAM administrativo común creado en todas las cuentas de la organización.

Para obtener más información, consulte Elemento de la política de JSON de IAM: Resource en la Guía del usuario de IAM.

Elemento **`Statement`**

Una política SCP consta de uno o varios elementos `Statement`. Solo puede tener una palabra clave `Statement` en una política, pero el valor puede ser una matriz de instrucciones JSON (rodeadas por caracteres [ ]).

El siguiente ejemplo muestra una única instrucción que consta de los elementos `Effect`, `Action` y `Resource`.

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

El siguiente ejemplo incluye dos instrucciones como una lista de matriz dentro de un elemento `Statement`. La primera sentencia permite todas las acciones, mientras que la segunda deniega cualquier EC2 acción. El resultado es que un administrador de la cuenta puede delegar cualquier permiso excepto los de Amazon Elastic Compute Cloud (Amazon EC2).

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
```

Para obtener más información, consulte Elementos de la política de JSON de IAM: Instrucción en la Guía del usuario de IAM.

Elemento de ID de instrucción (**`Sid`**)

El elemento `Sid` es un identificador opcional que se proporciona para la instrucción de la política. Puede asignar un valor de `Sid` a cada instrucción de una matriz de instrucciones. En el siguiente ejemplo de SCP se incluye una instrucción `Sid` de muestra.

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

Para obtener más información, consulte Elementos de la política de JSON de IAM: ID en la Guía del usuario de IAM.

Elemento **`Version`**

Todas las SCP deben incluir un elemento `Version` con el valor `"2012-10-17"`. Este es el mismo valor de versión que la versión más reciente de las políticas de permisos de IAM.

```
    "Version": "2012-10-17",
```

Para obtener más información, consulte Elementos de la política de JSON de IAM: Versión en la Guía del usuario de IAM.

Elementos no compatibles

Los siguientes elementos no son compatibles con SCPs:

- `Principal`
- `NotPrincipal`
- `NotResource`

Ejemplos de políticas de control de servicios

Los ejemplos de políticas de control de servicios (SCP) que se muestran en este tema solo tienen fines informativos.

Antes de usar estos ejemplos

Antes de usar estos ejemplos de SCP en la organización, haga lo siguiente:

- Revise las SCP atentamente y personalícelas para ajustarlas a sus requisitos únicos.
- Pruebe a fondo las SCP en su entorno con los Servicios de AWS que utilice.

  Las políticas de ejemplo de esta sección demuestran la implementación y el uso de las SCP. Ellas no son destinadas a ser interpretadas como recomendaciones AWS oficiales o prácticas óptimas que se apliquen exactamente como se indica. Es su responsabilidad probar cuidadosamente cualquier política basada en denegaciones para determinar su idoneidad para resolver los requisitos empresariales de su entorno. Las políticas de control de servicios basadas en denegación pueden limitar o bloquear involuntariamente el uso de Servicios de AWS, a menos que agregue las excepciones necesarias a la política. Para ver un ejemplo de tal excepción, vea el primer ejemplo que exime a los servicios globales de las reglas que bloquean el acceso a Regiones de AWS no deseado.
- Recuerde que una SCP afecta a todos los usuarios y roles e incluso al usuario raíz de todas las cuentas a las que se asocia.
- Recuerde que una SCP no repercute en roles vinculados a servicios. Los roles vinculados a servicios permiten que otros Servicios de AWS se integren con AWS Organizations y no se puedan restringir con SCP.

Tip

Puede utilizar los datos del último acceso al servicio de IAM para actualizar las SCP para restringir el acceso únicamente a los Servicios de AWS que necesite. Para obtener más información, consulte Visualización de los datos del último acceso al servicio de Organizations en la Guía del usuario IAM.

Cada una de las siguientes políticas es un ejemplo de una estrategia de política de lista de denegación . Las políticas de lista de denegación deben adjuntarse junto con otras políticas que permitan las acciones aprobadas en las cuentas afectadas. Por ejemplo, la política `FullAWSAccess` predeterminada permite el uso de todos los servicios de una cuenta. Esta política se adjunta de forma predeterminada a la raíz, a todas las unidades organizativas (OU) y a todas las cuentas. En realidad no concede los permisos; ninguna SCP lo hace. En su lugar, permite a los administradores

de la cuenta delegar el acceso a esas acciones asociando políticas de permisos de AWS Identity and Access Management (IAM) estándar adjuntar los usuarios, roles o grupos de la cuenta. Cada una de estas políticas de lista de denegación sustituye cualquier política mediante el bloqueo del acceso a los servicios o acciones especificados.

Ejemplos

- Ejemplos generales
  - Denegar acceso a AWS en función de la Región de AWS solicitada
  - Evitar que los usuarios y los roles de IAM realicen determinados cambios
  - Impedir que los usuarios y roles de IAM realicen cambios especificados, con una excepción para un rol de administrador especificado
  - Requisito de operación de API por parte de MFA
  - Bloquee el acceso al servicio del usuario raíz
  - Evitar que las cuentas de miembros dejen la organización.
- Ejemplo SCPs de AWS Chatbot
  - Denegación de todas las operaciones de IAM
  - Denegación de las solicitudes PUT de buckets de S3 procedentes de un canal de Slack específico
- SCP de ejemplo para Amazon CloudWatch
  - Evitar que los usuarios deshabiliten CloudWatch o modifiquen su configuración
- SCP de ejemplo para AWS Config
  - Evitar que los usuarios deshabiliten AWS Config o cambien sus reglas
- Ejemplo SCPs de Amazon Elastic Compute Cloud (Amazon EC2)
  - Exigir que EC2 las instancias de Amazon usen un tipo específico
  - Impida el lanzamiento de EC2 instancias sin IMDSv2
  - Impedir la desactivación del cifrado predeterminado de Amazon EBS
  - Impida crear y adjuntar volúmenes que no sean de gp3
- SCP de ejemplo para Amazon GuardDuty
  - Evitar que los usuarios deshabiliten GuardDuty o modifiquen su configuración
- SCP de ejemplo para AWS Resource Access Manager
  - Prevención de uso compartido externo
  - Permitir que determinadas cuentas compartan solo tipos de recursos especificados

- Evitar compartir con organizaciones o unidades organizativas (OU)
- Permitir el uso compartido solo con usuarios y roles de IAM especificados
- Ejemplos de SCP para Controlador de recuperación de aplicaciones de Amazon (ARC)
  - Impedir que los usuarios actualicen los estados de control de enrutamiento de ARC
- Ejemplos de SCP para Amazon S3
  - Impedir la carga de objetos sin cifrar en Amazon S3
- Ejemplo de SCP para etiquetar recursos
  - Requerir una etiqueta en los recursos creados especificados
  - Impedir que las etiquetas se modifiquen excepto por entidades autorizadas
- Ejemplo de SCP para Amazon Virtual Private Cloud (Amazon VPC)
  - Evitar que los usuarios eliminen los registros de flujo de Amazon VPC
  - Evitar que cualquier VPC que no tenga acceso a Internet lo obtenga

Ejemplos generales

Denegar acceso a AWS en función de la Región de AWS solicitada

Este SCP deniega el acceso a cualquier operación fuera de las regiones especificadas. Reemplazar `eu-central-1` y `eu-west-1` con el Regiones de AWS que desea usar. Proporciona exenciones para operaciones en servicios globales aprobados. En este ejemplo también se muestra cómo exonerar las solicitudes realizadas por cualquiera de las dos funciones de administrador especificadas.

> **Note**
>
> Para utilizar la SCP de denegación de región con AWS Control Tower, consulte Deny access to AWS based on the requested Región de AWS en la Guía de referencia de controles de AWS Control Tower.

Esta política utiliza el efecto `Deny` para denegar el acceso a todas las solicitudes de operaciones que no se encuentran en una de las dos regiones aprobadas (`eu-central-1` y `eu-west-1`). El elemento NotAction permite enumerar los servicios cuyas operaciones (u operaciones individuales) están exentas de esta restricción. Dado que los servicios globales tienen puntos de enlace alojados físicamente por la región `us-east-1`, deben quedar exentos de esta manera. Con una SCP

estructurada de esta manera, se permiten las solicitudes hechas a servicios globales en la región `us-east-1` si el servicio solicitado está incluido en el elemento `NotAction`. Cualquier otra solicitud a los servicios de la región `us-east-1` se deniega mediante esta política de ejemplo.

> **Note**
>
> Es posible que este ejemplo no incluya todos los últimos Servicios de AWS u operaciones globales. Sustituya la lista de servicios y operaciones por los servicios globales que las cuentas de la organización utilizan.
>
> > **Sugerencia**
> >
> > Puede ver los últimos datos del servicio a los que se ha accedido en la consola de IAM para determinar qué servicios globales utiliza la organización. La pestaña Asesor de acceso de la página de detalles de un usuario, grupo o rol de IAM muestra los servicios de AWS que ha utilizado esa entidad, ordenados por el acceso más reciente.

> **Consideraciones**
>
> - AWS KMS y AWS Certificate Manager admiten puntos de enlace regionales. Sin embargo, si desea utilizarlos con un servicio global como Amazon CloudFront, debe incluirlos en la lista de exclusión de servicios globales del siguiente ejemplo de SCP. Un servicio global como Amazon CloudFront normalmente requiere acceso a AWS KMS y ACM en la misma región, que para un servicio global es la región EE. UU. Este (Norte de Virginia) (`us-east-1`).
> - De forma predeterminada, AWS STS es un servicio global y debe incluirse en la lista de exclusión de servicios globales. Sin embargo, puede habilitar AWS STS para utilizar los puntos de enlace de la región en lugar de un único punto de enlace global. Si lo hace, puede eliminar STS de la lista de exención de servicio global en el siguiente ejemplo de SCP. Para obtener más información, consulte Administración de AWS STS en la Región de AWS.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
```

```
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Evitar que los usuarios y los roles de IAM realicen determinados cambios

Esta SCP restringe a las cuentas de usuarios y roles IAM para que no puedan realizar cambios en un rol de IAM especificado que ha creado en todas las cuentas de la organización.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
```

```
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

Impedir que los usuarios y roles de IAM realicen cambios especificados, con una excepción para un rol de administrador especificado

Esta SCP se basa en el ejemplo anterior, pero especifica una excepción para los administradores. Impide que los usuarios y roles de IAM de las cuentas afectadas realicen cambios en un rol administrativo común de IAM creado en todas las cuentas de la organización, excepto para los administradores que utilizan un rol específico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
```

```
        }
      }
    }
  ]
}
```

Requisito de operación de API por parte de MFA

Utilice una SCP similar a la siguiente para requerir que la autenticación multifactor (MFA) esté habilitada antes de que un usuario o rol de IAM puedan realizar una acción. En este ejemplo, la acción consiste en detener una instancia de Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

Bloquee el acceso al servicio del usuario raíz

La siguiente política restringe todo acceso a las acciones especificadas para del usuario raíz de una cuenta miembro. Si desea evitar que en sus cuentas se usen las credenciales raíz de determinadas maneras concretas, añada sus propias acciones a esta política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
```

```
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

Evitar que las cuentas de miembros dejen la organización.

La siguiente política bloquea el uso de la operación API `LeaveOrganization` para que los administradores de cuentas miembro no puedan eliminar sus cuentas de la organización.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo SCPs de AWS Chatbot

Ejemplos en esta categoría

- Denegación de todas las operaciones de IAM
- Denegación de las solicitudes PUT de buckets de S3 procedentes de un canal de Slack específico

Denegación de todas las operaciones de IAM

El siguiente SCP deniega todas las operaciones de IAM invocadas en todas AWS Chatbot las configuraciones.

```
{
    "Effect": "Deny",
    "Action": "iam:*",
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:ChatbotSourceArn": "arn:aws:chatbot::*:*"
        }
    }
}
```

Denegación de las solicitudes PUT de buckets de S3 procedentes de un canal de Slack específico

La siguiente política deniega las solicitudes PUT de Amazon S3 en el bucket especificado de todas las solicitudes que procedan de un canal de Slack.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExampleS3Deny",
            "Effect": "Deny",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringLike": {
                      "aws:ChatbotSourceArn": "arn:aws:chatbot::*:chat-configuration/
slack-channel/*"
                }
            }
        }
    ]
}
```

SCP de ejemplo para Amazon CloudWatch

Ejemplos en esta categoría

- Evitar que los usuarios deshabiliten CloudWatch o modifiquen su configuración

Evitar que los usuarios deshabiliten CloudWatch o modifiquen su configuración

Un operador de CloudWatch de nivel inferior necesita monitorear paneles y alarmas. Sin embargo, el operador no debe poder eliminar ni cambiar ningún panel o alarma que pueden haber aplicado las personas mayores. Esta SCP evita que los usuarios o las funciones de cualquier cuenta afectada ejecuten cualquiera de los comandos de CloudWatch que podrían eliminar o cambiar sus paneles o alarmas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

SCP de ejemplo para AWS Config

Ejemplos en esta categoría

- Evitar que los usuarios deshabiliten AWS Config o cambien sus reglas

Evitar que los usuarios deshabiliten AWS Config o cambien sus reglas

Esta SCP evita que los usuarios o las funciones de cualquier cuenta afectada ejecuten operaciones de AWS Config que podrían deshabilitar AWS Config o modificar sus reglas o disparadores.

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

```
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Ejemplo SCPs de Amazon Elastic Compute Cloud (Amazon EC2)

Ejemplos en esta categoría

- Exigir que EC2 las instancias de Amazon usen un tipo específico
- Impida el lanzamiento de EC2 instancias sin IMDSv2
- Impedir la desactivación del cifrado predeterminado de Amazon EBS
- Impida crear y adjuntar volúmenes que no sean de gp3

Exigir que EC2 las instancias de Amazon usen un tipo específico

Con esta SCP, se denegarán todos los lanzamientos de instancias que no usen el tipo de instancia `t2.micro`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
```

```
      }
    }
  ]
}
```

Impida el lanzamiento de EC2 instancias sin IMDSv2

La siguiente política impide a todos los usuarios lanzar EC2 instancias sin IMDSv2 ellas.

```
[
   {
      "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":"*"
```

```
    }
]
```

La siguiente política impide a todos los usuarios lanzar EC2 instancias sin ellas, IMDSv2 pero permite que identidades de IAM específicas modifiquen las opciones de metadatos de las instancias.

```
[
  {
    "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": "*",
    "Condition": {
      "ArnNotLike": {
```

```
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

Impedir la desactivación del cifrado predeterminado de Amazon EBS

La siguiente política impide que todos los usuarios deshabiliten el cifrado predeterminado de Amazon EBS.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

Impida crear y adjuntar volúmenes que no sean de gp3

La siguiente política impide a todos los usuarios crear o adjuntar volúmenes de Amazon EBS que no sean del tipo de volumen gp3. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreationAndAttachmentOfNonGP3Volumes",
      "Effect": "Deny",
      "Action": [
        "ec2:AttachVolume",
        "ec2:CreateVolume",
        "ec2:RunInstances"
      ],
      "Resource": "arn:aws:ec2:*:*:volume/*",
      "Condition": {
        "StringNotEquals": {
          "ec2:VolumeType": "gp3"
```

```
        }
      }
    }
  ]
}
```

Esto puede ayudar a aplicar una configuración de volumen estandarizada en toda la organización.

> **No se impiden las modificaciones del tipo de volumen**
>
> No puede restringir la acción de modificar un volumen gp3 existente a un volumen de Amazon EBS de otro tipo utilizando. SCPs Por ejemplo, este SCP no le impediría modificar un volumen gp3 existente por un volumen gp2. Esto se debe a que la clave de condición `ec2:VolumeType` comprueba el tipo de volumen antes de modificarlo.

SCP de ejemplo para Amazon GuardDuty

Ejemplos en esta categoría

- Evitar que los usuarios deshabiliten GuardDuty o modifiquen su configuración

Evitar que los usuarios deshabiliten GuardDuty o modifiquen su configuración

Esta SCP impide que los usuarios o los roles de cualquier cuenta afectada deshabiliten GuardDuty o modifiquen su configuración, ya sea directamente como un comando o a través de la consola. Permite el acceso de solo lectura a la información y los recursos de GuardDuty.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "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:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

SCP de ejemplo para AWS Resource Access Manager

Ejemplos en esta categoría

- Prevención de uso compartido externo
- Permitir que determinadas cuentas compartan solo tipos de recursos especificados
- Evitar compartir con organizaciones o unidades organizativas (OU)
- Permitir el uso compartido solo con usuarios y roles de IAM especificados

Prevención de uso compartido externo

En el siguiente ejemplo, SCP evita que los usuarios creen recursos compartidos que permiten compartir con usuarios de IAM y roles que no forman parte de la organización.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Permitir que determinadas cuentas compartan solo tipos de recursos especificados

La siguiente SCP permite cuentas 111111111111 y 222222222222 para crear recursos compartidos que compartan listas de prefijos y asociar listas de prefijos con recursos compartidos existentes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Allow",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
```

```
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

Evitar compartir con organizaciones o unidades organizativas (OU)

La siguiente SCP impide que los usuarios creen recursos compartidos que comparten recursos con una organización u OU.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

Permitir el uso compartido solo con usuarios y roles de IAM especificados

El siguiente ejemplo de SCP permite a los usuarios compartir recursos con solamente la organización `o-12345abcdef`, unidad organizativa `ou-98765fedcba`, y cuenta `111111111111`.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
        }
    ]
}
```

Ejemplos de SCP para Controlador de recuperación de aplicaciones de Amazon (ARC)

Ejemplos en esta categoría

- Impedir que los usuarios actualicen los estados de control de enrutamiento de ARC

Impedir que los usuarios actualicen los estados de control de enrutamiento de ARC

Un operador de ARC de nivel inferior necesita supervisar paneles y ver información de ARC. Sin embargo, el operador no debe poder actualizar los controles de enrutamiento para realizar conmutación por error para la aplicación de una Región de AWS a otra, como podría hacer un operador sénior. Esta SCP impide que los usuarios o roles de cualquier cuenta afectada pongan en marcha operaciones de ARC que actualicen los controles de enrutamiento de ARC.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
```

```
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Ejemplos de SCP para Amazon S3

> **Note**
>
> Amazon Simple Storage Service (Amazon S3) aplica automáticamente cifrado del servidor (SSE-S3) para cada objeto nuevo, a menos que especifique una opción de cifrado diferente. Para obtener más información, consulte Amazon S3 ahora cifra automáticamente todos los objetos nuevos en la Guía del usuario de Amazon S3.

Ejemplos en esta categoría

- Impedir la carga de objetos sin cifrar en Amazon S3

Impedir la carga de objetos sin cifrar en Amazon S3

La siguiente política impide que todos los usuarios carguen objetos no cifrados en buckets de S3.

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
```

```
    }
  }
}
```

La siguiente política impide que todos los usuarios carguen objetos no cifrados en los buckets de S3 y también impone un tipo de cifrado especificado (AES256 o aws:kms) para cargar objetos en sus cubos.

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

Ejemplo de SCP para etiquetar recursos

Ejemplos en esta categoría

- Requerir una etiqueta en los recursos creados especificados
- Impedir que las etiquetas se modifiquen excepto por entidades autorizadas

Requerir una etiqueta en los recursos creados especificados

La siguiente SCP impide que los usuarios y roles de IAM en las cuentas afectadas creen ciertos tipos de recursos si la solicitud no incluye las etiquetas especificadas.

> **Important**
>
> Recuerde probar las políticas basadas en denegación con los servicios que utiliza en su entorno. El siguiente ejemplo es un simple bloque de creación de secretos sin etiquetar o ejecución de instancias de Amazon EC2 sin etiquetar, y no incluye ninguna excepción. La siguiente política de ejemplo no es compatible con AWS CloudFormation como está escrito, porque ese servicio crea un secreto y luego lo etiqueta como dos pasos separados. Esta política de ejemplo bloquea eficazmente AWS CloudFormation de crear un secreto como parte de una pila, porque tal acción resultaría, aunque brevemente, en un secreto que no está etiquetado como sea necesario.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
```

```
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

Para obtener una lista de todos los servicios y las acciones que se admiten tanto en las SCP de AWS Organizations como en las políticas de permisos de IAM, consulte Actions, Resources, and Condition Keys for Servicios de AWS en la Guía del usuario de IAM.

Impedir que las etiquetas se modifiquen excepto por entidades autorizadas

El siguiente SCP muestra cómo una política puede permitir que solo los principales autorizados modifiquen las etiquetas adjuntas a los recursos. Esto es una parte importante del uso del control de acceso basado en atributos (ABAC) como parte de su estrategia de seguridad en la nube AWS. La política permite al autor de la llamada modificar las etiquetas solo en aquellos recursos donde la etiqueta de autorización (en este ejemplo, `access-project`) coincide exactamente con la misma etiqueta de autorización adjunta al usuario o rol de que realiza la solicitud. La política también impide que el usuario autorizado cambie el valor de la etiqueta que se utiliza para la autorización. El principal de llamada debe tener la etiqueta de autorización para realizar cualquier cambio.

Esta política solo impide que los usuarios no autorizados cambien las etiquetas. Un usuario autorizado que no esté bloqueado por esta política debe seguir teniendo una política del IAM

independiente que otorgue explícitamente el permiso `Allow` en las API de etiquetado pertinentes. Por ejemplo, si el usuario tiene una política de administrador con `Allow */*` (permitir todos los servicios y todas las operaciones), entonces la combinación da como resultado que el usuario administrador pueda cambiar solamente aquellas etiquetas que tienen un valor de etiqueta de autorización que coincide con el valor de etiqueta de autorización adjunto a la entidad principal del usuario. Esto se debe a que el `Deny` explícito en esta política anula el `Allow` explícito en la política de administrador.

> **Important**
>
> Esta no es una solución de política completa y no debe usarse como se muestra aquí. Este ejemplo solo pretende ilustrar parte de una estrategia ABAC y debe personalizarse y probarse para entornos de producción.
> Para obtener la política completa con un análisis detallado de cómo funciona, consulte Proteger las etiquetas de recursos utilizadas para la autorización mediante una política de control de servicios enAWS Organizations
> Recuerde probar las políticas basadas en denegación con los servicios que utiliza en su entorno.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
```

```
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
```

```
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Ejemplo de SCP para Amazon Virtual Private Cloud (Amazon VPC)

Ejemplos en esta categoría

- Evitar que los usuarios eliminen los registros de flujo de Amazon VPC
- Evitar que cualquier VPC que no tenga acceso a Internet lo obtenga

Evitar que los usuarios eliminen los registros de flujo de Amazon VPC

Esta SCP evita que los usuarios o roles de cualquier cuenta afectada eliminen los registros de flujo de Amazon Elastic Compute Cloud (Amazon EC2) o los grupos o secuencias de registros de CloudWatch.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

Evitar que cualquier VPC que no tenga acceso a Internet lo obtenga

Esta SCP evita que los usuarios o las funciones de cualquier cuenta afectada cambien la configuración de sus nubes virtuales privadas (VPC) de Amazon EC2 para concederles acceso directo a Internet. No bloquea el acceso directo existente ni ningún acceso que se direccione a través de su entorno de red local.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

Solución de problemas de políticas de control de servicio (SCP) con AWS Organizations

Utilice la información que se indica aquí para diagnosticar y corregir errores comunes en las políticas de control de servicio (SCP).

Las políticas de control de servicios (SCP) de AWS Organizations son similares a las políticas de IAM y tienen una sintaxis común. Esta sintaxis comienza con las reglas de JavaScript Object Notation (JSON). JSON describe un objeto con pares de nombre y valor que componen el objeto. La gramática de las políticas de IAM se basa en la definición de nombres y valores que tengan significado y puedan ser entendidos por los Servicios de AWS que usan políticas para conceder permisos.

AWS Organizations utiliza un subconjunto de la sintaxis y la gramática de IAM. Para obtener más información, consulte Sintaxis de SCP.

Errores de políticas comunes

- Más de un objeto de política
- Más de un elemento Statement
- El documento de política supera el tamaño máximo

Más de un objeto de política

Una SCP debe constar de uno y un solo objeto JSON. Los objetos se indican incluyéndolos en llaves { }. Aunque puede anidar otros objetos dentro de un objeto JSON añadiendo llaves ({}) adicionales en el par exterior, una política solo puede contener un par exterior de llaves { }. El siguiente ejemplo es incorrecto porque contiene dos objetos en la parte superior (indicados en *rojo*):

```
{
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
  }
}
```

Sin embargo, podría satisfacer la intención del ejemplo anterior con el uso de la gramática de políticas correcta. En lugar de incluir dos objetos de política completos, cada uno con su propio elemento `Statement`, puede combinar los dos bloques en un único elemento `Statement`. El elemento `Statement` tiene una matriz de dos objetos como su valor, tal y como se muestra en el ejemplo siguiente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
```

```
    }
  ]
}
```

Este ejemplo no se puede comprimir en una instrucción `Statement` con un solo elemento, porque los dos elementos tienen efectos diferentes. Por lo general, solo puede combinar instrucciones cuando los elementos `Effect` y `Resource` de cada instrucción sean idénticos.

Más de un elemento Statement

Este error podría parecer a simple vista una variante del error de la sección anterior. Sin embargo, es un tipo de error diferente desde el punto de vista sintáctico. En el siguiente ejemplo, solo hay un objeto de política indicado por un único par de llaves { } en el nivel superior. Sin embargo, ese objeto contiene dos elementos `Statement` en su interior.

Una SCP debe contener solo un elemento `Statement`, que consta del nombre (`Statement`) que aparece a la izquierda de un carácter de punto y coma, seguido de su valor a la derecha. El valor de un elemento `Statement` debe ser un objeto, identificado por llaves { }, que contiene un elemento `Effect`, un elemento `Action` y un elemento `Resource`. El siguiente ejemplo es incorrecto porque contiene dos elementos `Statement` en el objeto de política:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

Como un objeto de valor puede ser una matriz de varios objetos de valor, puede resolver este problema combinando los dos elementos `Statement` en un elemento con una matriz de objetos, tal y como se muestra en el ejemplo siguiente:

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
 ]
}
```

El valor del elemento `Statement` es una matriz de objetos. La matriz del ejemplo se compone de dos objetos, cada uno de los cuales es un valor correcto para un elemento `Statement`. Cada objeto de la matriz está separado por comas.

El documento de política supera el tamaño máximo

El tamaño máximo de un documento de SCP es 5120 bytes. Este tamaño máximo incluye todos los caracteres, incluido el espacio en blanco. Para reducir el tamaño de su SCP, puede eliminar todos los caracteres de espacio en blanco (como espacios y saltos de línea) que estén fuera de las comillas.

> **Note**
>
> Si guarda la política con la AWS Management Console, los espacios en blanco adicionales entre elementos JSON y fuera de las comillas se eliminan y no se tienen en cuenta. Si guarda la política mediante una operación de SDK o el AWS CLI, la política se guarda exactamente como usted proporcionó y no se produce la eliminación automática de caracteres.

Políticas de control de recursos (RCPs)

Las políticas de control de recursos (RCPs) son un tipo de política organizacional que puede usar para administrar los permisos en su organización. RCPsofrecen un control central sobre el número máximo de permisos disponibles para los recursos de su organización. RCPsle ayudan a garantizar que los recursos de sus cuentas se ajusten a las directrices de control de acceso de su organización.

RCPsestán disponibles solo en una organización que tenga todas las funciones habilitadas. RCPsno están disponibles si su organización ha activado únicamente las funciones de facturación unificada. Para obtener instrucciones sobre cómo habilitar RCPs, consulte Habilitar un tipo de política.

RCPspor sí solos no son suficientes para conceder permisos a los recursos de su organización. UnRCP. An RCP define una barrera de permisos o establece límites a las acciones que las identidades pueden realizar con los recursos de sus organizaciones. El administrador debe seguir adjuntando políticas basadas en la identidad a IAM los usuarios o roles, o políticas basadas en recursos a los recursos de sus cuentas para poder conceder realmente los permisos. Para obtener más información, consulte las políticas basadas en la identidad y las políticas basadas en recursos en la Guía del usuario. IAM

Los permisos efectivos son la intersección lógica entre lo que permiten las políticas de control de servicios (SCPs) RCPs y lo que permiten las políticas basadas en la identidad y en los recursos.

> ⚠ RCPsno afectan a los recursos de la cuenta de administración
>
> RCPsno afectan a los recursos de la cuenta de administración. Solo afectan a los recursos de las cuentas de los miembros de su organización. Esto también significa que RCPs se aplican a las cuentas de los miembros designadas como administradores delegados.

Temas en esta página

- Lista de Servicios de AWS ese apoyo RCPs
- Probando los efectos de RCPs
- Tamaño máximo de RCPs
- Adscribirse RCPs a diferentes niveles de la organización
- RCPefectos en los permisos
- Los recursos y las entidades no están restringidos por RCPs
- RCPevaluación
- Sintaxis de RCP
- Ejemplos de políticas de control de recursos

Lista de Servicios de AWS ese apoyo RCPs

RCPsse aplican a los siguientes recursos Servicios de AWS:

- Amazon S3
- AWS Security Token Service
- AWS Key Management Service
- Amazon SQS
- AWS Secrets Manager

Probando los efectos de RCPs

AWS le recomienda encarecidamente que no se limite RCPs a la raíz de su organización sin comprobar exhaustivamente el impacto que la política tiene en los recursos de sus cuentas. Puedes empezar por adjuntarlas RCPs a cuentas de prueba individuales, ascenderlas a niveles OUs más bajos de la jerarquía y, después, ir ascendiendo en la estructura de la organización según sea necesario. Una forma de determinar el impacto es revisar los AWS CloudTrail registros para ver si hay errores de acceso denegado.

Tamaño máximo de RCPs

Todos los caracteres de tu lista se RCP tienen en cuenta para su tamaño máximo. Los ejemplos de esta guía muestran los objetos RCPs formateados con espacios en blanco adicionales para mejorar su legibilidad. Sin embargo, para ahorrar espacio si el tamaño de la política se aproxima al tamaño máximo, puede eliminar todos los espacios en blanco, como espacios y saltos de línea, que estén fuera de las comillas.

> **Tip**
>
> Usa el editor visual para crear tu. RCP Este elimina automáticamente el espacio en blanco adicional.

Adscribirse RCPs a diferentes niveles de la organización

Puedes asociarte RCPs directamente a cuentas individuales o a la raíz de la organización. OUs Para obtener una explicación detallada de cómo RCPs funciona, consulteRCPevaluación.

RCPefectos en los permisos

RCPsson un tipo de política AWS Identity and Access Management (IAM). Están más estrechamente relacionadas con las políticas basadas en los recursos. Sin embargo, Dan RCP nunca concede

permisos. En su lugar, RCPs son controles de acceso que especifican el número máximo de permisos disponibles para los recursos de su organización. Para obtener más información, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

- RCPsse aplican a los recursos de un subconjunto de Servicios de AWS. Para obtener más información, consulte Lista de Servicios de AWS ese apoyo RCPs.
- RCPsafectan únicamente a los recursos gestionados por cuentas que forman parte de la organización a la que se ha adscrito. RCPs No afectan a los recursos de cuentas ajenas a la organización. Por ejemplo, pensemos en un bucket de Amazon S3 propiedad de la cuenta A de una organización. La política de bucket (una política basada en los recursos) concede acceso a los usuarios de la cuenta B ajenos a la organización. La cuenta A tiene un adjuntoRCP. Esto RCP se aplica al depósito S3 de la cuenta A, incluso cuando los usuarios acceden a ellos desde la cuenta B. Sin embargo, RCP no se aplica a los recursos de la cuenta B cuando acceden los usuarios de la cuenta A.
- A RCP restringe los permisos de los recursos en las cuentas de los miembros. Todos los recursos de una cuenta solo tienen los permisos permitidos por todos los padres que estén por encima de ella. Si un permiso está bloqueado en cualquier nivel por encima de la cuenta, un recurso de la cuenta afectada no tiene ese permiso, incluso si el propietario del recurso incorpora una política basada en los recursos que permite el acceso total a cualquier usuario.
- RCPsse aplican a los recursos que están autorizados como parte de una solicitud de operación. Estos recursos se encuentran en la columna «Tipo de recurso» de la tabla de acciones de la Referencia de autorización del servicio. Si no se especifica ningún recurso en la columna «Tipo de recurso», se aplicará el RCPs de la cuenta principal llamante. Por ejemplo, `s3:GetObject` autoriza el recurso objeto. Siempre que se `GetObject` realice una solicitud, se RCP solicitará a un agente competente que determine si el principal solicitante puede invocar la `GetObject` operación. Aplicable RCP es aquel RCP que se ha adjuntado a una cuenta, a una unidad organizativa (OU) o a la raíz de la organización propietaria del recurso al que se accede.
- RCPsafectan únicamente a los recursos de las cuentas de los miembros de la organización. No afectan a los recursos de la cuenta de administración. Esto también significa que RCPs se aplican a las cuentas de los miembros designadas como administradores delegados. Para obtener más información, consulte Prácticas recomendadas para la cuenta de administración.
- Cuando un director solicita el acceso a un recurso de una cuenta que tiene un elemento adjunto RCP (un recurso con una correspondienteRCP), esto RCP se incluye en la lógica de evaluación de políticas para determinar si se le permite o se deniega el acceso al principal.
- RCPsafectan a los permisos efectivos de los directores que intentan acceder a los recursos de la cuenta de un miembro con una correspondienteRCP, independientemente de si los directores

pertenecen a la misma organización o no. Esto incluye a los usuarios root. La excepción se produce cuando los directores son funciones vinculadas al servicio, ya RCPs que no se aplican a las llamadas realizadas por funciones vinculadas al servicio. Los roles vinculados al servicio te permiten Servicios de AWS realizar las acciones necesarias en tu nombre y no pueden restringirlos. RCPs

- A los usuarios y roles se les deben seguir concediendo permisos con las políticas de IAM permisos adecuadas, incluidas las políticas basadas en la identidad y en los recursos. Un usuario o rol sin ninguna política de IAM permisos no tiene acceso, incluso si una aplicable RCP permite todos los servicios, todas las acciones y todos los recursos.

Los recursos y las entidades no están restringidos por RCPs

No se puede utilizar RCPs para restringir lo siguiente:

- Cualquier acción sobre los recursos de la cuenta de administración.
- RCPsno afectan a los permisos efectivos de ningún rol vinculado a un servicio. Los roles vinculados al servicio son un tipo único de IAM rol que se vincula directamente a un AWS servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre. Los permisos de los roles vinculados al servicio no se pueden restringir mediante. RCPs RCPstampoco afectan a la capacidad de los AWS servicios para asumir un rol vinculado al servicio; es decir, la política de confianza del rol vinculado al servicio tampoco se ve afectada por la política de confianza del rol vinculado al servicio. RCPs
- RCPsno se solicitan para.Claves administradas por AWSAWS Key Management Service Claves administradas por AWS son creados, administrados y utilizados en su nombre por un Servicio de AWS. No puede cambiar ni administrar sus permisos.
- RCPsno afectan a los siguientes permisos:

Servicio	API	Recursos no autorizados por RCPs
AWS Key Management Service	`kms:RetireGrant`	RCPsno afectan al `kms:RetireGrant` permiso. Para obtener más información sobre cómo `kms:RetireGrant` se determina el permiso,

Servicio	API	Recursos no autorizados por RCPs
		consulta la sección sobre cómo retirar y revocar las subvenciones en la Guía para AWS KMS desarrolladores.

RCPevaluación

> **Note**
>
> La información de esta sección no se aplica a los tipos de políticas de administración, incluidas las políticas de copia de seguridad, las políticas de etiquetas, las políticas de chatbot o las políticas de exclusión de servicios de IA. Para obtener más información, consulte Descripción de la herencia de políticas de administración.

Como puede adjuntar varias políticas de control de recursos (RCPs) en diferentes niveles AWS Organizations, comprender cómo RCPs se evalúan puede ayudarlo a redactar las RCPs que arrojen el resultado correcto.

Estrategia de uso RCPs

La `RCPFullAWSAccess` política es una política AWS gestionada. Se adjunta automáticamente a la raíz de la organización, a todas las unidades organizativas y a todas las cuentas de la organización cuando se activan las políticas de control de recursos (RCPs). No puede separar esta política. Esta configuración predeterminada RCP permite que todos los principales y las acciones accedan a una fase de RCP evaluación, lo que significa que, hasta que empieces a crear y adjuntarRCPs, todos tus IAM permisos actuales seguirán funcionando como antes. Esta política AWS gestionada no concede el acceso.

Puede utilizar las `Deny` declaraciones para bloquear el acceso a los recursos de su organización. Si se deniega un permiso para un recurso de una cuenta específica, cualquier persona que vaya RCP desde la raíz hasta cada unidad organizativa situada en la ruta directa a la cuenta (incluida la propia cuenta de destino) puede denegar ese permiso.

Denylas declaraciones son una forma eficaz de implementar restricciones que deberían aplicarse a una parte más amplia de la organización. Por ejemplo, puede adjuntar una política para evitar que identidades externas a su organización accedan a sus recursos a nivel raíz y que sea efectiva para todas las cuentas de la organización. AWS le recomienda encarecidamente que no se vincule RCPs a la raíz de su organización sin comprobar exhaustivamente el impacto que la política tiene en los recursos de sus cuentas. Para obtener más información, consulte Probando los efectos de RCPs.

En la figura 1, hay un RCP anexo a la unidad organizativa de producción que contiene una Deny declaración explícita especificada para un servicio determinado. En consecuencia, se denegará el acceso al servicio tanto a la cuenta A como a la cuenta B, ya que se aplica una política de denegación aplicable a cualquier nivel de la organización para todas las cuentas OUs y las cuentas de los miembros correspondientes.

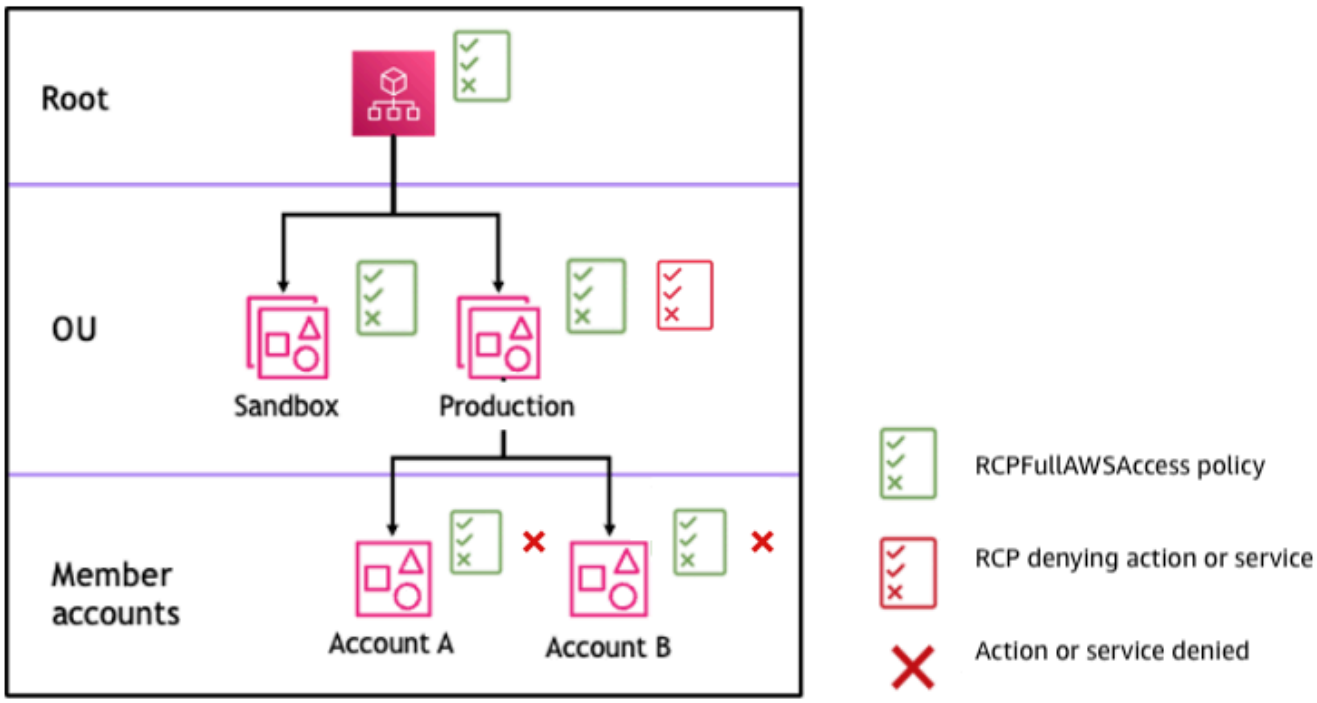


Figura 1: Ejemplo de estructura organizativa con una *Deny* declaración adjunta en Production OU y su impacto en las cuentas A y B

Sintaxis de RCP

Las políticas de control de recursos (RCPs) utilizan una sintaxis similar a la que utilizan las políticas basadas en recursos. Para obtener más información sobre las políticas del IAM y su sintaxis, consulte Información general de las políticas del AM en la Guía del usuario IAM.

Un RCP se estructura de acuerdo con las reglas de JSON. Utiliza los elementos que se describen en este tema.

> **Note**
>
> Todos los caracteres de tu RCP se tienen en cuenta para su tamaño máximo. Los ejemplos de esta guía muestran los archivos RCPs formateados con espacios en blanco adicionales para mejorar su legibilidad. Sin embargo, para ahorrar espacio si el tamaño de la política se aproxima al tamaño máximo, puede eliminar todos los espacios en blanco, como espacios y saltos de línea, que estén fuera de las comillas.

Para obtener información general sobre RCPs, consulte. Políticas de control de recursos (RCPs)

Resumen de elementos

En la siguiente tabla se resumen los elementos de política que puede utilizar. RCPs En la columna Efectos admitidos se muestra el tipo de efecto que puede utilizar con cada elemento de política. RCPs

> **Note**
>
> El efecto de solo **`Allow`** se admite en la **`RCPFullAWSAccess`** política
> El efecto de solo `Allow` se admite en la `RCPFullAWSAccess` política. Esta política se adjunta automáticamente a la raíz de la organización, a todas las unidades organizativas y a todas las cuentas de la organización cuando se activan las políticas de control de recursos (RCPs). No puede separar esta política. Este RCP predeterminado permite que el acceso a todos los principios y acciones pase por una evaluación del RCP, lo que significa que, hasta que empieces a crear y adjuntar RCPs, todos tus permisos de IAM actuales seguirán funcionando como antes. Esto no concede el acceso.

Elemento	Finalidad	
Versión	Especifica las reglas de sintaxis del lenguaje que	

Elemento	Finalidad
	se utilizarán para procesar la política.
Instrucción	Sirve como contenedor de elementos de política. Puede incluir varios estados de cuenta RCPs.
Statement ID (Sid) (ID de instrucción)	(Opcional) Proporciona un nombre fácil de recordar para la instrucción.
Effect	Define si la declaración RCP deniega el acceso a los recursos de una cuenta.
Entidad principal	Especifica el principal al que se le permite o deniega el acceso a los recursos de una cuenta.
Action	Especifica el AWS servicio y las acciones que el RCP permite o deniega.

Elemento	Finalidad
Resource	Especifica los AWS recursos a los que se aplica el RCP.
NotResource	Especifica los AWS recursos que están exentos del RCP. Se utiliza en lugar del elemento `Resource`.
Condición	Especifica las condiciones que determinan cuándo se aplica la instrucción.

Temas

- Elemento Version
- Elemento Statement
- Elemento de ID de instrucción (Sid)
- Elemento Effect
- Elemento Principal
- Elemento Action
- Elementos Resource y NotResource
- Elemento Condition
- Elementos no compatibles

Elemento **`Version`**

Cada RCP debe incluir un `Version` elemento con el valor. `"2012-10-17"` Este es el mismo valor de versión que la versión más reciente de las políticas de permisos de IAM.

```
    "Version": "2012-10-17",
```

Para obtener más información, consulte Elementos de la política de JSON de IAM: Versión en la Guía del usuario de IAM.

Elemento **`Statement`**

Un RCP consta de uno o más `Statement` elementos. Solo puede tener una palabra clave `Statement` en una política, pero el valor puede ser una matriz de instrucciones JSON (rodeadas por caracteres [ ]).

En el siguiente ejemplo, se muestra una sola instrucción que consta de `Resource` elementos únicos `EffectPrincipal`,`Action`, y.

```
 {
    "Statement": {
        "Effect": "Deny",
        "Principal": "*",
        "Action": "*",
        "Resource": "*"
    }
}
```

Para obtener más información, consulte Elementos de la política de JSON de IAM: Instrucción en la Guía del usuario de IAM.

Elemento de ID de instrucción (**`Sid`**)

El elemento `Sid` es un identificador opcional que se proporciona para la instrucción de la política. Puede asignar un valor de `Sid` a cada instrucción de una matriz de instrucciones. El siguiente ejemplo de RCP muestra un ejemplo de `Sid` sentencia.

```
{
    "Statement": {
        "Sid": "DenyAllActions",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "*",
        "Resource": "*"
    }
```

```
}
```

Para obtener más información, consulte IAM JSON Policy Elements: Sid en la Guía del usuario de IAM.

Elemento **`Effect`**

Cada instrucción debe contener un elemento `Effect`. Con el valor de `Deny` en el `Effect` elemento, puede restringir el acceso a recursos específicos o definir las condiciones para cuando RCPs estén en vigor. Para RCPs que eso se cree, el valor debe ser`Deny`. Para obtener más información, consulte la Guía del usuario de IAM sobre los elementos de política de JSON RCPevaluación y su efecto en la guía del usuario de IAM.

Elemento **`Principal`**

Cada declaración debe contener el `Principal` elemento. Solo puede especificar «*» en el `Principal` elemento de un RCP. Usa el `Conditions` elemento para restringir principios específicos.

Para obtener más información, consulte Elementos de la política JSON de IAM: principios en la Guía del usuario de IAM.

Elemento **`Action`**

Cada declaración debe contener el `Action` elemento.

El valor del `Action` elemento es una cadena o lista (una matriz JSON) de cadenas que identifica AWS los servicios y las acciones que la sentencia permite o deniega.

Cada cadena se compone de la abreviatura del servicio (como «s3", «sqs» o «sts»), escrita en minúsculas, seguida de dos puntos y, a continuación, de una acción del servicio. Por lo general, todas se escriben con una palabra que comienza con una letra mayúscula y el resto en minúscula. Por ejemplo: `"s3:ListAllMyBuckets"`.

También puede utilizar caracteres comodín como un asterisco (*) o un signo de interrogación (?) en un RCP:

- Utilice un asterisco (*) como carácter comodín como representación de varias acciones que comparten parte de un nombre. El valor `"s3:*"` significa todas las acciones del servicio Amazon S3. El valor solo `"sts:Get*"` coincide con las AWS STS acciones que comienzan por «Obtener».

- Utilice el carácter comodín del signo de interrogación de cierre (?) como representación de un carácter único.

> **Note**
>
> Comodín (*) y signos de interrogación (?) se pueden usar en cualquier parte del nombre de la acción
> A diferencia de SCPs, puede utilizar caracteres comodín como un asterisco (*) o un signo de interrogación (?) en cualquier parte del nombre de la acción.

Para obtener una lista de los servicios compatibles RCPs, consulteLista de Servicios de AWS ese apoyo RCPs. Para obtener una lista de las acciones y Servicio de AWS apoyos, consulte las acciones, los recursos y las claves de condición de los AWS servicios en la Referencia de autorización de servicios.

Para obtener más información, consulte Elementos de la política de JSON de IAM: Action en la Guía del usuario de IAM.

Elementos **`Resource`** y **`NotResource`**

Cada declaración debe contener el `NotResource` elemento `Resource` o.

Puede utilizar caracteres comodín como un asterisco (*) o un signo de interrogación (?) en el elemento de recurso:

- Utilice un asterisco (*) como carácter comodín como representación de varias acciones que comparten parte de un nombre.
- Utilice el carácter comodín del signo de interrogación de cierre (?) como representación de un carácter único.

Para obtener más información, consulte Elementos de la política JSON de IAM: recurso y consulte Elementos de la política JSON de IAM: NotResource en la Guía del usuario de IAM.

Elemento **`Condition`**

Puede especificar un `Condition` elemento en las declaraciones de rechazo de un RCP.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition:": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Este RCP deniega el acceso a las operaciones y los recursos de Amazon S3 a menos que la solicitud se produzca a través de un transporte seguro (la solicitud se envió a través de TLS).

Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Elementos no compatibles

Los siguientes elementos no se admiten en: RCPs

- `NotPrincipal`
- `NotAction`

Ejemplos de políticas de control de recursos

Los ejemplos de políticas de control de recursos (RCPs) que se muestran en este tema tienen únicamente fines informativos. Para ver ejemplos del perímetro de datos, consulte los ejemplos de políticas del perímetro de datos en GitHub.

> **Antes de usar estos ejemplos**
>
> Antes de usar estos ejemplos RCPs en su organización, haga lo siguiente:
>
> - Revise y personalice detenidamente RCPs para que se adapte a sus necesidades específicas.

- Pruébelo minuciosamente RCPs en su entorno con los AWS servicios que utiliza.

Los ejemplos de políticas de esta sección demuestran la implementación y el uso de RCPs. Ellas no son destinadas a ser interpretadas como recomendaciones AWS oficiales o prácticas óptimas que se apliquen exactamente como se indica. Es su responsabilidad probar cuidadosamente cualquier política para comprobar si es adecuada para resolver los requisitos empresariales de su entorno. Las políticas de control de recursos basadas en la denegación pueden limitar o bloquear involuntariamente el uso de AWS los servicios, a menos que añada las excepciones necesarias a la política.

Ejemplos generales

Temas

- RCPFullAWSAccess
- Protección policial confusa entre servicios
- Restrinja el acceso a sus recursos únicamente a las conexiones HTTPS
- Controles coherentes de la política de bucket de Amazon S3

RCPFullAWSAccess

La siguiente política es una política AWS administrada y se adjunta automáticamente a la raíz de la organización, a todas las unidades organizativas y a todas las cuentas de la organización cuando se activan las políticas de control de recursos (). RCPs No puede separar esta política. Este RCP predeterminado permite que todos los principales y las acciones accedan a sus recursos, lo que significa que, hasta que comience a crear y adjuntar RCPs, todos sus permisos de IAM actuales seguirán funcionando como antes. No necesita probar el efecto de esta política, ya que permitirá que el comportamiento de autorización existente continúe con sus recursos.

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

```
        }
    ]
}
```

Protección policial confusa entre servicios

Algunos Servicios de AWS (los servicios de llamadas) utilizan su Servicio de AWS capital para acceder a AWS los recursos de otros Servicios de AWS (los denominados servicios). Cuando un actor que no tenía la intención de tener acceso a un AWS recurso intenta utilizar la confianza de un Servicio de AWS director para interactuar con recursos a los que no estaba destinado a tener acceso, se conoce como el problema del diputado confuso entre servicios. Para obtener más información, consulte El problema del diputado confuso en la Guía del usuario de IAM

La siguiente política exige que Servicio de AWS los directores que accedan a sus recursos solo lo hagan en nombre de las solicitudes de su organización. Esta política aplica el control únicamente a las solicitudes que `aws:SourceAccount` estén `aws:SourceAccount` presentes, de modo que las integraciones de servicios que no requieran su uso no se vean afectadas. Si `aws:SourceAccount` está presente en el contexto de la solicitud, la `Null` condición se evaluará y provocará que se aplique la `aws:SourceOrgID` clave. `true`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RCPEnforceConfusedDeputyProtection",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:*",
                "sqs:*",
                "secretsmanager:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceOrgID": "my-org-id"
                },
                "Bool": {
                    "aws:PrincipalIsAWSService": "true"
                },
                "Null": {
                    "aws:SourceAccount": "false"
```

```
                }
            }
        }
    ]
}
```

Restrinja el acceso a sus recursos únicamente a las conexiones HTTPS

La siguiente política exige que el acceso a sus recursos solo se produzca en conexiones cifradas a través de HTTPS (TLS). Esto puede ayudarle a evitar que posibles atacantes manipulen el tráfico de la red.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceSecureTransport",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "sts:*",
                "s3:*",
                "sqs:*",
                "secretsmanager:*",
                "kms:*"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Controles coherentes de la política de bucket de Amazon S3

El siguiente RCP contiene varias declaraciones para aplicar controles de acceso coherentes en los buckets de Amazon S3 de su organización.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceS3TlsVersion",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "s3:TlsVersion": [
                        "1.2"
                    ]
                }
            }
        },
        {
            "Sid": "EnforceKMSEncryption",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
                }
            }
        }
    ]
}
```

- El identificador de la declaración`EnforceS3TlsVersion`: se requiere una versión TLS 1.2 como mínimo para acceder a los buckets de S3.
- El ID de la instrucción`EnforceKMSEncryption`: requiere que los objetos estén cifrados en el servidor con claves KMS.

Políticas de gestión en AWS Organizations

Las políticas de administración le permiten configurar Servicios de AWS y administrar sus funciones de forma centralizada. La forma en que esas políticas afectan a las OUs cuentas que las heredan depende del tipo de política de administración que se aplique. AWS Organizations Revise los

temas en esta sección para comprender los términos y conceptos pertinentes sobre las políticas de administración.

Temas

- Requisitos previos y permisos para las políticas de administración para AWS Organizations
- Descripción de la herencia de políticas de administración
- Visualización de políticas de administración en vigor
- Políticas declarativas
- Políticas de copia de seguridad
- Políticas de etiquetas
- Políticas de chatbot
- Políticas de exclusión de servicios de IA

Requisitos previos y permisos para las políticas de administración para AWS Organizations

En esta página se describen los requisitos previos y los permisos necesarios para administrar políticas de AWS Organizations.

Temas

- Requisitos previos de las políticas de administración
- Permisos para las políticas de administración

Requisitos previos de las políticas de administración

Para usar políticas de administración en una organización, es necesario lo siguiente:

- Su organización debe tener habilitadas todas las características.
- Debe iniciar sesión en la cuenta de administración de la organización o ser un administrador delegado.
- Su usuario o rol AWS Identity and Access Management (de IAM) debe tener los permisos que se indican en la siguiente sección.

Permisos para las políticas de administración

El siguiente ejemplo de política de IAM proporciona permisos para usar todos los aspectos de las políticas de administración de una organización.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información sobre las políticas y permisos de IAM, consulte la Guía del usuario de IAM.

Descripción de la herencia de políticas de administración

> **Important**
>
> La información de esta sección no se aplica a las políticas de autorización: políticas de control de servicios (SCPs) y políticas de control de recursos (RCPs). Para obtener más información sobre cómo SCPs y cómo RCPs trabajar en una AWS Organizations jerarquía, consulte Evaluación de SCP yRCPevaluación.

Puede asociar políticas de administración a entidades de organización (raíz de organización, unidad organizativa [OU] o cuenta) en su organización:

- Al adjuntar una política de administración a la raíz de la organización, todas las cuentas OUs y cuentas de la organización heredan esa política.
- Cuando asocia una política de administración a una unidad organizativa específica, las cuentas que están directamente en esa unidad organizativa o cualquier unidad organizativa secundaria heredan la política.
- Cuando se asocia una política de administración a una cuenta específica, solo afecta a esa cuenta.

Dado que puede asociar políticas de administración a varios niveles de la organización, las cuentas pueden heredar varias políticas.

En estos temas se explica cómo se procesan las políticas principales y secundarias en la política en vigor de una cuenta.

Temas

- Terminología de herencia
- Sintaxis de política y herencia para tipos de políticas de administración
- Operadores de herencia
- Ejemplos de herencia

Terminología de herencia

En este tema se utilizan los siguientes términos al analizar la herencia de políticas de administración.

Herencia de políticas

La interacción de políticas en distintos niveles de una organización, desplazándose desde la raíz de nivel superior de la organización, bajando por la jerarquía de unidades organizativas (OU) a cuentas individuales.

Puede adjuntar políticas a la raíz de la organización OUs, a las cuentas individuales y a cualquier combinación de estas entidades de la organización. La herencia de políticas de administración hace referencia a las políticas que se asocian a la raíz de la organización o a una unidad organizativa. Todas las cuentas que son miembros de la raíz de la organización o unidad organizativa donde se asocia una política de administración heredan esa política.

Por ejemplo, cuando se asocian las políticas de administración a la raíz de la organización, todas las cuentas de la organización heredan esa política. Esto se debe a que todas las cuentas de una organización siempre están bajo la raíz de la organización. Cuando asocia una política a una unidad organizativa específica, las cuentas que están directamente en esa unidad organizativa o cualquier unidad organizativa secundaria heredan esa política. Dado que puede asociar políticas a varios niveles de la organización, las cuentas pueden heredar varios documentos de políticas para un solo tipo de política.

Políticas principales

Políticas asociadas más alto en el árbol organizativo que las políticas asociadas a entidades más abajo en el árbol.

Por ejemplo, si asocia la política de administración A a la raíz de la organización, es solo una política. Si también asocia la política B a una unidad organizativa debajo de esa raíz, la política A es la política principal de la política B. La política B es la política secundaria de la política A. La política A y la política B se fusionan para crear la política de etiquetas en vigor para las cuentas de la unidad organizativa.

Políticas secundarias

Políticas asociadas a un nivel inferior en el árbol de la organización con respecto a la política principal.

Políticas en vigor

El documento de políticas único final que especifica las reglas que se aplican a una cuenta. La política en vigor es la agregación de cualquier política de etiquetas que herede la cuenta, además de cualquier política de etiquetas que se asocie directamente a la cuenta. Para obtener más información, consulte Visualización de políticas de administración en vigor.

Operadores de herencia

Operadores que controlan cómo se fusionan las políticas heredadas en una sola política efectiva. Se considera que estos operadores son una característica avanzada. Los autores de políticas experimentados pueden utilizarlas para limitar los cambios que puede realizar una política secundaria y cómo se combinan las configuraciones de las políticas. Para obtener más información, consulte Operadores de herencia.

Sintaxis de política y herencia para tipos de políticas de administración

La forma exacta en que las políticas afectan a las cuentas que las heredan OUs y a las que las heredan depende del tipo de política de administración que elija. Los tipos de políticas de administración incluyen:

- Políticas declarativas
- Políticas de copia de seguridad
- Políticas de etiquetas
- Políticas de chatbot
- Políticas de exclusión de servicios de IA

La sintaxis de los tipos de políticas de administración incluye Operadores de herencia, que permiten especificar con precisión qué elementos de las políticas principales se aplican y qué elementos se pueden anular o modificar cuando son heredados por el hijo y las cuentas. OUs

La política efectiva es el conjunto de reglas que se heredan de la raíz de la organización y OUs junto con las que se asocian directamente a la cuenta. La política en vigor especifica el conjunto de reglas final que se aplican a la cuenta. Puede ver la política en vigor de una cuenta que incluya el efecto de todos los operadores heredados en las políticas aplicadas. Para obtener más información, consulte Visualización de políticas de administración en vigor.

Operadores de herencia

Los operadores de herencia controlan cómo se fusionan las políticas heredadas y las políticas de la cuenta con la política de etiquetas en vigor de la cuenta. Estos operadores incluyen operadores de configuración de valores y operadores de control secundarios.

Cuando utilice el editor visual de la AWS Organizations consola, solo podrá utilizar el `@@assign` operador. Se considera que los otros operadores son una característica avanzada. Para utilizar el resto operadores, debe crear manualmente la política JSON. Los autores de políticas con experiencia pueden utilizar los operadores de herencia para controlar qué valores de etiqueta se aplican a la política en vigor y limitar los cambios que pueden realizar las políticas secundarias.

Operadores de configuración de valores

Puede utilizar los operadores de configuración de valores para controlar cómo interactúa la política con sus políticas principales:

- `@@assign` – Sobreescribe cualquier configuración de política heredada con la configuración especificada. Si la configuración especificada no se hereda, este operador la agrega a la política en vigor. Este operador se puede aplicar a cualquier configuración de política de cualquier tipo.
  - Para la configuración de un solo valor, este operador reemplaza el valor heredado por el valor especificado.
  - Para configuraciones de valores múltiples (matrices JSON), este operador elimina los valores heredados y los reemplaza con los valores especificados por esta política.
- `@@append` – Agrega la configuración especificada (sin quitar ninguna) a los heredados. Si la configuración especificada no se hereda, este operador la agrega a la política en vigor. Puede utilizar este operador solo con configuraciones de varios valores.
  - Este operador agrega los valores especificados a cualquier valor de la matriz heredada.
- `@@remove` – Elimina las configuraciones heredadas especificadas de la política efectiva, si existen. Puede utilizar este operador solo con configuraciones de varios valores.
  - Este operador quita solo los valores especificados de la matriz de valores heredados de las políticas principales. Otros valores pueden continuar existiendo en la matriz y pueden ser heredados por las políticas secundarias.

Operadores de control secundarios

El uso de operadores de control secundarios es opcional. Puede utilizar el operador `@@operators_allowed_for_child_policies` para controlar qué operadores de configuración de valores pueden utilizar las políticas secundarias. Puede permitir todos los operadores, algunos operadores específicos o ningún operador. De forma predeterminada, todos los operadores (`@@all`) están permitidos.

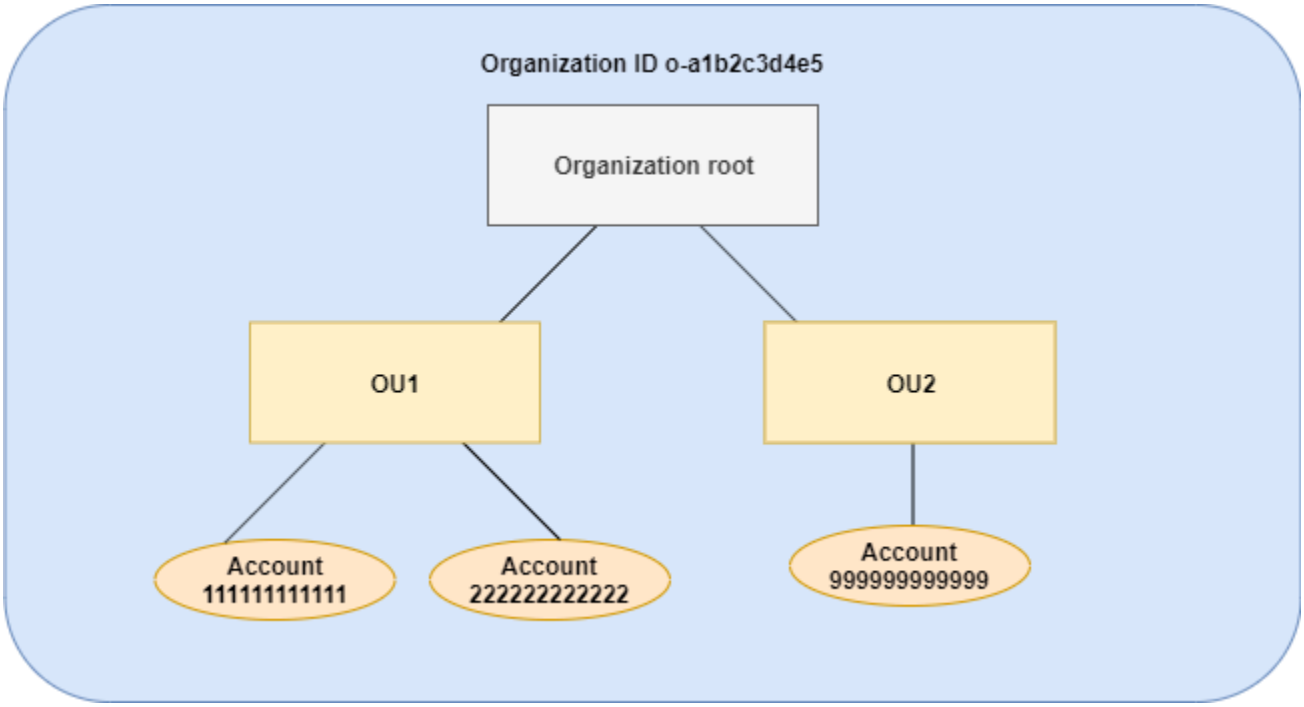
- `"@@operators_allowed_for_child_policies": ["@@all"]` — Los niños OUs y las cuentas pueden utilizar cualquier operador en las pólizas. De forma predeterminada, todos los operadores están permitidos en las políticas secundarias.
- `"@@operators_allowed_for_child_policies": ["@@assign", "@@append", "@@remove"]` — Las cuentas para niños OUs y las cuentas solo pueden usar los operadores especificados en las políticas para niños. Puede especificar uno o más operadores de configuración de valores en este operador de control secundario.
- `"@@operators_allowed_for_child_policies": ["@@none"]` — Los niños OUs y las cuentas no pueden usar operadores en las políticas. Puede usar este operador para bloquear eficazmente los valores definidos en una política principal de modo que las políticas secundarias no puedan agregar, anexar o quitar esos valores.

> **Note**
>
> Si un operador de control secundario heredado limita el uso de un operador, no puede revertir esa regla en una política secundaria. Si incluye operadores de control secundarios en una política principal, limitan los operadores de configuración de valores en todas las políticas secundarias.

Ejemplos de herencia

Estos ejemplos muestran cómo la herencia de políticas funciona al mostrar que las políticas de etiquetas principales y secundarias se fusionan en una política de etiquetas en vigor para una cuenta.

En los ejemplos se supone que tiene la estructura de organización que se muestra en el siguiente diagrama.



Ejemplos

- Ejemplo 1: Permitir que las políticas secundarias sobrescriban solo valores de etiquetas
- Ejemplo 2: Agregar nuevos valores a las etiquetas heredadas
- Ejemplo 3: Eliminar los valores de etiquetas heredadas
- Ejemplo 4: Restringir los cambios en las políticas secundarias
- Ejemplo 5: Conflictos con los operadores de control secundarios
- Ejemplo 6: Conflictos al anexar valores en el mismo nivel de jerarquía

Ejemplo 1: Permitir que las políticas secundarias sobrescriban solo valores de etiquetas

La siguiente política de etiquetas define la clave de etiquetas `CostCenter` y dos valores aceptables, `Development` y `Support`. Si asocia una política de etiquetas a la raíz de la organización, la política de etiquetas se encuentra en vigor para todas las cuentas en la organización.

Política A: política de etiqueta raíz de la organización

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
```

```
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Suponga que desea que los OU1 usuarios usen un valor de etiqueta diferente para una clave y que desea aplicar la política de etiquetas a tipos de recursos específicos. Dado que la política A no especifica qué operadores de control secundarios están permitidos, todos los operadores están permitidos. Puedes usar el `@@assign` operador y crear una política de etiquetas como la siguiente para adjuntarla OU1.

Política B: política OU1 de etiquetas

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Al especificar el operador `@@assign` para la etiqueta, se hace lo siguiente cuando la política A y la B se fusionan para formar la política de etiquetas en vigor para una cuenta:

- La política B sobrescribe los dos valores de etiquetas que se especificaron en la política principal, la política A. El resultado es que `Sandbox` es el único valor compatible para la clave de etiquetas `CostCenter`.
- La adición de `enforced_for` especifica que la etiqueta `CostCenter` debe utilizar el valor de etiquetas especificado en todos los recursos de Amazon Redshift y las tablas de Amazon DynamoDB.

Como se muestra en el diagrama, OU1 incluye dos cuentas: 1111 y 222222222222.

Política de etiquetas en vigor resultante para las cuentas 111111111111 y 222222222222

> **Note**
>
> No puede utilizar directamente el contenido de una política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo tiene por objeto comprender los resultados de la fusión.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Ejemplo 2: Agregar nuevos valores a las etiquetas heredadas

Puede haber casos en los que desee que todas las cuentas de su organización especifiquen una clave de etiquetas con una breve lista de valores aceptables. Para las cuentas de una unidad organizativa, es posible que desee permitir un valor adicional que solo puedan especificar esas

cuentas al crear recursos. En este ejemplo se especifica cómo hacerlo mediante el operador `@@append`. El operador `@@append` es una característica avanzada.

Al igual que el ejemplo 1, este ejemplo comienza con la política A para la política de etiquetas de la raíz de la organización.

Política A: política de etiqueta raíz de la organización

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Para este ejemplo, adjunte la política C a. OU2 La diferencia en este ejemplo es que el uso del operador `@@append` en la política C agrega, en lugar de sobrescribir, la lista de valores aceptables y la regla `enforced_for`.

Política C: política de OU2 etiquetas para anexar valores

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
                "@@append": [
```

```
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Adjuntar la política C a OU2 tiene los siguientes efectos cuando la política A y la política C se fusionan para formar la política de etiquetas efectiva para una cuenta:

- Dado que la política C incluye al operador `@@append`, permite agregar, no sobrescribir, la lista de valores de etiquetas aceptables especificados en la política A.
- Al igual que en la política B, la adición de `enforced_for` especifica que la etiqueta `CostCenter` se debe utilizar como valor de etiquetas especificado en todos los recursos de Amazon Redshift y tablas de Amazon DynamoDB. La sobrescritura (`@@assign`) y la adición (`@@append`) tienen el mismo efecto si la política principal no incluye un operador de control secundario que restringe lo que puede especificar una política secundaria.

Como se muestra en el diagrama, OU2 incluye una cuenta: 7139999. Las políticas A y C se fusionan para crear la política de etiquetas en vigor para la cuenta 999999999999.

Política de etiquetas en vigor para la cuenta 999999999999

> **Note**
>
> No puede utilizar directamente el contenido de una política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo tiene por objeto comprender los resultados de la fusión.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Development",
                "Support",
```

```
                "Marketing"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Ejemplo 3: Eliminar los valores de etiquetas heredadas

Puede haber casos en los que la política de etiquetas asociada a la organización defina más valores de etiquetas de los que desea utilizar una cuenta. En este ejemplo se explica cómo revisar una política de etiquetas mediante el operador `@@remove`. `@@remove` es una característica avanzada.

Al igual que otros ejemplos, este ejemplo comienza con la política A para la política de etiquetas de la raíz de la organización.

Política A: política de etiqueta raíz de la organización

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Para este ejemplo, asocie la política D a la cuenta 999999999999.

Política D: política de etiqueta de la cuenta 999999999999 para eliminar valores

```
{
    "tags": {
```

```
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

La asociación de la política D a la cuenta 999999999999 tiene los siguientes efectos cuando las políticas A, C y D se fusionan para formar la política de etiquetas en vigor:

- Suponiendo que ha realizado todos los ejemplos anteriores, las pólizas B, C y C son políticas secundarias de A. La política B solo está vinculada a ella OU1, por lo que no afecta a la cuenta.
- Para la cuenta 9999999999999, el único valor aceptable para la clave de etiquetas `CostCenter` es `Support`.
- La conformidad no se aplica para la clave de etiquetas `CostCenter`.

Nueva política de etiquetas en vigor para la cuenta 999999999999

> **Note**
>
> No puede utilizar directamente el contenido de una política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo tiene por objeto comprender los resultados de la fusión.

```
{
```

```
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

Si posteriormente añades más cuentas a OU2, sus políticas de etiquetado efectivas serán diferentes a las de la cuenta 99999999. Esto se debe a que la política D más restrictiva solo se asocia a la cuenta y no a la unidad organizativa.

Ejemplo 4: Restringir los cambios en las políticas secundarias

Puede haber casos en los que desee restringir los cambios en las políticas secundarias. En este ejemplo se explica cómo hacerlo mediante los operadores de control secundarios.

Este ejemplo comienza con una nueva política de etiquetas de la raíz de la organización y se supone que las políticas de etiquetas aún no se asocian a las entidades de la organización.

Política E: política de etiqueta raíz de la organización para restringir los cambios en las políticas secundarias

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

Cuando se asocia la política E a la raíz de la organización, la política impide que las políticas secundarias cambien la clave de la etiqueta `Project`. Sin embargo, las políticas secundarias pueden sobrescribir o anexar valores de etiquetas.

Supongamos que, a continuación, asocia la siguiente política F a una unidad organizativa.

Política F: política de etiqueta de unidad organizativa

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

La fusión de las políticas E y F tiene los siguientes efectos en las cuentas de la unidad organizativa:

- La política F es una política secundaria de la política E.
- La política F intenta cambiar el tratamiento del caso, pero no puede. Esto se debe a que la política E incluye el operador `"@@operators_allowed_for_child_policies": ["@@none"]` para la clave de etiqueta.
- Sin embargo, la política F puede añadir los valores de etiquetas para la clave. Esto se debe a que la política E incluye `"@@operators_allowed_for_child_policies": ["@@append"]` para el valor de etiqueta.

Política en vigor para las cuentas en la unidad organizativa

> **Note**
>
> No puede utilizar directamente el contenido de una política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la

fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo tiene por objeto comprender los resultados de la fusión.

```
{
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
            ]
        }
    }
}
```

Ejemplo 5: Conflictos con los operadores de control secundarios

Los operadores de control secundarios pueden existir en políticas de etiquetas asociadas al mismo nivel en la jerarquía de la organización. Cuando eso sucede, se utiliza la intersección de los operadores permitidos cuando las políticas se fusionan para formar la política efectiva para las cuentas.

Supongamos que las políticas G y H se asocian a la raíz de la organización.

Política G: política de etiqueta raíz de la organización 1

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

Política H: política de etiqueta raíz de la organización 2

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

En este ejemplo, una política en la raíz de la organización define que los valores de la clave de etiquetas solo se pueden anexar. La otra política asociada a la raíz de la organización permite que las políticas secundarias anexen y eliminen valores. La intersección de estos dos permisos se utiliza para las políticas secundarias. El resultado es que las políticas secundarias pueden anexar valores, pero no eliminar valores. Por lo tanto, la política secundaria puede anexar un valor a la lista de valores de etiquetas, pero no puede eliminar el valor `Maintenance`.

Ejemplo 6: Conflictos al anexar valores en el mismo nivel de jerarquía

Puede asociar varias políticas de etiquetas a cada entidad de la organización. Al hacerlo, las políticas de etiqueta asociadas a la misma entidad de la organización podrían incluir información conflictiva. Las políticas se evalúan en función del orden en que se asociaron a la entidad de la organización. Para cambiar la política que se evalúa primero, puede asociar una política y, a continuación, volver a asociarla.

Supongamos que la política J se asocia primero a la raíz de la organización y, a continuación, la política K se asocia a la raíz de la organización.

Política J: primera política de etiquetas adjunta al nodo raíz de la organización

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
```

```
}
```

Política K: segunda política de etiquetas adjunta al nodo raíz de la organización

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

En este ejemplo, la clave de etiquetas `PROJECT` se utiliza en la política de etiquetas en vigor porque la política que la definió se asoció primero a la raíz de la organización.

Política JK: política de etiquetas en vigor para la cuenta

La política en vigor para la cuenta es la siguiente.

> **Note**
>
> No puede utilizar directamente el contenido de una política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo tiene por objeto comprender los resultados de la fusión.

```
{
    "tags": {
        "project": {
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
            ]
        }
    }
}
```

Visualización de políticas de administración en vigor

Determine la política de administración en vigor de una cuenta de su organización.

¿Qué es una política de administración en vigor?

La política en vigor especifica las reglas finales que se aplican a una Cuenta de AWS para un tipo de política de administración. Es la agregación de una política de administración que hereda la cuenta, además de cualquier política para ese tipo de política de administración que esté asociada directamente a la cuenta. Cuando se asocia una política de administración al nodo raíz de la organización, esta se aplica a todas las cuentas de la organización. Cuando asocia una política de administración a una unidad organizativa (OU), esta se aplica a todas las cuentas y unidades organizativas que pertenecen a la unidad organizativa. Cuando se asocia una política de administración directamente a una cuenta, solo se aplica a esa Cuenta de AWS.

Para obtener información acerca de cómo se combinan las políticas en la política en vigor final, consulte Descripción de la herencia de políticas de administración.

Ejemplos de políticas de copia de seguridad

La política de copia de seguridad asociada al nodo raíz de la organización puede especificar que todas las cuentas de la organización hagan una copia de seguridad de todas las tablas de Amazon DynamoDB con una frecuencia de copia de seguridad predeterminada de una vez por semana. Una política de copia de seguridad independiente asociada directamente a una cuenta miembro con información fundamental en una tabla puede anular la frecuencia con un valor de una vez al día. La combinación de estas políticas de copia de seguridad compone la política de copia de seguridad en vigor. Esta política de copia de seguridad en vigor se determina de forma individual para cada cuenta de la organización. En este ejemplo, el resultado es que todas las cuentas de la organización realizan una copia de seguridad de sus tablas de DynamoDB una vez a la semana, excepto una cuenta que realiza una copia de seguridad de sus tablas diariamente.

Ejemplos de políticas de etiquetas

La política de etiquetas asociada al nodo raíz de la organización puede definir una etiqueta `CostCenter` con cuatro valores compatibles. Una política de etiquetas diferente asociada a la cuenta puede restringir la clave `CostCenter` a solo dos de los cuatro valores compatibles. La combinación de estas políticas de etiquetas comprende la política de etiquetas en vigor. El resultado es que solo dos de los cuatro valores de etiqueta compatibles definidos en la política de etiquetas de la raíz de la organización son compatibles con la cuenta.

Ejemplo de política de chatbots

AWS Chatbot reevaluará cualquier configuración de AWS Chatbot creada anteriormente en función de las políticas de chatbots vigentes y denegará cualquier acción previamente permitida si es coherente con la configuración permitida y las restricciones de la política en vigor. La política en vigor para una cuenta miembro define las barreras de protección y los ajustes permitidos. Por ejemplo, si se aplica a la cuenta miembro una política de chatbots que deniega el acceso a los canales públicos de Slack, se deshabilitarán las configuraciones de AWS Chatbot existentes para los canales públicos de Slack en la cuenta miembro. El chatbot no entregará notificaciones y los miembros del canal no podrán poner en marcha ninguna tarea en el canal bloqueado. La consola de AWS Chatbot marcará los canales afectados como deshabilitados con el mensaje de error correspondiente junto a ellos.

Ejemplo de exclusión de servicios de IA

La política de exclusión de los servicios de IA adjunta al nodo raíz de la organización podría especificar que todas las cuentas de la organización se excluyan del uso de contenidos por parte de todos los servicios de machine learning de AWS. Una política de exclusión de servicios de IA independiente adjunta directamente a una cuenta de miembro especifica que opta por el uso de contenido solo para Amazon Rekognition. La combinación de estas políticas de exclusión de servicios de IA incluye la política de exclusión efectiva de servicios de IA. El resultado es que todas las cuentas de la organización están excluidas de todos los Servicios de AWS, con la excepción de una cuenta que opte por Amazon Rekognition.

Cómo ver la política de administración en vigor

Puede ver la política en vigor de un tipo de política de administración de una cuenta desde la AWS Management Console, la API de AWS o AWS Command Line Interface.

Permisos mínimos

Para ver la política en vigor de un tipo de política de administración de una cuenta, debe tener permiso para poner en marcha las siguientes acciones:

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para ver la política en vigor de un tipo de política de administración de una cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, elija el nombre de la cuenta para la que desea ver la política en vigor. Es posible que tenga que expandir las unidades organizativas (elija la opción ▶) para encontrar la cuenta que desea.
3. En la pestaña Políticas, elija el tipo de política de administración cuya política en vigor quiera ver.
4. Seleccione Ver la política en vigor de esta Cuenta de AWS.

   La consola muestra la política efectiva aplicada a la cuenta especificada.

   > **Note**
   >
   > No puede copiar y pegar una política en vigor y usarla como JSON para otra política sin cambios significativos. Los documentos de la política deben incluir los operadores de herencia que especifican cómo se fusiona cada configuración en la política en vigor final.

AWS CLI & AWS SDKs

Para ver la política en vigor de un tipo de política de administración de una cuenta

Puede utilizar una de las siguientes opciones para ver la política en vigor:

- AWS CLI: describe-effective-policy

  En el siguiente ejemplo se muestra la política de exclusión efectiva de servicios de IA para una cuenta.

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
```

```
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- SDK de AWS: DescribeEffectivePolicy

Políticas declarativas

Las políticas declarativas le permiten declarar y aplicar de forma centralizada la configuración que desee para una determinada escala Servicio de AWS en toda la organización. Una vez conectada, la configuración siempre se mantiene cuando el servicio agrega nuevas funciones o APIs. Utilice políticas declarativas para evitar acciones no conformes. Por ejemplo, puede bloquear el acceso público a Internet a los recursos de Amazon VPC en toda su organización.

Las principales ventajas del uso de políticas declarativas son las siguientes:

- Facilidad de uso: puede aplicar la configuración básica para una Servicio de AWS con unas cuantas selecciones en las AWS Control Tower consolas AWS Organizations y o con unos pocos comandos mediante la tecla AWS CLI & AWS SDKs.
- Configúrelo una vez y olvídese: la configuración básica de an siempre Servicio de AWS se mantiene, incluso cuando el servicio introduce nuevas funciones o APIs. La configuración básica también se mantiene cuando se agregan nuevas cuentas a una organización o cuando se crean nuevos directores y recursos.
- Transparencia: el informe de estado de la cuenta permite revisar el estado actual de todos los atributos compatibles con las políticas declarativas de las cuentas incluidas en el ámbito de aplicación. También puedes crear mensajes de error personalizables, que pueden ayudar a los administradores a redirigir a los usuarios finales a las páginas wiki internas o proporcionar un mensaje descriptivo que ayude a los usuarios finales a entender por qué se ha producido un error en una acción.

Para obtener una lista completa de los atributos Servicios de AWS y las funciones compatibles, consulteSoportado Servicios de AWS y atributos.

Temas

- Cómo funcionan las políticas declarativas
- Mensajes de error personalizados para las políticas declarativas
- Informe de estado de la cuenta para políticas declarativas
- Soportado Servicios de AWS y atributos
- Cómo empezar con las políticas declarativas
- Mejores prácticas para el uso de políticas declarativas
- Generación del informe de estado de la cuenta para las políticas declarativas
- Sintaxis y ejemplos de políticas declarativas

Cómo funcionan las políticas declarativas

Las políticas declarativas se aplican en el plano de control del servicio, lo que constituye una diferencia importante de las políticas de autorización, como las políticas de control del servicio (SCPs) y las políticas de control de recursos (RCPs). Si bien las políticas de autorización regulan el acceso APIs, las políticas declarativas se aplican directamente a nivel del servicio para garantizar una intención duradera. Esto garantiza que la configuración básica se aplique siempre, incluso cuando el servicio introduzca nuevas funciones o APIs cuando el servicio introduzca nuevas funciones.

La siguiente tabla ayuda a ilustrar esta distinción y proporciona algunos casos de uso.

	Políticas de control de servicios	Políticas de control de recursos	Políticas declarativas		
¿Por qué?	Definir y aplicar de forma centralizada controles de acceso coherente s para los principales	Definir y aplicar de forma centralizada controles de acceso coherentes a los recursos a escala	Definir y aplicar de forma centralizada la configura ción básica de AWS los servicios a escala.		

	Políticas de control de servicios	Políticas de control de recursos	Políticas declarativas		
	(como los usuarios de IAM y las funciones de IAM) a escala.				
¿Cómo?	Controlando los permisos de acceso máximos disponibles de los directores a nivel de API.	Controlando los permisos de acceso máximos disponibles para los recursos a nivel de API.	Aplicando la configuración deseada de y Servicio de AWS sin utilizar acciones de la API.		
¿Rige las funciones vinculadas al servicio?	No	No	Sí		

	Políticas de control de servicios	Políticas de control de recursos	Políticas declarativas		
¿Mecanismo de retroalimentación	Error SCP de acceso no personalizable denegado.	Error de RCP de acceso no personalizable denegado.	Mensaje de error personalizable. Para obtener más información, consulte Mensajes de error personalizados para las políticas declarativas.		
Ejemplo de política de	Denegar acceso a AWS en función de la Región de AWS solicitada	Restrinja el acceso a sus recursos únicamente a las conexiones HTTPS	Configuración de imágenes permitida		

Una vez que haya creado y adjuntado una política declarativa, se aplicará y aplicará en toda la organización. Las políticas declarativas se pueden aplicar a toda la organización, a las unidades organizativas (OUs) o a las cuentas. Las cuentas que se unan a una organización heredarán automáticamente la política declarativa de la organización. Para obtener más información, consulte Descripción de la herencia de políticas de administración.

La política efectiva es el conjunto de reglas que se heredan de la raíz de la organización y OUs junto con las que se adjuntan directamente a la cuenta. La política en vigor especifica el conjunto de reglas final que se aplican a la cuenta. Para obtener más información, consulte Visualización de políticas de administración en vigor.

Si se separa una política declarativa, el estado del atributo volverá a su estado anterior antes de que se adjuntara la política declarativa.

Mensajes de error personalizados para las políticas declarativas

Las políticas declarativas le permiten crear mensajes de error personalizados. Por ejemplo, si una operación de la API falla debido a una política declarativa, puedes configurar el mensaje de error o proporcionar una URL personalizada, como un enlace a un wiki interno o un enlace a un mensaje que describa el error. Si no especifica un mensaje de error personalizado, AWS Organizations proporciona el siguiente mensaje de error predeterminado:`Example: This action is denied due to an organizational policy in effect.`

También puede auditar el proceso de creación de políticas declarativas, actualización de políticas declarativas y eliminación de políticas declarativas con. AWS CloudTrail CloudTrail puede señalar los errores de funcionamiento de la API debidos a políticas declarativas. Para obtener más información, consulte Registro y supervisión.

> **Important**
>
> No incluya información de identificación personal (PII) u otra información confidencial en un mensaje de error personalizado. La PII incluye información general que se puede utilizar para identificar o localizar a una persona. Abarca registros tales como los financieros, médicos, educativos o laborales. Los ejemplos de PII incluyen direcciones, números de cuentas bancarias y números de teléfono.

Informe de estado de la cuenta para políticas declarativas

El informe de estado de la cuenta le permite revisar el estado actual de todos los atributos compatibles con las políticas declarativas de las cuentas incluidas en el ámbito de aplicación. Puedes elegir las cuentas y unidades organizativas (OUs) que deseas incluir en el ámbito del informe, o bien elegir una organización completa seleccionando la raíz.

Este informe le ayuda a evaluar si está preparado, ya que proporciona un desglose por regiones y si el estado actual de un atributo es uniforme en todas las cuentas (a través de`numberOfMatchedAccounts`) o incoherente (a través de`numberOfUnmatchedAccounts`). También puede ver el valor más frecuente, que es el valor de configuración que se observa con más frecuencia para el atributo.

En la figura 1, hay un informe de estado de la cuenta generado, que muestra la uniformidad entre las cuentas para los siguientes atributos: acceso público a bloques de VPC y acceso público a bloques de imágenes, valores predeterminados de metadatos de instancia, acceso público a bloques de instantáneas y configuración de imágenes permitidas. Esto significa que, para cada atributo, todas las cuentas incluidas en el ámbito tienen la misma configuración para ese atributo.

El informe de estado de la cuenta generado muestra cuentas incoherentes para los siguientes atributos: configuración de imágenes permitida, valores predeterminados de metadatos de instancia, acceso a la consola en serie y acceso público a Snapshot Block. En este ejemplo, cada atributo con una cuenta incoherente se debe a que hay una cuenta con un valor de configuración diferente.

Si hay un valor más frecuente, se muestra en su columna correspondiente. Para obtener información más detallada sobre lo que controla cada atributo, consulte Sintaxis de políticas declarativas y ejemplos de políticas.

También puedes expandir un atributo para ver un desglose por región. En este ejemplo, se amplía el acceso público a Image Block y, en cada región, puede ver que también hay uniformidad en todas las cuentas.

La opción de adjuntar una política declarativa para aplicar una configuración básica depende del caso de uso específico. Utilice el informe de estado de la cuenta como ayuda para evaluar si está preparado antes de adjuntar una política declarativa.

Para obtener más información, consulte Generación del informe de estado de la cuenta.

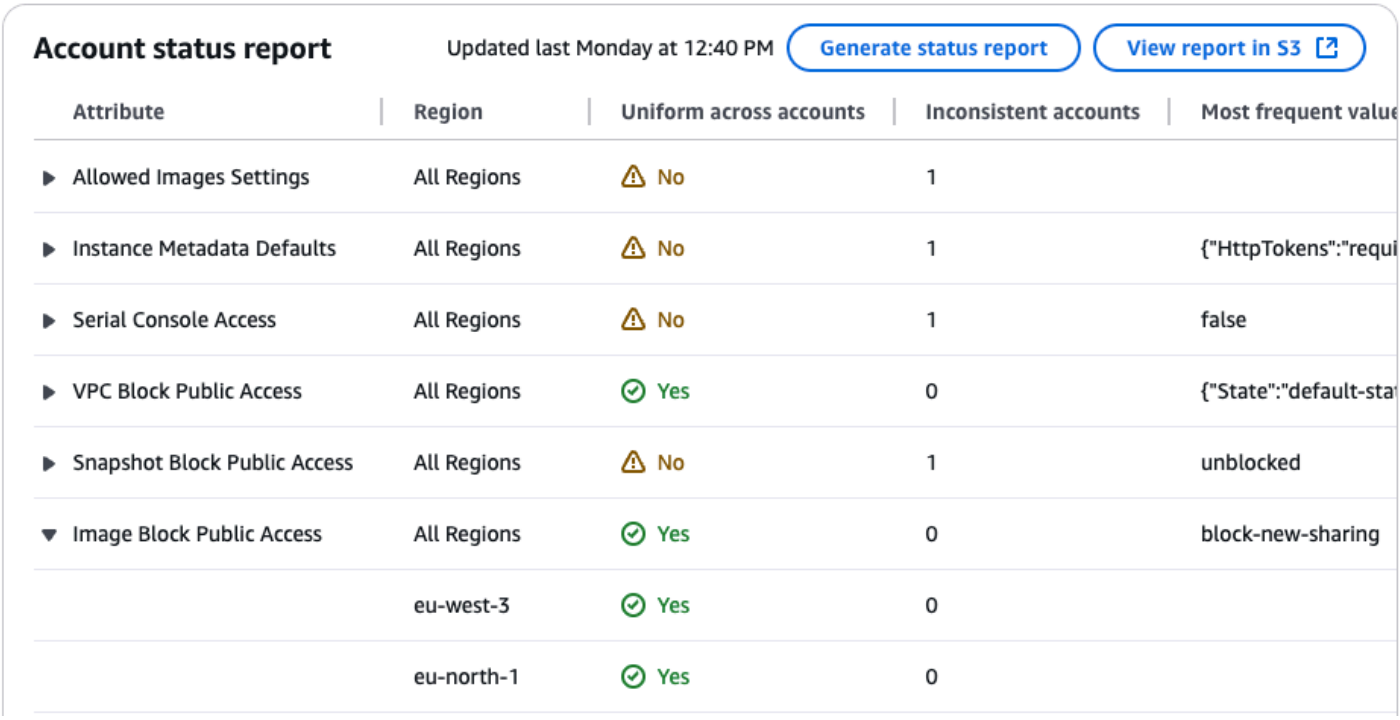


Figura 1: Ejemplo de informe de estado de cuenta con uniformidad en todas las cuentas de VPC Block Public Access e Image Block Public Access.

Soportado Servicios de AWS y atributos

Atributos compatibles para las políticas declarativas de EC2

En la siguiente tabla se muestran los atributos compatibles con los servicios EC2 relacionados con Amazon.

Políticas declarativas para EC2

AWS servicio	Atributo	Efecto de la política	Contenido de la política	Más información
Amazon VPC	Acceso público a bloques de VPC	Controla si los recursos de Amazon VPCs y las subredes pueden llegar a Internet a través de las puertas	Ver política	Para obtener más informaci ón, consulte Bloquear el acceso público VPCs y las subredes en la

AWS servicio	Atributo	Efecto de la política	Contenido de la política	Más información
		de enlace de Internet ()IGWs.		Guía del usuario de Amazon VPC.
Amazon EC2	Acceso a la consola en serie	Controla si se puede acceder a la consola EC2 serie.	Ver política	Para obtener más informaci ón, consulte Configurar el acceso a la consola EC2 serie en la Guía del usuario de Amazon Elastic Compute Cloud.
	Acceso público a Image Block	Controla si Amazon Machine Images (AMIs) se puede compartir públicamente.	Ver política	Para obtener más informaci ón, consulte Cómo bloquear el acceso público AMIs en la Guía del usuario de Amazon Elastic Compute Cloud.
	Configuración de imágenes permitida	Controla el descubrim iento y el uso de Amazon Machine Images (AMI) en Amazon EC2 con Allowed AMIs.	Ver política	Para obtener más información, consulte Amazon Machine Images (AMIs) en la Guía del usuario de Amazon Elastic Compute Cloud.

AWS servicio	Atributo	Efecto de la política	Contenido de la política	Más información
	Valores predeterminados de los metadatos de la instancia	Controla los valores predeterminados de IMDS para todos los lanzamientos de instancias nuevas EC2 .	Ver política	Para obtener más información, consulte Configurar las opciones de metadatos de instancia para instancias nuevas en la Guía del usuario de Amazon Elastic Compute Cloud.
Amazon EBS	Acceso público a Snapshot Block	Controla si las instantáneas de Amazon EBS son de acceso público.	Ver política	Para obtener más información, consulte Bloquear el acceso público a las instantáneas de Amazon EBS en la Guía del usuario de Amazon Elastic Block Store.

Cómo empezar con las políticas declarativas

Siga estos pasos para empezar a utilizar las políticas declarativas.

1. Obtenga información sobre los permisos que debe tener para realizar tareas de política declarativa.
2. Habilite las políticas declarativas para su organización.

> **Note**
>
> Es necesario habilitar el acceso de confianza
> Debe habilitar el acceso confiable al servicio en el que la política declarativa impondrá una configuración básica. Esto crea una función vinculada al servicio de solo lectura que se utiliza para generar el informe de estado de la cuenta con la configuración existente para las cuentas de toda la organización.
> Uso de la consola
> Si utiliza la consola Organizations, este paso forma parte del proceso para habilitar las políticas declarativas.
> Uso de AWS CLI
> Si usa el AWS CLI, hay dos separados APIs:
>
> - EnablePolicyType, que se utiliza para habilitar las políticas declarativas.
> - Habilite el AWSService acceso, que se utiliza para habilitar el acceso confiable.
>
> Para obtener más información sobre cómo habilitar el acceso confiable a un servicio específico, AWS CLI consulte, Servicios de AWS que puede utilizar con AWS Organizations.

3. Ejecute el informe de estado de la cuenta.
4. Cree una política declarativa.
5. Adjunte la política declarativa a la raíz, la unidad organizativa o la cuenta de su organización.
6. Consulta la política declarativa efectiva combinada que se aplica a una cuenta.

Para todos estos pasos, debe iniciar sesión como usuario de IAM, asumir un rol de IAM o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Información adicional

- Aprenda la sintaxis de las políticas declarativas y consulte ejemplos de políticas

Mejores prácticas para el uso de políticas declarativas

AWS recomienda las siguientes prácticas recomendadas para el uso de políticas declarativas.

Aproveche las evaluaciones de preparación

Utilice el informe sobre el estado de las cuentas de política declarativa para evaluar el estado actual de todos los atributos compatibles con las políticas declarativas de las cuentas incluidas en el ámbito de aplicación. Puede elegir las cuentas y las unidades organizativas (OUs) que desea incluir en el ámbito del informe, o bien elegir una organización completa seleccionando la raíz.

Este informe le ayuda a evaluar si está preparado, ya que proporciona un desglose por regiones y si el estado actual de un atributo es uniforme en todas las cuentas (a través de `numberOfMatchedAccounts`) o incoherente (a través de `numberOfUnmatchedAccounts`). También puede ver el valor más frecuente, que es el valor de configuración que se observa con más frecuencia para el atributo.

La opción de adjuntar una política declarativa para aplicar una configuración básica depende del caso de uso específico.

Para obtener más información y un ejemplo ilustrativo, consulte. Informe de estado de la cuenta para políticas declarativas

Comience con algo pequeño y, a continuación, escale

Para simplificar la depuración, comience con una política de pruebas. Valide el comportamiento y el impacto de cada cambio antes de realizar el siguiente cambio. Este enfoque reduce el número de variables que hay que tener en cuenta cuando se produce un error o un resultado inesperado.

Por ejemplo, puede empezar con una política de pruebas asociada a una sola cuenta en un entorno de pruebas no crítico. Una vez que hayas confirmado que funciona según tus especificaciones, puedes ir ascendiendo gradualmente en la estructura de la organización para incluir más cuentas y más unidades organizativas ()OUs.

Establezca procesos de revisión

Implemente procesos para supervisar los nuevos atributos declarativos, evaluar las excepciones a las políticas y realizar ajustes para mantener la alineación con los requisitos operativos y de seguridad de su organización.

Valide los cambios mediante **`DescribeEffectivePolicy`**

Tras realizar un cambio en una política declarativa, compruebe las políticas vigentes para las cuentas representativas situadas por debajo del nivel en el que realizó el cambio. Para ver la política en vigor

AWS Management Console, utilice la DescribeEffectivePolicyAPIoperación o una de sus AWS CLI AWS SDK variantes. Asegúrese de que el cambio que ha realizado haya tenido el impacto previsto en la política en vigor.

Comunícate y entrena

Asegúrese de que sus organizaciones entiendan el propósito y el impacto de sus políticas declarativas. Proporcione una orientación clara sobre los comportamientos esperados y sobre cómo gestionar los fallos debidos a la aplicación de las políticas.

Generación del informe de estado de la cuenta para las políticas declarativas

El informe de estado de la cuenta le permite revisar el estado actual de todos los atributos compatibles con las políticas declarativas de las cuentas incluidas en el ámbito de aplicación. Puedes elegir las cuentas y unidades organizativas (OUs) que deseas incluir en el ámbito del informe, o bien elegir una organización completa seleccionando la raíz.

Este informe le ayuda a evaluar si está preparado, ya que proporciona un desglose por regiones y si el estado actual de un atributo es uniforme en todas las cuentas (a través de `numberOfMatchedAccounts`) o incoherente (a través de `numberOfUnmatchedAccounts`). También puede ver el valor más frecuente, que es el valor de configuración que se observa con más frecuencia para el atributo.

La opción de adjuntar una política declarativa para aplicar una configuración básica depende del caso de uso específico.

Para obtener más información y un ejemplo ilustrativo, consulte. Informe de estado de la cuenta para políticas declarativas

Requisitos previos

Antes de poder generar un informe de estado de la cuenta, debe realizar los siguientes pasos

1. Solo `StartDeclarativePoliciesReport` API pueden llamarlos la cuenta de administración o los administradores delegados de una organización.
2. Debe tener un bucket de S3 antes de generar el informe (cree uno nuevo o utilice uno existente), debe estar en la misma región en la que se realiza la solicitud y debe tener una política de bucket de S3 adecuada. Para ver un ejemplo de política de S3, consulte Ejemplo de política de Amazon S3 en Examples in the Amazon EC2 API Reference

3. Debe habilitar el acceso confiable al servicio en el que la política declarativa impondrá una configuración básica. Esto crea una función vinculada al servicio de solo lectura que se utiliza para generar el informe de estado de la cuenta con la configuración existente para las cuentas de toda la organización.

   Uso de la consola

   Para la consola Organizations, este paso forma parte del proceso de activación de las políticas declarativas.

   Uso de AWS CLI

   Para el AWS CLI, utilice el E nableAWSService AccessAPI.

   Para obtener más información sobre cómo habilitar el acceso confiable a un servicio específico, AWS CLI consulte, Servicios de AWS que puede utilizar con AWS Organizations.
4. Solo se puede generar un informe por organización a la vez. Si se intenta generar un informe mientras hay otro en curso, se producirá un error.

Acceda al informe de estado de conformidad

Permisos mínimos

Para generar un informe de estado de conformidad, necesita permiso para ejecutar las siguientes acciones:

- `ec2:StartDeclarativePoliciesReport`
- `ec2:DescribeDeclarativePoliciesReports`
- `ec2:GetDeclarativePoliciesReportSummary`
- `ec2:CancelDeclarativePoliciesReport`
- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:DescribeOrganizationalUnit`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListAWSServiceAccessForOrganization`

AWS Management Console

Utilice el siguiente procedimiento para generar un informe de estado de la cuenta.

Para generar un informe de estado de la cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, selecciona Políticas declarativas para EC2.
3. En la EC2 página Políticas declarativas para, selecciona Ver el informe de estado de la cuenta en el menú desplegable Acciones.
4. En la página Ver informe de estado de la cuenta, selecciona Generar informe de estado.
5. En el widget Estructura organizativa, especifica qué unidades organizativas (OUs) deseas incluir en el informe.
6. Seleccione Submit (Enviar).

AWS CLI & AWS SDKs

Para generar un informe de estado de la cuenta

Utilice las siguientes operaciones para generar un informe de estado de conformidad, comprobar su estado y ver el informe:

- `ec2:start-declarative-policies-report`: Genera un informe de estado de la cuenta. El informe se genera de forma asíncrona y puede tardar varias horas en completarse. Para obtener más información, consulta StartDeclarativePoliciesReportAmazon EC2 API Reference.
- `ec2:describe-declarative-policies-report`: describe los metadatos de un informe de estado de la cuenta, incluido el estado del informe. Para obtener más información, consulta DescribeDeclarativePoliciesReportsAmazon EC2 API Reference.
- `ec2:get-declarative-policies-report-summary`: Recupera un resumen del informe de estado de la cuenta. Para obtener más información, consulta GetDeclarativePoliciesReportSummaryAmazon EC2 API Reference.
- `ec2:cancel-declarative-policies-report`: Cancela la generación de un informe de estado de la cuenta. Para obtener más información, consulta CancelDeclarativePoliciesReportAmazon EC2 API Reference.

Sintaxis y ejemplos de políticas declarativas

En esta página se describe la sintaxis de la política declarativa y se proporcionan ejemplos.

Consideraciones

- Al configurar un atributo de servicio mediante una política declarativa, puede afectar a varios. APIs Cualquier acción que no cumpla con las normas fallará.
- Los administradores de cuentas no podrán modificar el valor del atributo de servicio a nivel de cuenta individual.

Sintaxis de las políticas declarativas

Una política declarativa es un archivo de texto sin formato que se estructura de acuerdo con las reglas de JSON. La sintaxis de las políticas declarativas sigue la sintaxis de todos los tipos de políticas de administración. Para obtener una explicación completa de esa sintaxis, consulte Sintaxis y herencia de políticas para tipos de políticas de administración. Este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política declarativa.

El siguiente ejemplo muestra la sintaxis básica de la política declarativa:

```
{
    "ec2_attributes": {
        "exception_message": {
            "@@assign": "Your custom error message.https://myURL"
        },

        ...

        [Insert supported service attributes]

        ...
    }
}
```

- El nombre de clave del campo `ec2_attributes`. Las políticas declarativas siempre comienzan con un nombre de clave fijo para cada una de ellas. Servicio de AWS Es la línea superior del ejemplo de política anterior. Actualmente, las políticas declarativas solo admiten los servicios EC2 relacionados con Amazon.

- Enec2_attributes, puedes usar exception_message para configurar un mensaje de error personalizado. Para obtener más información, consulte Mensajes de error personalizados para políticas declarativas.
- Enec2_attributes, puede insertar una o más de las políticas declarativas admitidas. Para ver esos esquemas, consulte. Políticas declarativas compatibles

Políticas declarativas compatibles

Los siguientes son los atributos Servicios de AWS y atributos que admiten las políticas declarativas. En algunos de los ejemplos siguientes, el formato de espacio en blanco JSON podría comprimirse para ahorrar espacio.

VPC Block Public Access

Efecto de la política

Controla si los recursos de Amazon VPCs y las subredes pueden llegar a Internet a través de las puertas de enlace de Internet ()IGWs. Para obtener más información, consulte Configuración del acceso a Internet en la Guía del usuario de Amazon Virtual Private Cloud.

Contenido de la política

```
"vpc_block_public_access": {
    "internet_gateway_block": { // (optional)
        "mode": { // (required)
            "@@assign": "block_ingress" // off | block_ingress | block_bidirectional
        },
        "exclusions_allowed": { // (required)
            "@@assign": "enabled" // enabled | disabled
        }
    }
}
```

Los campos disponibles para este atributo son los siguientes:

- "internet_gateway":
  - "mode":
    - "off": El BPA de VPC no está activado.
    - "block_ingress": Se bloquea todo el tráfico de Internet hacia el VPCs (excepto VPCs el de las subredes, que están excluidas). Solo se permite el tráfico hacia y desde las puertas

de enlace NAT y las puertas de enlace de Internet solo de salida, ya que estas puertas de enlace solo permiten establecer conexiones salientes.

- `"block_bidirectional"`: Se bloquea todo el tráfico hacia y desde las pasarelas de Internet y las pasarelas de Internet que solo son de salida (excepto las excluidas VPCs y las subredes).

- `"exclusions_allowed"`: una exclusión es un modo que se puede aplicar a una sola VPC o subred y que la exime del modo BPA de VPC de la cuenta y permite el acceso bidireccional o solo de salida.
  - `"enabled"`: La cuenta puede crear las exclusiones.
  - `"disabled"`: La cuenta no puede crear exclusiones.

> **Note**
>
> Puede usar el atributo para configurar si se permiten las exclusiones, pero no puede crear exclusiones con este atributo en sí. Para crear exclusiones, debe crearlas en la cuenta propietaria de la VPC. Para obtener más información sobre la creación de exclusiones de BPA de VPC, consulte Crear y eliminar exclusiones en la Guía del usuario de Amazon VPC.

Consideraciones

Si utiliza este atributo en una política declarativa, no podrá utilizar las siguientes operaciones para modificar la configuración obligatoria de las cuentas incluidas en el ámbito de aplicación. Esta lista no es exhaustiva:

- `ModifyVpcBlockPublicAccessOptions`
- `CreateVpcBlockPublicAccessExclusion`
- `ModifyVpcBlockPublicAccessExclusion`

Serial Console Access

Efecto de la política

Controla si se puede acceder a la consola EC2 serie. Para obtener más información sobre la consola EC2 serie, consulte EC2 Serial Console en la Guía del usuario de Amazon Elastic Compute Cloud.

Contenido de la política

```
"serial_console_access": {
    "status": { // (required)
        "@@assign": "enabled" // enabled | disabled
    }
}
```

Los campos disponibles para este atributo son los siguientes:

- `"status"`:
  - `"enabled"`: se permite el acceso a la consola en EC2 serie.
  - `"disabled"`: el acceso a la consola EC2 serie está bloqueado.

Consideraciones

Si utiliza este atributo en una política declarativa, no podrá utilizar las siguientes operaciones para modificar la configuración obligatoria de las cuentas incluidas en el ámbito de aplicación. Esta lista no es exhaustiva:

- `EnableSerialConsoleAccess`
- `DisableSerialConsoleAccess`

Image Block Public Access

Efecto de la política

Controla si Amazon Machine Images (AMIs) se puede compartir públicamente. Para obtener más información AMIs, consulte Amazon Machine Images (AMIs) en la Guía del usuario de Amazon Elastic Compute Cloud.

Contenido de la política

```
"image_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing
    }
}
```

Los campos disponibles para este atributo son los siguientes:

- `"state"`:
  - `"unblocked"`: No hay restricciones a la hora de compartir públicamente AMIs.
  - `"block_new_sharing"`: Bloquea el nuevo intercambio público de AMIs. AMIs las que ya se compartieron públicamente permanecen disponibles públicamente.

Consideraciones

Si utiliza este atributo en una política declarativa, no podrá utilizar las siguientes operaciones para modificar la configuración obligatoria de las cuentas incluidas en el ámbito de aplicación. Esta lista no es exhaustiva:

- `EnableImageBlockPublicAccess`
- `DisableImageBlockPublicAccess`

Allowed Images Settings

Efecto de la política

Controla la detección y el uso de Amazon Machine Images (AMI) en Amazon EC2 con Allowed AMIs.. Para obtener más información AMIs, consulte Amazon Machine Images (AMIs) en la Guía del usuario de Amazon Elastic Compute Cloud.

Contenido de la política

Los campos disponibles para este atributo son los siguientes:

```
"allowed_images_settings": {
    "state": { // (required)
        "@@assign": "enabled" // enabled | disabled | audit_mode
    },
    "image_criteria": { // (optional)
        "criteria_1": {
            "allowed_image_providers": { // limit 200
                "@@append": [
                    "amazon" // amazon | aws_marketplace | aws_backup_vault | 12
 digit account ID
                ]
            }
```

```
        }
    }
}
```

- `"state"`:
  - `"enabled"`: El atributo está activo y se aplica.
  - `"disabled"`: El atributo está inactivo y no se aplica.
  - `"audit_mode"`: El atributo está en modo de auditoría. Esto significa que identificará las imágenes que no cumplan con los requisitos, pero no bloqueará su uso.
- `"image_criteria"`: una lista de `allowed_image_providers` objetos que definen las fuentes de AMI permitidas.
  - `"allowed_image_providers"`: una lista separada por comas de nombres o cuentas de proveedores. IDs

Consideraciones

Si utiliza este atributo en una política declarativa, no podrá utilizar las siguientes operaciones para modificar la configuración obligatoria de las cuentas incluidas en el ámbito de aplicación. Esta lista no es exhaustiva:

- `EnableAllowedImagesSettings`
- `ReplaceImageCriteriaInAllowedImagesSettings`
- `DisableAllowedImagesSettings`

Instance Metadata Defaults

Efecto de la política

Controla los valores predeterminados de IMDS para todos los lanzamientos de EC2 instancias nuevas. Para obtener más información sobre los valores predeterminados de IMDS, consulte IMDS en la Guía del usuario de Amazon Elastic Compute Cloud.

Contenido de la política

Los campos disponibles para este atributo son los siguientes:

```
"instance_metadata_defaults": {
```

```
    "http_tokens": { // (required)
        "@@assign": "required" // no_preference | required | optional
    },
    "http_put_response_hop_limit": { // (required)
        "@@assign": "4" // -1 | 1 -> 64
    },
    "http_endpoint": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    },
    "instance_metadata_tags": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    }
}
```

- `"http_tokens"`:
  - `"no_preference"`: Se aplican otros valores predeterminados. Por ejemplo, la AMI es la opción predeterminada, si corresponde.
  - `"required"`: IMDSv2 debe usarse. IMDSv1 no está permitido.
  - `"optional"`: Ambos IMDSv1 IMDSv2 están permitidos.

> **Note**
>
> Versión de metadatos
> Antes de `http_tokens` configurarla `required` (IMDSv2 debe usarse), asegúrate de que ninguna de tus instancias esté realizando IMDSv1 llamadas.

- `"http_put_response_hop_limit"`:
  - `"Integer"`: valor entero comprendido entre -1 y 64, que representa el número máximo de saltos que puede recorrer el token de metadatos. Para indicar que no hay preferencia, especifique -1.

> **Note**
>
> Límite de saltos
> Si `http_tokens` se establece en`required`, se recomienda `http_put_response_hop_limit` establecer un mínimo de 2. Para obtener más información, consulte Consideraciones sobre el acceso a los metadatos de las instancias en la Guía del usuario de Amazon Elastic Compute Cloud.

- "http_endpoint":
  - "no_preference": Se aplican otros valores predeterminados. Por ejemplo, la AMI es la opción predeterminada, si corresponde.
  - "enabled": Se puede acceder al punto final del servicio de metadatos de la instancia.
  - "disabled": No se puede acceder al punto final del servicio de metadatos de la instancia.
- "instance_metadata_tags":
  - "no_preference": Se aplican otros valores predeterminados. Por ejemplo, la AMI es la opción predeterminada, si corresponde.
  - "enabled": Se puede acceder a las etiquetas de instancia desde los metadatos de la instancia.
  - "disabled": No se puede acceder a las etiquetas de instancia desde los metadatos de la instancia.

Snapshot Block Public Access

Efecto de la política

Controla si las instantáneas de Amazon EBS son de acceso público. Para obtener más información sobre las instantáneas de EBS, consulte las instantáneas de Amazon EBS en la Guía del usuario de Amazon Elastic Block Store.

Contenido de la política

```
"snapshot_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing |
 block_all_sharing
    }
}
```

Los campos disponibles para este atributo son los siguientes:

- "state":
  - "block_all_sharing": Bloquea todo intercambio público de instantáneas. Las instantáneas que ya se compartieron públicamente se consideran privadas y ya no están disponibles públicamente.

- `"block_new_sharing"`: Bloquea el nuevo intercambio público de instantáneas. Las instantáneas que ya se compartieron públicamente permanecen disponibles públicamente.
- `"unblocked"`: No hay restricciones a la hora de compartir las instantáneas con el público.

Consideraciones

Si utiliza este atributo en una política declarativa, no podrá utilizar las siguientes operaciones para modificar la configuración obligatoria de las cuentas incluidas en el ámbito de aplicación. Esta lista no es exhaustiva:

- `EnableSnapshotBlockPublicAccess`
- `DisableSnapshotBlockPublicAccess`

Políticas de copia de seguridad

Las políticas de respaldo le permiten administrar y aplicar planes de respaldo de manera centralizada a los AWS recursos de las cuentas de una organización.

AWS Backuple permite crear planes de respaldo que definen cómo realizar copias de seguridad de sus AWS recursos. Las reglas del plan incluyen una variedad de ajustes, como la frecuencia de las copias de seguridad, el intervalo de tiempo durante el cual se realiza la copia de seguridad, la forma en que se Región de AWS contienen los recursos de los que se debe realizar la copia de seguridad y el almacén en el que se almacena la copia de seguridad. A continuación, puede aplicar un plan de respaldo a los grupos de AWS recursos identificados mediante etiquetas. También debe identificar una función AWS Identity and Access Management (IAM) que conceda AWS Backup permiso para realizar la operación de copia de seguridad en su nombre.

Las políticas de Backup AWS Organizations combinan todas esas piezas en documentos de JSONtexto. Puede adjuntar una política de copias de seguridad a cualquiera de los elementos de la estructura de su organización, como la raíz, las unidades organizativas (OUs) y las cuentas individuales. Organizations aplica reglas de herencia para combinar las políticas de la organización raíz, de cualquier matriz OUs o adjuntas a la cuenta. Esto da como resultado una política de copia de seguridad en vigor para cada cuenta. Esta política eficaz indica AWS Backup cómo hacer copias de seguridad automáticas de sus AWS recursos.

Funcionamiento de las políticas de copia de seguridad

Las políticas de copia de seguridad le proporcionan un control detallado sobre las copias de seguridad de sus recursos en cualquier nivel que requiera su organización. Por ejemplo, puede especificar en una política asociada al nodo raíz de la organización que se debe realizar una copia de seguridad de todas las tablas de Amazon DynamoDB. Esa política puede incluir una frecuencia de copia de seguridad predeterminada. A continuación, puede adjuntar una política de respaldo OUs que anule la frecuencia de respaldo de acuerdo con los requisitos de cada unidad organizativa. Por ejemplo, la unidad organizativa `Developers` puede especificar una frecuencia de copia de seguridad de una vez por semana, mientras que la unidad organizativa `Production` especifica una vez por día.

Puede crear políticas de copia de seguridad parciales que solo incluyan una parte de la información necesaria para realizar correctamente la copia de seguridad de sus recursos. Puede adjuntar estas políticas a diferentes partes del árbol organizativo, como la OU raíz o la unidad organizativa principal, con la intención de que esas políticas parciales las hereden las cuentas de nivel inferiorOUs. Cuando Organizations combina todas las políticas de una cuenta mediante reglas de herencia, la política en vigor resultante debe tener todos los elementos necesarios. De lo contrario, AWS Backup considera que la política no es válida y no hace copias de seguridad de los recursos afectados.

> **Important**
>
> AWS Backup solo puede realizar una copia de seguridad correcta cuando se aplica mediante una política completa y eficaz que contenga todos los elementos necesarios.
> Aunque una estrategia de política parcial como la descrita anteriormente puede funcionar, si una política en vigor de una cuenta está incompleta, se producirán errores o habrá recursos de los que no se realicen correctamente las copias de seguridad. Como estrategia alternativa, plantéese exigir que todas las políticas de copia de seguridad estén completas y sean válidas por sí mismas. Utilice los valores predeterminados proporcionados por las políticas asociadas a un nivel más alto en la jerarquía y reemplácelos cuando sea necesario en las políticas secundarias mediante la inclusión de operadores de control secundarios de herencia.

El plan de respaldo efectivo para cada Cuenta de AWS miembro de la organización aparece en la AWS Backup consola como un plan inmutable para esa cuenta. Puede verlo, pero no cambiarlo. Sin embargo, puede añadir o eliminar las etiquetas del plan de respaldo mediante TagResourcey. UntagResourceAPIs

Cuando se AWS Backup inicia una copia de seguridad basada en un plan de copia de seguridad creado por una política, puede ver el estado de la tarea de copia de seguridad en la AWS Backup consola. Un usuario de una cuenta de miembro puede ver el estado y los errores de los trabajos de copia de seguridad de esa cuenta de miembro. Si también habilitas el acceso a un servicio confiable con AWS Backup, un usuario de la cuenta de administración de la organización podrá ver el estado y los errores de todos los trabajos de respaldo de la organización. Para obtener más información, consulte Cómo habilitar la administración entre cuentas en la Guía para desarrolladores AWS Backup .

Introducción a las políticas de copia de seguridad

Siga estos pasos para empezar a utilizar las políticas de copia de seguridad.

1. Obtenga información sobre los permisos que debe tener para realizar tareas de políticas de copia de seguridad
2. Obtenga más información sobre algunas prácticas que recomendamos al utilizar políticas de copia de seguridad.
3. Habilite políticas de copia de seguridad para su organización.
4. Crear una política de copias de seguridad.
5. Asocie la política de copia de seguridad a la raíz, unidad organizativa o cuenta de su organización.
6. Vea la política de copia de seguridad en vigor combinada que se aplica a una cuenta.

En todos estos pasos, inicia sesión como IAM usuario, asume un IAM rol o inicia sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Información adicional

- Aprenda la sintaxis de las políticas de copia de seguridad y vea ejemplos de políticas

Prácticas recomendadas para el uso de políticas de copia de seguridad

AWS recomienda las siguientes prácticas para el uso de políticas de copia de seguridad:

Decidir una estrategia de política de copia de seguridad

Puede crear políticas de copia de seguridad en partes incompletas que se heredan y fusionan para crear una política completa para cada cuenta de miembro. Si lo hace, corre el riesgo de terminar con una política en vigor incompleta si realiza un cambio en un nivel sin considerar detenidamente

el impacto del cambio en todas las cuentas que estén por debajo de ese nivel. Para que esto no ocurra, le recomendamos que se asegure de que las políticas de copia de seguridad que implemente en todos los niveles estén completas por sí mismas. Trate las políticas principales como valores de políticas predeterminados que se pueden reemplazar por la configuración especificada en las políticas secundarias. De esta forma, incluso aunque no exista una política secundaria, la política heredada estará completa y utilizará los valores predeterminados. Puede controlar qué configuración se puede añadir, cambiar o eliminar en las políticas secundarias mediante los operadores de herencia de control secundarios.

Valide los cambios realizados en sus políticas de copia de seguridad mediante **`GetEffectivePolicy`**

Cuando realice un cambio en una política de copia de seguridad, compruebe las políticas en vigor de cuentas representativas que estén por debajo del nivel en el que haya realizado el cambio. Puede ver la política en vigor mediante la AWS Management Console o mediante la operación de la API GetEffectivePolicy o una de sus variantes de AWS SDK o AWS CLI. Asegúrese de que el cambio que ha realizado haya tenido el impacto previsto en la política en vigor.

Comience de forma sencilla y haga pequeños cambios

Para simplificar la depuración, comience con políticas sencillas y realice cambios de un elemento cada vez. Valide el comportamiento y el impacto de cada cambio antes de realizar el siguiente cambio. Este abordaje reduce el número de variables que tiene que tener en cuenta cuando se produce un error o un resultado inesperado.

Almacene copias de sus copias de seguridad en otros Regiones de AWS y cuentas de la organización

Para mejorar su posición de recuperación de desastres, puede almacenar copias de sus copias de seguridad.

- Una región diferente— Si almacena copias de la copia de seguridad en Regiones de AWS, ayuda a proteger la copia de seguridad contra daños accidentales o eliminaciones en la región original. Use la sección `copy_actions` de la política para especificar un almacén en una o varias regiones de la misma cuenta en la que se ejecuta el plan de copia de seguridad. Para ello, identifique la cuenta mediante la variable `$account` cuando especifique el ARN del almacén de copia de seguridad en el que se almacenará la copia de la copia de seguridad. La variable `$account` se reemplaza automáticamente en tiempo de ejecución con el ID de cuenta en el que se está ejecutando la política de copia de seguridad.

- Una cuenta diferente — Si almacena copias de la copia de seguridad en Cuentas de AWS, añade una barrera de seguridad que ayuda a proteger contra un actor malintencionado que pone en peligro una de sus cuentas. Use la sección `copy_actions` de la política para especificar un almacén en una o varias cuentas de la organización, independientemente de la cuenta en la que se ejecuta el plan de copia de seguridad. Para ello, identifique la cuenta usando el número de ID real de la cuenta cuando especifique el ARN del almacén de copia de seguridad en el que se almacenará la copia de la copia de seguridad.

Limite el número de planes por política

En las políticas que contienen varios planes es más complicado solucionar problemas ya que hay que validar un mayor número de salidas. Por ello, le recomendamos que haga que cada política contenga un solo plan de copia de seguridad para simplificar la depuración y la resolución de problemas. A continuación, puede añadir más políticas con otros planes para cumplir con otros requisitos. Este abordaje ayuda a mantener los problemas con un plan aislados en una política y evita que esos problemas compliquen la resolución de problemas con otras políticas y sus planes.

Utilice stack sets para crear los almacenes de copias de seguridad y los roles de IAM necesarios

Utilice la integración de los stack sets de AWS CloudFormation con Organizations para crear automáticamente los almacenes de copias de seguridad y los roles de AWS Identity and Access Management (IAM) necesarios en cada una de las cuentas miembro de su organización. Puede crear un conjunto de pilas que incluya los recursos que desea que estén disponibles automáticamente en todas las Cuenta de AWS de su organización. Este abordaje le permite ejecutar sus planes de copia de seguridad con la seguridad de que las dependencias ya se cumplen. Para obtener más información, consulte Crear un Stack Set con permisos autoadministrados en la Guía del usuario AWS CloudFormation.

Compruebe sus resultados revisando la primera copia de seguridad creada en cada cuenta

Cuando realice un cambio en una política, compruebe la siguiente copia de seguridad creada después de ese cambio para asegurarse de que el cambio tuvo el impacto deseado. Este paso va más allá de examinar la política en vigor y garantiza que AWS Backup interprete sus políticas e implemente los planes de copias de seguridad de la manera que pretendía.

Uso de eventos de AWS CloudTrail para monitorear las políticas de respaldo en su organización

Puede usar los eventos de AWS CloudTrail para supervisar cuándo se crean, actualizan o eliminan las políticas de copia de seguridad de cualquier cuenta de su organización, o cuando hay un plan de copia de seguridad organizativo no válido. Para obtener más información, consulte Cómo registrar eventos de administración entre cuentas en la Guía para desarrolladores AWS Backup.

Ejemplos y sintaxis de políticas de copia de seguridad

En esta página se describe la sintaxis de la política de copia de seguridad y se proporcionan ejemplos.

Sintaxis de las políticas de copia de seguridad

Una política de copia de seguridad es un archivo de texto sin formato que se estructura de acuerdo con las reglas de JSON. La sintaxis de las políticas de copia de seguridad sigue la sintaxis de todos los tipos de políticas de administración. Para obtener una explicación completa de esa sintaxis, consulte Sintaxis y herencia de políticas para tipos de políticas de administración. Este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política de copia de seguridad.

El bloque de una política de copia de seguridad es el plan de copia de seguridad y sus reglas. La sintaxis del plan de respaldo dentro de una política de AWS Organizations respaldo es estructuralmente idéntica a la sintaxis utilizada por AWS Backup, pero los nombres de las claves son diferentes. En las descripciones de los nombres clave de la política que aparecen a continuación, cada uno incluye el nombre de clave del AWS Backup plan equivalente. Para obtener más información sobre AWS Backup los planes, consulte CreateBackupPlanla Guía para AWS Backup desarrolladores.

> **Note**
>
> Al usar JSON, se rechazarán los nombres de clave duplicados. Si desea incluir varios planes, reglas o selecciones en una sola política, asegúrese de que el nombre de cada clave sea único.

Para ser completa y funcional, una política de copia de seguridad en vigor debe incluir algo más que un plan de copia de seguridad con su programación y sus reglas. La política también debe identificar

los recursos de Regiones de AWS los que se va a realizar la copia de seguridad, así como la función AWS Identity and Access Management (de IAM) que AWS Backup se puede utilizar para realizar la copia de seguridad.

La siguiente política funcionalmente completa muestra la sintaxis básica de las políticas de copia de seguridad. Si este ejemplo se adjuntara directamente a una cuenta, se AWS Backup haría una copia de seguridad de todos los recursos de esa cuenta en las `eu-north-1` regiones `us-east-1` y regiones que tienen la etiqueta `dataType` con un valor de `PII` o`RED`. Realiza una copia de seguridad de esos recursos diariamente a las 5.00 h en `My_Backup_Vault` y también almacena una copia en `My_Secondary_Vault`. Las dos bóvedas se encuentran en la misma cuenta que el recurso. También almacena una copia de la copia de seguridad en la `My_Tertiary_Vault` en una cuenta diferente, explícitamente especificada. Las bóvedas deben existir ya en cada una de las áreas especificadas Regiones de AWS para cada una de las Cuenta de AWS que reciben la política vigente. Si alguno de los recursos respaldados son EC2 instancias, se habilita la compatibilidad con Microsoft Volume Shadow Copy Service (VSS) para las copias de seguridad de esas instancias. La copia de seguridad aplica la etiqueta `Owner:Backup` a cada punto de recuperación.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "copy_actions": {
```

```
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"},
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        },
                        "arn:aws:backup:us-east-1:111111111111:backup-
vault:My_Tertiary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"},
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
```

```
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
        }
    }
}
```

La sintaxis de política de copia de seguridad incluye los siguientes componentes:

- Variables `$account`: en ciertas cadenas de texto de las políticas, puede usar la función `$account` para representar la Cuenta de AWS actual. Cuando AWS Backup ejecuta un plan en la política vigente, reemplaza automáticamente esta variable por la actual Cuenta de AWS en la que se ejecutan la política vigente y sus planes.

  > **Important**
  >
  > Solo puede utilizar la variable `$account` en elementos de la política que puedan incluir un nombre de recurso de Amazon (ARN), como aquellos que especifican el almacén de copia de seguridad en el que almacenar la copia de seguridad, o el rol de IAM con permisos para realizar la copia de seguridad.

  Por ejemplo, lo siguiente requiere que haya un depósito con el nombre `My_Vault` en cada uno de los lugares a los Cuenta de AWS que se aplique la política.

  ```
  arn:aws:backup:us-west-2:$account:backup-vault:My_Vault"
  ```

Le recomendamos que utilice conjuntos de AWS CloudFormation pilas y su integración con Organizations para crear y configurar automáticamente bóvedas de respaldo y funciones de IAM para cada cuenta de miembro de la organización. Para obtener más información, consulte Crear un conjunto de pilas con permisos autoadministrados en la Guía del usuario AWS CloudFormation .

- Operadores de herencia: las políticas de copia de seguridad pueden utilizar tanto la herencia de Operadores de configuración de valores como los Operadores de control secundarios.
- `plans`

  En el nivel superior, la clave de la política es la clave `plans`. Una política de copia de seguridad debe comenzar siempre con este nombre de clave fijado en la parte superior del archivo de la política. Puede tener uno o más planes de copia de seguridad con esta clave.
- Cada plan con la clave de nivel superior `plans` tiene un nombre de clave que consiste en el nombre del plan de copia de seguridad asignado por el usuario. En el ejemplo anterior, el nombre del plan de copia de seguridad es `PII_Backup_Plan`. Puede tener varios planes en una política, cada uno con sus propias `rules`, `regions`, `selections`, y `tags`.

  El nombre clave de este plan de respaldo en una política de respaldo se corresponde con el valor de la `BackupPlanName` clave en un plan. AWS Backup

  Cada plan puede contener los siguientes elementos:

  - `rules`— Esta clave contiene una colección de reglas. Cada regla se traduce en una tarea programada, con una hora de inicio y una ventana de tiempo en la que realizar la copia de seguridad de los recursos identificados por los elementos `selections` y `regions` de la política de copia de seguridad en vigor.
  - `regions`— Esta clave contiene una lista de matrices de Regiones de AWS cuyos recursos se pueden respaldar mediante esta política.
  - `selections`— Esta clave contiene una o más colecciones de recursos (dentro de la `regions` específica) que se hace una copia de seguridad en `rules`.
  - `advanced_backup_settings`— Esta clave contiene la configuración específica de las copias de seguridad que se ejecutan en determinados recursos.
  - `backup_plan_tags`: Esto especifica etiquetas adjuntas al plan de copia de seguridad en sí.
- `rules`

La clave de política `rules` se asigna a la clave `Rules` de un plan de AWS Backup . Puede tener una o más reglas con la clave `rules`. Cada regla se convierte en una tarea programada para realizar una copia de seguridad de los recursos seleccionados.

Cada regla contiene una clave cuyo nombre es el nombre de la regla. En el ejemplo anterior, el nombre de la regla es “My_Hourly_Rule”. El valor de la clave de regla es la siguiente recopilación de elementos de regla:

- `schedule_expression`— La clave de esta política se corresponde con la `ScheduleExpression` clave de un AWS Backup plan.

  Especifica la hora de inicio de la copia de seguridad. Esta clave contiene el operador de valor `@@assign` heredado y un valor de cadena con una expresión CRON que especifica cuándo AWS Backup se debe iniciar un trabajo de copia de seguridad. El formato general de la cadena CRON es: "cron( )". Cada uno es un número o comodín. Por ejemplo, `cron(0 5 ? * 1,3,5 *)` inicia la copia de seguridad a las 5.00 h todos los lunes, miércoles y viernes. `cron(0 0/1 ? * * *)` inicia la copia de seguridad cada hora a la hora, todos los días de la semana.

- `target_backup_vault_name`— Esta clave de política se relaciona con la `TargetBackupVaultName` clave de un AWS Backup plan.

  Especifica el nombre del almacén de copia de seguridad en el que se almacenará la copia de seguridad. El valor se crea mediante el uso de AWS Backup. Esta clave contiene el operador de valor heredado de `@@assign` y un valor de cadena con un nombre de almacén.

  > **Important**
  >
  > Cuando el plan de copia de seguridad se inicia por primera vez, el almacén ya debe existir. Le recomendamos que utilice conjuntos de AWS CloudFormation pilas y su integración con Organizations para crear y configurar automáticamente bóvedas de respaldo y funciones de IAM para cada cuenta de miembro de la organización. Para obtener más información, consulte Crear un conjunto de pilas con permisos autoadministrados en la Guía del usuario AWS CloudFormation .

- `start_backup_window_minutes`— Esta clave de política se corresponde con la `StartWindowMinutes` clave de un plan. AWS Backup

(Opcional) Especifica el número de minutos que se deben esperar antes de cancelar un trabajo que no se inicia correctamente. Esta clave contiene el operador de valor heredado de `@@assign` y un valor con un número entero de minutos.

- `complete_backup_window_minutes` – Esta clave de política se asigna a la clave `CompletionWindowMinutes` de un plan de AWS Backup

  (Opcional) Especifica el número de minutos después de los que un trabajo de copia de seguridad se inicia correctamente antes de que deba completarse o AWS Backup lo cancele. Esta clave contiene el operador de valor heredado de `@@assign` y un valor con un número entero de minutos.

- `enable_continuous_backup`— La clave de esta política se corresponde con la `EnableContinuousBackup` clave de un AWS Backup plan.

  (Opcional) Especifica si AWS Backup crea copias de seguridad continuas. `True`hace AWS Backup que se creen copias de seguridad continuas con capacidad de point-in-time restauración (PITR). `False`(o no especificado) provoca AWS Backup la creación de copias de seguridad instantáneas.

  > **Note**
  >
  > Debido a que las copias de seguridad habilitadas para PITR se pueden conservar durante un máximo de 35 días, debe elegir `False` o no especificar un valor si establece una de las siguientes opciones:
  >
  > - Defina `delete_after_days` en un valor mayor de 35.
  > - Establezca `move_to_cold_storage_after_days` en cualquier valor.

  Para obtener más información sobre las copias de seguridad continuas, consulte la Point-in-time recuperación en la Guía para AWS Backup desarrolladores.

- `lifecycle`— La clave de esta política se corresponde con la `Lifecycle` clave de un AWS Backup plan.

  (Opcional) Especifica cuándo AWS Backup pasa esta copia de seguridad a almacenamiento en frío y cuándo caduca.

  - `move_to_cold_storage_after_days` — La clave de esta política se corresponde con la `MoveToColdStorageAfterDays` clave de un AWS Backup plan.

Especifica el número de días después de que se produzca la copia de seguridad antes de que AWS Backup mueva el punto de recuperación al almacenamiento en frío. Esta clave contiene el operador de valores de herencia de`@@assign` y un valor con un número entero de días.

- `delete_after_days`— La clave de esta política se corresponde con la `DeleteAfterDays` clave de un AWS Backup plan.

  Especifica el número de días después de que se produzca la copia de seguridad antes de que AWS Backup elimine el punto de recuperación. Esta clave contiene el operador de valores de herencia de`@@assign` y un valor con un número entero de días. Este valor debe ser al menos 90 días posterior al número de días especificado en `move_to_cold_storage_after_days`.

- `opt_in_to_archive_for_supported_resources`— La clave de esta política se corresponde con la `OptInToArchiveForSupportedResources` clave de un AWS Backup plan.

  Si el valor se asigna como `true`, su plan de copia de seguridad lleva a cabo la transición de los recursos compatibles al nivel de almacenamiento de archivo (en frío) de acuerdo con la configuración del ciclo de vida. Para obtener más información sobre el nivel de Archivo de instantáneas de Amazon EBS, consulte Archivar instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS.

  Solo se puede habilitar esta configuración si se cumplen las siguientes condiciones:

  - Su política de copias de seguridad tiene una frecuencia de un mes o más.
  - `move_to_cold_storage_after_days` debe existir.
  - `delete_after_days` menos `move_to_cold_storage_after_days` es mayor o igual a 90 días.

  Esta clave contiene el operador de valor heredado de `@@assign` y un valor de `true` o `false`.

- `copy_actions`— La clave de esta política se corresponde con la `CopyActions` clave de un AWS Backup plan.

  (Opcional) Especifica que se AWS Backup debe copiar la copia de seguridad en una o más ubicaciones adicionales. Cada ubicación de copia de seguridad se describe de la siguiente manera:

- Clave cuyo nombre identifica de forma exclusiva esta acción de copia. En este momento, el nombre de clave debe ser el nombre de recurso de Amazon (ARN) del almacén de copia de seguridad. Esta clave contiene dos entradas.
  - `target_backup_vault_arn` – Esta clave de política se asigna a la clave `DestinationBackupVaultArn` de un plan de AWS Backup

    (Opcional) Especifica el almacén en el que se AWS Backup almacena una copia adicional de la copia de seguridad. El valor de esta clave contiene el Operador de valores de herencia `@@assign` y el ARN de la bóveda.
    - Para hacer referencia a un almacén en el Cuenta de AWS que se ejecuta la política de copias de seguridad, utilice la `$account` variable del ARN en lugar del número de ID de la cuenta. Cuando AWS Backup ejecuta el plan de respaldo, reemplaza automáticamente la variable por el número de ID de cuenta Cuenta de AWS en la que se ejecuta la política. Esto permite que la copia de seguridad se ejecute correctamente cuando la política de copia de seguridad se aplica a más de una cuenta de una organización.
    - Para hacer referencia a un almacén en un Cuenta de AWS diferente en la misma organización, utilice el número de ID de cuenta real en el ARN.

    > **Important**
    >
    > - Si falta esta clave, se utiliza una versión en minúsculas del ARN en el nombre de la clave principal. Como ARNs distinguen mayúsculas de minúsculas, es posible que esta cadena no coincida con el ARN real del almacén y el plan fracase. Por esta razón, le recomendamos que proporcione siempre esta clave y valor.
    > - El almacén de copia de seguridad que quiere copiar a la copia de seguridad ya debe existir la primera vez que inicie el plan de copia de seguridad. Se recomienda utilizar conjuntos de pilas de stack sets AWS CloudFormation y su integración con Organizations para crear y configurar automáticamente almacenes de copia de seguridad y roles de IAM para cada cuenta de miembro de la organización. Para obtener más información, consulte Crear un conjunto de pilas con permisos autoadministrados en la Guía del usuario AWS CloudFormation .
  - `lifecycle`— Esta clave de política se asigna a la `Lifecycle` clave situada debajo de la `CopyAction` clave de un AWS Backup plan.

(Opcional) Especifica cuándo se hace la AWS Backup transición de esta copia de una copia de seguridad a un almacenamiento en frío y cuándo caduca.

- `move_to_cold_storage_after_days` – Esta clave de política se asigna a la clave `MoveToColdStorageAfterDays` de un plan de AWS Backup .

  Especifica el número de días transcurridos desde la fecha de creación de la copia de seguridad antes de que el punto de recuperación AWS Backup se traslade al almacenamiento en frío. Esta clave contiene el operador de valores de herencia `de@@assign` y un valor con un número entero de días.

- `delete_after_days` – Esta clave de política se asigna a la clave `DeleteAfterDays` de un plan de AWS Backup

  Especifica el número de días transcurridos desde la realización de la copia de seguridad antes de AWS Backup eliminar el punto de recuperación. Esta clave contiene el operador de valores de herencia `de@@assign` y un valor con un número entero de días. Si realiza la transición de una copia de seguridad al almacenamiento en frío, debe permanecer allí un mínimo de 90 días, por lo que este valor debe ser un mínimo de 90 días mayor que el valor `move_to_cold_storage_after_days`.

- `recovery_point_tags`— Esta clave de política se corresponde con la `RecoveryPointTags` clave de un AWS Backup plan.

  (Opcional) Especifica las etiquetas que se AWS Backup adjuntan a cada copia de seguridad que crea a partir de este plan. El valor de esta clave contiene uno o varios de los siguientes elementos:

  - Un identificador para este par de nombre de clave y valor. Este nombre para cada elemento de `recovery_point_tags` es el nombre de la clave de etiqueta en minúscula, incluso aunque la `tag_key` tenga un tratamiento de mayúsculas y minúsculas diferente. Este identificador no distingue entre mayúsculas y minúsculas. En el ejemplo anterior, este par de claves se identificó con el nombre `0wner`. Cada par de claves contiene los siguientes elementos:

    - `tag_key`: especifica el nombre de clave de etiqueta que se adjuntará al plan de copia de seguridad. Esta clave contiene el operador de valor heredado de `@@assign` y un valor de cadena. El valor distingue entre mayúsculas y minúsculas.

    - `tag_value` – Especifica el valor que se adjunta al plan de copia de seguridad y que está asociado al `tag_key`. Esta clave contiene cualquiera de los operadores de valor heredado

y uno o más valores para reemplazar, adjuntar o quitar de la política en vigor. Estos valores distinguen entre mayúsculas y minúsculas.

- `regions`

  La clave `regions` de política especifica qué Regiones de AWS recursos AWS Backup busca para encontrar los recursos que coincidan con las condiciones de la `selections` clave. Esta clave contiene cualquiera de los operadores de valores heredados y uno o más valores de cadena para los Región de AWS códigos, por ejemplo:`["us-east-1", "eu-north-1"]`.

- `selections`

  La clave de política `selections` especifica los recursos de los que se realiza una copia de seguridad mediante las reglas de plan de esta política. Esta clave corresponde aproximadamente al BackupSelectionobjeto en AWS Backup. Los recursos se especifican mediante una consulta para hacer coincidir los nombres y valores de clave de etiqueta. La `selections` clave contiene dos claves debajo: `tags` y`resources`.

  > **Note**
  >
  > `resources`Las teclas `tags` y no se pueden usar juntas en la misma selección. Si desea una selección con condiciones de etiqueta y condiciones de recursos, debe usar las `resources` teclas. Una política efectiva debe tener una `tags` o varias `resources` en la selección para ser válida.

  - `tags`: especifica las etiquetas que identifican los recursos y el rol de IAM que tiene permiso para consultar los recursos y realizar una copia de seguridad de ellos. El valor de esta clave contiene uno o varios de los siguientes elementos:
    - Un identificador para este elemento de etiqueta. Este identificador de `tags` es el nombre de clave de etiqueta en minúsculas, incluso aunque la etiqueta que se consulta tiene un tratamiento de mayúsculas y minúsculas diferente. Este identificador no distingue entre mayúsculas y minúsculas. En el ejemplo anterior, se identificó un elemento con el nombre `My_Backup_Assignment`. Cada identificador de `tags` contiene los siguientes elementos:
      - `iam_role_arn`: especifica el rol de IAM que tiene permiso para acceder a los recursos identificados por la consulta de etiquetas en la Regiones de AWS especificada por la clave `regions`. Este valor contiene el operador del valor de `@@assign` herencia y un valor de cadena que contiene el ARN del rol. AWS Backup utiliza este rol para buscar y descubrir los recursos y para realizar la copia de seguridad.

Puede usar la variable `$account` en el ARN en lugar del número de ID de cuenta. Cuando se ejecuta el plan de respaldo AWS Backup, reemplaza automáticamente la variable por el número de ID de cuenta real de la cuenta Cuenta de AWS en la que se ejecuta la política.

> **Important**
>
> El rol ya debe existir cuando inicie el plan de copia de seguridad la primera vez. Le recomendamos que utilice conjuntos de AWS CloudFormation pilas y su integración con Organizations para crear y configurar automáticamente bóvedas de respaldo y funciones de IAM para cada cuenta de miembro de la organización. Para obtener más información, consulte Crear un conjunto de pilas con permisos autoadministrados en la Guía del usuario AWS CloudFormation .

- `tag_key` — Especifica el nombre de clave de etiqueta que se va a buscar. Esta clave contiene el operador de valor heredado de `@@assign` y un valor de cadena. El valor distingue entre mayúsculas y minúsculas.
- `tag_value`— Especifica el valor que debe asociarse a un nombre de clave que coincida. `tag_key` AWS Backup incluye el recurso en la copia de seguridad solo si ambos `tag_value` coinciden. `tag_key` Esta clave contiene cualquiera de los operadores de valor heredado y uno o más valores para reemplazar, adjuntar o quitar de la política en vigor. Estos valores distinguen entre mayúsculas y minúsculas.
- `conditions`— Especifique las claves de etiqueta y los valores que desee incluir o excluir. Puede utilizar `string_equals` o `string_not_equals to include or exclude tags of an exact match`. También puede `string_not_like` usar `string_like` e incluir o excluir etiquetas que contengan o no caracteres específicos.

> **Note**
>
> Hay un límite de 30 `conditions` para cada selección.

Ejemplo: especificar recursos con el **`tags`** bloque

El siguiente ejemplo incluye todos los recursos con los `tag_key` valores = “`env`” y `tag_value` = `"prod"` y`"gamma"`. En este ejemplo se excluyen los recursos con el `tag_key` = `"backup"` y el `tag_value` =`"false"`.

```
...
"selections":{
    "tags":{
        "selection_name":{
            "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "tag_key":{"@@assign": "env"},
            "tag_value":{"@@assign": ["prod", "gamma"]},
            "conditions":{
                "string_not_equals":{
                    "condition_name1":{
                        "condition_key": { "@@assign": "aws:ResourceTag/backup"  },
                        "condition_value": {  "@@assign": "false" }
                    }
                }
            }
        }
    }
},
...
```

- `resources`— Si desea especificar un recurso utilizando tanto las condiciones de etiqueta como las condiciones del recurso, debe usar la `resources` clave.
  - `iam_role_arn`: especifica el rol de IAM que tiene permiso para acceder a los recursos identificados por la consulta de etiquetas en la Regiones de AWS especificada por la clave `regions`. Este valor contiene el operador del valor de `@@assign` herencia y un valor de cadena que contiene el ARN del rol. AWS Backup utiliza este rol para buscar y descubrir los recursos y para realizar la copia de seguridad.

    Puede usar la variable `$account` en el ARN en lugar del número de ID de cuenta. Cuando se ejecuta el plan de respaldo AWS Backup, reemplaza automáticamente la variable por el número de ID de cuenta real de la cuenta Cuenta de AWS en la que se ejecuta la política.

    > **Important**
    >
    > El rol ya debe existir cuando inicie el plan de copia de seguridad la primera vez. Le recomendamos que utilice conjuntos de AWS CloudFormation pilas y su integración con Organizations para crear y configurar automáticamente bóvedas de respaldo y funciones de IAM para cada cuenta de miembro de la organización. Para obtener más

información, consulte Crear un conjunto de pilas con permisos autoadministrados en la Guía del usuario AWS CloudFormation .

> **Note**
>
> En AWS GovCloud (US) Regions, debe añadir el nombre de la partición al ARN. Por ejemplo, `"arn:aws:ec2:*:*:volume/*"` debe serlo. `"arn:aws-us-gov:ec2:*:*:volume/*"`

- `resource_types`— Especifica los tipos de recursos que desea incluir en el plan de respaldo.
- `not_resource_types`— Especifica los tipos de recursos que desea excluir del plan de respaldo.

  Organizations admite los siguientes tipos de recursos para `resource_types` y`not_resource_types`:

  - AWS Backup gateway máquinas virtuales: `"arn:aws:backup-gateway:*:*:vm/*"`
  - AWS CloudFormation pilas: `"arn:aws:cloudformation:*:*:stack/*"`
  - Tablas de Amazon DynamoDB: `"arn:aws:dynamodb:*:*:table/*"`
  - EC2 Instancias de Amazon: `"arn:aws:ec2:*:*:instance/*"`
  - Volúmenes de Amazon EBS: `"arn:aws:ec2:*:*:volume/*"`
  - Sistemas de archivos Amazon EFS: `"arn:aws:elasticfilesystem:*:*:file-system/*"`
  - Cúmulos de Amazon Aurora/Amazon DocumentDB/Amazon Neptune: `"arn:aws:rds:*:*:cluster:*"`
  - Bases de datos de Amazon RDS: `"arn:aws:rds:*:*:db:*"`
  - Clústeres de Amazon Redshift: `"arn:aws:redshift:*:*:cluster:*"`
  - Amazon S3: `"arn:aws:s3:::*"`
  - AWS Systems Manager para SAP Bases de datos HANA: `"arn:aws:ssm-sap:*:*:HANA/*"`
  - AWS Storage Gateway pasarelas: `"arn:aws:storagegateway:*:*:gateway/*"`
  - Bases de datos de Amazon Timestream: `"arn:aws:timestream:*:*:database/*"`
  - Sistemas de FSx archivos de Amazon: `"arn:aws:fsx:*:*:file-system/*"`

  - FSx Volúmenes de Amazon: `"arn:aws:fsx:*:*:volume/*"`
- `conditions`— Especifique las claves y los valores de las etiquetas que desee incluir o excluir. Puede utilizar `string_equals` o `string_not_equals to include or exclude tags of an exact match`. También puede `string_not_like` usar `string_like` e incluir o excluir etiquetas que contengan o no caracteres específicos.

> **Note**
>
> Hay un límite de 30 `conditions` para cada selección.

Ejemplos: especificar recursos con el **`resources`** bloque

Los siguientes son ejemplos del uso del `resources` bloque para especificar recursos.

Example: Select all resources in my account

La lógica booleana es similar a la que se puede utilizar en las políticas de IAM. El `"resource_types"` bloque utiliza un booleano AND para combinar los tipos de recursos.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        }
    }
},
...
```

Example: Select all resources in my account, but exclude Amazon EBS volumes

La lógica booleana es similar a la que se puede utilizar en las políticas de IAM. Los `"not_resource_types"` bloques `"resource_types"` y utilizan un booleano AND para combinar los tipos de recursos.

```
...
"resources":{
```

```
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true", but exclude Amazon EBS volumes

La lógica booleana es similar a la que se puede utilizar en las políticas de IAM. Los `"not_resource_types"` bloques `"resource_types"` y utilizan un booleano `AND` para combinar los tipos de recursos. El `"conditions"` bloque usa un booleano. `AND`

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key": { "@@assign":"aws:ResourceTag/backup"},
                    "condition_value": {  "@@assign":"true" }
                }
            }
```

```
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS DB instances tagged with both "backup" : "true" and "stage" : "prod"

La lógica booleana es similar a la que se puede utilizar en las políticas de IAM. El `"resource_types"` bloque utiliza un booleano AND para combinar los tipos de recursos. El `"conditions"` bloque usa un booleano AND para combinar los tipos de recursos y las condiciones de las etiquetas.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                },
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"prod"}
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS instances tagged with "backup" : "true" but not "stage" : "test"

La lógica booleana es similar a la que se puede utilizar en las políticas de IAM. El `"resource_types"` bloque utiliza un booleano `AND` para combinar los tipos de recursos. El `"conditions"` bloque usa un booleano `AND` para combinar los tipos de recursos y las condiciones de las etiquetas.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                  }
            },
            "string_not_equals":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"test"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "key1" and a value which begins with "include" but not with "key2" and value that contains the word "exclude"

La lógica booleana es similar a la que se puede utilizar en las políticas de IAM. El `"resource_types"` bloque utiliza un booleano `AND` para combinar los tipos de recursos.

El `"conditions"` bloque usa un booleano `AND` para combinar los tipos de recursos y las condiciones de las etiquetas.

En este ejemplo, observe el uso del carácter comodín (`*`) en`include*`, y`*exclude*`. `arn:aws:rds:*:*:db:*` Puede utilizar el carácter comodín (`*`) al principio, al final y al centro de una cadena.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "conditions":{
            "string_like":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key1"},
                    "condition_value":{"@@assign":"include*"}
                }
            },
            "string_not_like":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key2"},
                    "condition_value":{"@@assign":"*exclude*"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true" except Amazon FSx file systems and Amazon RDS resources

La lógica booleana es similar a la que se puede utilizar en las políticas de IAM. Los `"not_resource_types"` bloques `"resource_types"` y utilizan un booleano `AND` para combinar los tipos de recursos. El `"conditions"` bloque usa un booleano `AND` para combinar los tipos de recursos y las condiciones de las etiquetas.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "resource_types":{
                "@@assign": [
                    "*"
                ]
            },
            "not_resource_types":{
                "@@assign":[
                    "arn:aws:fsx:*:*:file-system/*",
                    "arn:aws:rds:*:*:db:*"
                ]
            },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                }
            }
        }
    }
},
...
```

- `advanced_backup_settings`: especifica la configuración de escenarios de copia de seguridad específicos. Esta clave contiene una o varias opciones de configuración. Cada configuración es una cadena de objetos JSON con los siguientes elementos:
  - Nombre de clave de objeto: cadena que especifica el tipo de recurso al que se aplica la siguiente configuración avanzada.
  - Valor del objeto: cadena de objeto JSON que contiene una o más configuraciones de copia de seguridad específicas del tipo de recurso asociado.

  En este momento, la única configuración de copia de seguridad avanzada que se admite permite ejecutar copias de seguridad del Microsoft Volume Shadow Copy Service (VSS) para Windows o SQL Server en una EC2 instancia de Amazon. El nombre de la clave debe ser el tipo de `"ec2"` recurso y el valor especifica que el `"windows_vss"` soporte es `disabled` para las copias de seguridad realizadas en esas EC2 instancias de Amazon `enabled` o para ellas.

Para obtener más información acerca de esta característica, consulte Creación de una copia de seguridad de Windows habilitada para VSS en la Guía para desarrolladores AWS Backup .

Ejemplo: especificar escenarios de respaldo con el **`advanced_backup_settings`** bloque

El siguiente ejemplo muestra cómo habilitar las copias de seguridad del Microsoft Volume Shadow Copy Service (VSS) para Windows o SQL Server que se ejecutan en EC2 instancias de Amazon.

```
...
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
},
...
```

- `backup_plan_tags`: Especifica etiquetas adjuntas al plan de copia de seguridad en sí. Esto no afecta a las etiquetas especificadas en ninguna regla o selección.

  (Opcional) Puede asociar etiquetas a sus planes de copia de seguridad. El valor de esta clave es una colección de elementos.

  El nombre de clave de cada elemento bajo `backup_plan_tags` es el nombre de clave de etiqueta en minúsculas, incluso si la etiqueta a consultar tiene un tratamiento de caso diferente. Este identificador no distingue entre mayúsculas y minúsculas. El valor de cada una de estas entradas consta de las siguientes claves:

  - `tag_key`: especifica el nombre de clave de etiqueta que se adjuntará al plan de copia de seguridad. Esta clave contiene el operador de valor heredado de `@@assign` y un valor de cadena. Este valor distingue entre mayúsculas y minúsculas.
  - `tag_value` – Especifica el valor que se adjunta al plan de copia de seguridad y que está asociado al `tag_key`. Esta clave contiene el operador de valor heredado de `@@assign` y un valor de cadena. Este valor distingue entre mayúsculas y minúsculas.

Ejemplos de políticas de copia de seguridad

Los ejemplos de políticas de copia de seguridad siguientes son solo para fines informativos. En algunos de los ejemplos siguientes, el formato de espacio en blanco JSON podría comprimirse para ahorrar espacio.

Ejemplo 1: política asignada a un nodo principal

En el ejemplo siguiente se muestra una política de copia de seguridad asignada a uno de los nodos principales de una cuenta.

Política principal: esta política se puede asociar al nodo raíz de la organización o a cualquier unidad organizativa que sea primaria de todas las cuentas previstas.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        },
                        "opt_in_to_archive_for_supported_resources": {
```

```
                            "@@assign": "false"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
```

```
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {
                        "@@assign": "enabled"
                    }
                }
            }
        }
    }
}
```

Si no se hereda ni se adjunta ninguna otra política a las cuentas, la política vigente que se muestra en cada una de las aplicables es la Cuenta de AWS que se muestra en el siguiente ejemplo. La expresión CRON hace que la copia de seguridad se ejecute una vez por hora, a la hora en punto. El ID de cuenta 123456789012 será el ID de cuenta real de cada cuenta.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
```

```
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
```

```
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
}
```

Ejemplo 2: una política principal se fusiona con una política secundaria

En el siguiente ejemplo, una política principal heredada y una política secundaria se heredan o se asocian directamente a una Cuenta de AWS fusión para formar la política efectiva.

Política principal: esta política se puede asociar al nodo raíz de la organización o a cualquier unidad organizativa principal.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "delete_after_days": { "@@assign": "180" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
```

```
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "delete_after_days": { "@@assign": "180" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII", "RED" ] }
                        }
                    }
                }
            }
    }
}
```

Política secundaria: esta política puede estar asociada directamente a la cuenta o a una unidad organizativa en cualquier nivel por debajo del nivel al que está asociada.

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
```

```
                        "delete_after_days": { "@@assign": "365" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "delete_after_days": { "@@assign": "365" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "MonthlyDatatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                        "tag_key": { "@@assign": "BackupType" },
                        "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                    }
                }
            }
        }
    }
}
```

Resultado de políticas en vigor: la política efectiva aplicada a las cuentas contiene dos planes, cada uno con su propio conjunto de reglas y conjunto de recursos a los que aplicar las reglas.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
```

```
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
```

```
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "delete_after_days": "365",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "monthlydatatype": {
                            "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                            "tag_key": "BackupType",
                            "tag_value": [ "MONTHLY", "RED" ]
                        }
                    }
                }
            }
        }
}
```

Ejemplo 3: una política principal evita los cambios realizados por una política secundaria

En el ejemplo siguiente, una política principal heredada utiliza los operadores de control secundarios para aplicar toda la configuración y evita que una política secundaria los modifique.

Política principal: esta política se puede asociar al nodo raíz de la organización o a cualquier unidad organizativa principal. La presencia de `"@@operators_allowed_for_child_policies":`

`["@@none"]` en cada nodo de la política significa que una política secundaria no puede realizar cambios de ningún tipo en el plan. Tampoco puede una política secundaria añadir planes adicionales a la política en vigor. Esta política se convierte en la política en vigor para cada unidad organizativa y cuenta bajo la unidad organizativa a la que está asociada.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
```

```
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "false"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
                                },
                                 "opt_in_to_archive_for_supported_resources": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
                }
            },
            "selections": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "ec2": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "windows_vss": {
                        "@@assign": "enabled",
                        "@@operators_allowed_for_child_policies": ["@@none"]
                    }
                }
            }
        }
    }
}
```

Resultado de políticas en vigor: si existe alguna política de copia de seguridad secundaria, se ignora y la política principal se convierte en la política efectiva.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
```

```
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:backup-vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "delete_after_days": "180",
                            "opt_in_to_archive_for_supported_resources": "false"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

Ejemplo 4: una política principal impide que una política secundaria realice cambios en un plan de copia de seguridad.

En el ejemplo siguiente, una política principal heredada utiliza los operadores de control secundarios para aplicar la configuración de un único plan y evita que una política secundaria los modifique. De todas formas, la política secundaria puede agregar planes adicionales.

Política principal: esta política se puede asociar al nodo raíz de la organización o a cualquier unidad organizativa principal. Este ejemplo es similar al ejemplo anterior con todos los operadores secundarios heredados bloqueados, excepto en el nivel superior de `plans`. La configuración `@@append` en ese nivel permite a las políticas secundarias agregar otros planes a la recopilación en la política en vigor. Cualquier cambio en el plan heredado sigue bloqueado.

Las secciones del plan se truncan para mayor claridad.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

Política secundaria: esta política puede estar asociada directamente a la cuenta o a una unidad organizativa en cualquier nivel por debajo del nivel al que está asociada. Esta política secundaria define un nuevo plan.

Las secciones del plan se truncan para mayor claridad.

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
```

```
}
```

Resultado de políticas en vigor — La política en vigor incluye ambos planes.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Ejemplo 5: una política secundaria reemplaza la configuración de una política principal

En el ejemplo siguiente, una política secundaria utiliza operadores de establecimiento de valores para anular algunas de las configuraciones heredadas de una política principal.

Política principal: esta política se puede asociar al nodo raíz de la organización o a cualquier unidad organizativa principal. Cualquiera de las opciones puede ser anulada por una política secundaria porque el comportamiento predeterminado, en ausencia de un operador de control secundario que lo impida, es permitir que la política secundaria `@@assign`, `@@append`, o `@@remove`. La política principal contiene todos los elementos necesarios para un plan de copia de seguridad válido, por lo que realiza una copia de seguridad de los recursos correctamente si se hereda tal y como está.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
```

```
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "delete_after_days": {"@@assign": "180"},
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

Política secundaria: la política secundaria incluye solo la configuración que debe ser diferente de la política principal heredada. Debe haber una política principal heredada que proporcione la otra configuración necesaria cuando se fusiona en una política en vigor. De lo contrario, la política de copia de seguridad efectiva contiene un plan de copia de seguridad no válido que no realiza una copia de seguridad de los recursos como se esperaba.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "delete_after_days": {"@@assign": "365"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    }
                }
            }
        }
    }
}
```

Resultado de políticas en vigor: la política en vigor incluye la configuración de ambas políticas, con la configuración proporcionada por la política secundaria anulando la configuración heredada de la principal. En este ejemplo, se producen los siguientes cambios:

- La lista de regiones se sustituye por una lista completamente diferente. Si desea agregar una región a la lista heredada, utilice `@@append` en lugar de `@@assign` en la política secundaria.
- AWS Backup actúa cada dos horas en lugar de cada hora.
- AWS Backup deja transcurrir 80 minutos para que comience la copia de seguridad en lugar de 60 minutos.

- AWS Backup utiliza la `Default` bóveda en lugar de`FortKnox`.
- El ciclo de vida se extiende tanto para la transferencia al almacenamiento en frío como para la eliminación eventual de la copia de seguridad.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": "false"

                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
```

```
                        "PII",
                        "RED"
                    ]
                }
            }
        }
    }
}
```

Políticas de etiquetas

Las políticas de etiquetas le permiten estandarizar las etiquetas adjuntas a AWS los recursos de las cuentas de una organización.

Puede utilizar políticas de etiquetas para mantener la coherencia de las etiquetas, incluido el tratamiento de casos preferentes de valores y claves de etiquetas.

¿Qué son las etiquetas?

Las etiquetas son etiquetas de atributos personalizadas que se asignan o que se AWS asignan a AWS los recursos. Cada etiqueta tiene dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta distinguen entre mayúsculas y minúsculas.
- Un campo opcional denominado valor de etiqueta (por ejemplo, `111122223333` o `Production`). Omitir el valor de etiqueta es lo mismo que utilizar una cadena vacía. Al igual que las claves de etiqueta, los valores de etiqueta distinguen entre mayúsculas y minúsculas.

En el resto de esta página se describen las políticas de etiquetas. Para obtener más información acerca de las etiquetas, consulte las siguientes fuentes:

- Para obtener información general sobre el etiquetado, incluidas las convenciones de nomenclatura y uso, consulte la Guía del usuario de Tagging AWS Resources.
- Para obtener una lista de los servicios que admiten el uso de etiquetas, consulte Resource Groups Tagging API Reference.
- Para obtener información sobre el uso de etiquetas para clasificar los recursos, consulte el documento técnico sobre las prácticas recomendadas para etiquetar AWS los recursos.

- Para obtener información acerca del etiquetado de recursos de Organizations, consulte Recursos de etiquetado AWS Organizations.
- Para obtener información sobre cómo etiquetar recursos en otros Servicios de AWS, consulte la documentación de ese servicio.

¿Qué son las políticas de etiquetas?

Las políticas de etiquetas son un tipo de política que le puede ayudar a estandarizar las etiquetas en todos los recursos en las cuentas de su organización. En una política de etiquetas, se especifican las reglas de etiquetado aplicables a los recursos cuando se etiquetan.

Por ejemplo, una política de etiquetas puede especificar que, cuando se asocia a un recurso la etiqueta `CostCenter`, esta debe utilizar el tratamiento de mayúsculas y minúsculas y los valores de etiqueta que define la política de etiquetas. Una política de etiquetas también puede especificar que se ejecuten operaciones de etiquetado no conformes en los tipos de recursos especificados. En otras palabras, no se pueden completar las solicitudes de etiquetado no conformes en los tipos de recursos especificados. No se evalúa la conformidad con la política de etiquetas de los recursos no etiquetados o las etiquetas que no están definidas en la política de etiquetas.

El uso de políticas de etiquetado implica trabajar con varios Servicios de AWS:

- Utilice AWS Organizations para administrar políticas de etiquetas. Cuando se inicia sesión en la cuenta de administración de la organización, se utiliza Organizations para habilitar la característica de políticas de etiquetas. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización. A continuación, puede crear políticas de etiquetas y asociarlas a las entidades de la organización para poner en vigor dichas reglas de etiquetado.
- Utilice AWS Resource Groups para administrar la conformidad con las políticas de etiquetas. Cuando se inicia sesión en una cuenta de la organización, se utiliza Resource Groups para buscar etiquetas no conformes en los recursos de la cuenta. Puede corregir las etiquetas no conformes en el AWS servicio en el que creó el recurso. También puede utilizar el editor de etiquetas y el etiquetado de Resource Groups API para etiquetar y desetiquetar recursos de varios servicios.

  Si inicia sesión en la cuenta de administración de la organización, puede ver la información de conformidad de todas las cuentas de la organización.

Las políticas de etiquetas solo están disponibles en las organizaciones que tienen todas las características habilitadas. Para obtener más información acerca de qué se necesita para utilizar políticas de etiquetas, consulte Requisitos previos y permisos para las políticas de administración para AWS Organizations.

> **Important**
>
> Para empezar con las políticas de etiquetas, le AWS recomendamos encarecidamente que siga el ejemplo de flujo de trabajo descrito en Introducción a las políticas de etiquetas antes de pasar a políticas de etiquetas más avanzadas. Es mejor conocer los efectos de asociar una política de etiquetas sencilla a una única cuenta antes de ampliar las políticas de etiquetas a toda una unidad organizativa u organización. Es especialmente importante conocer los efectos de una política de etiquetas antes de ejecutar la conformidad de cualquier política de etiquetas. Las tablas de la página Introducción a las políticas de etiquetas también ofrecen enlaces a instrucciones para tareas más avanzadas relacionadas con las políticas.

Prácticas recomendadas para utilizar políticas de etiquetas

AWS recomienda las siguientes prácticas recomendadas para el uso de políticas de etiquetas.

Elija una estrategia de uso de mayúsculas y minúsculas en etiquetas

Determine cómo desea usar las mayúsculas y minúsculas en las etiquetas e implemente de forma coherente esa estrategia en todos los tipos de recursos. Por ejemplo, decida si se va a utilizar `Costcenter`, `costcenter` o `CostCenter` y utilice la misma convención para todas las etiquetas. Para obtener resultados coherentes en los informes de conformidad, evite utilizar etiquetas similares con un tratamiento incoherente de mayúsculas y minúsculas. Esta estrategia le ayudará a definir políticas de etiquetas para su organización.

Utilice el flujo de trabajo recomendado

Comience poco a poco creando una política de etiquetas sencilla. A continuación, asóciela a una cuenta de miembro que pueda utilizar con fines de prueba. Utilice los flujos de trabajo que se describen en Introducción a las políticas de etiquetas.

Determine las reglas de etiquetado

Esto dependerá de las necesidades de su organización. Por ejemplo, puede que desee especificar que, cuando se adjunte una `CostCenter` etiqueta a un AWS Secrets Manager secreto, se utilice el tratamiento de mayúsculas y minúsculas especificado. Cree políticas de etiquetas que definan etiquetas conformes y asócielas a las entidades de la organización en las que desee que entren en vigor dichas reglas de etiquetado.

Forme a los administradores de la cuenta

Cuando esté listo para ampliar el uso de políticas de etiquetas, forme a los administradores de la cuenta de la siguiente manera:

- Comunique su estrategia de etiquetado.
- Haga hincapié en que los administradores han de utilizar etiquetas en tipos de recursos específicos.

  Esto es importante, ya que los recursos sin etiquetas se muestran como conformes en los resultados de conformidad.
- Proporcione instrucciones para la comprobación de la conformidad de las políticas de etiquetas. Indique a los administradores que busquen y corrijan las etiquetas no conformes en los recursos de sus cuentas mediante el procedimiento descrito en la sección Evaluación del cumplimiento de una cuenta en la Guía del usuario de los AWS recursos de etiquetado. Infórmeles de la frecuencia con la que desea que comprueben la conformidad.

Actúe con precaución al ejecutar el cumplimiento.

Forzar el cumplimiento puede impedir que los usuarios de las cuentas de su organización etiqueten los recursos que necesiten. Revise la información de Descripción de la aplicación de políticas. Consulte también los flujos de trabajo que se describen en Introducción a las políticas de etiquetas.

Considere la posibilidad de crear y establecer barreras SCP en torno a las solicitudes de creación de recursos

Los recursos que nunca han tenido etiquetas asociadas se muestran como conformes en los informes. Los administradores de cuentas aún pueden crear recursos sin etiquetar. En algunos casos, puedes usar una política de control de servicios (SCP) para establecer barreras en torno a las solicitudes de creación de recursos. Para ver un ejemploSCP, consulte. Requerir una etiqueta en los recursos creados especificados

Para saber si un AWS servicio admite el control del acceso mediante etiquetas, consulte Servicios de AWS That Work with IAM en la Guía del IAM usuario. Busque los servicios cuyo texto sea Sí en la columna ABAC(autorización basada en etiquetas). Elija el nombre del servicio para ver la documentación sobre la autorización y el control de acceso para dicho servicio.

Introducción a las políticas de etiquetas

El uso de políticas de etiquetas implica el uso de varios Servicios de AWS. Para empezar, revise las siguientes páginas. A continuación, siga los flujos de trabajo de esta página para familiarizarse con las políticas de etiquetas y sus efectos.

- Requisitos previos y permisos para las políticas de administración para AWS Organizations
- Prácticas recomendadas para utilizar políticas de etiquetas

Uso de políticas de etiquetas por primera vez

Siga estos pasos para comenzar a utilizar las políticas de etiquetas por primera vez.

Tarea	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
Paso 1: Habilite las políticas de etiquetado de su organización.	Esta es la cuenta de administración de la organización.	AWS Organizations
Paso 2: cree una política de etiquetas. Mantenga su primera política de etiquetas simple. Introduzca una clave de etiqueta en el tratamiento de mayúsculas y minúsculas que desea utilizar y deje el resto de opciones en sus valores predeterminados.	Esta es la cuenta de administración de la organización.	AWS Organizations
Paso 3: asocie una política de etiquetas a la cuenta de	Esta es la cuenta de administración de la organización.	AWS Organizations

Tarea	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
un solo miembro que pueda utilizar para las pruebas. Tendrá que iniciar sesión en esta cuenta en el siguiente paso.		
Paso 4: cree algunos recursos con etiquetas de conformidad y otros con etiquetas no conformes.	La cuenta de miembro que está utilizando para realizar pruebas.	Cualquier servicio de AWS con el que se sienta cómodo. Por ejemplo, puede utilizar AWS Secrets Manager y seguir el procedimiento en Creación de un secreto básico para crear secretos con secretos de conformidad y no conformes.
Paso 5: vea la política de etiquetas en vigor y evalúe el estado de conformidad de la cuenta.	La cuenta de miembro que está utilizando para realizar pruebas.	Resource Groups y el servicio de AWS en el que se creó el recurso. Si ha creado recursos con etiquetas de conformidad y no conformes, debería ver las etiquetas no conformes en los resultados.
Paso 6: repita el proceso para buscar y corregir los problemas de conformidad hasta que los recursos en la cuenta de pruebas cumplan con su política de etiquetas.	La cuenta de miembro que está utilizando para realizar pruebas.	Resource Groups y el servicio de AWS en el que se creó el recurso.

Tarea	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
En cualquier momento, puede evaluar el cumplimiento en toda la organización.	Esta es la cuenta de administración de la organización.	Grupos de recursos

[1] Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Ampliación del uso de políticas de etiquetas

Puede realizar las siguientes tareas en cualquier orden para ampliar el uso de las políticas de etiquetas.

Tarea avanzada	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
Cree políticas de etiquetas más avanzadas. Siga el mismo proceso que para los usuarios principiantes, pero pruebe otras tareas. Por ejemplo, defina claves o valores adicionales o especifique un tratamiento de mayúsculas y minúsculas diferente para una clave de etiquetas. Puede utilizar la información en Descripción de la herencia de políticas de administración y Sintaxis de la política de etiquetas para crear políticas de etiquetas más detalladas.	Esta es la cuenta de administración de la organización.	AWS Organizations

Tarea avanzada	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
Asocie políticas de etiquetas a cuentas o unidades organizativas adicionales. Compruebe la política de etiquetas en vigor de una cuenta después de asociar más políticas a ella o a cualquier unidad organizativa de la que la cuenta sea miembro.	Esta es la cuenta de administración de la organización.	AWS Organizations
Cree una SCP para precisar etiquetas cuando alguien cree nuevos recursos. Para ver un ejemplo, consulte Requerir una etiqueta en los recursos creados especificados.	Esta es la cuenta de administración de la organización.	AWS Organizations
Continúe evaluando el estado de cumplimiento de la cuenta con la política de etiquetas en vigor a medida que cambia. Corrija las etiquetas no conformes.	Una cuenta de miembro con una política de etiquetas efectiva.	Resource Groups y el servicio de AWS en el que se creó el recurso.
Evalúe el cumplimiento en toda la organización.	Esta es la cuenta de administración de la organización.	Grupos de recursos

[1] Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Aplicación de las políticas de etiquetas por primera vez

Para aplicar políticas de etiquetas por primera vez, siga un flujo de trabajo similar al del uso de políticas de etiquetas por primera vez y utilice una cuenta de prueba.

> **Warning**
>
> Tenga cuidado con forzar el cumplimiento. Asegúrese de que conoce los efectos del uso de políticas de etiquetas y siga el flujo de trabajo recomendado. Pruebe el funcionamiento de la ejecución en una cuenta de prueba antes de ampliarla a más cuentas. De lo contrario, podría impedir que los usuarios de las cuentas de su organización etiqueten los recursos que necesiten. Para obtener más información, consulte Descripción de la aplicación de políticas.

Tareas de aplicación de políticas	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
Paso 1: cree una política de etiquetas. Mantenga su primera política de etiquetas aplicada simple. Introduzca una clave de etiqueta en el tratamiento de mayúsculas y minúsculas y seleccione la opción Prevent noncompliant operations for this tag (Evitar las operaciones no conformes para esta etiqueta). A continuación, especifique un tipo de recurso para aplicarlo. Continuando con nuestro ejemplo anterior, puede optar por aplicarlo en secretos de Secrets Manager.	Esta es la cuenta de administración de la organización.	AWS Organizations

Tareas de aplicación de políticas	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
Paso 2: asocie una política de etiquetas a una única cuenta de prueba.	Esta es la cuenta de administración de la organización.	AWS Organizations
Paso 3: pruebe a crear algunos recursos con etiquetas de conformidad y otros con etiquetas no conformes. No se le debería permitir crear una etiqueta en un recurso del tipo especificado en la política de etiquetas con una etiqueta no conforme.	La cuenta de miembro que está utilizando para realizar pruebas.	Cualquier servicio de AWS con el que se sienta cómodo. Por ejemplo, puede utilizar AWS Secrets Manager y seguir el procedimiento en Creación de un secreto básico para crear secretos con secretos de conformidad y no conformes.
Paso 4: evalúe el estado de conformidad de la cuenta con la política de etiquetas en vigor y corrija las etiquetas no conformes.	La cuenta de miembro que está utilizando para realizar pruebas.	Resource Groups y el servicio de AWS en el que se creó el recurso.
Paso 5: repita el proceso para buscar y corregir los problemas de conformidad hasta que los recursos en la cuenta de pruebas cumplan con su política de etiquetas.	La cuenta de miembro que está utilizando para realizar pruebas.	Resource Groups y el servicio de AWS en el que se creó el recurso.
En cualquier momento, puede evaluar el cumplimiento en toda la organización.	Esta es la cuenta de administración de la organización.	Grupos de recursos

[1] Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Uso de Amazon EventBridge para supervisar etiquetas no conformes

Puede utilizar Amazon EventBridge, antes Eventos de Amazon CloudWatch, para llevar a cabo una monitorización cuando se introduzcan etiquetas no conformes. En el siguiente ejemplo de evento, el valor `"false"` de `tag-policy-compliant` indica que una nueva etiqueta no es compatible con la política de etiquetas en vigor.

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

Puede suscribirse a eventos y especificar cadenas o patrones para monitorizarlos. Para más información de EventBridge, consulte la Guía del usuario de Amazon EventBridge.

Descripción de la aplicación de políticas

Una política de etiquetas puede especificar que se apliquen operaciones de etiquetado no conformes en los tipos de recursos especificados. En otras palabras, no se pueden completar las solicitudes de etiquetado no conformes en los tipos de recursos especificados.

> **Important**
>
> La aplicación no afecta a los recursos que se crean sin etiquetas.

Para aplicar la conformidad de las políticas de etiquetas, realice una de las siguientes acciones al crear una política de etiquetas:

- En la pestaña Visual editor (Editor visual), seleccione Prevent noncompliant operations for this tag (Evitar las operaciones no conformes en esta etiqueta).
- En la pestaña JSON, utilice el campo `enforced_for`. Para obtener información acerca de la sintaxis de políticas de etiquetas, consulte Ejemplos y sintaxis de políticas de etiquetas.

Siga estas prácticas recomendadas para ejecutar la conformidad con las políticas de etiquetas:

- Actúe con precaución al ejecutar la conformidad. Asegúrese de que conoce los efectos del uso de políticas de etiquetas y siga los flujos de trabajo recomendados que se describen en Introducción a las políticas de etiquetas. Pruebe el funcionamiento de la ejecución en una cuenta de prueba antes de ampliarla a más cuentas. De lo contrario, podría impedir que los usuarios de las cuentas de su organización etiqueten los recursos que necesiten.
- Tenga en cuenta los tipos de recursos que puede aplicar en: solo puede imponer la conformidad de las política de etiquetas en tipos de recursos admitidos. Se indican los tipos de recursos que admiten la ejecución de la conformidad cuando se utiliza el editor visual para crear una política de etiquetas.
- Comprenda las interacciones con algunos servicios: algunos Servicios de AWS tienen agrupaciones de recursos tipo contenedor que crean recursos automáticamente para usted, y las etiquetas se pueden propagar de un recurso de un servicio a otro. Por ejemplo, las etiquetas de los grupos de Amazon EC2 Auto Scaling y los clústeres de Amazon EMR pueden propagarse automáticamente a las instancias de Amazon contenidas. EC2 Es posible que tenga políticas de etiquetas para Amazon EC2 que sean más estrictas que las de los grupos de Auto Scaling o los clústeres de EMR. Si habilita la ejecución, la política de etiquetas impide que se etiqueten los recursos y puede bloquear el escalado dinámico y el aprovisionamiento.

En las secciones siguientes se muestra cómo encontrar recursos no conformes y corregirlos para que sean compatibles.

Temas

- Encontrar recursos no conformes para una cuenta con AWS Organizations
- Corregir las etiquetas no conformes en los recursos con AWS Organizations
- Generar un informe de cumplimiento para toda la organización con AWS Organizations

- Servicios y tipos de recursos que admiten la aplicación de políticas

Encontrar recursos no conformes para una cuenta con AWS Organizations

En cada cuenta, puede obtener información acerca de los recursos no conformes. Debe ejecutar este comando desde todas las regiones en las que la cuenta tenga recursos.

Para buscar recursos no conformes para una cuenta con una política de etiquetas, ponga en marcha el siguiente comando para guardar los resultados en un archivo:

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

Corregir las etiquetas no conformes en los recursos con AWS Organizations

Después de encontrar etiquetas no conformes, realice las correcciones pertinentes mediante cualquiera de los siguientes métodos. Debe haber iniciado sesión en la cuenta que tiene el recurso con etiquetas no conformes:

- Utilice la consola o etiquete las operaciones de la API del AWS servicio que creó los recursos no conformes.
- Utilice las UntagResourcesoperaciones AWS Resource Groups TagResourcesy para añadir etiquetas que cumplan con la política vigente o para eliminar las etiquetas que no lo hagan.

Generar un informe de cumplimiento para toda la organización con AWS Organizations

En cualquier momento, puede generar un informe que enumere todos los recursos etiquetados de su Cuentas de AWS organización. El informe muestra si cada recurso cumple con la política de etiquetas en vigor. Tenga en cuenta que los cambios que realice a los recursos o una política de etiquetas pueden tardar hasta 48 horas en verse reflejados en el informe de conformidad de toda la organización. Por ejemplo, supongamos que tiene una política de etiquetas que define una etiqueta estandarizada nueva para un tipo de recurso. Los recursos de ese tipo que no tienen esta etiqueta aparecen como conformes en el informe durante un máximo de 48 horas.

Puede generar el informe de la cuenta de administración de la organización en la región `us-east-1`, dado que tiene acceso a un bucket de Amazon S3. El bucket debe tener una política de bucket asociada como se muestra en Política de bucket de Amazon S3 para almacenar informes. Para generar el informe, ejecute el siguiente comando:

```
$ aws resourcegroupstaggingapi start-report-creation --region us-east-1
```

Puede generar un informe a la vez.

Es posible que este informe tarde algo de tiempo en completarse. Puede comprobar su estado ejecutando el siguiente comando:

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

Después de que el comando anterior devuelva `SUCCEEDED`, puede abrir el informe desde el bucket de Amazon S3.

Servicios y tipos de recursos que admiten la aplicación de políticas

Los siguientes servicios y tipos de recursos admiten el cumplimiento con políticas de etiquetas:

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon API Gateway	• Claves de API • Nombres de dominio • Operaciones de la API REST • Escenarios	• `"apigateway:apikeys"` • `"apigateway:domainnames"` • `"apigateway:restapis"` • `"apigateway:restapis/stages"`
AWS Amplify	• Componente • Tema	• `"amplifyuibuilder:app/environment/components"` • `"amplifyuibuilder:app/environment/themes"`
AWS AppConfig	• Aplicación • Perfil de configuración • Implementación	• `"appconfig:application"` • `"appconfig:application/configurationprofile"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
	• Estrategia de implementación • Entorno	• `"appconfig:application/environment/deployment"` • `"appconfig:deploymentstrategy"` • `"appconfig:application/environment"`
AWS App Mesh	• Todos • Puerta de enlace de entrada • Malla • Ruta • Puerta de enlace virtual • Nodo virtual • Enrutador virtual • Servicio virtual	• `"appmesh:*"` • `"appmesh:mesh/virtualGateway/gatewayRoute"` • `"appmesh:mesh"` • `"appmesh:mesh/virtualRouter/route"` • `"appmesh:mesh/virtualGateway"` • `"appmesh:mesh/virtualNode"` • `"appmesh:mesh/virtualRouter"` • `"appmesh:mesh/virtualService"`
Amazon Athena	• Todos • Grupo de trabajo	• `"athena:*"` • `"athena:workgroup"`
AWS Audit Manager	• Evaluación • Marco de evaluación • Controlar	• `"auditmanager:assessment "` • `"auditmanager:assessmentFramework "` • `"auditmanager:control "`
AWS Backup	• Plan de copias de seguridad • Almacén • Puerta de enlace • Hipervisor • VM	• `"backup:backup-plan"` • `"backup:backup-vault"` • `"backup-gateway:gateway"` • `"backup-gateway:hypervisor"` • `"backup-gateway:vm"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS Batch	• Trabajo • Definición de trabajo • Cola de trabajos	• `"batch:job"` • `"batch:job-definition"` • `"batch:job-queue"`
AWS BugBust	• Evento	• `"bugbust:event"`
AWS Certificate Manager	• Todos • Certificados • Private Certificate Authority	• `"acm:*"` • `"acm:certificate"` • `"acm-pca:certificate-authority"`
Amazon Chime	• Instancia de aplicación • Canal • Canalización de medios • Reunión • Aplicaciones multimedia SIP • Instancia de aplicación de usuario • Conector de voz	• `"chime:app-instance"` • `"chime:app-instance/channel"` • `"chime:media-pipeline"` • `"chime:meeting"` • `"chime:sma"` • `"chime:app-instance/user"` • `"chime:vc"`
AWS Clean Rooms	• Colaboración • Tabla configurada • Pertenencia • Asociación de tablas configurada	• `"cleanrooms:collaboration"` • `"cleanrooms:configuredtable"` • `"cleanrooms:membership"` • `"cleanrooms:membership/configuredtableassociation"`
AWS Cloud9	• Entorno	• `"cloud9:environment"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon CloudFront	• Todos • Distribución	• `"cloudfront:*"` • `"cloudfront:distribution"`
AWS CloudTrail	• Todos • Trail	• `"cloudtrail:*"` • `"cloudtrail:trail"`
Amazon CloudWatch	• Todos • Alarma • Reglas de Contributor Insights • Flujos métricos	• `"cloudwatch:*"` • `"cloudwatch:alarm"` • `"cloudwatch:insight-rule"` • `"cloudwatch:metric-stream"`
Amazon CloudWatch Internet Monitor	• Supervisión	• `"internetmonitor:monitor"`
Amazon CloudWatch Logs	• Destino • Grupo de registro	• `"logs:destination"` • `"logs:log-group"`
Administrador de acceso a Amazon CloudWatch Observability	• Enlace • Sink	• `"oam:link"` • `"oam:sink"`
AWS CodeBuild	• Todos • Proyecto	• `"codebuild:*"` • `"codebuild:project"`
Amazon CodeCatalyst	• Connections	• `"codecatalyst:connections"`
AWS CodeCommit	• Todos • Repositorio	• `"codecommit:*"` • `"codecommit:repository"`
AWS CodePipeline	• Todos • Tipo de acción • Canalización • Webhook	• `"codepipeline:*"` • `"codepipeline:actiontype"` • `"codepipeline:pipeline"` • `"codepipeline:webhook"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon Cognito Identity	• Todos • Grupo de identidades	• `"cognito-identity:*"` • `"cognito-identity:identitypool"`
Grupos de usuarios de Amazon Cognito	• Todos • Grupo de usuarios	• `"cognito-idp:*"` • `"cognito-idp:userpool"`
Amazon Comprehend	• Todos • Clasificador de documentos • Reconocedor de entidades	• `"comprehend:*"` • `"comprehend:document-classifier"` • `"comprehend:entity-recognizer"`
AWS Config	• Todos • Autorización de agregación • Agregador de Config • Regla de Config	• `"config:*"` • `"config:aggregation-authorization"` • `"config:config-aggregator"` • `"config:config-rule"`
CodeGuru Revisor de Amazon	• Asociación	• `"codeguru-reviewer:association"`
CodeGuru Seguridad de Amazon	• Examen	• `"codeguru-security:scans"`
CodeConnections	• Connection • Host	• `"codestar-connections:connection"` • `"codestar-connections:host"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon Connect	• Flujo de contacto • Asociación de integración • Cola • Quick Connect • Perfil de enrutamiento • User	• `"connect:instance/contact-flow"` • `"connect:instance/integration-association"` • `"connect:instance/queue"` • `"connect:instance/transfer-destination"` • `"connect:instance/routing-profile"` • `"connect:instance/agent"`
Amazon Connect Wisdom	• Asistente • Asociación • Contenidos • Base de conocimientos • Sesión	• `"wisdom:assistant"` • `"wisdom:association"` • `"wisdom:content"` • `"wisdom:knowledge-base"` • `"wisdom:session"`
AWS Database Migration Service	• Todos • Punto de conexión • ES • Rep. • Subgrp • Tarea	• `"dms:*"` • `"dms:endpoint"` • `"dms:es"` • `"dms:rep"` • `"dms:subgrp"` • `"dms:task"`
Gestionador de vida útil de datos de Amazon	• Política	• `"dlm:policy"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS Direct Connect	• Todos • Dxcon • Dxlag • Dxvif	• `"directconnect:*"` • `"directconnect:dxcon"` • `"directconnect:dxlag"` • `"directconnect:dxvif"`
Amazon DynamoDB	• Todos • Tabla	• `"dynamodb:*"` • `"dynamodb:table"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon EC2	• Reserva de capacidad • Flotas de reservas de capacidad • Gateway de operador • Punto de conexión de Client VPN • Grupo de CoIP • Puerta de enlace de cliente • Host dedicado • Opciones de DHCP • Gateway de Internet de solo salida • Elastic IP • Periodo de eventos • Tarea de exportación de imágenes • Tarea de exportación de instancias • Flota • Imagen FPGA • Reserva de host • Imagen • Tarea de importación de imágenes • Tarea de importación de instantáneas • instancia	• `"ec2:capacity-reservation"` • `"ec2:capacity-reservation-fleet"` • `"ec2:carrier-gateway"` • `"ec2:client-vpn-endpoint"` • `"ec2:coip-pool"` • `"ec2:customer-gateway"` • `"ec2:dedicated-host"` • `"ec2:dhcp-options"` • `"ec2:egress-only-internet-gateway"` • `"ec2:elastic-ip"` • `"ec2:instance-event-window"` • `"ec2:export-image-task"` • `"ec2:export-instance-task"` • `"ec2:fleet"` • `"ec2:fpga-image"` • `"ec2:host-reservation"` • `"ec2:image"` • `"ec2:import-image-task"` • `"ec2:import-snapshot-task"` • `"ec2:instance"` • `"ec2:instance-connect-endpoint"` • `"ec2:internet-gateway"` • `"ec2:ipam"` • `"ec2:ipam-external-resource-verification-token"` • `"ec2:ipam-pool"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
	• Punto final Instance Connect • Puerta de enlace de Internet • Administrador de direcciones IP • Token de verificación de recursos externos del administrador de direcciones IP • Grupo de administradores de direcciones IP • Descubrimiento de recursos del administrador de direcciones IP • Asociación de descubrimiento de recursos para administradores de direcciones IP • Ámbito del administrador de direcciones IP • IPv4 Piscina • Par de claves • Plantilla de inicialización • Tabla de enrutamiento de puerta de enlace local	• `"ec2:ipam-resource-discovery"` • `"ec2:ipam-resource-discovery-association"` • `"ec2:ipam-scope"` • `"ec2:ipv4pool-ec2"` • `"ec2:key-pair"` • `"ec2:launch-template"` • `"ec2:local-gateway-route-table"` • `"ec2:local-gateway-route-table-virtual-interface-group-association"` • `"ec2:local-gateway-route-table-vpc-association"` • `"ec2:natgateway"` • `"ec2:network-acl"` • `"ec2:network-interface"` • `"ec2:network-insights-access-scope"` • `"ec2:network-insights-access-scope-analysis"` • `"ec2:network-insights-analysis"` • `"ec2:network-insights-path"` • `"ec2:placement-group"` • `"ec2:prefix-list"` • `"ec2:replace-root-volume-task"` • `"ec2:reserved-instances"` • `"ec2:route-table"` • `"ec2:security-group"` • `"ec2:snapshot"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
	• Asociación de grupo de interfaz virtual de tabla de enrutamiento de puerta de enlace local • Asociación de VPC de tabla de enrutamiento de puerta de enlace local • Puerta de enlace de NAT • ACL de red • Interfaz de red • Ámbito de acceso a información de la red • Análisis del ámbito de acceso a información de la red • Análisis de información de la red • Ruta de información de la red • Grupo de ubicación • Lista de prefijos • Tarea de reemplazo de un volumen raíz	• `"ec2:spot-fleet-request"` • `"ec2:spot-instances-request"` • `"ec2:subnet"` • `"ec2:subnet-cidr-reservation"` • `"ec2:traffic-mirror-filter"` • `"ec2:traffic-mirror-session"` • `"ec2:traffic-mirror-target"` • `"ec2:transit-gateway"` • `"ec2:transit-gateway-attachment"` • `"ec2:transit-gateway-connect-peer"` • `"ec2:transit-gateway-multicast-domain"` • `"ec2:transit-gateway-policy-table"` • `"ec2:transit-gateway-route-table"` • `"ec2:transit-gateway-route-table-announcement"` • `"ec2:verified-access-endpoint"` • `"ec2:verified-access-group"` • `"ec2:verified-access-instance"` • `"ec2:verified-access-trust-provider"` • `"ec2:volume"` • `"ec2:vpc-flow-log"` • `"ec2:vpc"` • `"ec2:vpc-endpoint"` • `"ec2:vpc-endpoint-service"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
	• instancias reservadas • Tabla de enrutamiento • Grupo de seguridad • Instantánea • Solicitud de flota de spot • Solicitud de instancias de spot • Subred • Reserva de CIDR de subred • Filtro de reflejo de tráfico • Sesión de reflejo de tráfico • Destino de reflejo de tráfico • Transit Gateway • Conexión de puerta de enlace de tránsito • Par de conexión de puerta de enlace de tránsito • Dominio de multidifusión de puerta de enlace de tránsito	• `"ec2:vpc-peering-connection"` • `"ec2:vpn-connection"` • `"ec2:vpn-gateway"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
	• Tablas de políticas de puerta de enlace de tránsito • Tabla de ruteo de la gateway de tránsito • Anuncio de tabla de enrutamiento de puerta de enlace de tránsito • Punto de conexión de acceso verificado • Grupo de acceso verificado • Instancia de acceso verificado • Proveedor de confianza de acceso verificado • Volumen • Registro de flujo de VPC • VPC • Punto de conexión VPC • Servicio de punto de conexión de VPC • Interconexión de VPC • Conexión de VPN	

Nombre del servicio	Tipo de recurso	Sintaxis JSON
	• Puerta de enlace de VPN	
Papelera de EC2 reciclaje de Amazon	• Regla	• `"rbin:rule"`
AWS Elastic Beanstalk	• Aplicación • Versión de la aplicación • Plantilla de configuración • Plataforma	• `"elasticbeanstalk:application"` • `"elasticbeanstalk:applicationversion"` • `"elasticbeanstalk:configurationtemplate"` • `"elasticbeanstalk:platform"`
Amazon Elastic Container Registry	• Repositorio	• `"ecr:repository"`
Amazon Elastic Container Service	• Proveedor de capacidad • Clúster • Servicio • Definición de tarea • Conjunto de tareas	• `"ecs:capacity-provider"` • `"ecs:cluster"` • `"ecs:service"` • `"ecs:task-definition"` • `"ecs:task-set"`
Amazon Elastic File System	• Todos • Sistema de archivos	• `"elasticfilesystem:*"` • `"elasticfilesystem:file-system"`
Amazon Elastic Kubernetes Service	• Clúster	• `"eks:cluster"`
Amazon Elastic Search	• Dominio	• `"es:domain"`
Amazon EMR	• Clúster • Editor	• `"elasticmapreduce:cluster"` • `"elasticmapreduce:editor"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon EMR sin servidor	• Aplicación	• `"emr-serverless:applications"`
AWS Resolución de la entidad	• Flujo de trabajo de coincidencias • Mapeo de esquemas	• `"entityresolution:matchingworkflow"` • `"entityresolution:schemamapping"`
Amazon ElastiCache	• Clúster	• `"elasticache:cluster"`
Amazon EventBridge	• Todos • Event bus • Regla	• `"events:*"` • `"events:event-bus"` • `"events:rule"`
Amazon EventBridge Pipes	• Pipe	• `"pipes:pipe"`
Amazon EventBridge Scheduler	• Grupo de horarios	• `"scheduler:schedule-group"`
Amazon Fraud Detector	• Detector • Versión de detector • Modelo • Regla • Variable	• `"frauddetector:detector"` • `"frauddetector:detector-version"` • `"frauddetector:model"` • `"frauddetector:rule"` • `"frauddetector:variable"`
Amazon Global Accelerator	• Acelerador	• `"globalaccelerator:accelerator"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Elastic Load Balancing	• Todos • Oyente • Regla de oyente • Equilibrador de carga • Grupo de destino	• `"elasticloadbalancing:*"` • `"elasticloadbalancing:listener"` • `"elasticloadbalancing:listener-rule"` • `"elasticloadbalancing:loadbalancer"` • `"elasticloadbalancing:targetgroup"`
Amazon FSx	• Todos • Copia de seguridad • Sistema de archivos	• `"fsx:*"` • `"fsx:backup"` • `"fsx:file-system"`
Amazon GuardDuty	• Detector • Filtro • Conjunto de IP • Conjunto de inteligencia sobre amenazas	• `"guardduty:detector"` • `"guardduty:detector/filter"` • `"guardduty:detector/ipset"` • `"guardduty:detector/threatintelset"`
AWS HealthLake	• Almacén de datos	• `"healthlake:datastore  "`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS HealthOmics	• Almacén de anotaciones • Versión del almacén de anotaciones • Tienda de referencia • Referencia • Ejecute • Grupo de ejecución • Tienda de secuencias • Conjunto de lectura • Tienda de variantes • Flujo de trabajo	• `"omics:annotationStore"` • `"omics:annotationStore/version"` • `"omics:referenceStore"` • `"omics:referenceStore/reference"` • `"omics:run"` • `"omics:runGroup"` • `"omics:sequenceStore"` • `"omics:sequenceStore/readSet"` • `"omics:variantStore"` • `"omics:workflow"`
Amazon Inspector	• Filtro	• `"inspector2:filter "`
AWS Identity and Access Management	• Perfil de instancia • MFA • Proveedor OIDC • Política • Proveedor SAML • Certificado de servidor	• `"iam:instance-profile"` • `"iam:mfa"` • `"iam:oidc-provider"` • `"iam:policy"` • `"iam:saml-provider"` • `"iam:server-certificate"`
AWS IoT Analytics	• Todos • Canal • Conjunto de datos • Almacén de datos • Canalización	• `"iotanalytics:*"` • `"iotanalytics:channel"` • `"iotanalytics:dataset"` • `"iotanalytics:datastore"` • `"iotanalytics:pipeline"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS IoT Events	• Todos • Modelo de detector • Input	• `"iotevents:*"` • `"iotevents:detectorModel"` • `"iotevents:input"`
AWS IoT Fleet Hub	• Aplicación	• `"iotfleethub:application"`
AWS IoT SiteWise	• Activo • Modelo de recurso	• `"iotsitewise:asset"` • `"iotsitewise:asset-model  "`
AWS IoT Greengrass	• Implementación masiva • Definición del conector • Definición del núcleo • Definición del dispositivo • Definición de la función • Definición del registrador • Definición del recurso • Definición de la suscripción	• `"greengrass:bulk"` • `"greengrass:connectorsDefinition"` • `"greengrass:coresDefinition"` • `"greengrass:devicesDefinition"` • `"greengrass:functionsDefinition"` • `"greengrass:loggersDefinition"` • `"greengrass:resourcesDefinition"` • `"greengrass:subscriptionsDefinition"`
AWS Key Management Service	• Todos • Clave	• `"kms:*"` • `"kms:key"`
Amazon Kinesis	• Todos • Aplicación	• `"kinesisanalytics:*"` • `"kinesisanalytics:application"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon Data Firehose	• Todos • Flujo de entrega	• `"firehose:*"` • `"firehose:deliverystream"`
AWS Lambda	• Todos • Función	• `"lambda:*"` • `"lambda:function"`
Amazon Macie	• Identificador de datos personalizado	• `"macie2:custom-data-identifier"`
Amazon MediaStore	• Contenedor	• `"mediastore:container"`
Amazon MQ	• Broker • Configuración	• `"mq:broker"` • `"mq:configuration"`
Amazon Network Firewall	• Firewall • Directiva de firewall • Grupo de reglas con estado • Grupo de reglas sin estado	• `"network-firewall:firewall"` • `"network-firewall:firewall-policy"` • `"network-firewall:stateful-rulegroup"` • `"network-firewall:stateless-rulegroup"`
Amazon OpenSearch Serverless	• Recopilación	• `"aoss:collection"`
AWS Organizations	• Cuenta • Organizational Unit • Política • Raíz	• `"organizations:account"` • `"organizations:ou"` • `"organizations:policy"` • `"organizations:root"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
SMS Voice V2 de Amazon Pinpoint	• Conjunto de configuración • Lista de exclusión • Número de teléfono • Grupo • ID de remitente	• `"sms-voice:configuration-set"` • `"sms-voice:opt-out-list"` • `"sms-voice:phone-number"` • `"sms-voice:pool"` • `"sms-voice:sender-id"`
Amazon RDS	• Grupo de parámetros del clúster • Punto de conexión de clúster • Suscripción a eventos • Grupo de opciones de base de datos • Grupo de parámetros de base de datos • Proxy de base de datos • Punto de conexión de proxy de base de datos • Instancia de base de datos reservada • Grupo de seguridad de base de datos • Grupo de subredes de base de datos • Grupo de destino	• `"rds:cluster-pg"` • `"rds:cluster-endpoint"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:db-proxy"` • `"rds:db-proxy-endpoint"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"` • `"rds:target-group"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon Redshift	• Todos • Clúster • Suscripción a eventos • Certificado de cliente del HSM • Configuración del HSM • Grupo de parámetros • Instantánea • Autorización de copia de snapshot • Programación de instantáneas • Grupo de subredes	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`
Amazon Redshift sin servidor	• Espacio de nombres • Grupo de trabajo	• `"redshift-serverless:namespace"` • `"redshift-serverless:workgroup"`
AWS Resource Access Manager	• Todos • Uso compartido de recursos	• `"ram:*"` • `"ram:resource-share"`
AWS Resource Groups	• Todos • Grupo	• `"resource-groups:*"` • `"resource-groups:group"`
Amazon Route 53	• Zona hospedada	• `"route53:hostedzone"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon Route 53 Resolver	• Todos • Punto de enlace de solucionador • Regla de solucionador	• `"route53resolver:*"` • `"route53resolver:resolver-endpoint"` • `"route53resolver:resolver-rule"`
Amazon S3	• Bucket • Storage Lens • Grupo de lentes de almacenamiento	• `"s3:bucket"` • `"s3:storage-lens"` • `"s3:storage-lens-group"`
Amazon SageMaker AI	• Config. de imagen de aplicación • Artefacto • Contexto • Trabajo de entrenamiento • Trabajo de procesamiento • Grupo de paquetes de modelos • UI de tareas humanas • Paquete de modelos • Acción • Canalización • Experimento • Definición del flujo • Proyecto	• `"sagemaker:app-image-config"` • `"sagemaker:artifact"` • `"sagemaker:context"` • `"sagemaker:training-job"` • `"sagemaker:processing-job "` • `"sagemaker:model-package-group"` • `"sagemaker:human-task-ui"` • `"sagemaker:model-package"` • `"sagemaker:action"` • `"sagemaker:pipeline"` • `"sagemaker:experiment"` • `"sagemaker:flow-definition"` • `"sagemaker:project"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS Secrets Manager	• Todos • secreta	• `"secretsmanager:*"` • `"secretsmanager:secret"`
AWS Lago de seguridad	• Lago de datos • Suscriptor	• `"securitylake:data-lake"` • `"securitylake:subscriber"`
AWS Service Catalog	• Aplicación • Grupo de atributos • Portafolio • Producto	• `"servicecatalog:applications"` • `"servicecatalog:attribute-groups "` • `"catalog:portfolio "` • `"catalog:product "`
Amazon Simple Notification Service (SNS)	• Tema	• `"sns:topic"`
Amazon Simple Queue Service (SQS)	• Cola	• `"sqs:queue"`
Amazon States Language	• Todos • Actividad • State Machine (Máquina de estado)	• `"states:*"` • `"states:activity "` • `"states:stateMachine  "`
AWS Step Functions	• Actividad	• `"states:activity"`
AWS Storage Gateway	• Todos • Puerta de enlace • Share • Cinta • Volumen	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:gateway/volume"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS Systems Manager	• Asociación • Ejecución de automatización • Documento • Maintenance Window (Período de mantenimiento) • Instancia administrada • Elemento de operaciones • Línea de base de revisiones • Contactos	• `"ssm:association"` • `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindow"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm-contacts:contact"`
Amazon Textract	• Adaptadores • Versiones	• `"textract:adapters"` • `"textract:adapters/versions"`
AWS Transfer Family	• Server • User • Flujo de trabajo	• `"transfer:server"` • `"transfer:user"` • `"transfer:workflow"`
Amazon Well-Architected	• Carga de trabajo	• `"wellarchitected:workload"`
AWS Wickr	• Network	• `"wickr:network"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon WorkSpaces	• Todos • Alias de conexión • Directorio • WorkSpace • WorkSpaces paquete • WorkSpaces imagen • WorkSpaces grupo de IP	• `"workspaces:*"` • `"workspaces:connectionalias"` • `"workspaces:directory"` • `"workspaces:workspace"` • `"workspaces:workspacebundle"` • `"workspaces:workspaceimage"` • `"workspaces:workspaceipgroup"`

Ejemplos y sintaxis de políticas de etiquetas

En esta página se describe la sintaxis de la política de etiquetas y se proporcionan ejemplos.

Sintaxis de la política de etiquetas

Una política de etiquetas es un archivo de texto sin formato que se estructura de acuerdo con las reglas de JSON. La sintaxis de las políticas de etiquetas sigue la sintaxis de los tipos de políticas de administración. Para obtener una explicación completa de esa sintaxis, consulte Descripción de la herencia de políticas de administración. Este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política de etiqueta.

La siguiente política de etiquetas muestra una sintaxis de política de etiquetas básica:

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200"
                ]
```

```
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

La sintaxis de política de etiquetas incluye los siguientes elementos:

- El nombre de clave del campo `tags`. Las políticas de etiquetas siempre comienzan con este nombre de clave fijo. Es la línea superior del ejemplo de política anterior.
- Una clave de política que identifica únicamente a la declaración de política. Debe coincidir con el valor de la clave de etiqueta, excepto en el tratamiento de mayúsculas y minúsculas. A diferencia de la clave de etiqueta (que se describe a continuación), el valor de política no distingue entre mayúsculas y minúsculas.

  En este ejemplo, `costcenter` es la clave de política.
- Al menos una clave de etiqueta que especifica la clave de etiqueta permitida con el uso de mayúsculas que desea que cumplan los recursos. Si no se define el tratamiento de mayúsculas y minúsculas, las minúsculas son el tratamiento predeterminado para las claves de etiqueta. El valor de la clave de etiqueta debe coincidir con el valor de la clave de política. No obstante, dado que el valor de la clave de política no distingue entre mayúsculas y minúsculas, el uso de mayúsculas puede ser diferente.

  En este ejemplo, `CostCenter` es la clave de etiqueta. Este es el tratamiento de mayúsculas y minúsculas que se requiere para conformidad con la política de etiquetas. Los recursos con tratamiento alternativo de mayúsculas y minúsculas para esta clave de etiqueta no son compatibles con la política de etiquetas.

  Puede definir varias claves de etiqueta en una política de etiquetas.
- (Opcional) Una lista de uno o varios valores de etiqueta aceptables para la clave de etiqueta. Si la política de etiquetas no especifica un valor de etiqueta para una clave de etiqueta, cualquier valor (incluso si no existe ninguno) se considera conforme.

  En este ejemplo, los valores aceptables para la clave de etiqueta `CostCenter` son `100` y `200`.

- (Opcional) Una opción `enforced_for` que indica si se debe evitar o no cualquier operación de etiquetado no conforme en los recursos y los servicios especificados. En la consola, es la opción Prevent noncompliant operations for this tag (Evitar las operaciones no conformes en esta etiqueta) del editor visual para crear políticas de etiquetas. La configuración predeterminada para esta opción es nula.

  La política de etiquetas de ejemplo especifica que la etiqueta `CostCenter`transferida a todos los recursos de AWS Secrets Manager debe cumplir con esta política.

  > **Warning**
  >
  > Únicamente tiene que cambiar esta opción de configuración predeterminada si tiene experiencia en el uso de políticas de etiquetas. De lo contrario, podría evitar que los usuarios de las cuentas de la organización creen los recursos que necesitan.

- Operadores que especifican cómo se combina la política de etiquetas con las otras políticas de etiquetas del árbol de organización para crear una política de etiquetas en vigor de la cuenta. En este ejemplo, se utiliza `@@assign` para asignar cadenas a `tag_key`, `tag_value` y `enforced_for`. Para obtener más información sobre los operadores, consulte Operadores de herencia.
- - Puede utilizar el comodín `*` en los valores de etiquetas y en los campos `enforced_for`.
  - Puede utilizar solo un comodín por valor de etiquetas. Por ejemplo, `*@example.com` está permitido, pero `*@*.com` no.
  - Para `enforced_for`, puede utilizar `<service>:*` con algunos servicios para habilitar la aplicación de todos los recursos de ese servicio. Para obtener una lista de los servicios y tipos de recursos compatibles `enforced_for`, consulte Servicios y tipos de recursos que admiten la aplicación de políticas.

    No puede utilizar un comodín para especificar todos los servicios ni para especificar un recurso para todos los servicios.

Ejemplos de políticas de etiquetas

Las políticas de etiquetas siguientes son solo para fines informativos.

> **Note**
>
> Antes de intentar usar estos ejemplos de políticas de etiquetas en la organización, tenga en cuenta lo siguiente:
>
> - Asegúrese de que ha seguido el flujo de trabajo recomendado para comenzar con las políticas de etiquetas.
> - Debería revisar y personalizar cuidadosamente estas políticas de etiquetas según sus requisitos únicos.
> - Todos los caracteres de la política de etiquetas están sujetos a un tamaño máximo. Los ejemplos que aparecen en esta guía muestran las políticas de etiquetas formateadas con espacios en blanco adicionales para mejorar su legibilidad. Sin embargo, para ahorrar espacio si el tamaño de política se acerca al tamaño máximo, puede eliminar cualquier espacio en blanco. Entre los ejemplos de espacio en blanco se incluyen caracteres de espacio y saltos de línea que están fuera de comillas.
> - Los recursos no etiquetados no aparecen como no conformes en los resultados.

Ejemplo 1: Definir las mayúsculas y minúsculas de la clave de etiquetas en toda la organización

En el ejemplo siguiente se muestra una política de etiquetas que solo define dos claves de etiqueta y el uso de mayúsculas en los que desea que las cuentas de su organización se estandarice.

Política A: política de etiqueta raíz de la organización

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
```

```
}
```

Esta política de etiquetas define dos claves de etiquetas `CostCenter` y `Project`. La asociación de esta política de etiquetas a la raíz de la organización tiene los siguientes efectos:

- Todas las cuentas de su organización heredan esta política de etiquetas.
- Todas las cuentas de su organización deben utilizar el tratamiento de mayúsculas y minúsculas definido para conformidad. Los recursos con `CostCenter` y `Project` etiquetas cumplen los requisitos. Los recursos con tratamiento de mayúsculas y minúsculas alternativo para la clave de etiqueta (por ejemplo `costcenter`, `Costcenter` o `COSTCENTER`) no cumplen los requisitos.
- Las líneas de `@@operators_allowed_for_child_policies": ["@@none"]` bloquean las claves de etiquetas. Las políticas de etiquetas que se asocian más abajo en el árbol de organización (políticas secundarias) no pueden utilizar operadores de configuración de valores para los cambios de la clave de etiquetas, incluido el tratamiento de mayúsculas y minúsculas.
- Como ocurre con todas las políticas de etiquetas, no se evalúa la conformidad con la política de etiquetas de los recursos no etiquetados o las etiquetas que no están definidas en la política de etiquetas.

AWS recomienda que utilice este ejemplo como guía para crear una política de etiquetas similar para las claves de etiquetas que desee utilizar. Asóciela a la raíz de la organización. A continuación, cree una política de etiquetas similar al siguiente ejemplo, que solo define los valores aceptables para las claves de etiqueta definidas.

Siguiente paso: Definir valores

Suponga que asoció la política de etiquetas anterior a la raíz de la organización. A continuación, puede crear una política de etiquetas como la siguiente y asociarla a una cuenta. Esta política define valores aceptables para las claves de etiquetas `CostCenter` y `Project`.

Política B: Política de etiqueta de cuenta

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
```

```
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

Si asocia la política A a la raíz de la organización y la política B a una cuenta, las políticas se combinan para crear la siguiente política de etiquetas efectiva para la cuenta:

Política A + política B = política de etiquetas en vigor para la cuenta

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

Para obtener más información acerca de la herencia de políticas, además de ejemplos acerca de cómo funcionan los operadores de herencia y ejemplos de políticas de etiquetas en vigor, consulte Descripción de la herencia de políticas de administración.

Ejemplo 2: Evitar el uso de una clave de etiqueta

Para evitar el uso de una clave de etiqueta, puede asociar una política de etiquetas como la siguiente a una entidad de organización.

Esta política de ejemplo especifica que no se aceptan valores para la clave de etiqueta `Color`. También especifica que no se permiten operadores en las políticas de etiquetas secundarias. Por lo tanto, se considera que las etiquetas de `Color` de los recursos de las cuentas afectadas no cumplen los requisitos. Además, la opción `enforced_for` realmente impide que las cuentas afectadas etiqueten solo tablas de Amazon DynamoDB con la etiqueta `Color`.

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Regiones compatibles

Las características de la política de etiquetas están disponibles en las siguientes regiones:

Nombre de la región	Parámetro de la región
Región Este de EE. UU. (Norte de Virginia)[1]	**us-east-1**
Región del este de EE. UU. (Ohio)	us-east-2
Región del oeste de EE. UU. (Norte de California)	us-west-1
Región del oeste de EE. UU. (Oregón)	us-west-2
Africa (Cape Town) Region[2]	af-south-1
Región Asia Pacífico (Hong Kong)[2]	ap-east-1
Región de Asia-Pacífico (Bombay)	ap-south-1
Asia-Pacífico (Hyderabad)[2]	ap-south-2
Asia Pacífico (Tokio)	ap-northeast-1
Región de Asia-Pacífico (Seúl)	ap-northeast-2
Región Asia-Pacífico (Osaka)	ap-northeast-3
Región de Asia-Pacífico (Singapur)	ap-southeast-1
Región de Asia-Pacífico (Sídney)	ap-southeast-2
Región Asia-Pacífico (Yakarta)[2]	ap-southeast-3
Región de Asia-Pacífico (Malasia)	ap-southeast-5
Asia-Pacífico (Melbourne)[2]	ap-southeast-4
Asia-Pacífico (Tailandia)	ap-southeast-7
Región de Canadá (centro)	ca-central-1
Oeste de Canadá (Calgary)[2]	ca-west-1
Región de Europa (Fráncfort)	eu-central-1

Nombre de la región	Parámetro de la región
Región Europa (Zúrich)[2]	`eu-central-2`
Europe (Milan) Region[2]	`eu-south-1`
Europa (España)[2]	`eu-south-2`
Región de Europa (Irlanda)	`eu-west-1`
Región de Europa (Londres)	`eu-west-2`
Región de Europa (París)	`eu-west-3`
Región Europa (Estocolmo)	`eu-north-1`
Región México (Central)	`mx-central-1`
Middle East (Bahrain) Region[2]	`me-south-1`
Región de América del Sur (São Paulo)	`sa-east-1`
Israel (Tel Aviv)UAE	`il-central-1`

[1]Debe especificar la región **`us-east-1`** cuando llame a las siguientes operaciones de Organizations:

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- Cualquier otra operación en la raíz de una organización, como ListRoots.

También debe especificar la región **`us-east-1`** cuando llame a las siguientes operaciones de la API de etiquetado de grupos de recursos que forman parte de la característica de políticas de etiquetas:

- DescribeReportCreation
- GetComplianceSummary
- StartReportCreation

> **Note**
>
> Para evaluar la conformidad de políticas de etiquetas en toda la organización, también debe tener acceso a un bucket de Amazon S3 en la región EE. UU. Este (Norte de Virginia) para el almacenamiento de informes. Para obtener más información, consulte la política de depósitos de Amazon S3 para el almacenamiento de informes en la Guía del usuario de Tagging AWS Resources.

²Estas regiones deben estar habilitadas manualmente. Para obtener más información sobre cómo habilitar y deshabilitar Regiones de AWS, consulte Specify which Regiones de AWS your account can use en la Guía de referencia de administración de cuentas de AWS . La consola Resource Groups no está disponible en estas regiones.

Políticas de chatbot

Las políticas de Chatbot te AWS Organizations permiten controlar el acceso a las cuentas de tu organización desde aplicaciones de chat como Slack y Microsoft Teams.

AWS Chatbotes un AWS servicio que permite DevOps a los equipos de desarrollo de software utilizar las salas de chat de los programas de mensajería para monitorear y responder a los eventos operativos en sus salas de chat. Nube de AWS AWS Chatbot procesa Servicio de AWS las notificaciones de Amazon Simple Notification Service (AmazonSNS) y las reenvía a las salas de chat para que los equipos puedan analizarlas y actuar en consecuencia de inmediato, independientemente de su ubicación.

Funcionamiento de las políticas de chatbot

Con las políticas de chatbot, la cuenta de administración o el administrador delegado de una organización pueden hacer lo siguiente en toda la organización:

- Indicar qué aplicaciones de chat compatibles (Amazon Chime, Microsoft Teams y Slack) se pueden usar.
- Restringir el acceso del cliente de chat a espacios de trabajo (Slack) y equipos (Microsoft Teams) específicos.
- Restringir la visibilidad de los canales de Slack a los canales públicos o privados.
- Establecer y aplicar ajustes de roles específicos.

Las políticas de chatbot restringen y tienen prioridad sobre la configuración de la cuenta, como los ajustes de roles y las políticas de barrera de protección del canal. Puede acceder a las políticas de chatbot y modificarlas desde la consola de AWS Chatbot o la consola de Organizations.

Una vez que las políticas se adjunten a las cuentas y unidades organizativas (OU), cualquier AWS Chatbot configuración actual y futura de las cuentas incluidas en el ámbito de aplicación cumplirá automáticamente con la configuración de gobierno y permisos. Para obtener más información, consulte Understanding management policy inheritance.

Si intenta llevar a cabo una acción restringida por una política de chatbot, aparecerá un mensaje de error en el que se le notificará que la acción no está permitida debido a la política de chatbot y le recomendará contactar con la cuenta de administración o con el administrador delegado de su organización.

> **Note**
>
> Las políticas de chatbot se validan en tiempo de ejecución. Esto significa que los recursos existentes se comprueban continuamente para comprobar su conformidad. No hay superposición con IAM los permisos existentes, ya que actualmente no se admiten IAM los permisos basados en tiempo de ejecución para enviar notificaciones o interactuar con AWS Chatbot ellos.

Introducción a las políticas de chatbot

Siga estos pasos para empezar a utilizar las políticas de copia de seguridad.

1. Obtenga información sobre los permisos que debe tener para llevar a cabo tareas de políticas de chatbot.
2. Habilite las políticas de chatbot de su organización.
3. Cree una política de chatbot.
4. Vincule la política de chatbot al nodo raíz, a una unidad organizativa o a una cuenta de su organización.
5. Vea la política de chatbot en vigor combinada que se aplica a una cuenta.

En todos estos pasos, debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Información adicional

- Aprende la sintaxis de las políticas de chatbots y consulta ejemplos de políticas

Ejemplos y sintaxis de políticas de chatbots

En este tema se describe la sintaxis de la política de chatbots y se proporcionan ejemplos.

Sintaxis de las políticas de chatbots

Una política de chatbots es un archivo de texto sin formato que se estructura de acuerdo con las reglas de JSON. La sintaxis de las políticas de chatbots sigue la sintaxis de los tipos de políticas de administración. Para obtener una explicación completa de esa sintaxis, consulte Descripción de la herencia de políticas de administración. Este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política de chatbots.

En el siguiente ejemplo se muestra la sintaxis básica de una política de chatbots:

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled" // enabled | disabled
             },
             "workspaces": { // limit 255
                   "@@assign":[
                      "Slack-Workspace-Id"
                   ]
             },
             "default":{
                "supported_channel_types":{
                   "@@assign":[
                      "private" // public | private
                   ]
                },
                "supported_role_settings":{
                   "@@assign":[
                      "user_role" // user_role | channel_role
                   ]
                }
             },
```

```
            "overrides":{ // limit 255
               "Slack-Workspace-Id":{
                  "supported_channel_types":{
                     "@@assign":[
                        "public" // public | private
                     ]
                  },
                  "supported_role_settings":{
                     "@@assign":[
                        "user_role" // user_role | channel_role
                     ]
                  }
               }
            }
         },
         "microsoft_teams":{
            "client":{
               "@@assign":"enabled"
            },
            "tenants":{ // limit 36
               "Microsoft-Teams-Tenant-Id":{ // limit 36
                  "@@assign":[
                     "Microsoft-Teams-Team-Id"
                  ]
               }
            },
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role" // user_role | channel_role
                  ]
               }
            },
            "overrides":{ // limit 36
               "Microsoft-Teams-Tenant-Id":{ // limit 36
                  "Microsoft-Teams-Team-Id":{
                     "supported_role_settings":{
                        "@@assign":[
                           "user_role" // user_role | channel_role
                        ]
                     }
                  }
               }
            }
```

```
          },
          "chime":{
            "client":{
               "@@assign":"disabled" // enabled | disabled
            }
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled" // enabled | disabled
         }
      }
   }
}
```

Esta política de chatbots incluye los siguientes elementos:

- El nombre de clave del campo `chatbot`. Las políticas de chatbots siempre comienzan con este nombre de clave fijo. Es la línea superior de esta política de ejemplo.
- En `chatbot`, hay un bloque de `platforms` que contiene la configuración de las diferentes aplicaciones de chat compatibles: Slack, Microsoft Teams y Amazon Chime.
  - Para Slack, están disponibles los siguientes campos:
    - `"client"`:
      - `"enabled"`: el cliente de Slack está habilitado. Se permiten las integraciones de Slack.
      - `"disabled"`: el cliente de Slack está deshabilitado. No se permiten las integraciones de Slack.
    - `"workspaces"`: lista de espacios de trabajo de Slack permitidos separados por comas. En este ejemplo, los espacios de trabajo de Slack permitidos son *`Slack-Workspace-Id1`* y *`Slack-Workspace-Id2`*.
    - `"default"`: la configuración predeterminada de los espacios de trabajo de Slack.
      - `"supported_channel_types"`:
        - `"public"`: los espacios de trabajo de Slack incluidos en el ámbito de aplicación permiten los canales públicos de Slack de forma predeterminada.
        - `"private"`: los espacios de trabajo de Slack incluidos en el ámbito de aplicación permiten los canales privados de Slack de forma predeterminada.
      - `supported_role_settings`:

        - `"user_role"`: los espacios de trabajo de Slack incluidos en el ámbito de aplicación permiten roles de IAM de usuario de forma predeterminada.
        - `"channel_role"`: Los espacios de trabajo de Slack incluidos en el ámbito de aplicación permiten roles de IAM de canal de forma predeterminada.
    - `"overrides"`: la configuración de anulación de los espacios de trabajo de Slack.
        - *`Slack-Workspace-Id2`*: lista separada por comas de los espacios de trabajo de Slack en los que se aplica la configuración de anulación. En este ejemplo, el espacio de trabajo de Slack es *`Slack-Workspace-Id2`*.
            - `"supported_channel_types"`:
                - `"public"`: anula la configuración de si los espacios de trabajo de Slack incluidos en el ámbito de aplicación permiten los canales públicos de Slack.
                - `"private"`: anula la configuración de si los espacios de trabajo de Slack incluidos en el ámbito de aplicación permiten los canales privados de Slack.
            - `supported_role_settings`:
                - `"user_role"`: anula la configuración de si los espacios de trabajo de Slack incluidos en el ámbito de aplicación permiten roles de IAM de usuario.
                - `"channel_role"`: anula la configuración de si los espacios de trabajo de Slack incluidos en el ámbito de aplicación permiten roles de IAM de canal.
- Para Microsoft Teams, están disponibles los siguientes campos:
    - `"client"`:
        - `"enabled"`: el cliente Microsoft Teams está habilitado. Se permiten las integraciones de Microsoft Teams.
        - `"disabled"`: el cliente de Microsoft Teams está deshabilitado. No se permiten las integraciones de Microsoft Teams.
    - `"tenants"`: lista separada por comas de los inquilinos permitidos de Microsoft Teams. En este ejemplo, el inquilino permitido es *`Microsoft-Teams-Tenant-Id`*.
        - *`Microsoft-Teams-Tenant-Id`*: lista separada por comas de los equipos permitidos dentro del inquilino. En este ejemplo, el equipo permitido es *`Microsoft-Teams-Team-Id`*.
    - `"default"`: la configuración predeterminada de los equipos del inquilino.
        - `supported_role_settings`:
            - `"user_role"`: los equipos incluidos en el ámbito de aplicación permiten roles de IAM de usuario de forma predeterminada.

        - `"channel_role"`: los equipos incluidos en el ámbito de aplicación permiten roles de IAM de canal de forma predeterminada.
    - `"overrides"`: la configuración de anulación para los inquilinos de Microsoft Teams.
        - *`Microsoft-Teams-Tenant-Id`*: lista de inquilinos separados por comas a los que se aplica la configuración de anulación. En este ejemplo, el inquilino es *`Microsoft-Teams-Tenant-Id`*.
            - *`Microsoft-Teams-Team-Id`*: lista separada por comas de los equipos del inquilino. En este ejemplo, el equipo permitido es *`Microsoft-Teams-Team-Id`*.
                - `supported_role_settings`:
                    - `"user_role"`: anula la configuración de si los equipos incluidos en el ámbito de aplicación permiten roles de IAM de usuario.
                    - `"channel_role"`: anula la configuración de si los equipos incluidos en el ámbito de aplicación permiten roles de IAM de canal.
    - Para Amazon Chime, están disponibles los siguientes campos:
        - `"client"`:
            - `"enabled"`: el cliente Amazon Chime está habilitado. Se permiten las integraciones de Amazon Chime.
            - `"disabled"`: el cliente Amazon Chime está deshabilitado. No se permiten las integraciones de Amazon Chime.
- En `chatbot`, hay un bloque de `default` que deshabilita AWS Chatbot en toda la organización a menos que se anule en un nivel inferior. Este valor predeterminado también deshabilita cualquier aplicación de chat nueva que sea compatible con AWS Chatbot. Por ejemplo, si AWS Chatbot es compatible con una nueva aplicación de chat, esta opción predeterminada también deshabilita esa aplicación de chat recién admitida.

> **Note**
>
> Para obtener más información sobre los roles de IAM de canal y los roles de IAM de usuario, consulte Understanding AWS Chatbot permissions en la Guía del administrador de AWS Chatbot.

Ejemplos de políticas de chatbots

Las políticas de copia de seguridad siguientes son solo para fines informativos.

Ejemplo 1: permitir solo los canales privados de Slack en un espacio de trabajo específico, deshabilitar Microsoft Teams y admitir todos los modos de autenticación

La siguiente política se centra en controlar las configuraciones permitidas para las integraciones de chatbots de Slack y Microsoft Teams.

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
                  ]
               },
               "supported_role_settings": {
                  "@@assign": [
                     "channel_role",
                     "user_role"
                  ]
               }
            }
         },
         "microsoft_teams": {
            "client": {
               "@@assign": "disabled"
            }
         },
         "chime":{
            "client":{
```

```
                "@@assign":"disabled"
            }
         },
         "default":{
            "client":{
               "@@assign":"disabled"
            }
         }
      }
   }
}
```

Para Slack

- El cliente de Slack está habilitado.
- Solo se permite el espacio de trabajo específico de Slack *`Slack-Workspace-Id`*.
- La configuración predeterminada es permitir solo los canales privados de Slack, los roles de IAM de canal y los roles de IAM de usuario.

Para Microsoft Teams

- El cliente de Microsoft Teams está deshabilitado.

Para Amazon Chime

- El cliente Amazon Chime está deshabilitado.

Detalles adicionales

- El bloque `default` de la parte inferior establece la desactivación del cliente, lo que se deshabilita AWS Chatbot en toda la organización a menos que se anule en un nivel inferior. Este valor predeterminado también deshabilita cualquier aplicación de chat nueva que sea compatible con AWS Chatbot. Por ejemplo, si AWS Chatbot es compatible con una nueva aplicación de chat, esta opción predeterminada también deshabilita esa aplicación de chat recién admitida.

Ejemplo 2: permitir solo las integraciones de Slack con roles de IAM de usuario

La siguiente política adopta un enfoque más permisivo con respecto a Slack, ya que permite todos los espacios de trabajo de Slack, pero restringe el modo de autenticación solo a los roles de IAM de usuario.

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client":{
               "@@assign":"enabled"
            },
            "workspaces":
               {
                  "@@assign":[
                     "*"
                  ]
               },
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role"
                  ]
               }
            }
         },
         "microsoft_teams":{
            "client":{
               "@@assign":"disabled"
            }
         },
         "chime":{
            "client":{
               "@@assign":"disabled"
            }
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled"
         }
      }
```

```
   }
}
```

Para Slack

- El cliente de Slack está habilitado.
- No se define ningún espacio de trabajo específico de Slack mediante el comodín `"*"`, por lo que todos los espacios de trabajo están permitidos.
- La configuración predeterminada es permitir solo los roles de IAM de usuario.

Para Microsoft Teams

- El cliente de Microsoft Teams está deshabilitado.

Para Amazon Chime

- El cliente Amazon Chime está deshabilitado.

Detalles adicionales

- El bloque `default` de la parte inferior establece la desactivación del cliente, lo que se deshabilita AWS Chatbot en toda la organización a menos que se anule en un nivel inferior. Este valor predeterminado también deshabilita cualquier aplicación de chat nueva que sea compatible con AWS Chatbot. Por ejemplo, si AWS Chatbot es compatible con una nueva aplicación de chat, esta opción predeterminada también deshabilita esa aplicación de chat recién admitida.

Ejemplo 3: permitir solo las integraciones de Microsoft Teams en un inquilino específico

El siguiente ejemplo de política bloquea la organización para que solo permita las integraciones de chatbots de Microsoft Teams dentro del inquilino especificado, al tiempo que bloquea por completo las integraciones de Slack.

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client": {
               "@@assign": "disabled"
```

```
            },
         },
         "microsoft_teams":{
            "client": {
               "@@assign": "enabled"
            },
            "tenants":{
               "Microsoft-Teams-Tenant-Id":{
                  "@@assign":[
                     "*"
                  ]
               }
            }
         },
         "chime": {
            "client":{
               "@@assign": "disabled"
            }
         }
      }
   }
}
```

Para Slack

- El cliente de Slack está deshabilitado.

Para Microsoft Teams

- Solo se permite el inquilino específico *Microsoft-Teams-Tenant-Id*, y se utiliza el comodín "*" para permitir la entrada a todos los equipos de ese inquilino.

Para Amazon Chime

- El cliente Amazon Chime está deshabilitado.

Detalles adicionales

- El bloque `default` de la parte inferior establece la desactivación del cliente, lo que se deshabilita AWS Chatbot en toda la organización a menos que se anule en un nivel inferior. Este valor

predeterminado también deshabilita cualquier aplicación de chat nueva que sea compatible con AWS Chatbot. Por ejemplo, si AWS Chatbot es compatible con una nueva aplicación de chat, esta opción predeterminada también deshabilita esa aplicación de chat recién admitida.

Ejemplo 4: permitir el acceso restringido de AWS Chatbot a los espacios de trabajo de Slack y a un inquilino de Microsoft Teams

La siguiente política permite el acceso restringido de AWS Chatbot a determinados espacios de trabajo de Slack y a un inquilino de Microsoft Teams.

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled"
             },
             "workspaces": {
                   "@@assign":[
                      "Slack-Workspace-Id1",
                      "Slack-Workspace-Id2"
                   ]
             },
             "default":{
                "supported_channel_types":{
                   "@@assign":[
                      "private"
                   ]
                },
                "supported_role_settings":{
                   "@@assign":[
                      "user_role"
                   ]
                }
             },
             "overrides":{
                "Slack-Workspace-Id2":{
                   "supported_channel_types":{
                      "@@assign":[
                         "public",
                         "private"
                      ]
```

```
                },
                "supported_role_settings":{
                   "@@assign":[
                      "channel_role",
                      "user_role"
                   ]
                }
             }
          }
       },
       "microsoft_teams":{
          "client":{
             "@@assign":"enabled"
          },
          "tenants":{
             "Microsoft-Teams-Tenant-Id":{
                "@@assign":[
                   "Microsoft-Teams-Team-Id"
                ]
             }
          },
          "default":{
             "supported_role_settings":{
                "@@assign":[
                   "user_role"
                ]
             }
          },
          "overrides":{
             "Microsoft-Teams-Tenant-Id":{
                "Microsoft-Teams-Team-Id":{
                   "supported_role_settings":{
                      "@@assign":[
                         "channel_role",
                         "user_role"
                      ]
                   }
                }
             }
          }
       }
    },
    "default":{
       "client":{
```

```
            "@@assign":"disabled"
         }
      }
   }
}
```

Para Slack

- El cliente de Slack está habilitado.
- Los espacios de trabajo de Slack permitidos son *Slack-Workspace-Id1* y *Slack-Workspace-Id2*.
- La configuración predeterminada de Slack es permitir solo los canales privados y los roles de IAM de usuario.
- Hay una modificación para el espacio de trabajo *Slack-Workspace-Id2* que permite tanto los canales públicos como los privados, así como los roles de IAM de canal y los roles de IAM de usuario.

Para Microsoft Teams

- Microsoft Teams está habilitado.
- Los inquilinos de Teams permitidos son *Microsoft-Teams-Tenant-Id* con el equipo *Microsoft-Teams-Team-Id*.
- La configuración predeterminada es permitir únicamente los roles de IAM de usuario.
- Hay una modificación para el inquilino *Microsoft-Teams-Tenant-Id* que permite tanto los roles IAM de canal como los roles de IAM de usuario para el equipo *Microsoft-Teams-Team-Id*.

Detalles adicionales

- El bloque `default` de la parte inferior establece la desactivación del cliente, lo que se deshabilita AWS Chatbot en toda la organización a menos que se anule en un nivel inferior. Esto significa que Amazon Chime está deshabilitado en este ejemplo. Este valor predeterminado también deshabilita cualquier aplicación de chat nueva que sea compatible con AWS Chatbot. Por ejemplo, si AWS Chatbot es compatible con una nueva aplicación de chat, esta opción predeterminada también deshabilita esa aplicación de chat recién admitida.

Políticas de exclusión de servicios de IA

Las políticas de exclusión de los servicios de IA te permiten controlar la recopilación de datos para los servicios de AWS IA en todas las cuentas de una organización.

AWS Los servicios de IA pueden usar y almacenar el contenido de los clientes para mejorar el servicio. La mejora del servicio consiste en el uso y el almacenamiento de contenido que no sea información personal para desarrollar, mejorar AWS y vincular tecnologías de aprendizaje automático e inteligencia artificial. Para ello, es posible que almacenemos contenido en o Región de AWS fuera del lugar en el Región de AWS que esté utilizando el servicio. Como AWS cliente, puede optar por que su contenido no se utilice para mejorar el servicio en cualquier momento.

Puedes crear políticas de exclusión para un servicio de IA individual o para todos los servicios compatibles con las políticas de exclusión de los servicios de IA. También puedes consultar la política vigente aplicable a cada cuenta para ver los efectos de tus elecciones de configuración.

Para obtener información más detallada, consulte AWS Machine Learning and Artificial Intelligence Services en las Condiciones del AWS servicio. Para ver una lista de los servicios compatibles con las políticas de exclusión de los servicios de IA, consulta la Lista de servicios de IA compatibles.

Temas

- Consideraciones a la hora de utilizar políticas de exclusión de servicios de IA
- Introducción a las políticas de exclusión de servicios de IA
- Exclusión de todos los servicios de IA de AWS compatibles
- Sintaxis y ejemplos de políticas de exclusión de servicios de IA

Consideraciones a la hora de utilizar políticas de exclusión de servicios de IA

La exclusión se aplica a todos, excepto Regiones de AWS AWS GovCloud (US)

Cuando especificas una preferencia de suscripción o exclusión para un servicio, esa configuración es global y se aplica a todos, Regiones de AWS excepto a los. AWS GovCloud (US) Regions Establecer el valor desde dentro de un Región de AWS se replica a todas las demás regiones.

La exclusión voluntaria puede afectar a la funcionalidad del servicio

AWS Es posible que los servicios de IA necesiten almacenar tu contenido para proporcionarte el servicio de una forma que no esté relacionada con ninguna mejora del servicio, y la exclusión podría

afectar a esa funcionalidad. Por ejemplo, Amazon Lex almacena los análisis de las expresiones como parte de proporcionarle dichos análisis. Para obtener información más detallada, consulte AWS Machine Learning and Artificial Intelligence Services en las Condiciones del AWS servicio.

Al excluirse, se elimina todo el contenido histórico asociado

Al inhabilitar el uso del contenido por parte de un servicio de AWS IA, ese servicio elimina todo el contenido histórico asociado con el que se compartió AWS antes de configurar la opción. Esta eliminación se limita a los datos almacenados que no son necesarios para proporcionar funciones de servicio.

Por ejemplo, utiliza un servicio mientras se haya suscrito. Ese servicio puede almacenar copias de su contenido para mejorar el servicio. Opta por no participar. Se eliminan todas las copias que el servicio haya almacenado para mejorar, pero no se eliminan los datos que se utilizan para proporcionarle el servicio.

Introducción a las políticas de exclusión de servicios de IA

Siga estos pasos para empezar a utilizar las políticas de exclusión de servicios de Inteligencia Artificial (IA).

1. Obtenga información sobre los permisos que debe tener para realizar tareas de políticas de copia de seguridad
2. Habilitar políticas de exclusión de servicios de IA para su organización.
3. Crear una política de exclusión de servicios de IA.
4. Asocie la política de exclusión de servicios de IA al nodo raíz, unidad organizativa o cuenta de su organización.
5. Vea la política de exclusión de servicios de IA en vigor combinada que se aplica a una cuenta.

En todos estos pasos, inicia sesión como usuario AWS Identity and Access Management (de IAM), asume un rol de IAM o inicia sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Información adicional

- Conozca la sintaxis de políticas para las políticas de exclusión de servicios de IA y vea ejemplos de políticas

Exclusión de todos los servicios de IA de AWS compatibles

En este tema:

- Puede dejar de participar tan solo pulsando un botón en la consola de AWS Organizations.
- Puede dejar de participar adjuntando el ejemplo de política proporcionado mediante la AWS CLI y los AWS SDK.
- Puede ver una lista de los Servicios de AWS incluidos en la política de exclusión de servicios de IA.

Exclusión de todos los servicios de IA de compatibles

Puede hacer que su organización ya no deje que se use su contenido para mejorar los servicios creando y adjuntando una política de exclusión de servicios de IA. Esta política se aplica a todos los servicios de IA de AWS en vigor actualmente y en el futuro. Las cuentas miembro no pueden actualizar la política.

AWS Management Console

Para dejar de participar en todos los servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de cancelación de servicios de IA, seleccione Cancelar todos los servicios.
3. En la página de confirmación de Cancelar todos los servicios, seleccione Cancelar todos los servicios.

AWS CLI & AWS SDKs

Para dejar de participar en todos los servicios de IA

1. Copie “Ejemplo 1: Excluir todos los servicios de IA para todas las cuentas de la organización” en Ejemplos de cancelación de servicios de IA.
2. Siga las instrucciones que se indican en Attaching and detaching AI services opt-out.

> **Note**
>
> Se requieren pasos adicionales para no participar en Amazon Monitron. Para obtener más información, consulte los Términos del servicio de AWS.

Lista de servicios compatibles con la política de exclusión de servicios de IA

A continuación se incluye una lista de los Servicios de AWS incluidos en la política de exclusión de servicios de IA:

- AWS Supply Chain
- AWS Database Migration Service
- Análisis de voz de Amazon Chime SDK
- Amazon CloudWatch
- Generador de perfiles de Amazon CodeGuru
- Amazon CodeWhisperer (ahora parte de Amazon Q Developer)
- Amazon Comprehend
- Amazon Connect
- Amazon Connect Optimization
- Amazon Connect Contact Lens
- Amazon DataZone
- AWS Entity Resolution
- Amazon Fraud Detector
- AWS Glue
- Amazon GuardDuty
- Amazon Lex
- Amazon Polly
- Amazon Q
- Amazon QuickSight
- Amazon Rekognition
- Amazon Security Lake
- Amazon Textract

- Amazon Transcribe
- Amazon Translate

Sintaxis y ejemplos de políticas de exclusión de servicios de IA

En este tema se describe la sintaxis de política de exclusión de servicios de Inteligencia Artificial (IA) y se proporcionan ejemplos.

Sintaxis para políticas de exclusión de servicios de IA

Una política de exclusión de servicios de IA es un archivo de texto sin formato que se estructura de acuerdo con las reglas de JSON. La sintaxis de las políticas de exclusión de servicios de IA sigue la sintaxis de los tipos de políticas de administración. Para obtener una explicación completa de esa sintaxis, consulte Descripción de la herencia de políticas de administración. Este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política de exclusión de servicios de IA.

> **Important**
>
> En esta sección son importantes las mayúsculas de los valores. Introduzca los valores con letras mayúsculas y minúsculas como se muestra en este tema. Las políticas no funcionan si utiliza mayúsculas inesperadas.

La siguiente política muestra la sintaxis básica de política de exclusión de servicios de IA. Si este ejemplo se asociara directamente a una cuenta, esa cuenta se excluiría explícitamente de un servicio y se optaría por otra. Otras políticas heredadas de niveles superiores (OU o políticas raíz) podrían optar por o excluir otros servicios.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
```

```
            }
        }
    }
}
```

Imagine la siguiente política de ejemplo asociada al nodo raíz de la organización. Establece el valor predeterminado para que la organización opte por la exclusión de todos los servicios de IA. Esto incluye automáticamente todos los servicios de IA que no estén explícitamente exentos de otra manera, incluidos los servicios de IA que AWS podría implementar en el futuro. Puede adjuntar políticas secundarias a unidades organizativas o directamente a cuentas para anular esta configuración para cualquier servicio de IA excepto Amazon Comprehend. La segunda entrada del ejemplo siguiente utiliza `@@operators_allowed_for_child_policies` establecido en `none` para evitar que se reemplace. La tercera entrada del ejemplo crea una exención de toda la organización para Amazon Rekognition. Opta en toda la organización por ese servicio, pero la política permite que las política secundarias se anulen cuando corresponda.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

La sintaxis de política de exclusión de servicios de IA incluye los siguientes elementos:

- El elemento `services`. Una política de exclusión de servicios de IA se identifica con este nombre fijo como el elemento que contiene JSON más externo.

Una política de exclusión de servicios de IA puede tener una o más sentencias bajo el elemento `services`. Cada sentencia contiene los siguientes elementos:

- Una clave de nombre de servicio que identifica un servicio de IA AWS. Los siguientes nombres clave son valores válidos para este campo:
  - **`default`**: representa todos los servicios de IA que actualmente están disponibles e incluye implícita y automáticamente cualquier servicio de IA que se pueda agregar en el futuro.
  - `awssupplychain`
  - `dms`
  - `chimesdkvoiceanalytics`
  - `cloudwatch`
  - `codeguruprofiler`
  - `codewhisperer`
  - `comprehend`
  - `connectamd`
  - `connectoptimization`
  - `contactlens`
  - `datazone`
  - `entityresolution`
  - `frauddetector`
  - `glue`
  - `guardduty`
  - `lex`
  - `polly`
  - `q`
  - `quicksightq`
  - `rekognition`
  - `securitylake`
  - `textract`
  - `transcribe`
  - `translate`

Cada declaración de política identificada por una clave de nombre de servicio puede contener los siguientes elementos:

- La clave de `opt_out_policy`. Esta clave debe estar presente. Esta es la única clave que puede colocar bajo una clave de nombre de servicio.

  El `opt_out_policy` clave puede contener solo el operador `@@assign` con uno de los siguientes valores:

  - `optOut`: opta por no utilizar contenido para el servicio de IA especificado.
  - `optIn`: elige optar por el uso de contenido para el servicio de IA especificado.

  > **Notas**
  >
  > - No puede usar la opción `@@append` y operadores `@@remove` de herencia en las políticas de exclusión de servicios de IA.
  > - No puede usar los operadores `@@enforced_for` de herencia en las políticas de exclusión de servicios de IA.

- En cualquier nivel, puede especificar la propiedad `@@operators_allowed_for_child_policies` para controlar lo que las políticas secundarias pueden hacer para anular la configuración impuesta por las políticas principales. Puede especificar uno de los siguientes valores:

  - `@@assign`: las políticas secundarias de esta política pueden utilizar el operador `@@assign` para anular el valor heredado con un valor diferente.
  - `@@none`: las políticas secundarias de esta política no pueden cambiar el valor.

  El comportamiento del `@@operators_allowed_for_child_policies` depende de dónde lo coloque. Puede usar las siguientes ubicaciones:

  - En la clave `services`: controla si una política secundaria puede agregar o cambiar la lista de servicios de la política efectiva.
  - En la clave para un servicio de IA específico o en la clave `default`: controla si una política secundaria puede agregar o cambiar la lista de claves bajo esta entrada específica.
  - En la clave `opt_out_policies` para un servicio específico: controla si una política secundaria puede cambiar solo la configuración de este servicio específico.

Ejemplos de políticas de exclusión de servicios de IA

Las políticas de copia de seguridad siguientes son solo para fines informativos.

Ejemplo 1: Excluir todos los servicios de IA para todas las cuentas de la organización

En el siguiente ejemplo se muestra una política que puede adjuntar al nodo raíz de su organización para excluir los servicios de IA para las cuentas de su organización.

> **Tip**
>
> Si copia el siguiente ejemplo utilizando el botón Copiar en la esquina superior derecha del ejemplo, la copia no incluye los números de línea. Está listo para pegar.

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] El `"@@operators_allowed_for_child_policies": ["@@none"]` que está en `services` impide que cualquier política secundaria agregue secciones nuevas para servicios individuales que no sean `default` que ya está allí. `Default` es el marcador de posición que representa “todos los servicios de IA”.
- [2] El `"@@operators_allowed_for_child_policies": ["@@none"]` que está en `default` impide que las políticas secundarias agreguen secciones nuevas que no sean `opt_out_policy` que ya está allí.
- [3] El `"@@operators_allowed_for_child_policies": ["@@none"]` que está en `opt_out_policy` evita que las políticas secundarias cambien el valor de la configuración `optOut` o que agreguen cualquier configuración adicional.

Ejemplo 2: Establecer una configuración predeterminada de la organización para todos los servicios, pero permitir que las políticas secundarias anulen la configuración de los servicios individuales

En el siguiente ejemplo de política se establece un valor predeterminado para toda la organización para todos los servicios de IA. El valor para `default` impide que una política secundaria cambie el valor `optOut` para el servicio `default`, el marcador de posición para todos los servicios de IA. Si esta política se aplica como política principal adjuntándola al nodo raíz o a una unidad organizativa, las políticas secundarias pueden cambiar la configuración de exclusión de servicios individuales, como se muestra en la segunda política.

- Porque no hay `"@@operators_allowed_for_child_policies": ["@@none"]` en la clave `services`, las políticas secundarias pueden agregar nuevas secciones para servicios individuales.
- El `"@@operators_allowed_for_child_policies": ["@@none"]` que está en `default` impide que las políticas secundarias agreguen secciones nuevas que no sean `opt_out_policy` que ya está allí.
- El `"@@operators_allowed_for_child_policies": ["@@none"]` que está en `opt_out_policy` evita que las políticas secundarias cambien el valor de la configuración `optOut` o que agreguen cualquier configuración adicional.

Política principal de exclusión de servicios de IA de usuario raíz de la organización

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

En la siguiente política de ejemplo se supone que la política del ejemplo anterior está asociada al nodo raíz de la organización o a una unidad organizativa principal y que se adjunta este ejemplo a una cuenta afectada por la política principal. Anula la configuración predeterminada de exclusión y opta explícitamente solo por el servicio Amazon Lex.

Política secundaria de exclusión de servicios de IA

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

La política efectiva resultante para el Cuenta de AWS es que la cuenta solo acepta Amazon Lex y opta por no participar en todos los demás servicios de IA AWS debido a la configuración heredada `default` de exclusión de la política principal.

Ejemplo 3: Definir una política de exclusión de servicios de IA de toda la organización para un único servicio

En el siguiente ejemplo se muestra una política de exclusión de servicios de IA que define una configuración `optOut` para un único servicio de IA. Si esta política está adjunta al nodo raíz de la organización, impide que cualquier política secundaria anule la configuración `optOut` para este servicio. Otros servicios no se abordan en esta política, pero podrían verse afectados por las políticas secundarias de otras unidades organizativas o cuentas.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Administrador delegado para AWS Organizations

Le recomendamos que utilice la cuenta AWS Organizations de administración y sus usuarios y funciones solo para las tareas que debe realizar esa cuenta. También le recomendamos que

almacene sus recursos de AWS en otras cuentas de miembros de la organización y los mantenga fuera de la cuenta de administración. Esto se debe a que las funciones de seguridad, como las políticas de control de servicios de SCPs Organizations (), no restringen los usuarios ni las funciones de la cuenta de administración.

Desde la cuenta de administración de la organización, puede delegar la administración de políticas para las organizaciones en cuentas de miembro especificadas para realizar acciones de políticas que, de forma predeterminada, solo están disponibles para la cuenta de administración.

Para ver ejemplos de políticas de delegación basadas en recursos, consulte Ejemplos de políticas basadas en recursos para AWS Organizations.

Temas

- Cree una política de delegación basada en los recursos con AWS Organizations
- Actualice una política de delegación basada en los recursos con AWS Organizations
- Consulte una política de delegación basada en los recursos con AWS Organizations
- Elimine una política de delegación basada en recursos con AWS Organizations

Cree una política de delegación basada en los recursos con AWS Organizations

Desde la cuenta de administración, cree una política de delegación basada en recursos para su organización y agregue una declaración que especifique qué cuenta de miembro puede llevar a cabo las acciones en las políticas. Puede agregar varias declaraciones en la política para denotar distintos conjuntos de permisos para las cuentas de los miembros.

Permisos mínimos

Para crear o actualizar una política de delegación basada en recursos, necesita permisos para poner en marcha las siguientes acciones:

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

Además, debe conceder a los roles y usuarios de la cuenta de administrador delegado los permisos de IAM correspondientes a las acciones requeridas. Sin los permisos de IAM, se

supone que la persona principal que realiza la llamada no tiene los permisos necesarios para gestionar las políticas. AWS Organizations

AWS Management Console

Agregue declaraciones a la política de delegación basada en recursos en la AWS Management Console utilizando uno de los siguientes métodos:

- Política JSON: pegue y personalice una política de delegación basada en recursos de ejemplo para usarla en su cuenta, o escriba su propio documento de política de JSON en el editor de JSON.
- Editor visual: cree una nueva política de delegación en el editor visual, que le guiará en la creación de una política de delegación sin tener que escribir la sintaxis JSON.

Uso del editor de políticas JSON para crear una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Configuración.
3. En la sección Administrador delegado para AWS Organizations, elija Delegar para crear la política de delegación de las organizaciones.
4. Especifique un documento de política JSON. Para obtener más información sobre el lenguaje de la política de IAM, consulte Referencia de políticas JSON de IAM.
5. Resuelva cualquier advertencia de seguridad, error o advertencia general generada durante la validación de la política y, a continuación, elija Create policy (Crear política) para guardar su trabajo.

Uso del editor visual para crear una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Configuración.

3. En la sección Administrador delegado para AWS Organizations, elija Delegar para crear la política de delegación de las organizaciones.
4. En la página Crear política de delegación, elija Add new statement (Agregar nueva declaración).
5. Establezca Effect (Efecto) en `Allow`.
6. Agregue `Principal` para definir las cuentas de miembros en las que desea delegar.
7. En la lista de Acciones, elija las acciones que quiera delegar. Puede utilizar Filtrar acciones para limitar las opciones.
8. Para especificar si la cuenta del miembro delegado puede adjuntar políticas a la raíz de la organización o a las unidades organizativas (OUs), defina. `Resources` También debe seleccionar `policy` como tipo de recurso. Puede especificar recursos de las siguientes maneras:

   - Seleccione Add a resource (Agregar un recurso) y cree el Nombre de recurso de Amazon (ARN) siguiendo las instrucciones del cuadro de diálogo.
   - Enumere el recurso ARNs manualmente en el editor. Para obtener más información sobre la sintaxis del ARN, consulte Amazon Resource Name (ARN) en la AWS Guía de referencia general. Para obtener información sobre el uso ARNs del elemento de recurso de una política, consulte Elementos de la política JSON de IAM: recurso.
9. Elija Add a condition (Agregar una condición) para especificar otras condiciones, incluido el tipo de política que desea delegar. Elija la Condition key (Clave de condición), Tag key (Clave de etiqueta) Qualifier (Calificador) y Operator (Operador) de la condición y, a continuación, escriba un **`Value`**. Cuando haya terminado elija Add condition (Añadir condición). Para obtener más información sobre el elemento Condición, consulte Elementos de política JSON de IAM: Condition.
10. Para añadir más bloques de permisos, elija Add new statement (Añadir nueva declaración). Para cada bloque, repita los pasos 5 a 9.
11. Resuelva cualquier advertencia de seguridad, error o advertencia general generada durante la validación de la política y, a continuación, elija Crear política para guardar su trabajo.

AWS CLI & AWS SDKs

Creación de una política de delegación

Puede utilizar el siguiente comando para crear una política de delegación:

- AWS CLI: put-resource-policy

  En el siguiente ejemplo se crea una política de delegación.

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: PutResourcePolicy

Acciones de política de delegación admitidas

Se admiten las siguientes acciones para políticas de delegación:

- `AttachPolicy`
- `CreatePolicy`
- `DeletePolicy`
- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `DetachPolicy`
- `DisablePolicyType`
- `EnablePolicyType`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`

- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`
- `TagResource`
- `UntagResource`
- `UpdatePolicy`

Claves de condición admitidas

Solo las claves de condición compatibles se AWS Organizations pueden usar para la política de delegación. Para obtener más información, consulte Condition keys for AWS Organizations en la Referencia de autorizaciones de servicio.

Actualice una política de delegación basada en los recursos con AWS Organizations

Desde la cuenta de administración, actualice una política de delegación basada en recursos para su organización y agregue una declaración que especifique qué cuenta de miembro puede llevar a cabo las acciones en las políticas. Puede agregar varias declaraciones en la política para denotar distintos conjuntos de permisos para las cuentas de los miembros.

Permisos mínimos

Para actualizar una política de delegación basada en recursos, necesita permisos para poner en marcha las siguientes acciones:

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

Además, debe conceder a los roles y usuarios de la cuenta de administrador delegado los permisos de IAM correspondientes a las acciones requeridas. Sin los permisos de IAM, se supone que la persona principal que realiza la llamada no tiene los permisos necesarios para gestionar las políticas. AWS Organizations

AWS Management Console

Agregue declaraciones a la política de delegación basada en recursos en la AWS Management Console utilizando uno de los siguientes métodos:

- Política JSON: pegue y personalice una política de delegación basada en recursos de ejemplo para usarla en su cuenta, o escriba su propio documento de política de JSON en el editor de JSON.
- Editor visual: cree una nueva política de delegación en el editor visual, que le guiará en la creación de una política de delegación sin tener que escribir la sintaxis JSON.

Uso del editor de políticas JSON para actualizar una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Configuración.
3. En la sección Administrador delegado para AWS Organizations, elija Editar para actualizar la política de delegación de Organizations.
4. Especifique un documento de política JSON. Para obtener más información sobre el lenguaje de la política de IAM, consulte Referencia de políticas JSON de IAM.
5. Resuelva las advertencias de seguridad, errores o advertencias generales generadas durante la validación de la política y luego elija Crear política.

Uso del editor visual para actualizar una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Configuración.
3. En la sección Administrador delegado para AWS Organizations, elija Editar para actualizar la política de delegación de Organizations.
4. En la página Crear política de delegación, elija Add new statement (Agregar nueva declaración).
5. Establezca Effect (Efecto) en `Allow`.

6. Agregue `Principal` para definir las cuentas de miembros en las que desea delegar.
7. En la lista de Acciones, elija las acciones que quiera delegar. Puede utilizar Filtrar acciones para limitar las opciones.
8. Para especificar si la cuenta del miembro delegado puede adjuntar políticas a la raíz de la organización o a las unidades organizativas (OUs), defina. `Resources` También debe seleccionar `policy` como tipo de recurso. Puede especificar recursos de las siguientes maneras:

   - Seleccione Add a resource (Agregar un recurso) y cree el Nombre de recurso de Amazon (ARN) siguiendo las instrucciones del cuadro de diálogo.
   - Enumere el recurso ARNs manualmente en el editor. Para obtener más información sobre la sintaxis del ARN, consulte Amazon Resource Name (ARN) en la AWS Guía de referencia general. Para obtener información sobre el uso ARNs del elemento de recurso de una política, consulte Elementos de la política JSON de IAM: recurso.
9. Elija Add a condition (Agregar una condición) para especificar otras condiciones, incluido el tipo de política que desea delegar. Elija la Condition key (Clave de condición), Tag key (Clave de etiqueta) Qualifier (Calificador) y Operator (Operador) de la condición y, a continuación, escriba un **`Value`**. Cuando haya terminado elija Add condition (Añadir condición). Para obtener más información sobre el elemento Condición, consulte Elementos de política JSON de IAM: Condition.
10. Para añadir más bloques de permisos, elija Add new statement (Añadir nueva declaración). Para cada bloque, repita los pasos 5 a 9.
11. Resuelva las advertencias de seguridad, errores o advertencias generales generadas durante la validación de la política y luego elija Guardar política.

AWS CLI & AWS SDKs

Creación o actualización de una política de delegación

Puede utilizar el siguiente comando para crear o actualizar una política de delegación:

- AWS CLI: put-resource-policy

  En el siguiente ejemplo se crea o actualiza la política de delegación.

```
$ aws organizations put-resource-policy --content
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: PutResourcePolicy

Acciones de política de delegación admitidas

Se admiten las siguientes acciones para políticas de delegación:

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy

- `TagResource`
- `UntagResource`
- `UpdatePolicy`

Claves de condición admitidas

Solo las claves de condición compatibles se AWS Organizations pueden usar para la política de delegación. Para obtener más información, consulte Condition keys for AWS Organizations en la Referencia de autorizaciones de servicio.

Consulte una política de delegación basada en los recursos con AWS Organizations

Desde la cuenta de administración, vea la política de delegación basada en recursos de su organización para saber qué administradores delegados tienen acceso a la administración de qué tipos de políticas.

> **Permisos mínimos**
>
> Para ver una política de delegación basada en recursos, necesita permisos para ejecutar la siguiente acción: `organizations:DescribeResourcePolicy`.

AWS Management Console

Para ver una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Configuración.
3. En la sección Administrador delegado para AWS Organizations, desplácese hacia abajo para ver la política de delegación completa.

AWS CLI & AWS SDKs

Visualización de una política de delegación

Puede utilizar el siguiente comando para ver una política de delegación:

- AWS CLI: describe-resource-policy

  En el siguiente ejemplo se recupera la política.

  ```
  $ aws organizations describe-resource-policy
  ```

- AWS SDK: DescribeResourcePolicy

Elimine una política de delegación basada en recursos con AWS Organizations

Cuando ya no necesite delegar la administración de políticas en su organización, puede eliminar la política de delegación basada en recursos de la cuenta de administración de la organización.

> **Important**
>
> Si elimina la política de delegación basada en recursos, no podrá recuperarla.

> **Permisos mínimos**
>
> Para eliminar la política de delegación basada en recursos, necesita permisos para ejecutar la siguiente acción:`organizations:DeleteResourcePolicy`.

AWS Management Console

Para eliminar una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Configuración.
3. En la sección Administrador delegado para AWS Organizations, elija Eliminar.

4. En el cuadro de diálogo de confirmación Delete policy (Eliminar política), escriba **`delete`**. A continuación, elija Delete policy (Eliminar política).

AWS CLI & AWS SDKs

Eliminación de una política de delegación

Puede utilizar el siguiente comando para eliminar una política de delegación:

- AWS CLI: delete-resource-policy

  En el siguiente ejemplo se elimina la política especificada.

  ```
  $ aws organizations delete-resource-policy
  ```

- AWS SDK: DeleteResourcePolicy

Habilitar un tipo de política

Antes de poder crear y adjuntar una política a su organización, debe habilitar ese tipo de políticas para su uso. Habilitar un tipo de política es una tarea única en la raíz de la organización. Puede habilitar un tipo de política únicamente desde la cuenta de administración de la organización o desde una cuenta de miembro designada como administrador delegado.

Permisos mínimos

Para habilitar un tipo de política, necesita permiso para ejecutar las siguientes acciones:

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:ListRoots`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para habilitar un tipo de política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija elegir nombre del tipo de política que desea habilitar.
3. En la página de tipos de política, selecciona Activar ***policy type***.

   La página se sustituye por una lista de las políticas disponibles del tipo especificado.

AWS CLI & AWS SDKs

Para habilitar un tipo de política

Puede utilizar uno de los siguientes comandos para habilitar un tipo de política:

- AWS CLI: enable-policy-type

  En el siguiente ejemplo, se muestra cómo habilitar políticas de copia de seguridad para la organización. Tenga en cuenta que debe especificar el ID del nodo raíz de su organización.

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

La lista de `PolicyTypes` en la salida ahora incluye el tipo de política especificado con el `Status` de `ENABLED`.

- AWS SDKs: EnablePolicyType

Deshabilitar un tipo de política

Si ya no desea utilizar un tipo de política determinado en su organización, puede deshabilitarlo para evitar su uso accidental. Puede deshabilitar un tipo de política únicamente desde la cuenta de administración de la organización o desde una cuenta de miembro designada como administrador delegado.

Consideraciones

Las políticas desactivadas se desvinculan de todas las entidades, pero no se eliminan

Cuando deshabilita un tipo de política, todas las políticas del tipo especificado se separan automáticamente de todas las entidades de la raíz de la organización. Las políticas no se eliminan.

(Solo tipo de política de control de servicios) Todas las entidades de la raíz se asocian inicialmente solo a la predeterminada **`FullAWSAccess`** SCP

(Solo tipo de política de control de servicios) Si vuelve a habilitar el tipo de SCP política más adelante, todas las entidades de la raíz de la organización se adjuntarán inicialmente solo a la configuración predeterminada `FullAWSAccess`SCP. Los archivos adjuntos SCPs de las entidades se pierden cuando SCPs están deshabilitados en la organización. Si desea volver a activarlos más adelanteSCPs, debe volver a adjuntarlos a la raíz y a las cuentas de la organizaciónOUs, según corresponda.

Desactivación de un tipo de política

Permisos mínimos

Para deshabilitarlasSCPs, necesitas permiso para ejecutar las siguientes acciones:

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations

- `organizations:ListRoots`: solo se requiere cuando se utiliza la consola de Organizations

AWS Management Console

Para deshabilitar un tipo de política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija el nombre del tipo de política que desea desactivar.
3. En la página de tipos de política, selecciona Inhabilitar ***policy type***.
4. En el cuadro de diálogo de confirmación, ingrese la palabra **`disable`**, y luego elija Desactivar.

   La lista de políticas disponibles del tipo especificado desaparece.

AWS CLI & AWS SDKs

Para deshabilitar un tipo de política

Puede utilizar uno de los comandos siguientes para deshabilitar un tipo de política:

- AWS CLI: disable-policy-type

  En el siguiente ejemplo, se muestra cómo desactivar las políticas de copia de seguridad para la organización. Tenga en cuenta que debe especificar el ID del nodo raíz de su organización.

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
```

```
}
```

La lista de `PolicyTypes` en la salida ya no incluye el tipo de política especificado.

- AWS SDKs: DisablePolicyType

Crear políticas de la organización con AWS Organizations

Después de habilitar políticas para su organización, puede crear una política.

En este tema se describe cómo crear políticas con AWS Organizations. Una política define los controles que se desean aplicar a un grupo de Cuentas de AWS.

Temas

- Creación de una política de control de servicios (SCP)
- Cree una política de control de recursos (RCP)
- Cree una política declarativa
- Creación de una política de copia de seguridad
- Creación de una política de etiquetas
- Creación de una política de chatbot
- Creación de una política de exclusión de servicios de IA

Creación de una política de control de servicios (SCP)

Permisos mínimos

Para SCPs crearlos, necesita permiso para ejecutar la siguiente acción:

- `organizations:CreatePolicy`

AWS Management Console

Para crear una política de control de servicios

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, seleccione Crear política.
3. En la página Create new service control policy (Crear política de control de servicios nueva), introduzca un Policy name (Nombre de política) y una Description (Descripción) opcional para la política.
4. (Opcional) Agregue una o varias etiquetas seleccionando Añadir etiqueta y a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información, consulte Recursos de etiquetado AWS Organizations.

   > **Note**
   >
   > En la mayoría de los pasos que siguen, discutimos el uso de los controles en el lado derecho del editor JSON para construir la política, elemento por elemento. Alternativamente, puede, en cualquier momento, simplemente ingresar texto en el editor JSON en el lado izquierdo de la ventana. Puede escribir directamente, o usar copiar y pegar.

5. Para crear la política, los siguientes pasos varían en función de si desea agregar una instrucción que deniega el acceso o lo permite. Para obtener más información, consulte Evaluación de SCP. Si utiliza `Deny` instrucciones, tiene un control adicional, ya que puede restringir el acceso a recursos específicos, definir las condiciones para su aplicación y utilizar el NotActionelemento. SCPs Para obtener más detalles acerca de la sintaxis, consulte Sintaxis de SCP.

   Para agregar una instrucción que deniega el acceso:

   a. En el panel de edición de declaraciones de la derecha del editor, en Añadir acciones, selecciona un AWS servicio.

      A medida que elige opciones a la derecha, el editor JSON se actualiza para mostrar la política de JSON correspondiente a la izquierda.

b. Después de seleccionar un servicio, se abre una lista que contiene las acciones disponibles para ese servicio. Puede elegir Todas las acciones o elegir una o varias acciones individuales que desea denegar.

   El JSON de la izquierda se actualiza para incluir las acciones seleccionadas.

   > **Note**
   >
   > Si selecciona una acción individual y, a continuación, también vuelve y también selecciona Todas las acciones, la entrada esperada para `servicename:*` se agrega al JSON, pero las acciones individuales que seleccionó anteriormente se dejan en el JSON y no se eliminan.

c. Si desea agregar acciones de servicios adicionales, puede elegir Todos los servicios al principio del casillero de la Instrucción y, a continuación, repita los dos pasos anteriores según sea necesario.

d. Especifique los recursos que hay que incluir en la instrucción.

   - Junto a Agregar un recurso, elija Agregar.
   - En el navegador Add resource (Agregar recurso), elija de la lista el servicio cuyos recursos desea controlar. Puede seleccionar entre solo los servicios que ha seleccionado en el paso anterior.
   - Bajo Tipo de recurso, elija el tipo de recurso que desea controlar.
   - Por último, complete el nombre de recurso de Amazon (ARN) en ARN de recurso para identificar el recurso específico al que desea controlar el acceso. Debe reemplazar todos los marcadores de posición que estén rodeados de llaves `{}`. Puede especificar comodines (`*`) donde la sintaxis ARN de ese tipo de recurso lo permite. Consulte la documentación de un tipo de recurso específico para obtener información sobre dónde puede usar comodines.
   - Guarde su adición a la política eligiendo Add resource (Agregar recurso). El elemento `Resource` en el JSON refleja sus adiciones o cambios. El elemento de Recurso es obligatorio.

> **Tip**
>
> Si desea especificar todos los recursos para el servicio seleccionado, elija la opción Todos los recursos en la lista, o edite la opción `Resource` directamente en el JSON para leer `"Resource":"*"`.

e. (Opcional) Para especificar las condiciones que determinan cuándo una declaración de política está en vigor, junto a Agregar condición, elija Agregar.

- Clave de condición: de la lista, puede elegir cualquier clave de condición que esté disponible para todos los AWS servicios (por ejemplo`aws:SourceIp`) o una clave específica para solo uno de los servicios que haya seleccionado para esta declaración.
- Calificador: (opcional) Cuando la solicitud tiene más de un valor para una clave de contexto multivalor, puede especificar un calificador para probar las solicitudes con esos valores. Para obtener más información, consulte las claves de contexto de un solo valor frente a las de varios valores en la Guía del usuario de IAM. Para comprobar si una solicitud puede tener varios valores, consulte las claves de acciones, recursos y condición que aparecen Servicios de AWS en la Referencia de autorización de servicios.
  - Valor predeterminado: prueba un valor único de la solicitud con el valor de la clave de condición de la política. La condición es verdadera si el valor de la solicitud coincide con el valor de la política. Si la política especifica más de un valor, entonces se tratan como una prueba “o”, y la condición es verdadera si los valores de solicitud coinciden con cualquiera de los valores de la política.
  - Para cualquier valor en una solicitud — Cuando la solicitud puede tener varios valores, esta opción prueba si al menos uno de los valores de solicitud coincide con al menos uno de los valores clave de condición de la política. La condición devuelve true si alguno de los valores de clave de la solicitud coincide con alguno de los valores de condición de la política. Si no hay una clave coincidente o si hay un conjunto de datos es nulo, la condición devuelve "false".
  - Para todos los valores en una solicitud — Cuando la solicitud puede tener varios valores, esta opción prueba si todos de los valores de solicitud coinciden con un valor de clave de condición de la política. La condición devuelve true si cada valor de clave de la solicitud coincide con al menos un valor de la política. También

devuelve true si no hay claves en la solicitud o si los valores de clave se resuelven en un conjunto de datos nulo, como una cadena vacía.

- Operador — El operador especifica el tipo de comparación que se va a realizar. Las opciones que se presentan dependen del tipo de datos de la clave de condición. Por ejemplo, la clave de condición global `aws:CurrentTime` le permite elegir entre cualquiera de los operadores de comparación de fechas, o `Null`, que puede usar para probar si el valor está presente en la solicitud.

  Para cualquier operador de condiciones, excepto la `Null` prueba, puede elegir la IfExistsopción.

- Valor — (Opcional) Especifique uno o varios valores para los que desea probar la solicitud.

Elija Add condition.

Para obtener más información acerca de las claves de condición, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

6. Para agregar una instrucción que permita el acceso:

   a. En el editor JSON de la izquierda, cambie la línea `"Effect": "Deny"` a `"Effect": "Allow"`.

   A medida que elige opciones a la derecha, el editor JSON se actualiza para mostrar la política de JSON correspondiente a la izquierda.

   b. Después de seleccionar un servicio, se abre una lista que contiene las acciones disponibles para ese servicio. Puede elegir Todas las acciones o elija una o varias acciones individuales que desea permitir.

   El JSON de la izquierda se actualiza para incluir las acciones seleccionadas.

> **Note**
>
> Si selecciona una acción individual y, a continuación, también vuelve y también selecciona Todas las acciones, la entrada esperada para *`servicename`*`:*` se agrega al JSON, pero las acciones individuales que seleccionó anteriormente se dejan en el JSON y no se eliminan.

c. Si desea agregar acciones de servicios adicionales, puede elegir Todos los servicios al principio del casillero de la Instrucción y, a continuación, repita los dos pasos anteriores según sea necesario.

7. (Opcional) Para agregar otra instrucción a la política, elija Add statement (Añadir instrucción) y use el editor visual para crear la siguiente declaración.
8. Cuando haya terminado de añadir instrucciones, elija Create policy (Crear política) para guardar la SCP.

Su nueva SCP aparecerá en la lista de políticas de la organización. Ahora puede adjuntar su SCP a la raíz o a las cuentas. OUs

AWS CLI & AWS SDKs

Para crear una política de control de servicios

Puede utilizar uno de los siguientes comandos para crear una SCP:

- AWS CLI: create-policy

  En el ejemplo siguiente se presupone que dispone de un archivo denominado `Deny-IAM.json` con el texto de la política JSON. Utiliza ese archivo para crear una nueva política de control de servicios.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
```

```
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> SCPs no surten efecto en la cuenta de administración ni en algunas otras situaciones. Para obtener más información, consulte Las tareas y entidades no están restringidas por SCPs.

Cree una política de control de recursos (RCP)

> **Permisos mínimos**
>
> Para RCPs crearla, necesita permiso para ejecutar la siguiente acción:
>
> - `organizations:CreatePolicy`

AWS Management Console

Para crear una política de control de recursos

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página de la política de control de recursos, elija Crear política.
3. En la página Crear una nueva política de control de recursos, introduzca un nombre de política y una descripción de la política opcional.
4. (Opcional) Agregue una o varias etiquetas seleccionando Añadir etiqueta y a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información, consulte Recursos de etiquetado AWS Organizations.

> **Note**
>
> En la mayoría de los pasos que siguen, discutimos el uso de los controles en el lado derecho del editor JSON para construir la política, elemento por elemento. Alternativamente, puede, en cualquier momento, simplemente ingresar texto en el editor JSON en el lado izquierdo de la ventana. Puede escribir directamente, o usar copiar y pegar.

5. Para añadir una declaración:

   a. En el panel de edición de declaraciones derecho del editor, en Añadir acciones, selecciona un AWS servicio.

      A medida que elige opciones a la derecha, el editor JSON se actualiza para mostrar la política de JSON correspondiente a la izquierda.

   b. Después de seleccionar un servicio, se abre una lista que contiene las acciones disponibles para ese servicio. Puede elegir Todas las acciones o elegir una o varias acciones individuales que desea denegar.

      El JSON de la izquierda se actualiza para incluir las acciones seleccionadas.

      > **Note**
      >
      > Si selecciona una acción individual y, a continuación, también vuelve y también selecciona Todas las acciones, la entrada esperada para `servicename:*` se agrega al JSON, pero las acciones individuales que seleccionó anteriormente se dejan en el JSON y no se eliminan.

   c. Si desea agregar acciones de servicios adicionales, puede elegir Todos los servicios al principio del casillero de la Instrucción y, a continuación, repita los dos pasos anteriores según sea necesario.

   d. Especifique los recursos que hay que incluir en la instrucción.

      - Junto a Agregar un recurso, elija Agregar.
      - En el navegador Add resource (Agregar recurso), elija de la lista el servicio cuyos recursos desea controlar. Puede seleccionar entre solo los servicios que ha seleccionado en el paso anterior.

- Bajo Tipo de recurso, elija el tipo de recurso que desea controlar.
- Complete el nombre del recurso de Amazon (ARN) en el ARN del recurso para identificar el recurso específico al que desea controlar el acceso. Debe reemplazar todos los marcadores de posición que estén rodeados de llaves `{}`. Puede especificar comodines (`*`) donde la sintaxis ARN de ese tipo de recurso lo permite. Consulte la documentación de un tipo de recurso específico para obtener información sobre dónde puede utilizar caracteres comodín.
- Guarde su adición a la política eligiendo Add resource (Agregar recurso). El elemento `Resource` en el JSON refleja sus adiciones o cambios. El elemento de Recurso es obligatorio.

> **Tip**
>
> Si desea especificar todos los recursos para el servicio seleccionado, elija la opción Todos los recursos en la lista, o edite la opción `Resource` directamente en el JSON para leer `"Resource":"*"`.

e. (Opcional) Para especificar las condiciones que determinan cuándo una declaración de política está en vigor, junto a Agregar condición, elija Agregar.

- Clave de condición: de la lista, puede elegir cualquier clave de condición que esté disponible para todos los AWS servicios (por ejemplo`aws:SourceIp`) o una clave específica del servicio para solo uno de los servicios que haya seleccionado para esta declaración.
- Calificador: (opcional) Cuando la solicitud tiene más de un valor para una clave de contexto multivalor, puede especificar un calificador para probar las solicitudes con esos valores. Para obtener más información, consulte las claves de contexto de un solo valor frente a las de varios valores en la Guía del usuario de IAM. Para comprobar si una solicitud puede tener varios valores, consulte las claves de acciones, recursos y condición que aparecen Servicios de AWS en la Referencia de autorización de servicios.
  - Valor predeterminado: prueba un valor único de la solicitud con el valor de la clave de condición de la política. La condición es verdadera si el valor de la solicitud coincide con el valor de la política. Si la política especifica más de un valor, entonces se tratan como una prueba “o”, y la condición es verdadera si los valores de solicitud coinciden con cualquiera de los valores de la política.

- Para cualquier valor en una solicitud — Cuando la solicitud puede tener varios valores, esta opción prueba si al menos uno de los valores de solicitud coincide con al menos uno de los valores clave de condición de la política. La condición devuelve true si alguno de los valores de clave de la solicitud coincide con alguno de los valores de condición de la política. Si no hay una clave coincidente o si hay un conjunto de datos es nulo, la condición devuelve "false".
- Para todos los valores en una solicitud — Cuando la solicitud puede tener varios valores, esta opción prueba si todos de los valores de solicitud coinciden con un valor de clave de condición de la política. La condición devuelve true si cada valor de clave de la solicitud coincide con al menos un valor de la política. También devuelve true si no hay claves en la solicitud o si los valores de clave se resuelven en un conjunto de datos nulo, como una cadena vacía.

- Operador — El operador especifica el tipo de comparación que se va a realizar. Las opciones que se presentan dependen del tipo de datos de la clave de condición. Por ejemplo, la clave de condición global `aws:CurrentTime` le permite elegir entre cualquiera de los operadores de comparación de fechas, o `Null`, que puede usar para probar si el valor está presente en la solicitud.

  Para cualquier operador de condiciones, excepto la `Null` prueba, puede elegir la IfExistsopción.
- Valor — (Opcional) Especifique uno o varios valores para los que desea probar la solicitud.

Elija Add condition.

Para obtener más información acerca de las claves de condición, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

f. (Opcional) Para usar el elemento `NotAction` para denegar el acceso a todas las acciones excepto las especificadas, sustituya `Action` en el panel izquierdo con `NotAction`, justo después de `"Effect": "Deny",`. Para obtener más información, consulte Elementos de la política JSON de IAM: NotAction en la Guía del usuario de IAM.

6. (Opcional) Para agregar otra instrucción a la política, elija Add statement (Añadir instrucción) y use el editor visual para crear la siguiente declaración.

7. Cuando haya terminado de añadir declaraciones, seleccione Crear política para guardar el RCP completo.

Tu nuevo RCP aparece en la lista de políticas de la organización. Ahora puede adjuntar su RCP a la raíz o a las OUs cuentas.

AWS CLI & AWS SDKs

Para crear una política de control de recursos

Puede usar uno de los siguientes comandos para crear un RCP:

- AWS CLI: create-policy

  En el ejemplo siguiente se presupone que dispone de un archivo denominado `Deny-IAM.json` con el texto de la política JSON. Utiliza ese archivo para crear una nueva política de control de recursos.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMRCP \
    --type RESOURCE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
resource_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMRCP",
            "Description": "Deny all IAM actions",
            "Type": "RESOURCE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> RCPs no surten efecto en la cuenta de administración ni en algunas otras situaciones. Para obtener más información, consulte Los recursos y las entidades no están restringidos por RCPs.

Cree una política declarativa

> **Permisos mínimos**
>
> Para crear una política declarativa, necesita permiso para ejecutar la siguiente acción:
>
> - `organizations:CreatePolicy`

AWS Management Console

Para crear una política declarativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas declarativas, elija Crear política.
3. En la EC2página Crear una nueva política declarativa para, introduzca un nombre de política y una descripción de la política opcional.
4. (Opcional) Puede agregar una o varias etiquetas a la política seleccionando Agregar etiqueta y a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información, consulte Recursos de etiquetado AWS Organizations.
5. Puede crear la política mediante el Visual editor (Editor visual) como se describe en este procedimiento. También puede ingresar o pegar texto de política en la pestaña JSON. Para obtener información sobre la sintaxis de la política declarativa, consulte. Sintaxis y ejemplos de políticas declarativas

Si decide utilizar el editor visual, seleccione el atributo de servicio que desee incluir en la política declarativa. Para obtener más información, consulte Soportado Servicios de AWS y atributos.

6. Elija Añadir atributo de servicio y configure el atributo según sus especificaciones. Para obtener información más detallada sobre cada efecto, consulteSintaxis y ejemplos de políticas declarativas.
7. Cuando haya terminado de editar la política, elija Crear política en la esquina inferior derecha de la página.

AWS CLI & AWS SDKs

Para crear una política declarativa

Puede usar una de las siguientes opciones para crear una política declarativa:

- AWS CLI: create-policy

1. Cree una política declarativa como la siguiente y guárdela en un archivo de texto.

```
{
    "ec2_attributes": {
        "image_block_public_access": {
            "state": {
                "@@assign": "block_new_sharing"
            }
        }
    }
}
```

Esta política declarativa especifica que todas las cuentas afectadas por la política deben estar configuradas para que las nuevas Amazon Machine Images (AMIs) no se puedan compartir públicamente. Para obtener información sobre la sintaxis de la política declarativa, consulte. Sintaxis y ejemplos de políticas declarativas

2. Importe el archivo de política JSON para crear una nueva política en la organización. En este ejemplo, el archivo JSON anterior se denominó `policy.json`.

```
$ aws organizations create-policy \
    --type DECLARATIVE_POLICY_EC2 \
```

```
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "DECLARATIVE_POLICY_EC2"
        }
    }
}
```

- AWS SDKs: CreatePolicy

Qué hacer a continuación

Tras crear una política declarativa, evalúe si está lista mediante el informe de estado de la cuenta. A continuación, puede hacer cumplir sus configuraciones de referencia. Para ello, puedes adjuntar la política a la raíz de la organización, a las unidades organizativas (OUs), Cuentas de AWS dentro de la organización o a una combinación de todas ellas.

Creación de una política de copia de seguridad

Permisos mínimos

Para crear una política de copia de seguridad, necesita permiso para ejecutar la siguiente acción:

- `organizations:CreatePolicy`

AWS Management Console

Puedes crear una política de copias de AWS Management Console seguridad de dos maneras:

- Un editor visual que le permite elegir opciones y generar el texto de la política JSON automáticamente.
- Un editor de texto que le permite crear directamente el texto de la política JSON usted mismo.

El editor visual facilita el proceso, pero limita su flexibilidad. Es una excelente manera de crear sus primeras políticas y sentirse cómodo al usarlas. Cuando comprenda cómo funcionan y haya comenzado a verse limitado por lo que ofrece el editor visual, puede añadir características avanzadas a sus políticas editando el texto de la política JSON usted mismo. El editor visual utiliza solo el operador de configuración de valores @@assign y no proporciona ningún acceso a los operadores de control secundarios. Solo puede agregar los operadores de control infantil si edita manualmente el texto de la política JSON.

Para crear una política de backup

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Backup policies (Políticas de copia de seguridad), seleccione Create policy (Crear política).
3. En la página Create policy (Crear política), introduzca un Policy name (Nombre de política) y una Description (Descripción) opcional para la política.
4. (Opcional) Puede agregar una o varias etiquetas a la política seleccionando Agregar etiqueta y a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información acerca del etiquetado, consulte Recursos de etiquetado AWS Organizations.
5. Puede crear la política mediante el Visual editor (Editor visual) como se describe en este procedimiento. También puede ingresar o pegar texto de política en la pestaña JSON. Para obtener información acerca de la sintaxis de las políticas de copia de seguridad, consulte Ejemplos y sintaxis de políticas de copia de seguridad.

   Si decide utilizar el Visual editor (Editor visual), seleccione las opciones de copia de seguridad adecuadas para su situación. Un plan de copia de seguridad consta de tres partes. Para obtener más información acerca de estos elementos del plan de copia de seguridad, consulte Crear un plan de copia de seguridad y Asignar recursos en la Guía del desarrollador AWS Backup .

a. Detalles generales del plan de copia de seguridad

   - El nombre del plan de copia de seguridad puede constar únicamente de caracteres alfanuméricos, guiones y guiones bajos.
   - Debe seleccionar al menos una región del plan de copia de seguridad de la lista. El plan puede hacer copias de seguridad de los recursos solo en los lugares seleccionados Regiones de AWS.

b. Una o más reglas de copia de seguridad que especifican cómo y cuándo debe funcionar AWS Backup . Cada regla de copia de seguridad define los siguientes elementos:

   - Una programación que incluye la frecuencia de la copia de seguridad y la ventana de tiempo en la que se puede realizar la copia de seguridad.
   - El nombre del almacén de copia de seguridad que se va a utilizar. El nombre del almacén de copia de seguridad puede constar únicamente de caracteres alfanuméricos, guiones y guiones bajos. Debe haber un almacén de copia de seguridad para que el plan pueda ejecutarse correctamente. Cree el almacén mediante la AWS Backup consola o AWS CLI los comandos.
   - (Opcional) Una o varias reglas Copy to region (Copiar en región) para copiar también las copias de seguridad en almacenes de otras Regiones de AWS.
   - Uno o más pares de clave y valor de etiqueta para asociar a los puntos de recuperación de copia de seguridad creados cada vez que se ejecuta este plan de copia de seguridad.
   - Opciones de ciclo de vida que especifican cuándo pasa la copia de seguridad al almacenamiento en frío y cuándo caduca la copia de seguridad.

   Seleccionar Agregar regla para agregar cada regla que necesite al plan.

   Para obtener más información sobre las reglas de copia de seguridad, consulte las Reglas de copia de seguridad en la Guía para desarrolladores AWS Backup .

c. Una asignación de recursos que especifica los recursos de los que AWS Backup debe realizar una copia de seguridad con este plan. La asignación se realiza especificando los pares de etiquetas que se AWS Backup utilizan para buscar y hacer coincidir los recursos

   - El nombre de la asignación de recursos puede constar únicamente de caracteres alfanuméricos, guiones y guiones bajos.
   - Especifique el rol de IAM que AWS Backup utilizará para realizar la copia de seguridad por su nombre.

En la consola, no especifique todo el Nombre de recurso de Amazon (ARN). Debe incluir tanto el nombre del rol como su prefijo, que especifica el tipo de rol. Los prefijos son típicamente `role` o `service-role`, y se separan del nombre del rol por una barra inclinada ('/'). Por ejemplo, puede escribir `role/MyRoleName` o `service-role/MyManagedRoleName`. Esto se convierte en un ARN completo para usted cuando se almacena en el JSON subyacente.

> **Important**
>
> El rol de IAM especificado ya debe existir en la cuenta a la que se aplica la política. De lo contrario, el plan de copia de seguridad podrá iniciar correctamente trabajos de copia de seguridad, pero dichos trabajos de copia de seguridad fallarán.

- Especifique una o más Clave de etiqueta de recursos y Valores de etiquetas para identificar los recursos de los que desea realizar una copia de seguridad. Si hay más de un valor de etiqueta, sepárelos con comas.

Seleccionar Agregar una asignación para agregar cada asignación de recursos configurada al plan de copia de seguridad.

Para obtener más información, consulte Asignar recursos a un plan de copia de seguridad en la Guía para desarrolladores AWS Backup .

6. Cuando haya terminado de crear la política, elija Create policy (Crear política). La política aparece en la lista de políticas de copia de seguridad disponibles.

AWS CLI & AWS SDKs

Para crear una política de backup

Puede utilizar uno de los siguientes elementos para crear una política de copia de seguridad:

- AWS CLI: create-policy

  Cree un plan de copia de seguridad como texto JSON similar al siguiente y guárdela en un archivo de texto. Para obtener reglas completas para la sintaxis, consulte Ejemplos y sintaxis de políticas de copia de seguridad.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII" ] }
                        }
                    }
                }
            }
        }
}
```

Este plan de respaldo especifica que AWS Backup debe hacer una copia de seguridad de todos los recursos de los afectados Cuentas de AWS que se encuentran en el especificado Regiones de AWS y que tienen la etiqueta `dataType` con un valor de`PII`.

A continuación, importe el archivo de política JSON del plan de copia de seguridad para crear una nueva política de copia de seguridad en la organización. Anote el ID de política que viene al final del ARN de política en el resultado.

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
}
```

- AWS SDKs: CreatePolicy

Creación de una política de etiquetas

> **Permisos mínimos**
>
> Para crear las políticas de etiquetas, necesita permiso para ejecutar la siguiente acción:
>
> - `organizations:CreatePolicy`

Puede crear una política de etiquetas AWS Management Console de dos maneras:

- Un editor visual que le permite elegir opciones y generar el texto de la política JSON automáticamente.
- Un editor de texto que le permite crear directamente el texto de la política JSON usted mismo.

El editor visual facilita el proceso, pero limita su flexibilidad. Es una excelente manera de crear sus primeras políticas y sentirse cómodo al usarlas. Cuando comprenda cómo funcionan y haya comenzado a verse limitado por lo que ofrece el editor visual, puede añadir características avanzadas a sus políticas editando el texto de la política JSON usted mismo. El editor visual utiliza solo el operador de configuración de valores @@assign y no proporciona ningún acceso a los operadores de control secundarios. Solo puede agregar los operadores de control infantil si edita manualmente el texto de la política JSON.

AWS Management Console

Puede crear una política de etiquetas AWS Management Console de dos maneras:

- Un editor visual que le permite elegir opciones y generar el texto de la política JSON automáticamente.
- Un editor de texto que le permite crear directamente el texto de la política JSON usted mismo.

El editor visual facilita el proceso, pero limita su flexibilidad. Es una excelente manera de crear sus primeras políticas y sentirse cómodo al usarlas. Cuando comprenda cómo funcionan y haya comenzado a verse limitado por lo que ofrece el editor visual, puede añadir características avanzadas a sus políticas editando el texto de la política JSON usted mismo. El editor visual utiliza solo el operador de configuración de valores @@assign y no proporciona ningún acceso a los operadores de control secundarios. Solo puede agregar los operadores de control infantil si edita manualmente el texto de la política JSON.

Para crear una política de etiquetas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Tag policies (Políticas de etiquetas), seleccione Create policy (Crear política).
3. En la página Create policy (Crear política), introduzca un Policy name (Nombre de política) y una Description (Descripción) opcional para la política.

4. (Opcional) Puede agregar una o varias etiquetas al objeto de la política en sí. Estas etiquetas no forman parte de la política. Para ello, elija Agregar etiqueta y, a continuación, ingrese una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información, consulte Recursos de etiquetado AWS Organizations.
5. Puede crear la política de etiquetas mediante el Visual editor (Editor visual) como se describe en este procedimiento. También puede escribir o pegar una política de etiquetas en la pestaña JSON. Para obtener información acerca de la sintaxis de políticas de etiquetas, consulte Sintaxis de la política de etiquetas.

   Si decide utilizar el editor visual, especifique lo siguiente:
6. En Nueva clave de etiqueta 1, especifique el nombre de la clave de etiqueta que desea agregar.
7. En Opciones de cumplimiento, puede seleccionar las siguientes opciones:

   a. Use las mayúsculas que especificó anteriormente para la clave de la etiqueta: deje esta opción desactivada (la opción predeterminada) para especificar que la política de etiquetas principal heredada, si existiera, debe definir el tratamiento de las mayúsculas y minúsculas en la clave de etiqueta.

      Habilite esta opción si desea asignar un uso específico de las mayúsculas en la clave de etiqueta mediante esta política. Si selecciona esta opción, el uso de mayúsculas que haya especificado en Tag Key (Clave de etiqueta) anula el tratamiento de las mayúsculas y minúsculas especificado en una política principal heredada.

      Si no existe ninguna política principal y no se habilita esta opción, solo las claves de etiqueta con todos los caracteres en minúscula se consideran conformes. Para obtener más información acerca de la herencia de políticas principales, consulte Descripción de la herencia de políticas de administración.

      > **Tip**
      >
      > Tenga en cuenta el uso de la política de etiquetas de ejemplo que se muestra en Ejemplo 1: Definir las mayúsculas y minúsculas de la clave de etiquetas en toda la organización como guía para crear una política de etiquetas que defina las claves de etiqueta y su tratamiento de las mayúsculas y minúsculas. Asóciela a la raíz

de la organización. Más adelante, puede crear y adjuntar políticas de etiquetas adicionales a OUs nuestras cuentas para crear reglas de etiquetado adicionales.

b. Especifique los valores permitidos para la clave de esta etiqueta: habilite esta opción si desea agregar valores permitidos a esta clave de etiqueta a cualquier valor heredado de una política principal.

   De forma predeterminada, esta opción está desactivada, lo que significa que solo se consideran conformes esos valores definidos y heredados de una política principal. Si no existe ninguna política principal y no especifica valores de etiqueta, entonces cualquier valor (incluso la ausencia de valores) se considera conforme.

   Para actualizar la lista de valores de etiqueta aceptables, seleccione Specify allowed values for this tag key (Especificar los valores permitidos en esta clave de etiqueta) y, a continuación, elija Specify values (Especificar valores). Cuando se le soliciten, introduzca los nuevos valores (un valor por casillero) y elija Save changes (Guardar cambios).

8. En Tipos de recursos que aplicar, puede seleccionar Evitar las operaciones no conformes para esta etiqueta.

   Recomendamos que deje esta opción desactivada (la opción predeterminada) a menos que tenga experiencia con el uso de políticas de etiquetas. Asegúrese de haber revisado las recomendaciones en Descripción de la aplicación de políticas y evaluar minuciosamente. De lo contrario, podría impedir que los usuarios de las cuentas de su organización etiqueten los recursos que necesiten.

   Si desea ejecutar la conformidad con esta clave de etiqueta, seleccione la casilla de verificación y, a continuación, Especificar los tipos de recursos. Cuando se le solicite, seleccione los tipos de recursos que desea incluir en la política. A continuación, elija Guardar cambios.

   > **Important**
   >
   > Al seleccionar esta opción, cualquier operación que manipule etiquetas para recursos de los tipos especificados tendrá éxito solo si la operación da como resultado etiquetas que cumplan con la política.

9. (Opcional) Para agregar otra clave de etiqueta a esta política de etiquetas, elija Add tag key (Agregar clave de etiqueta). A continuación, realice los pasos 6-9 para definir la clave de etiqueta.
10. Cuando haya terminado de crear la política de etiquetas, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para crear una política de etiquetas

Puede utilizar una de las siguientes opciones para crear una política de etiquetas:

- AWS CLI: create-policy

  Puede utilizar cualquier editor de texto para crear una política de etiquetas. Utilice la sintaxis de JSON y guarde la política de etiquetas como un archivo con cualquier nombre y extensión en una ubicación que desee. Las políticas de etiquetas pueden tener un máximo de 2500 caracteres, espacios incluidos. Para obtener información acerca de la sintaxis de políticas de etiquetas, consulte Sintaxis de la política de etiquetas.

  Para crear una política de etiquetas

  1. Cree una política de etiquetas en un archivo de texto que tenga un aspecto similar a la siguiente:

     Contenido de `testpolicy.json`:

     ```
     {
         "tags": {
             "CostCenter": {
                 "tag_key": {
                     "@@assign": "CostCenter"
                 }
             }
         }
     }
     ```

     Esta política de etiquetas define la clave de la etiqueta `CostCenter`. La etiqueta puede aceptar cualquier valor o no tener ninguno. Una política como esta significa que un recurso al que se le ha adjuntado la CostCenter etiqueta con o sin un valor es compatible.

2. Cree una política que contenga el contenido de la política del archivo. Se ha truncado el espacio en blanco adicional en la salida para legibilidad.

```
$ aws organizations create-policy \
    --name "MyTestTagPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type TAG_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

- AWS SDKs: CreatePolicy

Creación de una política de chatbot

> **Permisos mínimos**
>
> Para crear una política de chatbot, necesita permiso para poner en marcha la siguiente acción:
>
> - `organizations:CreatePolicy`

AWS Management Console

Puedes crear una política de chatbot AWS Management Console de dos maneras:

- Un editor visual que le permite elegir opciones y generar el texto de la política JSON automáticamente.
- Un editor de texto que le permite crear directamente el texto de la política JSON usted mismo.

El editor visual facilita el proceso, pero limita su flexibilidad. Es una excelente manera de crear sus primeras políticas y sentirse cómodo al usarlas. Cuando comprenda cómo funcionan y haya comenzado a verse limitado por lo que ofrece el editor visual, puede añadir características avanzadas a sus políticas editando el texto de la política JSON usted mismo. El editor visual utiliza solo el operador de configuración de valores @@assign y no proporciona ningún acceso a los operadores de control secundarios. Solo puede agregar los operadores de control infantil si edita manualmente el texto de la política JSON.

Para crear una política de chatbot

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de chatbot, seleccione Crear una política.
3. En la página Crear una nueva política de chatbot, ingrese un Nombre de política y una Descripción opcional para la política.
4. (Opcional) Puede agregar una o varias etiquetas a la política seleccionando Agregar etiqueta y a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información, consulte Recursos de etiquetado AWS Organizations.
5. Puede crear la política mediante el Visual editor (Editor visual) como se describe en este procedimiento. También puede ingresar o pegar texto de política en la pestaña JSON. Para obtener información acerca de la sintaxis de políticas de chatbot, consulte Ejemplos y sintaxis de políticas de chatbots.

   Si elige usar el editor visual, configure su política de chatbot especificando los controles de acceso para los clientes de chat.

   a. Elija una de las siguientes opciones en Configurar el acceso al cliente de chat de Amazon Chime
      - Denegar el acceso a Chime.
      - Permitir el acceso a Chime.

b. Seleccione una de las siguientes opciones en Configurar el acceso al cliente de chat de Microsoft Teams

- Denegar el acceso a todos los equipos
- Permitir el acceso a todos los usuarios
- Restringir el acceso a equipos concretos

c. Elija una de las siguientes opciones en Configurar el acceso al cliente de chat de Slack

- Denegar el acceso a todos los espacios de trabajo de Slack
- Permitir el acceso a todos los espacios de trabajo de Slack
- Restringir el acceso a espacios de trabajo de Slack concretos

> **Note**
>
> Además, puedes seleccionar Limitar el AWS Chatbot uso solo a los canales privados de Slack.

d. Seleccione las siguientes opciones en Definir los tipos de permisos de IAM

- Habilitar el rol de IAM de canal: todos los miembros del canal comparten los permisos del rol de IAM para poner en marcha tareas en un canal. Un rol de canal es adecuado si los miembros del canal requieren los mismos permisos.
- Habilitar el rol de IAM de usuario: los miembros del canal deben elegir un rol de usuario de IAM para llevar a cabo las acciones (es necesario acceder a la consola para elegir los roles). Los roles de usuario son adecuados si los miembros del canal requieren permisos diferentes y pueden elegir sus roles de usuario.

6. Cuando haya terminado de crear la política, elija Create policy (Crear política). La política aparece en la lista de políticas de copia de seguridad de chatbot.

AWS CLI & AWS SDKs

Para crear una política de chatbot

Puede utilizar una de las siguientes opciones para crear una política de chatbot:

- AWS CLI: create-policy

Puede utilizar cualquier editor de texto para crear una política de chatbot. Utilice la sintaxis de JSON y guarde la política de chatbot como un archivo con cualquier nombre y extensión en

una ubicación que desee. Las políticas de chatbot pueden tener un máximo de ? caracteres, espacios incluidos. Para obtener información acerca de la sintaxis de políticas de etiquetas, consulte Ejemplos y sintaxis de políticas de chatbots.

Para crear una política de chatbot

1. Cree una política de chatbot en un archivo de texto que tenga un aspecto similar al siguiente:

   Contenido de `testpolicy.json`:

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
                  ]
               }
            }
         },
         "microsoft_teams": {
            "client": {
               "@@assign": "disabled"
            }
         }
      }
   }
}
```

   Esta política de chatbot solo permite los canales privados de Slack en un espacio de trabajo específico, desactiva Microsoft Teams y admite todos los ajustes de roles.

2. Cree una política que contenga el contenido de la política del archivo. Se ha truncado el espacio en blanco adicional en la salida para legibilidad.

```
$ aws organizations create-policy \
    --name "MyTestChatbotPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type CHATBOT_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-a1b2c3d4e5",
            "Name": "MyTestChatbotPolicy",
            "Description": "My Test policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-
Id"]},"supported_channel_types":{"@@assign":["private"]}},"microsoft_teams":
{"client":{"@@assign":"disabled"}}}}}"
    }
}
```

- AWS SDKs: CreatePolicy

Creación de una política de exclusión de servicios de IA

> **Permisos mínimos**
>
> Para crear una política de exclusión de servicios de IA, necesita permiso para ejecutar la siguiente acción:
>
> - `organizations:CreatePolicy`

AWS Management Console

Para crear una política de exclusión de servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de exclusión de servicios de IA, seleccione Create policy (Crear política).
3. En la página Crear nueva política de exclusión de servicios de IA, introduzca un Nombre de política y una Descripción opcional para la política.
4. (Opcional) Puede agregar una o varias etiquetas a la política seleccionando Agregar etiqueta y a continuación, introduzca una clave y un valor opcional. Dejar el valor en blanco lo establece en una cadena vacía; no es `null`. Puede adjuntar hasta 50 etiquetas a una política. Para obtener más información, consulte Recursos de etiquetado AWS Organizations.
5. Ingrese o pegue el texto de la política en la pestaña JSON. Para obtener información acerca de la sintaxis de política de exclusión de servicios de IA, consulte Sintaxis y ejemplos de políticas de exclusión de servicios de IA. Para ver las políticas de ejemplo que puede utilizar como punto de partida, consulte Ejemplos de políticas de exclusión de servicios de IA.
6. Cuando haya terminado de editar la política, elija Crear política en la esquina inferior derecha de la página.

AWS CLI & AWS SDKs

Para crear una política de exclusión de servicios de IA

Puede utilizar una de las siguientes opciones para crear una política de etiquetas:

- AWS CLI: create-policy

1. Cree una política de exclusión de servicios de IA como la siguiente y guárdela en un archivo de texto. Tenga en cuenta que "`optOut`" y "`optIn`" distinguen entre mayúsculas y minúsculas.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
```

```
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Esta política de exclusión de servicios de IA especifica que todas las cuentas afectadas por la política se excluyen de todos los servicios de IA excepto Amazon Rekognition.

2. Importe el archivo de política JSON para crear una nueva política en la organización. En este ejemplo, el archivo JSON anterior se denominó `policy.json`.

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
    }
}
```

- AWS SDKs: CreatePolicy

Actualización de las políticas de la organización con AWS Organizations

Cuando cambien los requisitos de su política, puede actualizar una política existente.

En este tema se describe cómo actualizar las políticas con AWS Organizations. Una política define los controles que se desean aplicar a un grupo de ellos Cuentas de AWS.

Temas

- Actualización de una política de control de servicio (SCP)
- Actualice una política de control de recursos (RCP)
- Actualice una política declarativa
- Actualización de una política de copias de seguridad
- Actualización de una política de etiquetas
- Actualización de una política de chatbot
- Actualización de una política de exclusión de servicios de IA

Actualización de una política de control de servicio (SCP)

Puede cambiar el nombre o cambiar el contenido de una política iniciando sesión en la cuenta de administración de su organización. El cambio de contenido de una SCP afecta inmediatamente a los usuarios, grupos y roles de todas las cuentas asociadas.

Permisos mínimos

Para actualizar una SCP, necesita permiso para ejecutar las siguientes acciones:

- `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")
- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para actualizar una política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, elija el nombre de la política que desea actualizar.
3. En la página de detalles de la política, elija Editar política.
4. Realice una de las siguientes modificaciones, o todas:
   - Puede cambiar el nombre de la política introduciendo un nuevo nombre en Nombre de la política.
   - Puede cambiar la descripción ingresando texto nuevo en Policy description (Descripción de la política).
   - Puede editar el texto de la política editando la política en formato JSON en el panel izquierdo. O bien, puede elegir una declaración en el editor de la derecha y modificar sus elementos utilizando los controles. Para obtener más detalles acerca de cada control, consulte la Creación de un procedimiento SCP que se muestra anteriormente en este tema.
5. Cuando haya finalizado, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política

Puede utilizar uno de los comandos siguientes para actualizar una política:

- AWS CLI: update-policy

  En el siguiente ejemplo se cambia el nombre de una política.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
```

```
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

En el ejemplo siguiente se agrega o cambia la descripción de una política de control de servicios.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

En el ejemplo siguiente se cambia el documento de política del SCP especificando un archivo que contiene el nuevo texto de política JSON.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
```

```
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

Actualice una política de control de recursos (RCP)

Puede cambiar el nombre o cambiar el contenido de una política iniciando sesión en la cuenta de administración de su organización. Cambiar el contenido de un RCP afecta inmediatamente a los recursos de todas las cuentas asociadas.

Permisos mínimos

Para actualizar un RCP, necesita permiso para ejecutar las siguientes acciones:

- `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")
- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para actualizar una política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página de la política de control de recursos, elija el nombre de la política que desee actualizar.
3. En la página de detalles de la política, elija Editar política.
4. Realice una de las siguientes modificaciones, o todas:
   - Puede cambiar el nombre de la política introduciendo un nuevo nombre en Nombre de la política.
   - Puede cambiar la descripción ingresando texto nuevo en Policy description (Descripción de la política).
   - Puede editar el texto de la política editando la política en formato JSON en el panel izquierdo. O bien, puede elegir una declaración en el editor de la derecha y modificar sus elementos utilizando los controles. Para obtener más información sobre cada control, consulte el procedimiento de creación de un RCP que aparece anteriormente en este tema.
5. Cuando haya finalizado, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política

Puede utilizar uno de los comandos siguientes para actualizar una política:

- AWS CLI: update-policy

  En el siguiente ejemplo se cambia el nombre de una política.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
```

```
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

El siguiente ejemplo agrega o cambia la descripción de una política de control de recursos.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

En el siguiente ejemplo, se cambia el documento de política del RCP especificando un archivo que contiene el nuevo texto de la política de JSON.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
```

```
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDKs: UpdatePolicy

Actualice una política declarativa

> **Permisos mínimos**
>
> Para actualizar una política declarativa, debe tener permiso para ejecutar las siguientes acciones:
>
> - `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")
> - `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el Nombre de recurso de Amazon (ARN) de la política especificada (o "*")

AWS Management Console

Para actualizar una política declarativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas declarativas, elija el nombre de la política que desee actualizar.

3. En la página de detalles de la política, elija Editar política.
4. Puede introducir un nuevo Nombre de la política, Descripción de la política o editar el texto de la política JSON. Para obtener información sobre la sintaxis de la política declarativa, consulte. Sintaxis y ejemplos de políticas declarativas
5. Cuando haya terminado de actualizar la política, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política

Puede utilizar uno de los comandos siguientes para actualizar una política:

- AWS CLI: update-policy

  En el siguiente ejemplo, se cambia el nombre de una política declarativa.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2-configuration":{"ec2_attributes":
{"image_block_public_access":{"state":{"@@assign":"block_new_sharing"}}}}".
    }
}
```

  El siguiente ejemplo agrega o cambia la descripción de una política declarativa.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
```

```
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
    }
}
```

- AWS SDKs: UpdatePolicy

Actualización de una política de copias de seguridad

Cuando inicia sesión en la cuenta de administración de su organización, puede editar una política que requiera cambios en la organización.

Permisos mínimos

Para actualizar una política de copia de seguridad, debe tener permiso para ejecutar las siguientes acciones:

- `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política que actualizar (o "*")
- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política que actualizar (o "*")

AWS Management Console

Para actualizar una política de copia de seguridad

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Backup policies (Políticas de copia de seguridad), elija el nombre de la política que desea actualizar.
3. Elija Editar política.
4. Puede introducir un nuevo Nombre de la política, Descripción de la política. Puede cambiar el contenido de la política mediante el Visual editor (Editor visual) o editando directamente el JSON.
5. Cuando haya terminado de actualizar la política, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política de copia de seguridad

Puede utilizar uno de los comandos siguientes para actualizar una política de copia de seguridad:

- AWS CLI: update-policy

  En el siguiente ejemplo se cambia el nombre de una política de copia de seguridad

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

  En el siguiente ejemplo se agrega o cambia la descripción de una política de copia de seguridad.

```
$ aws organizations update-policy \
```

```
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

En el ejemplo siguiente se cambia el documento de política JSON adjunto a una política de copia de seguridad. En este ejemplo, el contenido se toma de un archivo llamado `policy.json` con el siguiente texto:

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" },
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
```

```
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" },
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}}"
}
```

- AWS SDKs: UpdatePolicy

Actualización de una política de etiquetas

Permisos mínimos

Para actualizar una política de etiquetas, debe tener permiso para ejecutar las siguientes acciones:

- `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")
- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para actualizar una política de etiquetas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Tag policies (Políticas de etiquetas), elija la política de etiquetas que desea actualizar.
3. Elija Editar política.
4. Puede introducir un nuevo Nombre de la política, Descripción de la política. Puede cambiar el contenido de la política mediante el Editor visual o editando el JSON.
5. Cuando haya terminado de actualizar la política de etiquetas, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política

Puede utilizar uno de los comandos siguientes para actualizar una política:

- AWS CLI: update-policy

  En el siguiente ejemplo se cambia el nombre de una política de etiquetas.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

En el siguiente ejemplo se agrega o cambia la descripción de una política de etiquetas.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

En el ejemplo siguiente se cambia el documento de política JSON adjunto a una política de exclusión de servicio de IA. En este ejemplo, el contenido se toma de un archivo llamado `policy.json` con el siguiente texto:

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- AWS SDKs: UpdatePolicy

Actualización de una política de chatbot

Permisos mínimos

Para actualizar una política de chatbot, debe tener permiso para llevar a cabo las siguientes acciones:

- `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")
- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para actualizar una política de chatbot

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de chatbot, elija la política de chatbot que desee actualizar.
3. Elija Editar política.
4. Puede introducir un nuevo Nombre de la política, Descripción de la política. Puede cambiar el contenido de la política mediante el Editor visual o editando el JSON.
5. Cuando haya terminado de actualizar la política de etiquetas, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política

Puede utilizar uno de los comandos siguientes para actualizar una política:

- AWS CLI: update-policy

  En el siguiente ejemplo se cambia el nombre de una política de chatbot.

```
$ aws organizations update-policy \
```

```
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed chatbot policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-i9j8k7l6m5",
            "Name": "Renamed chatbot policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-Id"]},"default":
{"supported_channel_types":{"@@assign":["private"]}}},"microsoft_teams":{"client":
{"@@assign":"disabled"}}}}}"
    }
}
```

- AWS SDKs: UpdatePolicy

Actualización de una política de exclusión de servicios de IA

> **Permisos mínimos**
>
> Para actualizar una política de exclusión de IA, debe tener permiso para ejecutar las siguientes acciones:
>
> - `organizations:UpdatePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")
> - `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el Nombre de recurso de Amazon (ARN) de la política especificada (o "*")

AWS Management Console

Para actualizar una política de exclusión de servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de exclusión de servicios de IA, elija el nombre de la política que desea actualizar.
3. En la página de detalles de la política, elija Editar política.
4. Puede introducir un nuevo Nombre de la política, Descripción de la política o editar el texto de la política JSON. Para obtener información acerca de la sintaxis de política de exclusión de servicios de IA, consulte Sintaxis y ejemplos de políticas de exclusión de servicios de IA. Para ver las políticas de ejemplo que puede utilizar como punto de partida, consulte Ejemplos de políticas de exclusión de servicios de IA.
5. Cuando haya terminado de actualizar la política, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para actualizar una política

Puede utilizar uno de los comandos siguientes para actualizar una política:

- AWS CLI: update-policy

  En el siguiente ejemplo se cambia el nombre de una política de exclusión de servicios de IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

En el ejemplo siguiente se agrega o cambia la descripción de una política de exclusión de servicios de IA.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

En el ejemplo siguiente se cambia el documento de política JSON adjunto a una política de exclusión de servicio de IA. En este ejemplo, el contenido se toma de un archivo llamado `policy.json` con el siguiente texto:

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
```

```
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n}\n"}
}
```

- AWS SDKs: UpdatePolicy

Edición de etiquetas adjuntas a las políticas de la organización con AWS Organizations

En este tema se describe cómo editar las etiquetas con las que se adjuntan las políticas AWS Organizations. Una política define los controles que se desean aplicar a un grupo de Cuentas de AWS.

Temas

- Edición de etiquetas vinculadas a una política de control de servicio (SCP)
- Edite las etiquetas adjuntas a una política de control de recursos (RCP)

- Edite las etiquetas adjuntas a una política declarativa
- Edición de etiquetas vinculadas a una política de copia de seguridad
- Edición de etiquetas vinculadas a una política de etiquetas
- Edición de etiquetas vinculadas a una política de chatbot
- Edición de etiquetas vinculadas a una política de exclusión de servicios de IA

Edición de etiquetas vinculadas a una política de control de servicio (SCP)

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o quitar las etiquetas adjuntas a una SCP. Para obtener más información acerca del etiquetado, consulte Recursos de etiquetado AWS Organizations.

> **Permisos mínimos**
>
> Para editar las etiquetas adjuntas a una SCP de su organización , debe contar con los permisos siguientes:
>
> - `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
> - `organizations:DescribePolicy`: solo se requiere cuando se utiliza la consola de Organizations
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas asociadas a una SCP

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, elija el nombre de la política con las etiquetas que desea editar.
3. En la página de detalles de la política, elija la pestaña Etiquetas y, a continuación, elija Administrar etiquetas.

4. Realice una de las siguientes modificaciones, o todas:
   - Para cambiar el valor de una etiqueta, ingrese un nuevo valor sobre el antiguo. No se puede modificar directamente la clave de etiqueta. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y, a continuación, agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
5. Cuando haya finalizado, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para editar las etiquetas asociadas a una SCP

Puede utilizar uno de los comandos siguientes para editar las etiquetas adjuntas a una SCP:

- AWS CLI: tag-resource y untag-resource
- AWS SDKs: TagResource y UntagResource

Edite las etiquetas adjuntas a una política de control de recursos (RCP)

Al iniciar sesión en la cuenta de administración de su organización, puede añadir o eliminar las etiquetas adjuntas a un RCP. Para obtener más información acerca del etiquetado, consulte Recursos de etiquetado AWS Organizations.

Permisos mínimos

Para editar las etiquetas adjuntas a un RCP de su AWS organización, debe tener los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:DescribePolicy`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:TagResource`

- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas adjuntas a un RCP

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página de la política de control de recursos, elija el nombre de la política con las etiquetas que desee editar.
3. En la página de detalles de la política, selecciona la pestaña Etiquetas y, a continuación, selecciona Administrar etiquetas.
4. Realice una de las siguientes modificaciones, o todas:
   - Para cambiar el valor de una etiqueta, ingrese un nuevo valor sobre el antiguo. No se puede modificar directamente la clave de etiqueta. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y, a continuación, agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
5. Cuando haya finalizado, elija Save changes (Guardar cambios).

AWS CLI & AWS SDKs

Para editar las etiquetas adjuntas a un RCP

Puede utilizar uno de los siguientes comandos para editar las etiquetas adjuntas a un RCP:

- AWS CLI: tag-resource y untag-resource
- AWS SDKs: TagResource y UntagResource

Edite las etiquetas adjuntas a una política declarativa

Al iniciar sesión en la cuenta de administración de su organización, puede añadir o eliminar las etiquetas adjuntas a una política declarativa. Para obtener más información acerca del etiquetado, consulte Recursos de etiquetado AWS Organizations.

Permisos mínimos

Para editar las etiquetas adjuntas a una política declarativa en su AWS organización, debe tener los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:DescribePolicy`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas adjuntas a una política declarativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página de políticas declarativas, elija el nombre de la política con las etiquetas que desee editar.
3. En la página de detalles elegida de la política, elija la opción Etiquetas y, a continuación, elija Administrar etiquetas.
4. Puede realizar cualquiera de estas acciones en esta página:
   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No puede modificar la clave. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente eligiendo Eliminar.

- Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.

5. Seleccione Guardar los cambios después de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas adjuntas a una política declarativa

Puede utilizar uno de los siguientes comandos para editar las etiquetas adjuntas a una política declarativa:

- AWS CLI: tag-resource y untag-resource
- AWS SDKs: TagResource y UntagResource

Edición de etiquetas vinculadas a una política de copia de seguridad

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o eliminar las etiquetas asociadas a una política de copia de seguridad. Para obtener más información acerca del etiquetado, consulte Recursos de etiquetado AWS Organizations.

Permisos mínimos

Para editar las etiquetas adjuntas a una política de copia de seguridad en su organización , debe contar con los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola: para navegar a la política)
- `organizations:DescribePolicy` (solo consola: para navegar a la política)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas adjuntas a una política de copia de seguridad

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Página de Políticas de copia de seguridad
3. Elija el nombre de la política que tenga las etiquetas que quiere modificar.

   Aparece la página de detalles de la política.
4. En la pestaña Etiquetas, elija Administrar etiquetas.
5. Puede realizar cualquiera de estas acciones en esta página:

   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No puede modificar la clave. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
6. Seleccione Guardar los cambios después de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas adjuntas a una política de copia de seguridad

Puede utilizar uno de los siguientes comandos para editar las etiquetas asociadas a una política de copia de seguridad:

- AWS CLI: tag-resource y untag-resource
- AWS SDKs: TagResource y UntagResource

Edición de etiquetas vinculadas a una política de etiquetas

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o quitar las etiquetas adjuntas a una política de etiquetas. Para ello, siga los pasos que se describen a continuación.

Permisos mínimos

Para editar las etiquetas adjuntas a una política de etiquetas en su organización , debe contar con los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola: para navegar a la política)
- `organizations:DescribePolicy` (solo consola: para navegar a la política)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas asociadas a una política de etiquetas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de etiquetas, elija elegir nombre de la política con las etiquetas que desea editar.
3. En la página de detalles elegida de la política, elija la opción Etiquetas y, a continuación, elija Administrar etiquetas.
4. Puede realizar cualquiera de estas acciones en esta página:
   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No puede modificar la clave. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.

5. Seleccione Guardar los cambios después de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas asociadas a una política de etiquetas

Puede utilizar uno de los comandos siguientes para editar las etiquetas adjuntas a una política de etiquetas:

- AWS CLI: tag-resource y untag-resource
- AWS SDKs: TagResource y UntagResource

Edición de etiquetas vinculadas a una política de chatbot

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o quitar las etiquetas vinculadas a una política de chatbot. Para ello, siga los pasos que se describen a continuación.

Permisos mínimos

Para editar las etiquetas vinculadas a una política de chatbot en su organización, debe contar con los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola: para navegar a la política)
- `organizations:DescribePolicy` (solo consola: para navegar a la política)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas vinculadas a una política de chatbot

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Políticas de chatbot, elija el nombre de la política con las etiquetas que desee editar.
3. En la página de detalles elegida de la política, elija la opción Etiquetas y, a continuación, elija Administrar etiquetas.
4. Puede realizar cualquiera de estas acciones en esta página:
   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No puede modificar la clave. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
5. Seleccione Guardar los cambios después de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas vinculadas a una política de chatbot

Puede utilizar uno de los comandos siguientes para editar las etiquetas vinculadas a una política de chatbot:

- AWS CLI: tag-resource y untag-resource
- AWS SDKs: TagResource y UntagResource

Edición de etiquetas vinculadas a una política de exclusión de servicios de IA

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o quitar las etiquetas adjuntas a una política de exclusión de servicios de IA. Para obtener más información acerca del etiquetado, consulte Recursos de etiquetado AWS Organizations.

> **Permisos mínimos**
>
> Para editar las etiquetas asociadas a una política de exclusión de servicios de IA en su organización de , debe contar con los permisos siguientes:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:DescribePolicy`: solo se requiere cuando se utiliza la consola de Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas adjuntas a una política de exclusión de servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la páginaPolíticas de exclusión de servicios de IA, elija el nombre de la política con las etiquetas que desea editar.
3. En la página de detalles elegida de la política, elija la opción Etiquetas y, a continuación, elija Administrar etiquetas.
4. Puede realizar cualquiera de estas acciones en esta página:
   - Edite el valor de cualquier etiqueta introduciendo un nuevo valor sobre el anterior. No puede modificar la clave. Para cambiar una clave, debe eliminar la etiqueta con la clave anterior y agregar una etiqueta con la nueva clave.
   - Elimine una etiqueta existente eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
5. Seleccione Guardar los cambios después de haber realizado todas las adiciones, eliminaciones y ediciones que desee realizar.

AWS CLI & AWS SDKs

Para editar las etiquetas adjuntas a una política de exclusión de servicios de IA

Puede utilizar uno de los siguientes comandos para editar las etiquetas asociadas a una política de exclusión de servicios de IA:

- AWS CLI: tag-resource y untag-resource
- AWS SDKs: TagResource y UntagResource

Adjuntar las políticas de la organización con AWS Organizations

En este tema se explica cómo vincular políticas con AWS Organizations. Una política define los controles que desea aplicar a un grupo de Cuentas de AWS.

Temas

- Adjunte políticas con AWS Organizations

Adjunte políticas con AWS Organizations

Permisos mínimos

Para vincular políticas, debe tener permiso para poner en marcha la siguiente acción:

- `organizations:AttachPolicy`

Permisos mínimos

Para adjuntar una política de autorización (SCP o RCP) a una raíz, una unidad organizativa o una cuenta, necesita permiso para ejecutar la siguiente acción:

- `organizations:AttachPolicy` con un elemento `Resource` en la misma declaración de política que incluye "*" o el Nombre de recurso de Amazon (ARN) de la política especificada y el ARN del nodo raíz, unidad organizativa o cuenta a la que desea adjuntar la política

AWS Management Console

Service control policies (SCPs)

Puede asociar una SCP navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una SCP navegando hasta el nodo raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, desplácese y luego marque la casilla de verificación situada junto al nodo raíz, unidad organizativa o cuenta a la que desea adjuntar una SCP. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
3. En la pestaña Políticas, en la entrada de Políticas de control de servicios, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de datos adjuntos SCPs de la pestaña Políticas se actualiza para incluir la nueva incorporación. El cambio en la política se hace efectivo de manera inmediata, afectando a los permisos y los roles de los usuarios IAM de la cuenta asociada o de todas las cuentas situadas bajo el nodo raíz o la unidad organizativa.

Para adjuntar una SCP navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios elija el nombre de la política que desea adjuntar.
3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta a la que desea adjuntar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.

5. Elija Asociar política.

   La lista de datos adjuntos SCPs de la pestaña Objetivos se actualiza para incluir la nueva incorporación. El cambio en la política se hace efectivo de manera inmediata, afectando a los permisos y los roles de los usuarios IAM de la cuenta asociada o de todas las cuentas situadas bajo el nodo raíz o la unidad organizativa.

Resource control policies (RCPs)

Para adjuntar un RCP, vaya a la política o a la raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para adjuntar un RCP, vaya a la raíz, la unidad organizativa o la cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la Cuentas de AWSpágina, navegue hasta la raíz, la OU o la cuenta a la que desee adjuntar un RCP y, a continuación, seleccione la casilla de verificación situada junto a ella. Puede que tenga que expandirse OUs (elegir ▶) para encontrar la OU o la cuenta que desee.
3. En la pestaña Políticas, en la entrada de Políticas de control de recursos, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de adjuntos RCPs de la pestaña Políticas se actualiza para incluir la nueva incorporación. El cambio de política entra en vigor inmediatamente y afecta a los permisos de los recursos de la cuenta adjunta o de todas las cuentas de la unidad organizativa o raíz adjunta.

Para adjuntar un RCP, navegue hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página de la política de control de recursos, elija el nombre de la política que desee adjuntar.

3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta a la que desea adjuntar la política. Puede que tenga que ampliar OUs (elegir ▶) para encontrar la OU o la cuenta que desee.
5. Elija Asociar política.

   La lista de datos adjuntos RCPs de la pestaña Objetivos se actualiza para incluir la nueva incorporación. El cambio de política entra en vigor inmediatamente y afecta a los permisos de los recursos de la cuenta adjunta o de todas las cuentas de la unidad organizativa o raíz adjunta.

Declarative policies

Para adjuntar una política declarativa, vaya a la política o a la raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para adjuntar una política declarativa, navegue hasta la raíz, la unidad organizativa o la cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, busque y seleccione el nombre del nodo raíz, unidad organizativa o cuenta a la que desea asociar la política. Puede que tenga que ampliar OUs (elegir ▶) para encontrar la OU o la cuenta que desee.
3. En la pestaña Políticas, en la entrada de Políticas declarativas, seleccione Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de políticas declarativas adjuntas en la pestaña Políticas se actualiza para incluir la nueva incorporación. El cambio en la política surtirá efecto de inmediato.

Para adjuntar una política declarativa, navegue hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Políticas declarativas, elija el nombre de la política que desee adjuntar.
3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta a la que desea adjuntar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
5. Elija Asociar política.

   La lista de políticas declarativas adjuntas en la pestaña Objetivos se actualiza para incluir la nueva incorporación. El cambio en la política surtirá efecto de inmediato.

Backup policies

Puede asociar una política de copia de seguridad navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una política de copia de seguridad navegando hasta el nodo raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, busque y seleccione el nombre del nodo raíz, unidad organizativa o cuenta a la que desea asociar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
3. En la pestaña Políticas, en la entrada de Políticas de copia de seguridad, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de políticas de copia de seguridad asociadas en la pestaña Políticas se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

Para adjuntar una política de copia de seguridad navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Políticas de copia de seguridad elija el nombre de la política que desea adjuntar.
3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta a la que desea adjuntar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
5. Elija Asociar política.

   La lista de políticas de copia de seguridad asociadas en la pestaña Objetivos se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

Tag policies

Puede asociar una política de etiquetas navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una política de etiquetas navegando hasta el nodo raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, busque y seleccione el nombre del nodo raíz, unidad organizativa o cuenta a la que desea asociar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
3. En la pestaña Políticas, en la entrada de Políticas de etiquetas, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de políticas de etiquetas asociadas en la pestaña Políticas se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

Para adjuntar una política de etiquetas navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Políticas de etiquetas, elija el nombre de la política que desea adjuntar.
3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta a la que desea adjuntar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
5. Elija Asociar política.

   La lista de políticas de etiquetas asociadas en la pestaña Objetivos se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

Chatbot policies

Puede asociar una política de etiquetas navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para vincular una política de chatbot navegando hasta el nodo raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, busque y seleccione el nombre del nodo raíz, unidad organizativa o cuenta a la que desea asociar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
3. En la pestaña Políticas, en la entrada de Políticas de chatbot, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de políticas de chatbot asociadas en la pestaña Políticas se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

Para vincular una política de etiquetas navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de chatbot, elija el nombre de la política que desea vincular.

3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta a la que desea adjuntar la política. Puede que tenga que ampliar OUs (elegir ▶) para encontrar la OU o la cuenta que desee.
5. Elija Asociar política.

   La lista de políticas de chatbot vinculadas en la pestaña Objetivos se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

AI services opt-out policies

Puede asociar una política de exclusión de servicios de IA navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una política de exclusión de servicios de IA navegando hasta el nodo raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, busque y seleccione el nombre del nodo raíz, unidad organizativa o cuenta a la que desea asociar la política. Puede que tenga que ampliar OUs (elegir ▶) para encontrar la OU o la cuenta que desee.
3. En la pestaña Políticas, en la entrada de Políticas de exclusión de servicios de IA, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de políticas de exclusión de los servicios de IA adjuntas en la pestaña Políticas se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

Para adjuntar una política de exclusión de servicios de IA navegando hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Políticas de exclusión de servicios de IA, elija el nombre de la política que desea adjuntar.
3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta a la que desea adjuntar la política. Puede que tenga que ampliar OUs (elegir ▶) para encontrar la OU o la cuenta que desee.
5. Elija Asociar política.

   La lista de políticas de exclusión de los servicios de IA adjuntas en la pestaña Objetivos se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para vincular una política

En los siguientes ejemplos de código, se muestra cómo utilizar `AttachPolicy`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información sobre GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
```

```
        /// <summary>
        /// Initializes the Organizations client object and then calls the
        /// AttachPolicyAsync method to attach the policy to the root
        /// organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new AttachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- Para obtener más información sobre la API, consulta AttachPolicyla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Asociación de una política a un nodo raíz, unidad organizativa o cuenta

Ejemplo 1

El siguiente ejemplo de código muestra cómo adjuntar una política de control de servicio (SCP) a una unidad organizativa.

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

Ejemplo 2

El siguiente ejemplo de código muestra cómo adjuntar una política de control de servicio directamente a una cuenta:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- Para obtener más información sobre la API, consulta AttachPolicyla Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
```

```
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- Para obtener más información sobre la API, consulta AttachPolicyla AWS Referencia de API de SDK for Python (Boto3).

El cambio en la política se hace efectivo de manera inmediata, afectando a los permisos y los roles de los usuarios IAM de la cuenta asociada o de todas las cuentas situadas bajo el nodo raíz o la OU.

Separar las políticas de la organización con AWS Organizations

En este tema se explica cómo desvincular políticas con AWS Organizations. Una política define los controles que desea aplicar a un grupo de Cuentas de AWS.

Temas

- Separe las políticas con AWS Organizations

Separe las políticas con AWS Organizations

> **Permisos mínimos**
>
> Para desvincular una política de la raíz de una organización, unidad organizativa o cuenta, debe tener permiso para poner en marcha la siguiente acción:
>
> - `organizations:DetachPolicy`

> **Note**
>
> No puede separar la política de última autorización (SCP o RCP) de una raíz, una unidad organizativa o una cuenta. Debe haber al menos un SCP y un RCP conectados a cada raíz, unidad organizativa y cuenta en todo momento.

AWS Management Console

Service control policies (SCPs)

Puede desconectar una SCP navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee desconectar la política.

Para desconectar una SCP navegando hasta el nodo raíz, unidad organizativa o cuenta a la que está adjunta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar una política. Puede que tenga que ampliar OUs (elegir ▶) para encontrar la OU o la cuenta que desee. Elija el nombre del nodo raíz, unidad organizativa o cuenta.
3. En la pestaña Políticas, elija el botón de opción situado junto a la SCP que desea desconectar y, a continuación, elija Desconectar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   La lista de archivos adjuntos SCPs está actualizada. El cambio de política que se origina al desconectar la SCP entra en vigor inmediatamente. Por ejemplo, cuando se desasocia una SCP, este cambio afecta inmediatamente a los permisos de los usuarios y roles de IAM de la cuenta o cuentas anteriormente asociadas situados bajo el nodo raíz de la organización o unidad organizativa anteriormente asociadas.

Para desconectar una SCP navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, elija el nombre de la política que desea desconectar de un nodo raíz, unidad organizativa o cuenta.
3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
4. Elija Desasociar.
5. En el cuadro de diálogo de confirmación, elija Desconectar.

   La lista de archivos adjuntos SCPs está actualizada. El cambio de política que se origina al desconectar la SCP entra en vigor inmediatamente. Por ejemplo, cuando se desasocia una SCP, este cambio afecta inmediatamente a los permisos de los usuarios y roles de IAM de la cuenta o cuentas anteriormente asociadas situados bajo el nodo raíz de la organización o unidad organizativa anteriormente asociadas.

Resource control policies (RCPs)

Para separar un RCP, vaya a la política o a la raíz, unidad organizativa o cuenta de la que desee desvincular la política. Después de separar un RCP de una entidad, ese RCP ya no se aplica a ningún recurso que se haya visto afectado por la entidad ahora separada.

> **Note**
>
> No se puede separar la política **`RCPFullAWSAccess`**
> La `RCPFullAWSAccess` política se adjunta automáticamente a la raíz, a todas las unidades organizativas y a todas las cuentas de la organización. No puede separar esta política.

Para separar un RCP navegando hasta la raíz, la unidad organizativa o la cuenta a la que está conectado

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar una política. Puede que tenga que expandirse OUs (elegir) para encontrar la OU o la cuenta que desee. Elija el nombre del nodo raíz, unidad organizativa o cuenta.
3. En la pestaña Políticas, elija el botón de radio situado junto al RCP que desee separar y, a continuación, seleccione Separar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   Se actualiza la lista de adjuntos RCPs . El cambio de política provocado por la desvinculación del RCP entra en vigor inmediatamente. Por ejemplo, la desvinculación de un RCP afecta inmediatamente a los permisos de los usuarios y funciones de IAM en la cuenta o cuentas anteriormente asociadas a la organización raíz o unidad organizativa anteriormente asociada.

Para separar un RCP, navegue hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página de la política de control de recursos, elija el nombre de la política que desee separar de una raíz, unidad organizativa o cuenta.
3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
4. Elija Desasociar.
5. En el cuadro de diálogo de confirmación, elija Desconectar.

La lista de archivos adjuntos RCPs está actualizada. El cambio de política provocado por la desvinculación del RCP entra en vigor inmediatamente. Por ejemplo, la desvinculación de un RCP afecta inmediatamente a los permisos de los usuarios y funciones de IAM en la cuenta o cuentas anteriormente asociadas a la organización raíz o unidad organizativa anteriormente asociada.

Declarative policies

Para separar una política declarativa, vaya a la política o a la raíz, unidad organizativa o cuenta de la que desee desvincular la política.

Para separar una política declarativa, navegue hasta la raíz, la unidad organizativa o la cuenta a la que está asociada

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar una política. Puede que tenga que ampliar OUs (elegir ▶) para encontrar la OU o la cuenta que desee. Elija el nombre del nodo raíz, unidad organizativa o cuenta.
3. En la pestaña Políticas, pulse el botón de radio situado junto a la política declarativa que desee separar y, a continuación, seleccione Separar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   Se actualiza la lista de políticas declarativas adjuntas. El cambio en la política surtirá efecto de inmediato.

Para separar una política declarativa, navegue hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página de políticas declarativas, elija el nombre de la política que desee separar de una raíz, unidad organizativa o cuenta.

3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
4. Elija Desasociar.
5. En el cuadro de diálogo de confirmación, elija Desconectar.

   Se actualiza la lista de políticas declarativas adjuntas. El cambio en la política surtirá efecto de inmediato.

Backup policies

Puede desconectar una política de copia de seguridad navegando hasta la política o el nodo raíz, unidad organizativa o cuenta de la que desee desconectar la política.

Para desconectar una política de copia de seguridad navegando hasta el nodo raíz, unidad organizativa o cuenta a la que está adjunta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar una política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee. Elija el nombre del nodo raíz, unidad organizativa o cuenta.
3. En la pestaña Políticas elija el botón de opción situado junto a la política de copia de seguridad que desea desconectar y, a continuación, elija Desconectar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   La lista de políticas de copia de seguridad asociadas se actualiza. El cambio en la política surtirá efecto de inmediato.

Para desconectar una política de copia de seguridad navegando hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de copia de seguridad elija el nombre de la política que desea desconectar de un nodo raíz, unidad organizativa o cuenta.
3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
4. Elija Desasociar.
5. En el cuadro de diálogo de confirmación, elija Desconectar.

   La lista de políticas de copia de seguridad asociadas se actualiza. El cambio en la política surtirá efecto de inmediato.

Tag policies

Puede desconectar una política de etiquetas navegando hasta la política o el nodo raíz, unidad organizativa o cuenta de la que desee desconectar la política.

Para desconectar una política de etiqueta navegando hasta el nodo raíz, unidad organizativa o cuenta a la que está adjunta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar una política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee. Elija el nombre del nodo raíz, unidad organizativa o cuenta.
3. En la pestaña Políticas, elija el botón de opción situado junto a la política de etiquetas que desea desconectar y, a continuación, elija Desconectar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

Actualización de la lista de políticas de etiquetas asociadas. El cambio en la política surtirá efecto de inmediato.

Para desconectar una política de etiquetas navegando hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de etiquetas, elija el nombre de la política que desea desconectar de un nodo raíz, unidad organizativa o cuenta.
3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
4. Elija Desasociar.
5. En el cuadro de diálogo de confirmación, elija Desconectar.

   Actualización de la lista de políticas de etiquetas asociadas. El cambio en la política surtirá efecto de inmediato.

Chatbot policies

Puede desvincular una política de chatbot navegando hasta la política o el nodo raíz, unidad organizativa o cuenta de donde vaya a desvincular la política.

Para desvincular una política de chatbot navegando hasta el nodo raíz, unidad organizativa o cuenta a la que está vinculada

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar una política. Puede que tenga que ampliar OUs (elegir)

para encontrar la OU o la cuenta que desee. Elija el nombre del nodo raíz, unidad organizativa o cuenta.

3. En la pestaña Políticas, elija el botón de opción situado junto a la política de chatbot que desea desvincular y, a continuación, elija Separar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   La lista de políticas de chatbot vinculadas está actualizada. El cambio en la política surtirá efecto de inmediato.

Para desvincular una política de chatbot navegando hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de chatbot, elija el nombre de la política que desea desconectar de un nodo raíz, unidad organizativa o cuenta.
3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar la política. Puede que tenga que ampliar OUs (elegir
   para encontrar la OU o la cuenta que desee.
4. Elija Desasociar.
5. En el cuadro de diálogo de confirmación, elija Desconectar.

   La lista de políticas de chatbot vinculadas está actualizada. El cambio en la política surtirá efecto de inmediato.

AI services opt-out policies

Puede desconectar una política de exclusión de servicios de IA navegando hasta la política o el nodo raíz, unidad organizativa o cuenta de la que desee desconectar la política.

Para desconectar una política de exclusión de servicios de IA navegando hasta el nodo raíz, unidad organizativa o cuenta a la que está adjunta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar una política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee. Elija el nombre del nodo raíz, unidad organizativa o cuenta.
3. En la página Políticas, elija el botón de opción situado junto a la política de exclusión de servicios de IA que desea desconectar y, a continuación, elija Desconectar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   Se actualiza la lista de políticas de exclusión de servicios de IA adjuntas. El cambio en la política surtirá efecto de inmediato.

Para separar una política de exclusión de servicios de IA navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de exclusión de servicios de IA, elija el nombre de la política que desea desconectar de un nodo raíz, unidad organizativa o cuenta.
3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar la política. Puede que tenga que ampliar OUs (elegir) para encontrar la OU o la cuenta que desee.
4. Elija Desasociar.
5. En el cuadro de diálogo de confirmación, elija Desconectar.

   Se actualiza la lista de políticas de exclusión de servicios de IA adjuntas. El cambio en la política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para vincular una política

En los siguientes ejemplos de código, se muestra cómo utilizar `DetachPolicy`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información sobre GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";
        var targetId = "r-0000";

        var request = new DetachPolicyRequest
        {
            PolicyId = policyId,
```

```
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- Para obtener más información sobre la API, consulta DetachPolicyla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Desasociación de una política de un nodo raíz, unidad organizativa o cuenta

En el siguiente ejemplo se muestra cómo desasociar una política de una unidad organizativa:

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- Para obtener más información sobre la API, consulta DetachPolicyla Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- Para obtener más información sobre la API, consulta DetachPolicyla AWS Referencia de API de SDK for Python (Boto3).

El cambio de política entra en vigor de forma inmediata y afecta a los permisos de los usuarios, funciones y recursos de IAM, si procede, en la cuenta asociada o en todas las cuentas de la raíz o la OU adjunta.

Obtener información sobre las políticas de su organización

En este tema se describen varias maneras de obtener información acerca de las políticas de la organización. Estos procedimientos se aplican a todos los tipos de políticas. Debe habilitar un tipo de política en la raíz de la organización antes de poder asociar políticas de ese tipo a cualquier entidad en la raíz de esa organización.

Temas

- Enumeración de todas las políticas
- Mostrar las políticas asociadas a un nodo raíz, unidad organizativa o cuenta
- Listar todas las raíces OUs y cuentas a las que está asociada una política
- Obtener información sobre una política

Enumeración de todas las políticas

> **Permisos mínimos**
>
> Para mostrar las políticas de su organización, debe contar con el permiso siguiente:
>
> - `organizations:ListPolicies`

Puede ver las políticas de su organización en AWS Management Console o mediante un comando AWS Command Line Interface (AWS CLI) o una operación AWS del SDK.

AWS Management Console

Para enumerar todas las políticas de una organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija la política que desea enumerar.

   Si el tipo de política especificado está habilitado, la consola muestra una lista de todas las políticas de ese tipo que están disponibles actualmente en la organización.
3. Vuelva a la página de Políticas y repita para cada tipo de política.

AWS CLI & AWS SDKs

En los siguientes ejemplos de código, se muestra cómo utilizar `ListPolicies`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
            Filter = "SERVICE_CONTROL_POLICY",
```

```
                MaxResults = 5,
            };

            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- Para obtener más información sobre la API, consulta ListPolicieslа Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Recuperación de una lista de todas las políticas de una organización de un tipo determinado

En el siguiente ejemplo, se muestra cómo obtener una lista de SCPs, tal como se especifica en el parámetro de filtro:

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

La salida incluye una lista de políticas con información resumida:

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
```

```
                }
        ]
}
```

- Para obtener más información sobre la API, consulte ListPoliciesla Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- Para obtener más información sobre la API, consulta ListPoliciesla AWS Referencia de API de SDK for Python (Boto3).

Mostrar las políticas asociadas a un nodo raíz, unidad organizativa o cuenta

Permisos mínimos

Para mostrar las políticas que están asociadas a un nodo raíz, unidad organizativa (OU) o cuenta de su organización, debe contar con el permiso siguiente:

- `organizations:ListPoliciesForTarget` con un elemento `Resource` en la misma instrucción de política que incluye el Nombre de recurso de Amazon (ARN) de el objetivo especificado (o "*")

AWS Management Console

Para mostrar todas las políticas que están asociadas directamente a un nodo raíz, unidad organizativa o cuenta específica

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, elija el nombre del nodo raíz, unidad organizativa o cuenta cuyas políticas desea ver. Puede que tenga que ampliar OUs (elegir ▶) para encontrar la unidad organizativa que busca.
3. En la página del nodo raíz, unidad organizativa o cuenta, elija la pestaña Políticas.

   La pestaña Políticas muestra todas las políticas asociadas a ese nodo raíz, unidad organizativa o cuenta, agrupadas por tipo de política.

AWS CLI & AWS SDKs

Para mostrar todas las políticas que están asociadas directamente a un nodo raíz, unidad organizativa o cuenta específica

Puede utilizar uno de los siguientes comandos para enumerar las políticas que están adjuntas a una entidad:

- AWS CLI: list-policies-for-target

En el ejemplo siguiente se enumeran todas las políticas de control de servicios asociadas a la unidad organizativa especificada. Debe especificar tanto el ID del nodo raíz, la unidad organizativa o la cuenta como el tipo de política que desea enumerar.

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDKs: ListPoliciesForTarget

Listar todas las raíces OUs y cuentas a las que está asociada una política

Permisos mínimos

Para mostrar las entidades que tienen asociada una política, debe contar con el permiso siguiente:

- `organizations:ListTargetsForPolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para enumerar todas las raíces y cuentas a las que se ha adjuntado una política específica OUs

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija el tipo de política y, a continuación, elija el nombre de la política cuyos datos adjuntos desea examinar.
3. Elija la pestaña Objetivos, para mostrar una tabla de cada nodo raíz, unidad organizativa y cuenta a la que está asociada la política.

AWS CLI & AWS SDKs

Para enumerar todas las OUs raíces y cuentas que tienen una política específica adjunta

Puede utilizar uno de los siguientes comandos para enumerar entidades que tengan una política:

- AWS CLI: list-targets-for-policy

  El siguiente ejemplo muestra todos los archivos adjuntos a la raíz y las cuentas de la política especificada. OUs

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
```

```
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```

- AWS SDKs: ListTargetsForPolicy

Obtener información sobre una política

Permisos mínimos

Para mostrar los detalles de una política, debe contar con el permiso siguiente:

- `organizations:DescribePolicy` con un elemento `Resource` en la misma instrucción de política que incluye el ARN de la política especificada (o "*")

AWS Management Console

Para obtener información sobre una política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija el tipo de política de la política que desea examinar y, a continuación, elija el nombre de la política.

   La página de la política muestra la información disponible sobre la política, incluido su ARN, descripción y objetivos adjuntos.

- La pestaña de Contenidos muestra el contenido actual de la política en formato JSON.
- La pestaña Objetivos muestra una lista de las raíces y las cuentas a las que está asociada la política. OUs
- La pestaña Etiquetas muestra las etiquetas adjuntas a la política. Nota: la pestaña Etiquetas no está disponible para AWS políticas administradas.

Para editar la política, elija Edit policy (Editar política). Dado que cada tipo de política tiene requisitos de edición diferentes, consulte las instrucciones para crear y actualizar políticas de su tipo de política especificado.

AWS CLI & AWS SDKs

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribePolicy`.

CLI

AWS CLI

Obtención de información acerca de una política

En el siguiente ejemplo se muestra cómo solicitar información acerca de una política:

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

El resultado incluye un objeto de política que contiene detalles acerca de la política:

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
```

```
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- Para obtener más información sobre la API, consulte DescribePolicyla Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- Para obtener más información sobre la API, consulta DescribePolicyla AWS Referencia de API de SDK for Python (Boto3).

Eliminar políticas de la organización con AWS Organizations

Cuando ya no necesites una política y después de separarla de todas las unidades organizativas (OUs) y cuentas, podrás eliminarla.

En este tema se describe cómo eliminar políticas con AWS Organizations. Una política define los controles que desea aplicar a un grupo de Cuentas de AWS.

Temas

- Elimine las políticas con AWS Organizations

Elimine las políticas con AWS Organizations

Cuando inicia sesión en la cuenta de administración de su organización, puede eliminar una política que ya no necesite en su organización.

Para poder eliminar una política, primero debe desconectarla de todas las entidades asociadas.

> **Note**
>
> - No puede eliminar ningún SCP AWS administrado, como el SCP mencionado. `FullAWSAccess`
> - No puede eliminar ningún RCP AWS administrado, como el RCP mencionado. `RCPFullAWSAccess`

> **Permisos mínimos**
>
> Para eliminar una SCP, necesita permiso para poner en marcha la siguiente acción:
>
> - `organizations:DeletePolicy`

AWS Management Console

Service control policies (SCPs)

Para eliminar SCP

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, elija el nombre de la SCP que desea eliminar.
3. Primero debe separar la política que desea eliminar de todas las raíces y cuentas OUs. Elija el icono Implementación, elija el botón de opción situado junto a cada nodo raíz, OU o cuenta que se muestra en la lista Implementación y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.
4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

Resource control policies (RCPs)

Para eliminar un RCP

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de recursos, elija el nombre del RCP que desee eliminar.
3. Primero debe separar la política que desea eliminar de todas las raíces y OUs cuentas. Elija el icono Implementación, elija el botón de opción situado junto a cada nodo raíz, OU o cuenta que se muestra en la lista Implementación y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.
4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

Declarative policies

Para eliminar una política declarativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas declarativas, elija el nombre de la política que desee eliminar.
3. Primero debe separar la política que desea eliminar de todas las raíces y OUs cuentas. Elija el icono Implementación, elija el botón de opción situado junto a cada nodo raíz, OU o cuenta que se muestra en la lista Implementación y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.
4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

Backup policies

Para eliminar una política de copia de seguridad

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Tag policies (Políticas de copia de seguridad), elija el nombre de la política de copia de seguridad que desea eliminar.
3. Primero debe separar la política de copias de seguridad que desee eliminar de todas las raíces y OUs cuentas. Elija el icono Implementación, elija el botón de opción situado junto a cada nodo raíz, OU o cuenta que se muestra en la lista Implementación y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.
4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

Tag policies

Para eliminar una política de etiquetas

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Etiquetar políticas, elija la política que desee eliminar.
3. Primero debe separar la política que desea eliminar de todas las raíces y cuentas. OUs Elija la pestaña Objetivos, elija el botón de opción situado junto a cada nodo raíz, unidad organizativa o cuenta que se muestra en la lista de Objetivos y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.
4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

Chatbot policies

Para eliminar una política de chatbot

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de chatbot, elija el nombre de la política que desea eliminar.
3. Primero debe separar la política que desea eliminar de todas las raíces y OUs cuentas. Elija el icono Implementación, elija el botón de opción situado junto a cada nodo raíz, OU o cuenta que se muestra en la lista Implementación y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.
4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

AI services opt-out policies

Para eliminar una política de exclusión de servicios de IA

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de exclusión de servicios de IA, elija el nombre de la política que desea eliminar.
3. Primero debe separar la política que desea eliminar de todas las raíces y OUs cuentas. Elija el icono Implementación, elija el botón de opción situado junto a cada nodo raíz, OU o cuenta que se muestra en la lista Implementación y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.
4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

AWS CLI & AWS SDKs

Para eliminar una política

En los siguientes ejemplos de código, se muestra cómo utilizar `DeletePolicy`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
```

```
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully deleted Policy: {policyId}.");
        }
        else
        {
            Console.WriteLine($"Could not delete Policy: {policyId}.");
        }
    }
}
```

- Para obtener más información sobre la API, consulta DeletePolicyla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Eliminación de una política

En el siguiente ejemplo se muestra cómo eliminar una política de una organización. En el ejemplo se asume que anteriormente se ha desvinculado la política de todas las entidades:

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- Para obtener más información sobre la API, consulta DeletePolicyla Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- Para obtener más información sobre la API, consulta DeletePolicyla AWS Referencia de API de SDK for Python (Boto3).

Recursos de etiquetado AWS Organizations

Una etiqueta es una etiqueta de atributo personalizada que se agrega a un AWS recurso para facilitar la identificación, la organización y la búsqueda de recursos. Cada etiqueta tiene dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta pueden tener 128 caracteres como máximo y distingue entre mayúsculas y minúsculas.
- Un valor de etiqueta (por ejemplo, `111122223333` o `Production`). Los valores de etiqueta pueden tener una longitud de hasta 256 caracteres y, al igual que las claves de etiqueta, distinguen mayúsculas y minúsculas. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Omitir el valor de etiqueta es lo mismo que utilizar una cadena vacía.

Para obtener más información acerca de los caracteres permitidos en una clave o valor de etiqueta, consulte la sección Parámetro de etiquetas de la API de etiquetas en la Referencia de la API de etiquetado para Resource Groups.

Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Para obtener más información, consulte Prácticas recomendadas para etiquetar AWS recursos.

> **Tip**
>
> Use las políticas de etiquetas para ayudar a estandarizar su implementación de las etiquetas en todos los recursos en las cuentas de su organización.

Temas

- Consideraciones
- Uso de etiquetas
- Agregar, actualizar y quitar etiquetas

Consideraciones

AWS Organizations admite las siguientes operaciones de etiquetado cuando se inicia sesión en la cuenta de administración:

Puede agregar etiquetas a los siguientes tipos de recursos de la organización

- Cuentas de AWS
- Unidades organizativas
- Nodo raíz de la organización
- Políticas

Puede agregar etiquetas en los siguientes momentos

- Al crear el recurso: especifique las etiquetas en la consola Organizations o utilice el parámetro `Tags` con una de las operaciones de la API de `Create`. Esto no es aplicable al nodo raíz de la organización.
- Después de crear el recurso — Utilice la consola Organizations o llame a la operación `TagResource`.

Otras consideraciones

Puede ver las etiquetas de cualquiera de los recursos que se pueden etiquetar AWS Organizations mediante la consola o mediante una llamada a la `ListTagsForResource` operación.

Puede eliminar etiquetas de un recurso especificando las claves que desea eliminar mediante la consola o llamando a la operación `UntagResource`.

Uso de etiquetas

Las etiquetas le ayudan a organizar los recursos en su organización, al permitirle agruparlos según las categorías que le sean útiles. Por ejemplo, puede asignar una etiqueta “Departamento” que realice el seguimiento del departamento propietario. Puede asignar una etiqueta “Entorno” para rastrear si un recurso determinado forma parte de sus entornos alfa, beta, gamma o producción.

Puede usar etiquetas para lo siguiente:

- Imponer estándares de etiquetado en sus recursos.
- Controlar el acceso a los recursos.

Agregar, actualizar y quitar etiquetas

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar las etiquetas adjuntas a los recursos en su organización.

Adición de etiquetas a un recurso cuando lo crea

> **Permisos mínimos**
>
> Para agregar etiquetas a un recurso cuando lo crea, debe tener los siguientes permisos:
>
> - Permiso para crear un recurso del tipo especificado
> - `organizations:TagResource`
> - `organizations:ListTagsForResource`: solo se requiere cuando se utiliza la consola de Organizations

Puede incluir claves y valores de etiqueta asociados a los siguientes recursos a medida que los crea.

- Cuenta de AWS
  - Cuenta creada
  - Cuenta invitada
- Unidad organizativa (OU)
- Política
  - Política de control de servicios
  - Política de control de recursos
  - Política declarativa
  - Política de copia de seguridad
  - Política de etiquetas
  - Política de chatbot
  - Política de exclusión de servicios de IA

El nodo raíz de la organización se genera al crear inicialmente la organización, por lo que solo puede agregarle etiquetas como un recurso existente.

Adición o actualización de etiquetas en un recurso existente

También puede agregar nuevas etiquetas o actualizar los valores de las etiquetas asociadas a recursos existentes.

Permisos mínimos

Para agregar o actualizar etiquetas a los recursos de su organización, necesita los siguientes permisos:

- `organizations:TagResource`
- `organizations:ListTagsForResource`: solo se requiere cuando se utiliza la consola de Organizations

Para quitar etiquetas de los recursos de su organización, necesita los siguientes permisos:

- `organizations:UntagResource`

AWS Management Console

Para agregar, actualizar o quitar etiquetas para un recurso existente

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Desplácese hasta la cuenta, nodo raíz, unidad organizativa o política y haga clic en su nombre para abrir su página de detalles.
3. En la pestaña Etiquetas, elija Administrar etiquetas.
4. Puede agregar nuevas etiquetas, modificar los valores de etiquetas existentes o quitar etiquetas.

   Para agregar una etiqueta, elija Add Tag (Agregar etiqueta) y, a continuación, ingrese la Clave y el Valor de la etiqueta.

   Para eliminar una etiqueta, elija Eliminar.

Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Utilice el uso de mayúsculas que desee definir como estándar. También debe cumplir con los requisitos de las políticas de etiquetas que se apliquen.

5. Repita el paso anterior tantas veces como necesite.
6. Elija Guardar cambios.

AWS CLI & AWS SDKs

Para agregar o actualizar etiquetas a un recurso existente

Puede utilizar uno de los siguientes comandos para agregar etiquetas a los recursos etiquetables de su organización:

- AWS CLI: tag-resource
- AWS SDKs: TagResource

Para eliminar etiquetas de un recurso de la organización

Puede utilizar uno de los siguientes comandos para eliminar etiquetas:

- AWS CLI: untag-resource
- AWS SDKs: UntagResource

Uso AWS Organizations con otros Servicios de AWS

Puede usar el acceso de confianza para habilitar un AWS servicio compatible que especifique, denominado servicio de confianza, para realizar tareas en su organización y sus cuentas en su nombre. Esto implica conceder permisos al servicio de confianza, pero no afecta de ninguna otra manera a los permisos de los usuarios o roles. Cuando se habilita el acceso, el servicio de confianza puede crear un rol de IAM denominado rol vinculado al servicio en cada cuenta de la organización. Este rol tiene una política de permisos que permite al servicio de confianza realizar las tareas que se describen en la documentación del servicio. Esto le permite especificar las opciones y los detalles de configuración que desea que el servicio de confianza mantenga en las cuentas de la organización en su nombre. El servicio de confianza solo crea roles vinculados al servicio cuando necesita realizar acciones de administración en cuentas, y no necesariamente en todas las cuentas de la organización.

Important

Recomendamos encarecidamente que, cuando la opción esté disponible, habilite y deshabilite el acceso de confianza utilizando únicamente la consola del servicio de confianza AWS CLI o sus equivalentes API operativos. Esto permite al servicio de confianza realizar cualquier inicialización necesaria al habilitar el acceso de confianza, como la creación de los recursos necesarios y la limpieza necesaria de los recursos al deshabilitar el acceso de confianza.

Para obtener información acerca de cómo habilitar o deshabilitar el acceso a servicios de confianza a su organización mediante el servicio de confianza, consulte el vínculo Más información en la columna Admite el acceso de confianza en Servicios de AWS que puedes usar con AWS Organizations.

Si deshabilita el acceso mediante la consola, CLI los comandos o API las operaciones de Organizations, se producen las siguientes acciones:

- El servicio ya no puede crear un rol vinculado a un servicio en las cuentas de su organización. Esto significa que el servicio no puede realizar operaciones en su nombre en ninguna cuenta nueva de su organización. El servicio aún puede realizar operaciones en cuentas antiguas hasta que el servicio complete su limpieza desde AWS Organizations.
- El servicio ya no puede realizar tareas en las cuentas de los miembros de la organización, a menos que esas operaciones estén explícitamente permitidas por las IAM políticas asociadas a tus funciones. Esto incluye cualquier agregación de datos de las cuentas de

miembro a la cuenta de administración o a una cuenta de administrador delegada, cuando proceda.

- Algunos servicios detectan esto y limpian los datos o recursos restantes relacionados con la integración, mientras que otros servicios dejan de acceder a la organización pero dejan los datos históricos y la configuración para permitir una posible reactivación de la integración.

En su lugar, el uso de la consola o los comandos del otro servicio para deshabilitar la integración garantiza que el otro servicio pueda limpiar los recursos necesarios solo para la integración. La forma en que el servicio limpia sus recursos en las cuentas de la organización depende de ese servicio. Para obtener más información, consulte la documentación del otro servicio de AWS .

Permisos necesarios para habilitar el acceso de confianza

El acceso confiable requiere permisos para dos servicios: AWS Organizations y el servicio confiable. Para habilitar el acceso de confianza, elija uno de los escenarios siguientes:

- Si tiene credenciales con permisos tanto AWS Organizations en el servicio de confianza como en el servicio de confianza, habilite el acceso mediante las herramientas (consola o AWS CLI) que proporciona el servicio de confianza. Esto permite que el servicio habilite el acceso confiable AWS Organizations en su nombre y cree los recursos necesarios para que el servicio funcione en su organización.

  Los permisos mínimos para estas credenciales son los siguientes:

  - `organizations:EnableAWSServiceAccess`. También puede utilizar la clave de condición `organizations:ServicePrincipal` con esta operación para limitar las solicitudes que esas operaciones realizan a una lista de nombres de principal de servicio aprobados. Para obtener más información, consulte Claves de condición.
  - `organizations:ListAWSServiceAccessForOrganization`— Necesario si utiliza la AWS Organizations consola.
  - Los permisos mínimos necesarios que requiere el servicio de confianza dependen del servicio. Para obtener más información, consulte la documentación del servicio de confianza.
- Si una persona tiene credenciales con permisos AWS Organizations pero otra tiene credenciales con permisos en el servicio de confianza, lleve a cabo estos pasos en el siguiente orden:

1. La persona que tenga credenciales con permisos de AWS Organizations entrada debe usar la AWS Organizations consola AWS CLI, la o una AWS SDK para habilitar el acceso confiable al servicio de confianza. Esto concederá permiso al otro servicio para llevar a cabo la configuración necesaria en la organización cuando se realice el siguiente paso (paso 2).

   Los AWS Organizations permisos mínimos son los siguientes:

   - `organizations:EnableAWSServiceAccess`
   - `organizations:ListAWSServiceAccessForOrganization`— Necesario únicamente si se utiliza la AWS Organizations consola

   Para ver los pasos para habilitar el acceso confiable en AWS Organizations, consulteCómo habilitar o deshabilitar el acceso de confianza.
2. La persona que tiene credenciales con permisos en el servicio de confianza habilita ese servicio para trabajar con AWS Organizations. Esto indica al servicio que debe realizar todas las inicializaciones necesarias, como la creación de los recursos necesarios para que el servicio de confianza funcione en la organización. Para obtener más información, consulte las instrucciones específicas de los servicios en Servicios de AWS que puedes usar con AWS Organizations.

Permisos necesarios para deshabilitar el acceso de confianza

Si ya no desea permitir que el servicio de confianza realice tareas en la organización o en las cuentas de esta, elija uno de los escenarios siguientes.

> **Important**
>
> La deshabilitación del acceso del servicio de confianza no impide que los usuarios y los roles con los permisos apropiados utilicen dicho servicio. Para impedir por completo el acceso de los usuarios y los roles a un AWS servicio, puede eliminar los IAM permisos que otorgan ese acceso o puede usar las políticas de control del servicio (SCPs) en AWS Organizations. Puede solicitarlos solo SCPs a las cuentas de los miembros. SCPsno se aplican a la cuenta de administración. Le recomendamos que no ejecute servicios en la cuenta de administración. En su lugar, ejecútelos en las cuentas de los miembros, donde podrá controlar la seguridad mediante el uso deSCPs.

- Si tiene credenciales con permisos tanto AWS Organizations en el servicio de confianza como en el servicio de confianza, deshabilite el acceso mediante las herramientas (consola o AWS CLI) que

están disponibles para el servicio de confianza. A continuación, el servicio realiza una limpieza eliminando los recursos que ya no son necesarios y deshabilitando el acceso de confianza del servicio en AWS Organizations en su nombre.

Los permisos mínimos para estas credenciales son los siguientes:

- `organizations:DisableAWSServiceAccess`. También puede utilizar la clave de condición `organizations:ServicePrincipal` con esta operación para limitar las solicitudes que esas operaciones realizan a una lista de nombres de principal de servicio aprobados. Para obtener más información, consulte Claves de condición.
- `organizations:ListAWSServiceAccessForOrganization`— Necesario si utilizas la AWS Organizations consola.
- Los permisos mínimos necesarios que requiere el servicio de confianza dependen del servicio. Para obtener más información, consulte la documentación del servicio de confianza.

- Si las credenciales con permisos introducidos AWS Organizations no son las credenciales con permisos del servicio de confianza, lleve a cabo estos pasos en el siguiente orden:

  1. La persona con permisos en el servicio de confianza primero deshabilita el acceso utilizando dicho servicio. Esto indica al servicio de confianza que debe eliminar los recursos necesarios para el acceso de confianza. Para obtener más información, consulte las instrucciones específicas de los servicios en Servicios de AWS que puedes usar con AWS Organizations.
  2. La persona con los permisos AWS Organizations ingresados podrá entonces usar la AWS Organizations consola o deshabilitar el acceso AWS SDK al servicio de confianza. AWS CLI Esto eliminará los permisos para el servicio de confianza de la organización y las cuentas de esta.

     Los AWS Organizations permisos mínimos son los siguientes:

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization`— Necesario únicamente si se utiliza la AWS Organizations consola

     Para conocer los pasos para deshabilitar el acceso de confianza en AWS Organizations, consulteCómo habilitar o deshabilitar el acceso de confianza.

Cómo habilitar o deshabilitar el acceso de confianza

Si solo tiene permisos AWS Organizations y desea habilitar o deshabilitar el acceso de confianza a su organización en nombre del administrador del otro AWS servicio, utilice el siguiente procedimiento.

Important

Recomendamos encarecidamente que, cuando la opción esté disponible, active y desactive el acceso de confianza utilizando únicamente la consola del servicio de confianza AWS CLI o sus equivalentes API operativos. Esto permite al servicio de confianza realizar cualquier inicialización necesaria al habilitar el acceso de confianza, como la creación de los recursos necesarios y la limpieza necesaria de los recursos al deshabilitar el acceso de confianza. Para obtener información acerca de cómo habilitar o deshabilitar el acceso a servicios de confianza a su organización mediante el servicio de confianza, consulte el vínculo Más información en la columna Admite el acceso de confianza en Servicios de AWS que puedes usar con AWS Organizations.
Si deshabilita el acceso mediante la consola, CLI los comandos o API las operaciones de Organizations, se producen las siguientes acciones:

- El servicio ya no puede crear un rol vinculado a un servicio en las cuentas de su organización. Esto significa que el servicio no puede realizar operaciones en su nombre en ninguna cuenta nueva de su organización. El servicio aún puede realizar operaciones en cuentas antiguas hasta que el servicio complete su limpieza desde AWS Organizations.
- El servicio ya no puede realizar tareas en las cuentas de los miembros de la organización, a menos que esas operaciones estén explícitamente permitidas por las IAM políticas asociadas a tus funciones. Esto incluye cualquier agregación de datos de las cuentas de miembro a la cuenta de administración o a una cuenta de administrador delegada, cuando proceda.
- Algunos servicios detectan esto y limpian los datos o recursos restantes relacionados con la integración, mientras que otros servicios dejan de acceder a la organización pero dejan los datos históricos y la configuración para permitir una posible reactivación de la integración.

En su lugar, el uso de la consola o los comandos del otro servicio para deshabilitar la integración garantiza que el otro servicio pueda limpiar los recursos necesarios solo para la integración. La forma en que el servicio limpia sus recursos en las cuentas de la organización

depende de ese servicio. Para obtener más información, consulte la documentación del otro AWS servicio.

AWS Management Console

Habilitar el acceso al servicio de confianza

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila del servicio que desea habilitar y elija su nombre.
3. Elija Habilitar acceso de confianza.
4. En el cuadro de diálogo de confirmación, marque la casilla Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
5. Si está habilitando el acceso, dígale al administrador del otro AWS servicio que ya puede habilitar el otro servicio para que funcione AWS Organizations.

Para deshabilitar el acceso de confianza

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila del servicio que desea deshabilitar y elija su nombre.
3. Espere a que el administrador del otro servicio le diga que el servicio está desactivado y que sus recursos han sido limpiados.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.

AWS CLI, AWS API

Para habilitar o deshabilitar el acceso del servicio de confianza

Puede usar los siguientes AWS CLI comandos u API operaciones para habilitar o deshabilitar el acceso a servicios de confianza:

- AWS CLI: AWS organizaciones enable-aws-service-access
- AWS CLI: AWS organizaciones disable-aws-service-access
- AWS API: E nableAWSService Access
- AWS API: isableAWSServiceAcceso D

AWS Organizations y funciones vinculadas al servicio

AWS Organizations utiliza funciones IAM vinculadas al servicio para permitir que los servicios de confianza realicen tareas en tu nombre en las cuentas de los miembros de tu organización. Al configurar un servicio de confianza y autorizar su integración con la organización, dicho servicio puede solicitar que AWS Organizations cree una función vinculada a sí mismo en su cuenta de miembro. El servicio de confianza realiza acción de forma asíncrona según lo necesite, pero no necesariamente en todas las cuentas de la organización al mismo tiempo. El rol vinculado al servicio tiene IAM permisos predefinidos que permiten al servicio de confianza realizar solo tareas específicas dentro de esa cuenta. En general, AWS administra todas las funciones vinculadas a servicios, lo que significa que normalmente no puede modificar las funciones ni las políticas adjuntas.

Para que todo esto sea posible, al crear una cuenta en una organización o aceptar una invitación para unir su cuenta existente a una organización, AWS Organizations aprovisiona la cuenta de miembro con un rol vinculado a un servicio denominado `AWSServiceRoleForOrganizations`. Solo el propio AWS Organizations servicio puede asumir esta función. El rol tiene permisos que permiten AWS Organizations crear roles vinculados al servicio para otros. Servicios de AWS Este rol vinculado a un servicio está presente en todas las organizaciones.

Aunque no lo recomendamos, si su organización tiene solo las características de facturación unificada habilitadas, el rol vinculado a un servicio denominado `AWSServiceRoleForOrganizations` no se utiliza nunca y puede eliminarlo. Si más adelante desea habilitar todas las características de la organización, el rol es necesario y debe restaurarlo. Las siguientes comprobaciones se producen cuando inicia el proceso para habilitar todas las características:

- Por cada cuenta de miembro que se haya invitado a unirse a la organización – El administrador de dicha cuenta recibe una solicitud para que acepte habilitar todas las características. Para aceptar correctamente la solicitud, el administrador debe tener los permisos `organizations:AcceptHandshake` e `iam:CreateServiceLinkedRole` si el rol vinculado a un servicio (`AWSServiceRoleForOrganizations`) no existe todavía. Si el rol `AWSServiceRoleForOrganizations` ya existe, el administrador necesita únicamente el

permiso `organizations:AcceptHandshake` para aceptar la solicitud. Cuando el administrador acepta la solicitud, AWS Organizations crea el rol vinculado al servicio si aún no existe.

- Por cada cuenta de miembro que se haya creado en la organización – El administrador de la cuenta recibe una solicitud para volver a crear el rol vinculado al servicio. (El administrador de la cuenta de miembro no recibe una solicitud para habilitar todas las funciones porque el administrador de la cuenta de administración (antes conocida como "cuenta maestra") se considera el propietario de las cuentas de miembro creadas). AWS Organizations crea el rol vinculado al servicio cuando el administrador de la cuenta de miembro acepta la solicitud. El administrador debe tener los permisos `organizations:AcceptHandshake` e `iam:CreateServiceLinkedRole` para aceptar correctamente el protocolo de enlace.

Después de habilitar todas las características de su organización, ya no puede eliminar el rol vinculado al servicio `AWSServiceRoleForOrganizations` de cualquier cuenta.

> **Important**
>
> AWS Organizations SCPsnunca afectan a los roles vinculados al servicio. Estas funciones están exentas de cualquier SCP restricción.

Uso del rol AWSServiceRoleForDeclarativePoliciesEC2Report vinculado al servicio

Organizations utiliza la función `AWSServiceRoleForDeclarativePoliciesEC2Report` vinculada al servicio para describir los estados de los atributos de las cuentas de los miembros a fin de crear informes de políticas declarativas. Los permisos del rol se definen en. AWS política gestionada: DeclarativePoliciesEC2Report

Servicios de AWS que puedes usar con AWS Organizations

Con él AWS Organizations , puede realizar actividades de administración de cuentas a gran escala mediante la consolidación de varias organizaciones Cuentas de AWS en una sola. La consolidación de cuentas simplifica el uso de otras. Servicios de AWS Puede aprovechar los servicios de administración de múltiples cuentas disponibles en AWS Organizations Select Servicios de AWS para realizar tareas en todas las cuentas que son miembros de su organización.

En la siguiente tabla Servicios de AWS se enumeran los servicios que puede utilizar y las ventajas de utilizarlos a nivel de toda la organización. AWS Organizations

Acceso confiable: puede habilitar un AWS servicio compatible para realizar operaciones en toda la Cuentas de AWS organización. Para obtener más información, consulte Uso AWS Organizations con otros Servicios de AWS.

Administrador delegado para Servicios de AWS: un AWS servicio compatible puede registrar una cuenta de AWS miembro en la organización como administrador de las cuentas de la organización en ese servicio. Para obtener más información, consulte Administrador delegado de los Servicios de AWS que funcionan con Organizations.

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Account Management Gestione los detalles y los metadatos de todos los Cuentas de AWS componentes de su organización.	Gestione los detalles de la cuenta, los contactos alternativos y las regiones de todos los Cuentas de AWS miembros de su organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Application Migration Service AWS Application Migration Service permite lift-and-shift a las empresas disponer de AWS una gran cantidad de servidores físicos, virtuales o en la nube sin problemas de compatibilidad, interrupciones en el rendimiento ni períodos de transición prolongados.	Puede administrar migraciones a gran escala en varias cuentas.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
AWS Artifact Descargue los informes AWS de conformidad en materia de seguridad, como los informes ISO y PCI.	Puede aceptar acuerdos en nombre de todas las cuentas de su organización.	 Sí Más información	 No
AWS Audit Manager Automatice la recopilación continua de pruebas para ayudarle a auditar el uso de los servicios en la nube.	Audite continuamente su AWS uso en varias cuentas de su organización para simplificar la evaluación del riesgo y el cumplimiento.	 Sí Más información	 Sí Más información

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Backup Administre y supervise las copias de seguridad de todas las cuentas de su organización.	Puede configurar y administrar los planes de respaldo para toda la organización o para los grupos de cuentas de las unidades de la organización (OUs). Puede supervisar las copias de seguridad de todas sus cuentas de manera	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	centralizada.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Billing and Cost Management Proporciona una visión general de sus datos de gestión financiera en la AWS nube y le ayuda a tomar decisiones más rápidas e informadas.	Permite que los datos de asignación de costos divididos recuperen AWS Organizations información, si corresponde, y recopilen datos de telemetría para los servicios de datos de asignación de costos divididos por los que ha optado.	 Sí Más información	 No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	Para obtener más información, consulte ¿Qué es? AWS Billing and Cost Management en la guía del usuario de Billing and Cost Management.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS CloudFormation Stacksets Cree, actualice o elimine pilas de varias cuentas y regiones en una sola operación.	Un usuario de la cuenta de administración o una cuenta de administrador delegada puede crear un conjunto de pilas con permisos administrados por servicios que implemente instancias de pila en cuentas de la organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS CloudTrail Habilite la auditoría de riesgos y operaciones, el gobierno y la conformidad de su cuenta.	Un usuario con una cuenta de administración o una cuenta de administrador delegado puede crear un seguimiento de la organización o un almacén de datos de eventos que registre todos los eventos de todas las cuentas de la	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	organización.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon CloudWatch Supervise sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real. Puede utilizar las CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir para sus recursos y aplicaciones.	Úselo CloudWatch para descubrir y comprender el estado de la configuración de telemetría de sus AWS recursos desde una vista central en la CloudWatch consola. Al integrarse con Organizations, puede realizar modificaciones	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	en las configuraciones compatibles con CloudWatch for Organizations.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Compute Optimizer Obtenga recomendaciones de optimización AWS informática.	Puede analizar todos los recursos que se encuentran en las cuentas de su organización para obtener recomendaciones de optimización. Para obtener más información, consulte Cuentas admitidas por Compute Optimizer en la Guía del usuario	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	de AWS Compute Optimizer.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Config Evalúe, audite y analice las configuraciones de sus recursos de AWS .	Puede obtener una vista de toda la organización del estado de conformidad. También puede utilizar las operaciones de la AWS Config API para gestionar AWS Config las reglas y los paquetes de conformidad Cuentas de AWS en toda la	 Sí Más información	 Sí Más información: Reglas de Config Paquetes de conformidad Acumulación de datos de multicuentas y multiregiones	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	organización. Puede utilizar una cuenta de administrador delegada para agregar la configuración de recursos y los datos de conformidad de todas las cuentas de miembros de una organización en AWS Organizations. Para obtener más			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	información, consulte Registro de un administrador delegado en la AWS Config Guía para desarrolladores de .			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Control Tower Configure y controle un entorno de AWS seguro con varias cuentas que cumpla con las normas correspondientes.	Puedes configurar una landing zone, un entorno de múltiples cuentas para todos tus AWS recursos. Este entorno incluye una organización y entidades de organización. Puede utilizar este entorno para hacer cumplir	 Sí Más información	 No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	las normas de conformidad en todos sus Cuentas de AWSámbitos. Para obtener más información, consulte Cómo AWS Control Tower y Administrar cuentas a través de AWS Organizations en la Guía del usuario de AWS			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	Control Tower .			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Centro de optimización de costes de AWS Recopile recomendaciones de costos para todos los productos de AWS optimización.	Puede identificar, filtrar y agregar fácilmente las recomendaciones de optimización de AWS costos en todas las cuentas de sus AWS Organizations miembros y AWS regiones. Para obtener más información, consulte Centro de optimización de	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	costos en la Guía del usuario de Centro de optimización de costos.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon Detective Genere visualizaciones a partir de sus datos de registro para analizar, investigar e identificar rápidamente la causa raíz de los hallazgos de seguridad o actividades sospechosas.	Puede integrar Amazon Detective AWS Organizations para garantizar que su gráfico de comportamiento de detective proporcione visibilidad de la actividad de todas las cuentas de su organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
El DevOps gurú de Amazon Analice los datos operativos y las métricas y eventos de las aplicaciones para identificar comportamientos que se desvían de los patrones operativos normales. Los usuarios reciben una notificación cuando DevOps Guru detecta un problema o riesgo operativo.	Puede integrarlo AWS Organizations para gestionar la información de todas las cuentas de toda su organización. Delega un administrador para ver, ordenar y filtrar información de todas las cuentas y obtener el estado de toda la organización de	 Sí Más información	 Sí Más información

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	todas las aplicaciones supervisadas.			
AWS Directory Service Configure y ejecute directorios en la AWS nube o conecte sus AWS recursos con un Microsoft Active Directory local existente.	Puede integrarlo AWS Organizations para AWS Directory Service compartir directorios sin problemas entre varias cuentas y cualquier VPC de una región.	 Sí Más información	 No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
Amazon EventBridge Supervise sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.	Puedes habilitar el uso compartido de todos los EventBridge eventos de Amazon, anteriormente Amazon CloudWatch Events, en todas las cuentas de tu organización. Para obtener más información, consulta Enviar y recibir	 No	 No

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	EventBridge eventos de Amazon entre Cuentas de AWS en la Guía del EventBridge usuario de Amazon.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon Elastic Compute Cloud El administrador de direcciones IP (IPAM) de Amazon VPC proporciona capacidad informática escalable y bajo demanda en la nube. AWS	Permita que el administrador de Organizations cree un informe sobre la configuración existente para las cuentas de su organización cuando utilice la función de políticas declarativas.	 Sí Más información	 No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Firewall Manager Configure y administre de forma centralizada las reglas de firewall para las aplicaciones web en sus cuentas y aplicaciones.	Puede configurar y administrar AWS WAF las reglas de forma centralizada en todas las cuentas de su organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon GuardDuty GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa la información de diversas fuentes de datos. Utiliza fuentes de información de amenazas y machine learning para identificar la actividad inesperada y potencialmente no permitida, así como la actividad malintencionada en su entorno de AWS .	Puede designar una cuenta de miembro GuardDuty para ver y administrar todas las cuentas de su organización. Al agregar cuentas de miembros, se GuardDuty habilitan automáticamente esas cuentas en la seleccionada Región de AWS.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	También puede automatizar la GuardDuty activación de las nuevas cuentas que se agreguen a su organización. Para obtener más información, consulta GuardDuty Organisations in the Amazon GuardDuty User Guide.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Health Obtenga visibilidad de los eventos que pueden afectar a los problemas de rendimiento o disponibilidad de los recursos para Servicios de AWS.	Puede agregar AWS Health eventos en todas las cuentas de su organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Identity and Access Management Controle de forma segura el acceso a AWS los recursos.	Puede utilizar los datos del último acceso al servicio de IAM para conocer mejor la actividad de AWS en su organización. Puede utilizar estos datos para crear y actualizar las políticas de control de servicios (SCPs) que restringen	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	el acceso únicamente a los AWS servicios que utilizan las cuentas de su organización. Para ver un ejemplo, consulte Uso de datos para ajustar los permisos de una unidad organizativa en la Guía del usuario de IAM.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	La gestión del acceso raíz de IAM le permite gestionar de forma centralizada las credenciales de los usuarios raíz y realizar tareas privilegiadas en las cuentas de los miembros.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
IAM Access Analyzer Analice las políticas basadas en los recursos de su AWS entorno para identificar las políticas que permiten el acceso a un director fuera de su zona de confianza.	Puede designar una cuenta de miembro para que sea administrador de IAM Access Analyzer. Para obtener más información, consulte Habilitación de Access Analyzer en la guía del usuario de IAM.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon Inspector Escanee automáticamente sus AWS cargas de trabajo en busca de vulnerabilidades para descubrir EC2 instancias de Amazon e imágenes de contenedores que residen en Amazon ECR para detectar vulnerabilidades de software y exposiciones no deseadas de la red.	Delegue un administrador para habilitar o desactivar los análisis de cuentas de miembros, ver datos de búsqueda agregados de toda la organización, crear y administrar reglas de supresión. Para obtener más información,	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	consulte Administración de varias cuentas con AWS Organizations en la Guía del usuario de Amazon Inspector.			
AWS License Manager Simplifique el proceso de transferencia de las licencias de software a la nube.	Puede habilitar el descubrimiento entre cuentas de recursos informáticos en toda su organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon Macie Descubre y clasifica el contenido crítico para su empresa mediante el machine learning para ayudarle a cumplir los requisitos de privacidad y seguridad de datos. Evalúa continuamente el contenido almacenado en Amazon S3 y le notifica posibles problemas.	Puede configurar Amazon Macie para todas las cuentas de su organización para obtener una vista consolidada de todos los datos en Amazon S3, en todas las cuentas desde una cuenta de administrador de Macie designada. Puede configurar Macie	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	para proteger automáticamente los recursos de las cuentas nuevas a medida que crece la organización. Se le alerta para corregir las configuraciones de política incorrectas en los buckets de S3 de toda la organización.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Managed Services (AMS) Informes de autoservicio (SSR) Recopila datos de varios AWS servicios nativos y proporciona acceso a informes sobre las principales ofertas de AMS. SSR proporciona la información que puede utilizar para respaldar las operaciones, la administración de la configuración, la administración de activos, la administración de la seguridad	Puede activar el SSR agregado, una función que permite a los clientes ver los informes de autoservicio consolidados de toda la organización a través de su cuenta de administración o de una cuenta de administrador delegado.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
y el cumplimiento.				
AWS Marketplace Un catálogo digital curado que puede utilizar para encontrar, comprar, desplegar y gestionar el software, los datos y los servicios de terceros que necesita para crear soluciones y dirigir sus negocios.	Puede compartir las licencias de sus AWS Marketplace suscripciones y compras entre las cuentas de su organización.	 Sí Más información	 No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Marketplace Marketplace privado Le proporciona un amplio catálogo de productos disponibles en AWS Marketplace, junto con un control detallado de esos productos.	Le permite crear varias experiencias de mercado privado asociadas a toda la organización, una o varias cuentas de la organización OUs, cada una con su propio conjunto de productos aprobados. AWS Los administradores también pueden	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	aplicar la marca de la empresa a cada experiencia de mercado privado con el logotipo, los mensajes y la combinación de colores de su empresa o equipo.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Marketplace panel de información sobre compras Le permite ver los acuerdos y los datos de análisis de costes de todas sus AWS Marketplace compras en las AWS cuentas de su organización.	AWS Marketplace El panel de información sobre adquisiciones escucha los cambios de la organización, como la incorporación de una cuenta a la organización, y agrega los datos de los acuerdos correspondientes para crear sus	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	paneles de control.			
AWS Network Manager Le permite gestionar de forma centralizada su red principal de WAN AWS en la nube y su red AWS Transit Gateway en todas las AWS cuentas, regiones y ubicaciones locales.	Puedes gestionar y supervisar tus redes globales de forma centralizada con las pasarelas de tránsito y sus recursos adjuntos en varias AWS cuentas de tu organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon Q Developer Amazon Q Developer es un asistente conversacional generativo con inteligencia artificial que puede ayudarlo a comprender, crear, ampliar y operar AWS aplicaciones.	La versión de suscripción de pago de Amazon Q Developer requiere la integración de Organizations.	 Sí Más información	 No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
AWS Resource Access Manager Comparta AWS recursos específicos de su propiedad con otras cuentas.	Puede compartir recursos dentro de su organización sin intercambiar invitaciones adicionales. Entre los recursos que puede compartirse incluyen reglas de solucionador de Route 53, reservas de capacidad bajo demanda	 Sí Más información	 No

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	y mucho más. Para obtener información sobre cómo compartir reservas de capacidad, consulta la Guía del EC2 usuario de Amazon o la Guía del EC2 usuario de Amazon. Para obtener una lista de recursos compartibles,			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	consulte Recursos compatibles en la Guía del usuario de AWS RAM .			
Explorador de recursos de AWS Explore sus recursos en una experiencia similar a la de un motor de búsqueda en Internet.	Habilite la búsqueda multicuenta.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Security Hub Consulta tu estado de seguridad AWS y compara tu entorno con los estándares y las mejores prácticas del sector de la seguridad.	Puede habilitar automáticamente Security Hub para todas las cuentas de su organización, incluidas las cuentas nuevas a medida que se agregan. Esto aumenta la cobertura de las comprobaciones y hallazgos de Security Hub, lo que	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	proporciona una imagen más precisa de su postura general de seguridad.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon S3 Storage Lens Obtenga visibilidad de sus métricas de actividad y uso del almacenamiento de Amazon S3 con recomendaciones prácticas para optimizar el almacenamiento.	Configure Amazon S3 Storage Lens para obtener visibilidad de las tendencias de actividad y uso del almacenamiento de Amazon S3, así como de las recomendaciones para todas las cuentas de miembros de su organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Respuesta a incidentes de seguridad AWS servicio de seguridad que proporciona asistencia en tiempo real y con asistencia humana en caso de incidentes de seguridad las 24 horas del día, los 7 días de la semana, para ayudar a los clientes a responder rápidamente a los incidentes de ciberseguridad, como el robo de credenciales	Cobertura de seguridad para toda la organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon Security Lake Amazon Security Lake centraliza los datos de seguridad de fuentes en la nube, en las instalaciones y personalizadas en un lago de datos almacenado en su cuenta.	Cree un lago de datos que recopile registros y eventos en sus cuentas.	 Sí Más información	 Sí Más información	
AWS Service Catalog Cree y administre catálogos de servicios de TI aprobados para su uso en AWS.	Puede compartir carteras y copiar productos entre cuentas con mayor facilidad, sin compartir la cartera. IDs	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Service Quotas Consulte y administre sus cuotas de servicio, también conocidas como límites, desde una ubicación central.	Puede crear una plantilla de solicitud de cuota para solicitar automáticamente un aumento de cuotas cuando se creen las cuentas de su organización.	 Sí Más información	 No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS IAM Identity Center Proporciona acceso de inicio de sesión único para todas sus cuentas y aplicaciones en la nube.	Los usuarios pueden iniciar sesión en el portal de AWS acceso con sus credenciales corporativas y acceder a los recursos de la cuenta de administración o las cuentas de los miembros que tengan asignadas.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Systems Manager Habilite la visibilidad y el control de sus AWS recursos.	Puede sincronizar los datos de operaciones Cuentas de AWS en toda la organización mediante Systems Manager Explorer. Puede administrar plantillas de cambios, aprobaciones e informes para todas las cuentas de miembros de su organizac	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	ión desde una cuenta de administrador delegada mediante Systems Manager Change Manager.			
AWS User Notifications Una ubicación central para sus AWS notificaciones.	Puede configurar y ver las notificaciones de forma centralizada en todas las cuentas de su organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Políticas de etiquetas Use etiquetas estandarizadas en los recursos de las cuentas de su organización.	Puede crear políticas de etiquetado para definir reglas de etiquetado para recursos y tipos de recursos específicos y adjuntar esas políticas a las unidades y cuentas de la organización para aplicar esas reglas.	 Sí Más información	 No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Trusted Advisor Trusted Advisor inspecciona su AWS entorno y hace recomendaciones cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad.	Realiza Trusted Advisor comprobaciones para todos los miembros Cuentas de AWS de tu organización.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Well-Architected Tool AWS Well-Architected Tool Esto le ayuda a documentar el estado de sus cargas de trabajo y a compararlas con las mejores prácticas de AWS arquitectura más recientes.	Permite a ambos AWS WA Tool y a los clientes de Organizations simplificar el proceso de compartir AWS WA Tool recursos con otros miembros de su organización.	 Sí Más información	 No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon VPC IP Address Manager (IPAM) IPAM es una función de VPC que le facilita la planificación, el seguimiento y la supervisión de las direcciones IP de sus cargas de AWS trabajo.	Monitoree el uso de direcciones IP en toda la organización y comparta grupos de direcciones IP entre las cuentas de miembro.	 Sí Más información	 Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Analizador de accesibilidad de Amazon VPC Reachability Analyzer es una herramienta de análisis de configuración que le permite realizar pruebas de conectividad entre un recurso de origen y un recurso de destino en sus nubes privadas virtuales (). VPCs	Realice un seguimiento de las rutas a través de las cuentas de sus organizaciones.	 Sí Más información	 Sí Más información	

AWS Account Management y AWS Organizations

AWS Account Management le ayuda a administrar la información y los metadatos de las cuentas de todos los Cuentas de AWS miembros de su organización. Puede configurar, modificar o eliminar la información de contacto alternativa de cada una de las cuentas de miembro de su organización. Para

obtener más información, consulte Uso de AWS Account Management en su organización en la Guía del usuario de AWS Account Management .

Utilice la siguiente información para ayudarle a integrarse AWS Account Management con AWS Organizations.

Para habilitar el acceso de confianza con Account Management

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

La administración de cuentas requiere un acceso confiable AWS Organizations antes de poder designar una cuenta de miembro como administrador delegado de este servicio para su organización.

Solo puede habilitar el acceso confiable mediante las herramientas de Organizations.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Account Management.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Account Management diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Account Management que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Account Management como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Para desactivar el acceso de confianza con Account Management

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con AWS Account Management.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Account Management.
4. Seleccione Deshabilitar el acceso de confianza.

5. En el cuadro de AWS Account Management diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Account Management que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Account Management como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

Habilitación de una cuenta de administrador delegado para Account Management

Cuando se designa una cuenta de miembro como administrador delegado de la organización, los usuarios y los roles de la cuenta designada pueden administrar los metadatos de la Cuenta de AWS de otras cuentas de miembro de la organización. Si no habilita una cuenta de administrador delegado, estas tareas solo las puede realizar la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de los detalles de la cuenta.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para administración de cuentas en la organización.

Para obtener instrucciones generales sobre cómo configurar una política de delegación, consulte Cree una política de delegación basada en los recursos con AWS Organizations.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el principal de servicio de la cuenta `account.amazonaws.com` como parámetros.

AWS Application Migration Service (Servicio de migración de aplicaciones) y AWS Organizations

AWS Application Migration Service simplifica, agiliza y reduce el costo de migrar aplicaciones a. AWS Al integrarse con Organizations, puede usar la característica de visualización global para administrar migraciones a gran escala en varias cuentas. Para obtener más información, consulte Setting up your AWS Organizations en la Guía del usuario de Application Migration Service.

Utilice la siguiente información para ayudarle a integrarse con. AWS Application Migration Service AWS Organizations

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite que Application Migration Service lleve a cabo operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Application Migration Service y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForApplicationMigrationService`

Entidades principales de servicio utilizadas por Application Migration Service

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Application Migration Service otorgan acceso a las siguientes entidades principales de servicio:

- `mgn.amazonaws.com`

Activación del acceso de confianza con Application Migration Service

Cuando habilita el acceso de confianza con Application Migration Service, puede usar la característica de visualización global, que le permite administrar migraciones a gran escala entre varias cuentas. La vista global proporciona visibilidad y la capacidad de realizar acciones específicas en los servidores de origen, las aplicaciones y las oleadas de distintas AWS cuentas. Para obtener más información, consulte Configuración de sus AWS organizaciones en la guía del AWS Application Migration Service usuario.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS Application Migration Service consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Application Migration Service consola o las herramientas para permitir la integración con Organizations.

Esto permite AWS Application Migration Service realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Application Migration Service. Para obtener más información, consulte esta nota.
Si habilitas el acceso confiable mediante la AWS Application Migration Service consola o las herramientas, no necesitas completar estos pasos.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Application Migration Service.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Application Migration Service diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Application Migration Service que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

Ejecute el siguiente comando para habilitarlo AWS Application Migration Service como un servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal mgn.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Desactivación del acceso de confianza con Application Migration Service

Solo un administrador de la cuenta de administración de Organizations puede deshabilitar el acceso de confianza con Application Migration Service.

Puede deshabilitar el acceso de confianza mediante las herramientas AWS Application Migration Service o las AWS Organizations herramientas.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Application Migration Service consola o las herramientas para deshabilitar la integración con Organizations. Esto permite AWS Application Migration Service realizar cualquier limpieza que sea necesaria, como eliminar recursos o acceder a funciones que el servicio ya no necesite. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas por AWS Application Migration Service.
> Si inhabilitas el acceso de confianza mediante la AWS Application Migration Service consola o las herramientas, no necesitas completar estos pasos.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Application Migration Service.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS Application Migration Service diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Application Migration Service que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Application Migration Service como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Habilitación de una cuenta de administrador delegado para Application Migration Service

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y los roles de esa cuenta pueden llevar a cabo las acciones administrativas para Application Migration Service que, de lo contrario, solo podrían hacerlas los usuarios o roles en la cuenta de administración de la organización. Esto le permite separar la administración de la organización de la administración de Application Migration Service. Para obtener más información, consulte Setting up your AWS Organizations en la Guía del usuario de Application Migration Service.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Application Migration Service en la organización

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal mgn.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el servicio de la cuenta `mgn.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para Application Migration Service

Solo un administrador de la cuenta de administración de Organizations puede eliminar un administrador delegado para Application Migration Service. Puede eliminar el administrador delegado mediante Organizations `DeregisterDelegatedAdministrator` CLI o la SDK operación.

AWS Artifact y AWS Organizations

AWS Artifact es un servicio que le permite descargar informes de cumplimiento AWS de normas de seguridad, como ISO PCI informes. Con AWS Artifactél, un usuario de la cuenta de administración de la organización puede aceptar automáticamente acuerdos en nombre de todas las cuentas de los miembros de una organización, incluso cuando se añaden nuevos informes y cuentas. Los usuarios de las cuentas de miembro pueden ver y descargar acuerdos. Para obtener más información, consulta Administrar un acuerdo para varias cuentas en AWS Artifact en la Guía del AWS Artifact usuario.

Usa la siguiente información para ayudarte a integrarte AWS Artifact con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le AWS Artifact permite realizar operaciones de apoyo en las cuentas de su organización.

Puede eliminar o modificar esta función solo si deshabilita el acceso de confianza entre AWS Artifact y Organizations, o si elimina la cuenta de miembro de la organización.

Aunque puede eliminar o modificar este rol si elimina la cuenta de miembro de la organización, no lo recomendamos.

Se desaconseja modificar el rol porque puede provocar problemas de seguridad, como el diputado confuso entre servicios. Para obtener más información sobre la protección contra el diputado confuso, consulte Prevención contra el diputado entre servicios en la Guía del usuario de AWS Artifact .

- `AWSServiceRoleForArtifact`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza AWS Artifact otorgan acceso a los siguientes directores de servicio:

- `artifact.amazonaws.com`

Habilitar el acceso de confianza con AWS Artifact

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede habilitar el acceso confiable mediante las herramientas de Organizations.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Artifact.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Artifact diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Artifact que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Artifact como un servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal artifact.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Deshabilitación del acceso con AWS Artifact

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con AWS Artifact.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

AWS Artifact requiere un acceso confiable con AWS Organizations para trabajar con los acuerdos de la organización. Si deshabilita el acceso de confianza AWS Organizations mientras lo utiliza AWS Artifact para los acuerdos de la organización, dejará de funcionar porque no podrá acceder a la organización. Todos los acuerdos organizativos que aceptes AWS Artifact permanecerán en vigor, pero no podrás acceder a ellos AWS Artifact. El AWS Artifact rol que AWS Artifact crea permanece. Si vuelve a habilitar el acceso de confianza, AWS Artifact seguirá funcionando como lo hacía antes sin necesidad de volver a configurar el servicio.

Una cuenta independiente que se elimine de una organización ya no tendrá acceso a ningún acuerdo de la organización.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Artifact.

4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS Artifact diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Artifact que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Artifact como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

AWS Audit Manager y AWS Organizations

AWS Audit Manager le ayuda a auditar continuamente su AWS consumo para simplificar la evaluación del riesgo y el cumplimiento de las normas y 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 los controles de las partes interesadas y le ayuda a crear informes listos para auditorías con mucho menos esfuerzo manual.

Al integrar Audit Manager con AWS Organizations, puede recopilar pruebas de una fuente más amplia al incluir varias pruebas Cuentas de AWS de su organización en el ámbito de sus evaluaciones.

Para obtener más información, consulte Enable AWS Organizations en la Guía del usuario de Audit Manager.

Utilice la siguiente información para ayudarle a integrarse AWS Audit Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Audit Manager realizar operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Audit Manager y Organizations, o si elimina la cuenta de miembro de la organización.

Para obtener más información sobre cómo Audit Manager utiliza este rol, consulte Uso de roles vinculados a servicios en la Guía del usuario de AWS Audit Manager .

- `AWSServiceRoleForAuditManager`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Las funciones vinculadas a servicios utilizadas por Audit Manager otorgan acceso a las siguientes entidades de servicio:

- `auditmanager.amazonaws.com`

Para habilitar el acceso de confianza con el Audit Manager

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Audit Manager requiere un acceso confiable AWS Organizations antes de poder designar una cuenta de miembro como administrador delegado de su organización.

Puede habilitar el acceso confiable mediante la AWS Audit Manager consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Audit Manager consola o las herramientas para permitir la integración con Organizations. Esto permite AWS Audit Manager realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Audit Manager. Para obtener más información, consulte esta nota.
> Si habilitas el acceso confiable mediante la AWS Audit Manager consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso de confianza mediante la consola Audit Manager

Para obtener instrucciones acerca de cómo habilitar el acceso de confianza, consulte Configuración en la Guía del usuario de AWS Audit Manager .

> **Note**
>
> Si configura un administrador delegado mediante la AWS Audit Manager consola, se le habilitará AWS Audit Manager automáticamente el acceso de confianza.

Puede habilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Audit Manager como un servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal auditmanager.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Para deshabilitar el acceso de confianza con Audit Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con AWS Audit Manager.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Audit Manager como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal auditmanager.amazonaws.com
```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Para habilitar una cuenta de administrador delegado para Audit Manager

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y los roles de esa cuenta pueden realizar acciones administrativas para Audit Manager

que, de lo contrario, solo pueden realizar usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la gestión de Audit Manager.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations con el siguiente permiso puede configurar una cuenta de miembro como administrador delegado para Audit Manager en la organización: `audit-manager:RegisterAccount`

Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegada para Audit Manager, consulte Configuración en la Guía del usuario de AWS Audit Manager .

Si configura un administrador delegado mediante la AWS Audit Manager consola, Audit Manager le habilitará automáticamente un acceso de confianza.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS SDK: Llame a la `RegisterAccount` operación e indíquela `delegatedAdminAccount` como parámetro para delegar la cuenta de administrador.

AWS Backup y AWS Organizations

AWS Backup es un servicio que le permite gestionar y supervisar los AWS Backup trabajos de su organización. Si inicia sesión como usuario en la cuenta de administración de la organización, puede habilitar la protección y la supervisión de las copias de seguridad en toda la organización. AWS Backup Le ayuda a lograr el cumplimiento mediante el uso de políticas de respaldo para aplicar AWS Backup planes a los recursos de forma centralizada en todas las cuentas de su organización. Al

utilizar ambas AWS Backup y de AWS Organizations forma conjunta, puede obtener los siguientes beneficios:

Protección

Puede habilitar el tipo de política de respaldo en su organización y, a continuación, crear políticas de respaldo para adjuntarlas a la raíz o cuentas de la organización. OUs Una política de respaldo combina un AWS Backup plan con los demás detalles necesarios para aplicar el plan automáticamente a sus cuentas. Las políticas que se asocian directamente a una cuenta se combinan con las políticas heredadas de la organización raíz y de cualquier entidad matriz OUs para crear una política efectiva que se aplique a la cuenta. La política incluye el ID de un IAM rol que tiene permisos para ejecutarse AWS Backup en los recursos de tus cuentas. AWS Backup utiliza la IAM función para realizar la copia de seguridad en su nombre, tal como se especifica en el plan de copia de seguridad de la política vigente.

Supervisión

Cuando habilita el acceso de confianza para AWS Backup en su organización, puede usar la consola de AWS Backup para ver detalles sobre los trabajos de copia de seguridad, restauración y copia de cualquiera de las cuentas de su organización. Para obtener más información, consulte Monitorear los trabajos de copia de seguridad en la Guía del desarrollador de AWS Backup .

Para obtener más información al respecto AWS Backup, consulte la Guía para AWS Backup desarrolladores.

Utilice la siguiente información como ayuda para realizar la integración AWS Backup con AWS Organizations.

Habilitar el acceso de confianza con AWS Backup

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS Backup consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Backup consola o las herramientas para permitir la integración con Organizations. Esto permite AWS

Backup realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Backup. Para obtener más información, consulte esta nota.
Si habilitas el acceso confiable mediante la AWS Backup consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso confiable mediante el uso AWS Backup, consulte Habilitar la copia de seguridad en múltiples Cuentas de AWS versiones en la Guía para AWS Backup desarrolladores.

Deshabilitación del acceso con AWS Backup

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

AWS Backup requiere un acceso confiable AWS Organizations para permitir la supervisión de las tareas de copia de seguridad, restauración y copia en todas las cuentas de su organización. Si deshabilita el acceso de confianza AWS Backup, perderá la posibilidad de ver los trabajos fuera de la cuenta corriente. El AWS Backup rol que AWS Backup crea permanece. Si más adelante vuelve a habilitar el acceso de confianza, AWS Backup seguirá funcionando como antes, sin necesidad de volver a configurar el servicio.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Backup como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal backup.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Habilitar una cuenta de administrador delegado para AWS Backup

Consulte Administrador delegado en la Guía para desarrolladores de AWS Backup .

AWS Billing and Cost Management y AWS Organizations

AWS Billing and Cost Management proporciona un conjunto de funciones que le ayudan a configurar su facturación, recuperar y pagar facturas y analizar, organizar, planificar y optimizar sus costes. Cuando usa Billing and Cost Management con, AWS Organizations permite que los datos de asignación de costos divididos recuperen AWS Organizations información, si corresponde, y recopilen datos de telemetría para los servicios de datos de asignación de costos divididos que eligió.

Utilice la siguiente información como ayuda para integrarse AWS Billing and Cost Management con. AWS Organizations

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Administración de facturación y costos llevar a cabo operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Administración de facturación y costos y Organizations, o si elimina la cuenta de miembro de la organización.

Para obtener más información, consulte Roles vinculados a servicios de facturación de Administración de facturación y costos en la Guía del usuario de Administración de facturación y costos.

- `AWSServiceRoleForSplitCostAllocationData`

Entidades principales del servicio utilizadas por Administración de facturación y costos

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a

servicios utilizados por Administración de facturación y costos otorgan acceso a las siguientes entidades principales de servicio:

Administración de facturación y costos utiliza la entidad principal de servicio de `billing-cost-management.amazonaws.com`.

Habilitación del acceso de confianza con Administración de facturación y costos

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Con el acceso de confianza habilitado a través de una cuenta de administración, los clientes pueden aprovechar la característica de datos de asignación de costos divididos en Administración de facturación y costos. Cuando los clientes habilitan los datos de asignación de costos divididos para Amazon Elastic Kubernetes Service con Amazon Managed Service para Prometheus, se invoca el acceso de confianza para crear roles vinculados a servicios para todas las cuentas de miembro de la organización. Esto permite que los datos de asignación de costos divididos recopilen datos de telemetría de los espacios de trabajo de Amazon Managed Service para Prometheus de los clientes y lleven a cabo la asignación de costos en función de esas métricas.

Solo puede habilitar el acceso confiable mediante las herramientas de Organizations.

Puede habilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Billing and Cost Management como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Deshabilitación del acceso de confianza

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Billing and Cost Management como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

AWS CloudFormation StackSets y AWS Organizations

AWS CloudFormation StackSets le permite crear, actualizar o eliminar pilas en varias Cuentas de AWS y Regiones de AWS con una sola operación. StackSets la integración con AWS Organizations le permite crear conjuntos de pilas con permisos administrados por el servicio, utilizando un rol vinculado al servicio que tiene el permiso correspondiente en cada cuenta de miembro. Esto permite implementar instancias de pila en todas las cuentas de miembro de su organización. No tienes que crear los AWS Identity and Access Management roles necesarios; StackSets crea el IAM rol en cada cuenta de miembro en tu nombre.

También puede elegir habilitar implementaciones automáticas en cuentas que se añaden a su organización en el futuro. Con la implementación automática habilitada, los roles y la implementación de las instancias del conjunto de pilas asociadas se agregan automáticamente a todas las cuentas que se agreguen en el futuro a esa unidad organizativa.

Con el acceso confiable entre StackSets y Organizations activado, la cuenta de administración tiene permisos para crear y administrar conjuntos de pilas para su organización. La cuenta de administración puede registrar hasta cinco cuentas de miembros como administradores delegados. Con el acceso de confianza habilitado, los administradores delegados también tienen permisos para crear y administrar stack sets para su organización. Los conjuntos de pila con permisos administrados por servicios se crean en la cuenta de gestión, incluidos los conjuntos de pila creados por administradores delegados.

> **Important**
>
> Los administradores delegados tienen permisos completos para implementar en cuentas de la organización. La cuenta de administración no puede limitar los permisos de administrador delegados para implementar OUs o realizar operaciones de conjuntos de pilas específicos.

Para obtener más información sobre la integración StackSets con Organizations, consulte Trabajar con AWS CloudFormation StackSets en la Guía del AWS CloudFormation usuario.

Utilice la siguiente información como ayuda para integrarse AWS CloudFormation StackSets con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función permite a AWS CloudFormation Stacksets realizar operaciones compatibles en las cuentas de tu organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre StackSets AWS CloudFormation y Organizations, o si elimina la cuenta de miembro de la organización.

- cuenta de administración: `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

Para crear el rol `AWSServiceRoleForCloudFormationStackSetsOrgMember` vinculado a un servicio para las cuentas de miembros en su organización, debe crear primero un conjunto de pilas

en la cuenta de administración. Esto crea una instancia del conjunto de pilas, que luego crea el rol en las cuentas del miembro.

- Cuentas de miembros: `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Para obtener más información sobre la creación de conjuntos de pilas, consulta Cómo trabajar con ellos AWS CloudFormation StackSets en la Guía del AWS CloudFormation usuario.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Las funciones vinculadas a servicios que utilizan AWS CloudFormation Stacksets otorgan acceso a los siguientes principios de servicio:

- cuenta de administración: `stacksets.cloudformation.amazonaws.com`

  Puede modificar o eliminar este rol solo si ha desactivado el acceso de confianza entre StackSets y Organizations.
- Cuentas de miembros: `member.org.stacksets.cloudformation.amazonaws.com`

  Puedes modificar o eliminar este rol de una cuenta solo si primero inhabilitas el acceso de confianza entre StackSets and Organizations o si primero eliminas la cuenta de la organización o unidad organizativa (OU) de destino.

Habilitar el acceso de confianza con Stacksets AWS CloudFormation

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo un administrador de la cuenta de administración de Organizations tiene permisos para habilitar el acceso confiable con otro AWS servicio. Puede habilitar el acceso de confianza mediante la consola de AWS CloudFormation o la consola de Organizations.

Solo puede habilitar el acceso confiable mediante AWS CloudFormation StackSets.

Para habilitar el acceso confiable mediante la consola de AWS CloudFormation Stacksets, consulta Habilitar el acceso confiable con AWS Organizations en la Guía del AWS CloudFormation usuario.

Deshabilitar el acceso de confianza con Stacksets AWS CloudFormation

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo el administrador de una cuenta de administración de Organizations tiene permisos para deshabilitar el acceso de confianza con otro AWS servicio. Solo puede deshabilitar el acceso de confianza mediante la consola de Organizations. Si deshabilita el acceso de confianza con Organizations mientras lo usa StackSets, se conservan todas las instancias de pila creadas anteriormente. Sin embargo, los stack sets implementados mediante los permisos del rol vinculado a servicios ya no pueden realizar implementaciones en cuentas administradas por Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS CloudFormation consola o la consola de Organizations.

> **Important**
>
> Si inhabilitas el acceso de confianza mediante programación (por ejemplo, con AWS CLI o con unAPI), ten en cuenta que se eliminará el permiso. Es mejor deshabilitar el acceso de confianza con la AWS CloudFormation consola.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS CloudFormation StackSets.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS CloudFormation StackSets diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.

6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS CloudFormation StackSets que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS CloudFormation StackSets como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

Habilitar una cuenta de administrador delegado para Stacksets AWS CloudFormation

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y los roles de esa cuenta pueden realizar acciones administrativas para Stacksets AWS CloudFormation que, de lo contrario, solo pueden realizar usuarios o roles en la cuenta de administración de la organización. Esto te ayuda a separar la administración de la organización de la administración de Stacksets. AWS CloudFormation

Para obtener instrucciones sobre cómo designar una cuenta de miembro como administrador delegado de StackSets AWS CloudFormation en la organización, consulte Registro de un administrador delegado en la Guía del usuario de AWS CloudFormation .

AWS CloudTrail y AWS Organizations

AWS CloudTrail es un AWS servicio que le ayuda a habilitar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de sus Cuenta de AWS Con AWS CloudTrailél, un usuario de una cuenta de administración puede crear un registro de la organización que registre todos los eventos

de todos los Cuentas de AWS miembros de esa organización. Los registros de seguimiento de la organización se aplican automáticamente a todas las cuentas de miembros de la organización. Las cuentas de miembros pueden ver el registro de seguimiento de la organización, pero no pueden modificarlo o eliminarlo. De forma predeterminada, las cuentas de miembros no tienen acceso a los archivos de registro del registro de seguimiento de la organización en el bucket de Amazon S3. Esto lo ayuda a aplicar y reforzar de manera uniforme su estrategia de registro entre las cuentas en su organización.

Para obtener más información, consulte Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Utilice la siguiente información para ayudarle a integrarse AWS CloudTrail con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le CloudTrail permite realizar operaciones de apoyo en las cuentas de su organización.

Puede eliminar o modificar esta función solo si deshabilita el acceso de confianza entre CloudTrail y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForCloudTrail`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza CloudTrail otorgan acceso a los siguientes directores de servicio:

- `cloudtrail.amazonaws.com`

Habilitar el acceso de confianza con CloudTrail

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Si habilitas el acceso confiable mediante la creación de una ruta desde la AWS CloudTrail consola, el acceso confiable se configura automáticamente (recomendado). También puedes habilitar el

acceso confiable mediante la AWS Organizations consola. Debes iniciar sesión con tu cuenta AWS Organizations de administración para crear un registro de la organización.

Si opta por crear un registro de la organización mediante el AWS CLI o el AWS API, debe configurar manualmente el acceso confiable. Para obtener más información, consulte Habilitar CloudTrail como servicio de confianza AWS Organizations en la Guía del AWS CloudTrail usuario.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS CloudTrail consola o las herramientas para permitir la integración con Organizations.

Puede habilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS CloudTrail como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Deshabilitación del acceso con CloudTrail

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

AWS CloudTrail requiere un acceso confiable AWS Organizations para trabajar con los registros de la organización y los almacenes de datos de los eventos de la organización. Si inhabilitas el acceso confiable AWS Organizations mientras lo usas AWS CloudTrail, se eliminarán todos los registros organizativos de las cuentas de los miembros porque no CloudTrail pueden acceder a la organización. Todos los registros de seguimiento de la organización de las cuentas de administración y los almacenes de datos de eventos de la organización se convierten en registros y almacenes de datos de eventos de la cuenta. El `AWSServiceRoleForCloudTrail` rol creado para la integración entre la cuenta CloudTrail y AWS Organizations permanece en ella. Si vuelves a habilitar el acceso confiable, no CloudTrail se realizará ninguna acción en los almacenes de datos de senderos y eventos existentes. La cuenta de administración debe actualizar todos los almacenes de datos de eventos y registros de seguimiento de la cuenta para aplicarlos a la organización.

Para convertir un registro de seguimiento o almacén de datos de eventos de la cuenta en un registro de seguimiento o almacén de datos de eventos de la organización, haga lo siguiente:

- Desde la CloudTrail consola, actualiza el almacén de datos de rutas o eventos y selecciona la opción Activar para todas las cuentas de mi organización.
- Desde allí AWS CLI, haga lo siguiente:
  - Para actualizar una ruta, ejecute el update-trailejecute el comando e incluya el `--is-organization-trail` parámetro.
  - Para actualizar un banco de datos de eventos, ejecute el update-event-data-storecomando e incluya el `--organization-enabled` parámetro.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con AWS CloudTrail. Puede deshabilitar el acceso de confianza solo con las herramientas de Organizations, ya sea mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en una de las AWS SDKs.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS CloudTrail.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS CloudTrail diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS CloudTrail que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS CloudTrail como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Habilitar una cuenta de administrador delegado para CloudTrail

Cuando lo utilizas CloudTrail con Organizations, puedes registrar cualquier cuenta de la organización para que actúe como administrador CloudTrail delegado y gestione los almacenes de datos de eventos y senderos de la organización en nombre de la organización. Un administrador delegado es una cuenta de miembro de una organización que puede realizar las mismas tareas administrativas que la cuenta de administración. CloudTrail

> **Permisos mínimos**
>
> Solo un administrador de la cuenta de administración de Organizations puede registrar un administrador delegado para CloudTrail.

Puede registrar una cuenta de administrador delegado mediante la CloudTrail consola o mediante Organizations `RegisterDelegatedAdministrator` CLI o la SDK operación. Para registrar un administrador delegado mediante la CloudTrail consola, consulte Añadir un administrador CloudTrail delegado.

Deshabilitar un administrador delegado para CloudTrail

Solo un administrador de la cuenta de administración de Organizations puede eliminar a un administrador delegado para CloudTrail. Puede eliminar el administrador delegado mediante la CloudTrail consola o mediante la SDK operación Organizations `DeregisterDelegatedAdministrator` CLI u. Para obtener información sobre cómo eliminar un administrador delegado mediante la CloudTrail consola, consulte Eliminar un administrador CloudTrail delegado.

Amazon CloudWatch y AWS Organizations

Puede usar Organizations for Amazon CloudWatch para descubrir y comprender el estado de la configuración de telemetría de sus AWS recursos desde una vista centralizada en la CloudWatch consola. Esto simplifica el proceso de auditar las configuraciones de recopilación de telemetría en varios tipos de recursos de su organización o cuenta. AWS

Al integrarse con Organizations, puede realizar modificaciones en las configuraciones compatibles con Amazon CloudWatch for Organizations. Debe habilitar el acceso confiable para usar la configuración de telemetría en toda su organización.

Para obtener más información, consulte Auditoría de configuraciones de telemetría en la Guía CloudWatch del usuario de Amazon.

Utiliza la siguiente información para ayudarte a integrar Amazon CloudWatch con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

Cree el siguiente rol vinculado al servicio en la cuenta de administración de su organización. El rol vinculado al servicio se crea automáticamente en las cuentas de los miembros cuando habilitas el acceso confiable. Esta función le CloudWatch permite realizar operaciones compatibles en las cuentas de su organización. Puede eliminar o modificar este rol solo si deshabilita el acceso confiable entre CloudWatch and Organizations o si elimina la cuenta del miembro de la organización.

- `AWSServiceRoleForObservabilityAdmin`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza CloudWatch otorgan acceso a los siguientes directores de servicio:

- `observabilityadmin.amazonaws.com`

Habilitar el acceso de confianza con CloudWatch

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puedes habilitar el acceso de confianza mediante la CloudWatch consola de Amazon o la AWS Organizations consola.

> **Important**
>
> Te recomendamos encarecidamente que, siempre que sea posible, utilices la CloudWatch consola o las herramientas de Amazon para permitir la integración con Organizations. Esto permite a Amazon CloudWatch realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Sigue estos pasos solo si no puedes activar la

integración con las herramientas proporcionadas por Amazon CloudWatch. Para obtener más información, consulte esta nota.
Si habilitas el acceso de confianza mediante la CloudWatch consola o las herramientas de Amazon, no necesitas completar estos pasos.

Para habilitar el acceso confiable mediante la CloudWatch consola

Consulte Activar la auditoría CloudWatch telemétrica en la Guía del CloudWatch usuario de Amazon.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una operación de API en una de las. AWS SDKs

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elige Amazon CloudWatch en la lista de servicios.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de CloudWatch diálogo Habilitar el acceso de confianza para Amazon, escribe enable para confirmar y, a continuación, selecciona Habilitar el acceso de confianza.
6. Si eres el administrador de Only AWS Organizations, dile al administrador de Amazon CloudWatch que ahora puede habilitar ese servicio para que funcione AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Usa los siguientes AWS CLI comandos u operaciones de API para habilitar el acceso a un servicio confiable:

- AWS CLI: enable-aws-service-access

Ejecuta el siguiente comando para habilitar Amazon CloudWatch como un servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal observabilityadmin.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: habilita el AWSService acceso

Deshabilitación del acceso con CloudWatch

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Puedes deshabilitar el acceso de confianza mediante Amazon CloudWatch o las AWS Organizations herramientas.

> **Important**
>
> Te recomendamos encarecidamente que, siempre que sea posible, utilices la CloudWatch consola o las herramientas de Amazon para deshabilitar la integración con Organizations. Esto permite a Amazon CloudWatch realizar cualquier limpieza que necesite, como eliminar recursos o acceder a funciones que el servicio ya no necesita. Continúa con estos pasos solo si no puedes deshabilitar la integración con las herramientas proporcionadas por Amazon CloudWatch.
> Si inhabilitas el acceso de confianza mediante la CloudWatch consola o las herramientas de Amazon, no necesitas completar estos pasos.

Para deshabilitar el acceso de confianza mediante la CloudWatch consola

Consulte Cómo desactivar la auditoría CloudWatch telemétrica en la Guía del usuario de Amazon CloudWatch

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una operación de la API de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Usa los siguientes AWS CLI comandos u operaciones de API para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecuta el siguiente comando para inhabilitar Amazon CloudWatch como servicio de confianza en Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal observabilityadmin.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: deshabilita el AWSService acceso

Habilitar una cuenta de administrador delegado para CloudWatch

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y los roles de esa cuenta pueden realizar acciones administrativas para CloudWatch que, de lo contrario, solo podrían realizarlas los usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la de CloudWatch.

> **Permisos mínimos**
>
> Solo un administrador de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado de CloudWatch la organización.

Puede registrar una cuenta de administrador delegado mediante la CloudWatch consola o mediante la operación `RegisterDelegatedAdministrator` CLI o SDK de Organizations. Para obtener información sobre cómo registrar a un administrador delegado mediante la CloudWatch consola, consulte Activar la auditoría CloudWatch telemétrica en la guía del usuario de Amazon CloudWatch .

Desactivar un administrador delegado para CloudWatch

> **Permisos mínimos**
>
> Solo un administrador de la cuenta de administración de Organizations puede eliminar a un administrador delegado de CloudWatch la organización.

Puede eliminar el administrador delegado mediante la CloudWatch consola o mediante la operación `DeregisterDelegatedAdministrator` CLI o SDK de Organizations. Para obtener más información, consulta Cómo desactivar la auditoría CloudWatch telemétrica en la Guía CloudWatch del usuario de Amazon.

AWS Compute Optimizer y AWS Organizations

AWS Compute Optimizer es un servicio que analiza las métricas de configuración y utilización de sus AWS recursos. Los ejemplos de recursos incluyen instancias de Amazon Elastic Compute Cloud (AmazonEC2) y grupos de Auto Scaling. Compute Optimizer informa si sus recursos son óptimos y genera recomendaciones de optimización para reducir el costo y mejorar el rendimiento de sus cargas de trabajo. Para obtener más información sobre Compute Optimizer, consulte la Guía del usuario de AWS Compute Optimizer.

Utilice la siguiente información para ayudarle a integrarse AWS Compute Optimizer con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Compute Optimizer realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Compute Optimizer y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForComputeOptimizer`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Compute Optimizer otorgan acceso a las siguientes entidades de servicio:

- `compute-optimizer.amazonaws.com`

Habilitación del acceso de confianza Compute Optimizer

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS Compute Optimizer consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Compute Optimizer consola o las herramientas para permitir la integración con Organizations. Esto permite AWS Compute Optimizer realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Compute Optimizer. Para obtener más información, consulte esta nota.
> Si habilitas el acceso confiable mediante la AWS Compute Optimizer consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso de confianza mediante la consola Compute Optimizer

Debe iniciar sesión en la consola de Compute Optimizer mediante la cuenta de administración de su organización. Inscríbase en nombre de su organización siguiendo las instrucciones en Habilitación del acceso a la cuenta en la Guía del usuario de AWS Compute Optimizer .

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Compute Optimizer.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Compute Optimizer diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Compute Optimizer que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Compute Optimizer como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Deshabilitación del acceso de confianza con Compute Optimizer

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con AWS Compute Optimizer.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Compute Optimizer como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Habilitar una cuenta de administrador delegado para Compute Optimizer

Cuando se designa una cuenta de miembro como administrador delegado de la organización, los usuarios y los roles de la cuenta designada pueden administrar los metadatos de la Cuenta de AWS de otras cuentas de miembro de la organización. Si no habilita una cuenta de administrador delegado, estas tareas solo las puede realizar la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de los detalles de la cuenta.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Compute Optimizer en la organización

Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegada para Compute Optimizer, consulte https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html en la Guía del usuario de AWS Compute Optimizer .

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal compute-optimizer.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el principal de servicio de la cuenta `account.amazonaws.com` como parámetros.

Deshabilitar un administrador delegado para Compute Optimizer

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para Compute Optimizer.

Para deshabilitar la cuenta de administrador delegada de Compute Optimizer mediante la consola de Compute Optimizer, consulte https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html en la Guía del usuario de AWS Compute Optimizer .

Para eliminar a un administrador delegado mediante el AWS AWS CLI, consulte deregister-delegated-administratorla Referencia de AWS AWS CLI comandos.

AWS Config y AWS Organizations

La agregación de datos de varias cuentas y regiones AWS Config le permite agregar AWS Config datos de varias cuentas y Regiones de AWS convertirlos en una sola cuenta. La acumulación de datos de varias cuentas y regiones permite a los administradores centrales de TI monitorear la conformidad de varias Cuentas de AWS de la compañía. Un agregador es un tipo de recurso AWS Config que recopila AWS Config datos de varias regiones y cuentas de origen. Cree un agregador en la región en la que desee ver los datos agregados AWS Config . Al crear un agregador, puede optar por agregar una cuenta individual IDs o su organización. Para obtener más información al respecto AWS Config, consulta la Guía para AWS Config desarrolladores.

También se puede utilizar AWS Config APIspara gestionar AWS Config las reglas Cuentas de AWS en toda la organización. Para obtener más información, consulta la sección Habilitar AWS Config reglas en todas las cuentas de tu organización en la Guía para AWS Config desarrolladores.

Utilice la siguiente información como ayuda para realizar la integración AWS Config con AWS Organizations.

Roles vinculados a servicios

La siguiente función vinculada al servicio le permite AWS Config realizar operaciones compatibles en las cuentas de su organización.

- `AWSServiceRoleForConfig`

Obtenga más información sobre la creación de este rol en Permisos para el IAM rol asignado AWS Config en la AWS Config Guía para desarrolladores

Obtenga más información sobre cómo se AWS Config utilizan las funciones vinculadas a servicios en la Guía para desarrolladores AWS ConfigAWS Config

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AWS Config y Organizations, o si elimina la cuenta de miembro de la organización.

Habilitar el acceso de confianza con AWS Config

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la consola o la AWS Config consola. AWS Organizations

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Config consola o las herramientas para permitir la integración con Organizations. Esto permite AWS Config realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Config. Para obtener más información, consulte esta nota.
>
> Si habilitas el acceso confiable mediante la AWS Config consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso confiable mediante la AWS Config consola

Para permitir el acceso confiable al AWS Organizations uso AWS Config, cree un agregador de cuentas múltiples y añada la organización. Para obtener más información sobre cómo configurar un agregador de varias cuentas, consulte Creating Aggregators en la Guía del desarrollador de AWS Config .

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las. AWS SDKs

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Config.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Config diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.

6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Config que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Config como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Deshabilitación del acceso con AWS Config

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

Ejecute el siguiente comando para inhabilitarlo AWS Config como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal config.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Centro de optimización de costes de AWS y AWS Organizations

Centro de optimización de costes de AWS es una función de AWS Billing and Cost Management que le ayuda a consolidar y priorizar las recomendaciones de optimización de costos en todas sus AWS cuentas y AWS regiones, para que pueda aprovechar al máximo sus AWS gastos. Cuando utiliza Cost Optimization Hub con, AWS Organizations puede identificar, filtrar y agregar fácilmente las recomendaciones de optimización de AWS costos en las cuentas de los miembros y AWS regiones de su Organización.

Para obtener más información, consulte Centro de optimización de costos en la Guía del usuario de AWS Cost Management .

Utilice la siguiente información para ayudarle a integrarse Centro de optimización de costes de AWS con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite al Centro de optimización de costos llevar a cabo operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Centro de optimización de costos y Organizations, o si elimina la cuenta de miembro de la organización.

Para obtener más información, consulte Service-linked role permissions for Cost Optimization Hub en la Guía del usuario de AWS Cost Management .

- `AWSServiceRoleForCostOptimizationHub`

Entidades principales del servicio utilizadas por Centro de optimización de costos

Centro de optimización de costos utiliza la entidad principal de servicio de `cost-optimization-hub.bcm.amazonaws.com`.

Habilitación del acceso de confianza con Centro de optimización de costos

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Cuando activa el uso de la cuenta de administración de su organización e incluye todas las cuentas de miembro de la organización, el acceso de confianza de Centro de optimización de costos se habilita automáticamente en la cuenta de su organización.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en uno de los AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija Centro de optimización de costes de AWS.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de Centro de optimización de costes de AWS diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador Centro de optimización de costes de AWS que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo Centro de optimización de costes de AWS como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Deshabilitación del acceso de confianza

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

> **Important**
>
> Si deshabilita el acceso de confianza de Centro de optimización de costos después de registrarse, Centro de optimización de costos deniega el acceso a las recomendaciones de las cuentas de miembro de su organización. Además, las cuentas de miembro de la organización no están habilitadas para Centro de optimización de costos. Para obtener más información, consulte Cost Optimization Hub and Organizations trusted access en la Guía del usuario de AWS Cost Management .

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo Centro de optimización de costes de AWS como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

Activación de una cuenta de administrador delegado para Centro de optimización de costos

Cuando designa una cuenta de miembro como administrador delegado para la organización, la cuenta designada puede recuperar las recomendaciones de Centro de optimización de costos para todas las cuentas de su organización y administrar las preferencias de Centro de optimización de costos, lo que le brinda una mayor flexibilidad para identificar de forma centralizada las oportunidades de optimización de recursos.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations con el siguiente permiso puede configurar una cuenta de miembro como administrador delegado para Centro de optimización de costos en la organización:

Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegado para Centro de optimización de costos, consulte Delegate an administrator account en la Guía del usuario de AWS Cost Management .

Desactivación de un administrador delegado para Centro de optimización de costos

Solo un administrador de la cuenta de administración de Organizations puede eliminar un administrador delegado para Centro de optimización de costos.

Para deshabilitar la cuenta de administrador delegado del Centro de optimización de costos mediante la consola, consulte Delegate an administrator account en la Guía del usuario de AWS Cost Management .

Para eliminar un administrador delegado mediante el AWS CLI, consulte `deregister-delegated-administrator`la AWS Config CLIReferencia.

AWS Control Tower y AWS Organizations

AWS Control Tower ofrece una forma sencilla de configurar y gobernar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas. AWS Control Tower la orquestación amplía las capacidades de. AWS Organizations AWS Control Tower aplica controles preventivos y de detección (barreras) para evitar que sus organizaciones y cuentas se aparten de las mejores prácticas (desviaciones).

AWS Control Tower la orquestación amplía las capacidades de. AWS Organizations

Para obtener más información, consulte la Guía del usuario de AWS Control Tower .

Utilice la siguiente información para ayudarle a integrarse AWS Control Tower con AWS Organizations.

Roles necesarios para la integración

El rol `AWSControlTowerExecution` debe estar presente en todas las cuentas inscritas. Permite AWS Control Tower administrar sus cuentas individuales y enviar información sobre ellas a sus cuentas de Audit y Log Archive.

Para obtener más información sobre los roles utilizados por AWS Control Tower, consulte Cómo AWS Control Tower funciona con los roles para crear y administrar cuentas y Uso de políticas basadas en la identidad (IAMpolíticas) para. AWS Control Tower

Principios de servicio utilizados por AWS Control Tower

AWS Control Tower utiliza el principal `controltower.amazonaws.com` de servicio.

Habilitar el acceso de confianza con AWS Control Tower

AWS Control Tower utiliza un acceso confiable para detectar desviaciones, realizar controles preventivos y realizar un seguimiento de los cambios en la cuenta y la unidad organizativa que provocan desviaciones.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede habilitar el acceso confiable mediante las herramientas de Organizations.

Para habilitar el acceso de confianza desde la consola de Organizations, seleccione **Enable access** junto a AWS Control Tower.

Puede habilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Control Tower como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Deshabilitación del acceso con AWS Control Tower

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

> **Important**
>
> Si desactivas AWS Control Tower el acceso de confianza, tu zona de AWS Control Tower aterrizaje se verá desplazada. La única forma de corregir la deriva es utilizar la reparación de la zona de aterrizaje de AWS Control Tower. Volver a habilitar el acceso confiable en

Organizaciones no soluciona la deriva. Obtenga más información sobre la deriva en la guía del usuario de AWS Control Tower .

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Control Tower como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

Amazon Detective y AWS Organizations

Amazon Detective utiliza sus datos de registro para generar visualizaciones que le permiten analizar, investigar e identificar la causa raíz de los hallazgos de seguridad o actividades sospechosas.

AWS Organizations El uso le permite asegurarse de que su gráfico de comportamiento de Detective proporcione visibilidad de la actividad en todas las cuentas de su organización.

Cuando concede acceso de confianza a Detective, el servicio Detective puede reaccionar automáticamente a los cambios en la membresía de la organización. El administrador delegado puede habilitar cualquier cuenta de organización como cuenta de miembro en el gráfico de comportamiento. El Detective también puede habilitar automáticamente nuevas cuentas de organización como cuentas de miembro. Las cuentas de organización no pueden desasociarse del gráfico de comportamiento.

Para obtener más información, consulte Uso de Amazon Detective en su organización en la Guía de administración de Amazon Detective.

Utilice la siguiente información para ayudarle a integrar Amazon Detective con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Detective realizar operaciones soportadas por las cuentas de su organización.

Puede eliminar o modificar este rol sólo si desactiva el acceso de confianza entre Detective y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForDetective`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de Detective conceden acceso a las siguientes entidades principales de servicio:

- `detective.amazonaws.com`

Para habilitar el acceso de confianza con Detective

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

> **Note**
>
> Cuando se designa un administrador delegado para Amazon Detective, se Detective habilita automáticamente el acceso de confianza para Detective en su organización.
> Detective necesita un acceso confiable AWS Organizations antes de poder designar una cuenta de miembro como administrador delegado de este servicio para su organización.

Solo puede habilitar el acceso confiable mediante las herramientas de Organizations.

Puede habilitar el acceso confiable mediante la AWS Organizations consola.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elija Amazon Detective en la lista de servicios.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso de confianza para Amazon Detective, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si eres el administrador de Only AWS Organizations, dile al administrador de Amazon Detective que ahora puede habilitar ese servicio para que funcione AWS Organizations desde la consola de servicios.

Para desactivar el acceso de confianza con Detective

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con Amazon Detective.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elija Amazon Detective en la lista de servicios.
4. Seleccione Deshabilitar el acceso de confianza.

5. En el cuadro de diálogo Inhabilitar el acceso de confianza para Amazon Detective, escriba disable para confirmar y, a continuación, seleccione Disable Trusted Access.
6. Si usted es el administrador de Only AWS Organizations, dígale al administrador de Amazon Detective que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas;.

Habilitación de una cuenta de administrador delegado para Detective

La cuenta de administrador delegado de Detective es la cuenta de administrador de un gráfico de comportamiento de Detective. El administrador delegado determina qué cuentas de organización se van a habilitar y desactivar como cuentas de miembro en ese gráfico de comportamiento. El administrador delegado puede configurar Detective para habilitar automáticamente nuevas cuentas de organización como cuentas de miembro a medida que se agregan a la organización. Para obtener información sobre cómo un administrador delegado administra las cuentas de la organización, consulte Gestión de cuentas de organización como cuentas de miembro en la Guía de administración de Amazon Detective.

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para Detective.

Puede especificar una cuenta de administrador delegado desde la consola de Detective o API bien mediante la SDK operación Organizations CLI u.

> **Permisos mínimos**
>
> Sólo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Detective en la organización

Para configurar un administrador delegado mediante la consola de Detective oAPI, consulte Designación de una cuenta de administrador de Detectives para una organización en la Guía de administración de Amazon Detective.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal detective.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el principal de servicio de la cuenta `account.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para Detective

Puede eliminar al administrador delegado mediante la consola de Detective o API mediante la SDK operación Organizations `DeregisterDelegatedAdministrator` CLI u. Para obtener información sobre cómo eliminar a un administrador delegado mediante la consola de Detectives o las Organizaciones APIAPI, consulte Designación de una cuenta de administrador de detectives para una organización en la Guía de administración de Detectives de Amazon.

Amazon DevOps Guru y AWS Organizations

Amazon DevOps Guru analiza los datos operativos y las métricas y eventos de las aplicaciones para identificar comportamientos que se desvían de los patrones operativos normales. Los usuarios reciben una notificación cuando DevOps Guru detecta un problema o riesgo operativo.

El uso de DevOps Guru permite el soporte multicuenta AWS Organizations, por lo que puede designar una cuenta de miembro para gestionar la información de toda la organización. A continuación, este administrador delegado puede ver, ordenar y filtrar información de todas las cuentas de su organización para desarrollar una visión holística del estado de todas las aplicaciones supervisadas de su organización sin necesidad de personalización adicional.

Para obtener más información, consulte Supervisar las cuentas de su organización en la Guía del usuario de Amazon DevOps Guru.

Utilice la siguiente información para ayudarle a integrar Amazon DevOps Guru con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le permite a DevOps Guru realizar operaciones de soporte en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre DevOps Guru y Organizations, o si elimina la cuenta del miembro de la organización.

- `AWSServiceRoleForDevOpsGuru`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza DevOps Guru otorgan acceso a los siguientes directores de servicio:

- `devops-guru.amazonaws.com`

Para obtener más información, consulte Uso de roles vinculados a servicios para DevOps Guru en la Guía del usuario de Amazon DevOps Guru.

Para habilitar el acceso confiable con Guru DevOps

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

> **Note**
>
> Cuando designa un administrador delegado para Amazon DevOps Guru, DevOps Guru habilita automáticamente el acceso confiable de DevOps Guru para su organización. DevOpsGuru necesita un acceso confiable AWS Organizations antes de poder designar una cuenta de miembro como administrador delegado de este servicio para su organización.

> **Important**
>
> Le recomendamos encarecidamente que, siempre que sea posible, utilice la consola o las herramientas de Amazon DevOps Guru para permitir la integración con Organizations. Esto permite a Amazon DevOps Guru realizar cualquier configuración que necesite, como la creación de los recursos que necesite el servicio. Siga estos pasos solo si no puede habilitar la integración con las herramientas que proporciona Amazon DevOps Guru. Para obtener más información, consulte esta nota.

Puede habilitar el acceso confiable mediante la AWS Organizations consola o la consola de DevOps Guru.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de Amazon DevOps Guru, elija el nombre del servicio y, a continuación, elija Habilitar acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si es el administrador de Only AWS Organizations, dígale al administrador de Amazon DevOps Guru que ahora puede habilitar ese servicio mediante su consola para trabajar con él AWS Organizations.

DevOps Guru console

Para habilitar el acceso a un servicio confiable mediante la consola de DevOps Guru

1. Inicie sesión como administrador en la cuenta de administración y abra la consola DevOps Guru: Amazon DevOps Guru console
2. Elija Habilitar acceso de confianza.

Para deshabilitar el acceso de confianza con DevOps Guru

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con Amazon DevOps Guru.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elige Amazon DevOps Guru en la lista de servicios.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de diálogo Disable Trusted Access for Amazon DevOps Guru, escriba disable para confirmar y, a continuación, seleccione Disable Trusted Access.
6. Si usted es el administrador de Only AWS Organizations, dígale al administrador de Amazon DevOps Guru que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas;.

Habilitar una cuenta de administrador delegado para Guru DevOps

La cuenta de administrador delegado de DevOps Guru puede ver los datos de información de todas las cuentas de miembros incorporadas a DevOps Guru desde la organización. Para obtener información sobre cómo un administrador delegado administra las cuentas de la organización, consulte Supervisar las cuentas de su organización en la Guía del usuario de Amazon DevOps Guru.

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para DevOps Guru.

Puede especificar una cuenta de administrador delegado desde la consola de DevOps Guru o mediante la SDK operación Organizations `RegisterDelegatedAdministrator` CLI u.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado de DevOps Guru en la organización.

DevOps Guru console

Para configurar un administrador delegado en la consola de Guru DevOps

1. Inicie sesión como administrador en la cuenta de administración y abra la consola DevOps Guru: Amazon DevOps Guru console
2. Elija Registrar administrador delegado. Puede elegir una cuenta de administración o cualquier cuenta de miembro como administrador delegado.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el principal de servicio de la cuenta `account.amazonaws.com` como parámetros.

Deshabilitar un administrador delegado para Guru DevOps

Puede eliminar el administrador delegado mediante la consola de DevOps Guru o mediante la SDK operación Organizations `DeregisterDelegatedAdministrator` CLI u. Para obtener información sobre cómo eliminar a un administrador delegado mediante la consola de DevOps Guru, consulte Supervisar las cuentas de su organización en la Guía del usuario de Amazon DevOps Guru.

AWS Directory Service y AWS Organizations

AWS Directory Service para Microsoft Active Directory, o bien AWS Managed Microsoft AD, le permite ejecutar Microsoft Active Directory (AD) como un servicio gestionado. AWS Directory Service facilita la configuración y la ejecución de directorios en la AWS nube o la conexión de sus AWS recursos con un Microsoft Active Directory local existente. AWS Managed Microsoft AD también se integra perfectamente AWS Organizations para permitir un uso compartido de directorios sin

problemas en varias regiones Cuentas de AWS y VPC en cualquier otra región. Para obtener más información, consulte la Guía de administración de AWS Directory Service.

Para compartir un directorio AWS Directory Service entre una organización, la organización debe tener habilitadas todas las funciones y el directorio debe estar en la cuenta de administración de la organización.

Utilice la siguiente información para ayudarle a integrarse AWS Directory Service con AWS Organizations.

Habilitar el acceso de confianza con AWS Directory Service

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS Directory Service consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Directory Service consola o las herramientas para permitir la integración con Organizations. Esto permite AWS Directory Service realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Directory Service. Para obtener más información, consulte esta nota.
> Si habilitas el acceso confiable mediante la AWS Directory Service consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso confiable mediante la AWS Directory Service consola

Para compartir un directorio, que habilita automáticamente el acceso de confianza, consulte Compartir el directorio en la Guía de administración AWS Directory Service . Para step-by-step obtener instrucciones, consulte el tutorial: Cómo compartir su directorio AWS administrado de Microsoft AD.

Puede habilitar el acceso confiable mediante la AWS Organizations consola.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Directory Service.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso de confianza para AWS Directory Service, escriba habilitar para confirmar y, a continuación, elija Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Directory Service que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

Deshabilitación del acceso con AWS Directory Service

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Si deshabilita el acceso de confianza AWS Organizations mientras lo usa AWS Directory Service, todos los directorios compartidos anteriormente seguirán funcionando con normalidad. Sin embargo, ya no podrá compartir nuevos directorios en la organización hasta que rehabilite el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.

3. En la lista de servicios, elija AWS Directory Service.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS Directory Service diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Directory Service que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas;.

Amazon Elastic Compute Cloud y AWS Organizations

Amazon Elastic Compute Cloud proporciona capacidad informática escalable y bajo demanda en la AWS nube. Cuando utilizas Amazon EC2 with Organizations, permites que el administrador de la organización cree un informe sobre la configuración existente para las cuentas de su organización después de utilizar la función EC2 de políticas declarativas de Amazon.

Utilice la siguiente información para ayudarle a integrar Amazon Elastic Compute Cloud con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función permite EC2 a Amazon realizar operaciones compatibles en las cuentas de su organización.

Puedes eliminar o modificar este rol solo si inhabilitas el acceso de confianza entre Amazon EC2 y Organizations, o si eliminas la cuenta de miembro de la organización.

- `AWSServiceRoleForDeclarativePoliciesEC2Report`

Principios de servicio utilizados por Amazon EC2

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Las funciones vinculadas a servicios que utiliza Amazon EC2 otorgan acceso a los siguientes directores de servicio:

- `report.declarative-policies-ec2.amazonaws.com`

Habilitar el acceso confiable con Amazon EC2

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Para permitir que el administrador de Organizations cree un informe sobre la configuración existente para las cuentas de su organización, debes habilitar el acceso confiable.

Solo puede habilitar el acceso confiable mediante las herramientas de Organizations.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elija Amazon Elastic Compute Cloud en la lista de servicios.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso de confianza para Amazon Elastic Compute Cloud, escribe enable para confirmar y, a continuación, selecciona Habilitar el acceso de confianza.
6. Si usted es el administrador de Only AWS Organizations, dígale al administrador de Amazon Elastic Compute Cloud que ahora puede habilitar ese servicio para que funcione AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

Ejecute el siguiente comando para habilitar Amazon Elastic Compute Cloud como un servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal report.declarative-policies-ec2.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Deshabilitación del acceso de confianza

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para deshabilitar Amazon Elastic Compute Cloud como un servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal report.declarative-policies-ec2.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

AWS Firewall Manager y AWS Organizations

AWS Firewall Manager es un servicio de administración de seguridad que se utiliza para configurar y gestionar de forma centralizada las reglas de firewall y otras protecciones en todas las Cuentas de AWS aplicaciones de su organización. Con Firewall Manager, puede implementar AWS WAF reglas, crear AWS Shield Advanced protecciones, configurar y auditar los grupos de seguridad de Amazon Virtual Private Cloud (AmazonVPC) e implementar AWS Network Firewall s. Utilice Firewall Manager para configurar las reglas de protección una única vez de forma que se apliquen automáticamente en todas las cuentas y recursos de la organización, incluso cuando se agreguen nuevas cuentas y recursos. Para obtener más información al respecto AWS Firewall Manager, consulte la Guía para AWS Firewall Manager desarrolladores.

Utilice la siguiente información como ayuda para realizar la integración AWS Firewall Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Firewall Manager realizar operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Firewall Manager y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForFMS`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Firewall Manager otorgan acceso a las siguientes entidades de servicio:

- `fms.amazonaws.com`

Habilitación del acceso de confianza Firewall Manager

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS Firewall Manager consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Firewall Manager consola o las herramientas para permitir la integración con Organizations. Esto permite AWS Firewall Manager realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Firewall Manager. Para obtener más información, consulte esta nota.
> Si habilitas el acceso confiable mediante la AWS Firewall Manager consola o las herramientas, no necesitas completar estos pasos.

Debe iniciar sesión con su cuenta AWS Organizations de administración y configurar una cuenta dentro de la organización como cuenta de AWS Firewall Manager administrador. Para obtener más información, consulte Establecimiento de la cuenta de administrador de AWS Firewall Manager en la Guía para desarrolladores AWS Firewall Manager .

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Firewall Manager.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Firewall Manager diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Firewall Manager que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Firewall Manager como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Deshabilitación del acceso de confianza con Firewall Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Puede deshabilitar el acceso de confianza mediante las herramientas AWS Firewall Manager o las AWS Organizations herramientas.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Firewall Manager consola o las herramientas para deshabilitar la integración con Organizations. Esto permite AWS Firewall Manager realizar cualquier limpieza que sea necesaria, como eliminar recursos o acceder a funciones que el servicio ya no necesite. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas por AWS Firewall Manager.
> Si inhabilitas el acceso de confianza mediante la AWS Firewall Manager consola o las herramientas, no necesitas completar estos pasos.

Para deshabilitar el acceso de confianza mediante la consola Firewall Manager

Puedes cambiar o revocar la cuenta de AWS Firewall Manager administrador siguiendo las instrucciones de la Guía para AWS Firewall Manager desarrolladores sobre cómo designar una cuenta diferente como cuenta de AWS Firewall Manager administrador.

Si revoca la cuenta de administrador, debe iniciar sesión en la cuenta de AWS Organizations administración y configurar una nueva cuenta de administrador para. AWS Firewall Manager

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Firewall Manager.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS Firewall Manager diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Firewall Manager que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Firewall Manager como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal fms.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Para habilitar una cuenta de administrador delegado para Firewall Manager

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para Firewall Manager que, de lo contrario, solo pueden ser realizadas por usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión de Firewall Manager.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Firewall Manager en la organización.

Para obtener instrucciones sobre cómo designar una cuenta de miembro como administradora del Firewall Manager de la organización, consulte Configurar la cuenta de AWS Firewall Manager administrador en la Guía para AWS Firewall Manager desarrolladores.

Amazon GuardDuty y AWS Organizations

Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa diversas fuentes de datos, utilizando fuentes de inteligencia sobre amenazas y aprendizaje automático para identificar actividades inesperadas, potencialmente no autorizadas y maliciosas en su AWS entorno. Esto puede incluir problemas como la escalada de privilegios, el uso de credenciales expuestas, la comunicación con direcciones IP o dominios maliciosos o la presencia de malware en las instancias de Amazon Elastic Compute Cloud y en las cargas de trabajo de los contenedores. URLs

Puede ayudar a simplificar la administración GuardDuty utilizando Organizations para administrar GuardDuty todas las cuentas de su organización.

Para obtener más información, consulta Administrar GuardDuty cuentas con AWS Organizations en la Guía del GuardDuty usuario de Amazon

Utiliza la siguiente información para ayudarte a integrar Amazon GuardDuty con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

Los siguientes roles vinculados al servicio se crean automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Estas funciones le GuardDuty permiten realizar operaciones de soporte en las cuentas de su organización. Puedes eliminar un rol solo si inhabilitas el acceso de confianza entre GuardDuty and Organizations o si eliminas la cuenta del miembro de la organización.

- El rol `AWSServiceRoleForAmazonGuardDuty` vinculado al servicio se crea automáticamente en las cuentas que se han integrado con GuardDuty Organizations. Para obtener más información, consulta Gestión de GuardDuty cuentas con Organizations en la Guía del GuardDuty usuario de Amazon
- El rol `AmazonGuardDutyMalwareProtectionServiceRolePolicy` vinculado al servicio se crea automáticamente en las cuentas que tienen habilitada la protección GuardDuty contra malware. Para obtener más información, consulte Permisos de roles vinculados a servicios para GuardDuty Malware Protection en la Guía del usuario de Amazon GuardDuty

Los principales de servicios utilizados por los roles vinculados a servicios

- `guardduty.amazonaws.com`, utilizado por el rol vinculado al servicio `AWSServiceRoleForAmazonGuardDuty`.
- `malware-protection.guardduty.amazonaws.com`, utilizado por el rol vinculado al servicio `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

Habilitar el acceso de confianza con GuardDuty

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puedes habilitar el acceso de confianza a través de Amazon GuardDuty.

Amazon GuardDuty requiere un acceso de confianza AWS Organizations antes de que puedas designar una cuenta de miembro como GuardDuty administrador de tu organización. Si configuras un

administrador delegado mediante la GuardDuty consola, te habilita GuardDuty automáticamente el acceso de confianza.

Sin embargo, si desea configurar una cuenta de administrador delegado mediante la AWS CLI o una de las AWS SDKs, debe llamar explícitamente a la operación E nableAWSService Access y proporcionar la principal de servicio como parámetro. A continuación, puede llamar EnableOrganizationAdminAccountpara delegar la cuenta de GuardDuty administrador.

Deshabilitación del acceso con GuardDuty

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecuta el siguiente comando para inhabilitar Amazon GuardDuty como servicio de confianza en Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

Habilitar una cuenta de administrador delegado para GuardDuty

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y los roles de esa cuenta pueden realizar acciones administrativas para GuardDuty que,

de lo contrario, solo podrían realizarlas los usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la de GuardDuty.

> **Permisos mínimos**
>
> Para obtener información sobre los permisos necesarios para designar una cuenta de miembro como administrador delegado, consulte Permisos necesarios para designar un administrador delegado en la Guía del usuario de Amazon GuardDuty

Para designar una cuenta de miembro como administrador delegado para GuardDuty

Consulte Designar un administrador delegado y añadir cuentas de miembros (consola) y Designar un administrador delegado y añadir cuentas de miembros () API

AWS Health y AWS Organizations

AWS Health proporciona una visibilidad continua del rendimiento de sus recursos y de la disponibilidad de sus Servicios de AWS cuentas. AWS Health ofrece eventos en los que sus AWS recursos y servicios se ven afectados por un problema o se verán afectados por cambios futuros. Tras activar la vista de la organización, un usuario de la cuenta de administración de la organización puede agregar AWS Health eventos en todas las cuentas de la organización. La vista organizativa solo muestra AWS Health los eventos entregados después de que la función esté habilitada y los conserva durante 90 días.

Puede habilitar la vista de la organización mediante la AWS Health consola, el AWS Command Line Interface (AWS CLI) o el AWS Health API.

Para obtener más información, consulte Agregar AWS Health eventos en la Guía del AWS Health usuario.

Utilice la siguiente información para ayudarle a integrarse AWS Health con AWS Organizations.

Roles vinculados a servicios de integración

La función `AWSServiceRoleForHealth_Organizations` vinculada al servicio permite AWS Health realizar operaciones compatibles en las cuentas de su organización.

Este rol se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso confiable llamando a la EnableHealthServiceAccessForOrganizationAPIoperación. De lo

contrario, cree el rol mediante la AWS Health consola o APICLI, tal y como se describe en la sección Creación de un rol vinculado a un servicio de la Guía del IAMusuario.

Puede eliminar o modificar este rol solo si deshabilita el acceso confiable entre AWS Health and Organizations o si elimina la cuenta del miembro de la organización.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza AWS Health otorgan acceso a los siguientes directores de servicio:

- `health.amazonaws.com`

Habilitar el acceso de confianza con AWS Health

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Al activar la función de visualización de la organización AWS Health, el acceso confiable también se habilita automáticamente.

Puede habilitar el acceso confiable mediante la AWS Health consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Health consola o las herramientas para permitir la integración con Organizations. Esto permite AWS Health realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Health. Para obtener más información, consulte esta nota.
>
> Si habilitas el acceso confiable mediante la AWS Health consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso confiable mediante la AWS Health consola

Puede habilitar el acceso de confianza mediante AWS Health una de las siguientes opciones:

- Usa la AWS Health consola. Para obtener más información, consulte Vista organizativa (consola) en la Guía del usuario de AWS Health .
- Utilice la AWS CLI. Para obtener más información, consulte Vista organizativa (CLI) en la Guía del AWS Health usuario.
- Llame a la EnableHealthServiceAccessForOrganizationAPIoperación.

Puede habilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Health como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Deshabilitación del acceso con AWS Health

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Tras deshabilitar la función de visualización de la organización, AWS Health deja de agregar eventos para todas las demás cuentas de la organización. Esto también deshabilita automáticamente el acceso de confianza.

Puede deshabilitar el acceso de confianza mediante las herramientas AWS Health o las AWS Organizations herramientas.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Health consola o las herramientas para deshabilitar la integración con Organizations. Esto permite AWS Health realizar cualquier limpieza que sea necesaria, como eliminar recursos o acceder a funciones que el servicio ya no necesite. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas por AWS Health.
> Si inhabilitas el acceso de confianza mediante la AWS Health consola o las herramientas, no necesitas completar estos pasos.

Para deshabilitar el acceso de confianza mediante la AWS Health consola

Puede deshabilitar el acceso de confianza con una de las siguientes opciones:

- Usa la AWS Health consola. Para obtener más información, consulte Deshabilitar la vista organizativa (consola) en la Guía del usuario de AWS Health .
- Utilice la AWS CLI. Para obtener más información, consulte Desactivar la vista de organización (CLI) en la Guía del AWS Health usuario.
- Llame a la DisableHealthServiceAccessForOrganizationAPIoperación.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Health como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal health.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Habilitar una cuenta de administrador delegado para AWS Health

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y los roles de esa cuenta pueden realizar acciones administrativas para AWS Health que, de lo contrario, solo podrían realizarlas los usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la de AWS Health.

Para designar una cuenta de miembro como administrador delegado para AWS Health

Consulte Registrar un administrador delegado de la vista organizacional

Para eliminar un administrador delegado para AWS Health

Consulte Eliminar un administrador delegado de la vista organizacional

AWS Identity and Access Management y AWS Organizations

AWS Identity and Access Management es un servicio web para controlar de forma segura el acceso a AWS los servicios.

Puede utilizar los datos del último acceso al servicio de IAM para conocer mejor la actividad de AWS en su organización. Puede utilizar estos datos para crear y actualizar las políticas de control de servicios (SCPs) que restringen el acceso únicamente a los AWS servicios que utilizan las cuentas de su organización.

Para ver un ejemplo, consulte Uso de datos para ajustar los permisos de una unidad organizativa en la Guía del usuario de IAM.

IAM le permite administrar de forma centralizada las credenciales de los usuarios raíz y realizar tareas privilegiadas en las cuentas de los miembros. Tras activar la gestión del acceso raíz, que permite un acceso fiable a IAM AWS Organizations, podrá proteger de forma centralizada las credenciales de los usuarios raíz de las cuentas de los miembros. Las cuentas de miembros no pueden iniciar sesión con su usuario raíz ni recuperar la contraseña de su usuario raíz. La cuenta de administración o una cuenta de administrador delegado para IAM también pueden realizar algunas tareas privilegiadas en las cuentas de los miembros mediante el acceso raíz de corta duración.

Las sesiones con privilegios de corta duración le proporcionan credenciales temporales que puede utilizar para realizar acciones con privilegios en la cuenta de un miembro de su organización.

Para obtener más información, consulte Administrar de forma centralizada el acceso raíz de las cuentas de los miembros en la Guía del usuario de IAM.

Utilice la siguiente información para ayudarle a integrarse AWS Identity and Access Management con AWS Organizations.

Habilitar un acceso confiable con IAM

Al habilitar la administración del acceso raíz, se habilita el acceso confiable para IAM in. AWS Organizations

Inhabilitar el acceso de confianza con IAM

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta de AWS Organizations administración puede deshabilitar el acceso de confianza con. AWS Identity and Access Management

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una operación de la API de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Identity and Access Management.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS Identity and Access Management diálogo Desactivar el acceso de confianza para, escribe disable para confirmar y, a continuación, selecciona Inhabilitar el acceso de confianza.

6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Identity and Access Management que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puedes usar los siguientes AWS CLI comandos u operaciones de API para deshabilitar el acceso a un servicio confiable:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Identity and Access Management como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal iam.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: deshabilita el AWSService acceso

Habilitación de una cuenta de administrador delegado para IAM

Al designar una cuenta de miembro como administrador delegado de la organización, los usuarios y las funciones de esa cuenta pueden realizar tareas privilegiadas en las cuentas de los miembros que, de otro modo, solo podrían realizar los usuarios o los roles de la cuenta de administración de la organización. Para obtener más información, consulte Realizar una tarea privilegiada en una cuenta de miembro de Organizations en la Guía del usuario de IAM.

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para IAM.

Puede especificar una cuenta de administrador delegado desde la consola o la API de IAM, o mediante la operación CLI o SDK de Organizations.

Inhabilitar un administrador delegado para IAM

Solo un administrador de la cuenta de administración de Organizations o de la cuenta de administrador delegado de IAM puede eliminar una cuenta de administrador delegado de la organización. Puede deshabilitar la administración delegada mediante la operación `DeregisterDelegatedAdministrator` CLI o SDK de Organizations.

Amazon Inspector y AWS Organizations

Amazon Inspector es un servicio automatizado de gestión de vulnerabilidades que analiza continuamente las cargas de trabajo de Amazon EC2 y de los contenedores para detectar vulnerabilidades de software y exposiciones no intencionadas en la red.

Con Amazon Inspector, puede administrar varias cuentas asociadas simplemente delegando una cuenta de administrador para Amazon Inspector. AWS Organizations El administrador delegado administra Amazon Inspector para la organización y recibe permisos especiales para realizar tareas en nombre de su organización, tales como:

- Habilitar o desactivar los análisis de cuentas de miembro
- Ver datos de búsqueda agregados de toda la organización
- Crear y administrar reglas de supresión

Para obtener más información, consulte Administración de varias cuentas con AWS Organizations en la Guía del usuario de Amazon Inspector.

Utilice la siguiente información para ayudarle a integrar Amazon Inspector con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Amazon Inspector realizar operaciones soportadas en las cuentas de su organización.

Puede eliminar o modificar este rol sólo si desactiva el acceso de confianza entre Amazon Inspector y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForAmazonInspector2`

Para obtener más información, consulte Uso de roles vinculados a servicios de Amazon Inspector en la Guía del usuario de Amazon Inspector.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio utilizados por Amazon Inspector permiten el acceso a los siguientes entidades de servicio:

- `inspector2.amazonaws.com`

Para habilitar el acceso de confianza con Amazon Inspector

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Amazon Inspector requiere un acceso AWS Organizations de confianza antes de poder designar una cuenta de miembro como administrador delegado de este servicio para su organización.

Al designar un administrador delegado para Amazon Inspector, Amazon Inspector habilita automáticamente el acceso de confianza a Amazon Inspector para su organización.

Sin embargo, si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, debe llamar explícitamente a la `EnableAWSServiceAccess` operación y proporcionar el principal del servicio como parámetro. A continuación, puede llamar a `EnableDelegatedAdminAccount` para delegar la cuenta de administrador del Inspector.

Puede habilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitar Amazon Inspector como un servicio de confianza en Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS APIR: nableAWSServiceAcceso electrónico

> **Note**
>
> Si está utilizando la `EnableAWSServiceAccess`API, también debe llamar para `EnableDelegatedAdminAccount`delegar la cuenta de administrador del Inspector.

Para desactivar el acceso de confianza con Amazon Inspector

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con Amazon Inspector.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para deshabilitar Amazon Inspector como servicio de confianza en Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: isableAWSServiceAcceso 3D

Habilitación de una cuenta de administrador delegado para Amazon Inspector

Con Amazon Inspector, puede administrar varias cuentas de una organización mediante un administrador delegado con AWS Organizations servicio.

La cuenta AWS Organizations de administración designa una cuenta de la organización como cuenta de administrador delegado de Amazon Inspector. El administrador delegado administra Amazon Inspector para la organización y se le conceden permisos especiales para realizar tareas en nombre de su organización, tales como: habilitar o desactivar los escaneos para las cuentas de los miembros, ver los datos de búsqueda agregados de toda la organización y crear y administrar las reglas de supresión

Para obtener información sobre cómo un administrador delegado administra las cuentas de la organización, consulte Descripción de la relación entre las cuentas de administrador y de miembro en la Guía del usuario de Amazon Inspector.

Sólo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para Amazon Inspector.

Puede especificar una cuenta de administrador delegado desde la consola de Amazon Inspector o API bien mediante la SDK operación Organizations CLI u.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Amazon Inspector en la organización

Para configurar un administrador delegado mediante la consola de Amazon Inspector, consulte Paso 1: Habilitar Amazon Inspector - Entorno multicuenta en la Guía del usuario de Amazon Inspector.

> **Note**
>
> Debe llamar a `inspector2:enableDelegatedAdminAccount` en cada región en la que se utiliza Amazon Inspector.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el principal de servicio de la cuenta `account.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para Amazon Inspector

Solo un administrador de la cuenta AWS Organizations de administración puede eliminar una cuenta de administrador delegado de la organización.

Puede eliminar al administrador delegado mediante la consola de Amazon Inspector o API mediante la SDK operación Organizations `DeregisterDelegatedAdministrator` CLI u. Para quitar un administrador delegado mediante la consola de Amazon Inspector, consulte Eliminación de un administrador delegado en la Guía del usuario de Amazon Inspector.

AWS License Manager y AWS Organizations

AWS License Manager agiliza el proceso de llevar las licencias de los proveedores de software a la nube. A medida que vaya creando una infraestructura en la nube AWS, podrá ahorrar costes al aprovechar bring-your-own-license (BYOL) las oportunidades, es decir, al reutilizar su inventario de licencias existente para utilizarlo con los recursos de la nube. Con controles basados en reglas en el consumo de licencias, los administradores pueden establecer límites fijos o flexibles en las implementaciones nuevas o existentes en la nube, impidiendo de este modo el uso de servidor no conforme antes de que se produzca.

Para obtener más información acerca del Administrador de licencias de License Manager, consulte la Guía del usuario de License Manager.

Al vincular License Manager con AWS Organizations, puede:

- Habilitar el descubrimiento entre cuentas de recursos informáticos en toda su organización.
- Ver y administrar suscripciones comerciales de Linux que posea y ejecute en AWS. Para obtener más información, consulte Suscripciones de Linux en AWS License Manager.

Utilice la siguiente información como ayuda para realizar la integración AWS License Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

Los siguientes roles vinculados al servicio se crean automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Estos roles permiten que License Manager realice operaciones admitidas en las cuentas de su organización.

Puede eliminar o modificar roles solo si deshabilita el acceso de confianza entre License Manager y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

Para obtener más información, consulte License Manager: rol de cuenta de administración, License Manager: rol de cuenta de miembro y License Manager: rol de suscripciones de Linux.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por License Manager otorgan acceso a las siguientes entidades de servicio:

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

Habilitación del acceso de confianza License Manager

Solo puede habilitar el acceso confiable mediante AWS License Manager.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Para habilitar el acceso de confianza con el License Manager

Debe iniciar sesión en la consola de License Manager con su cuenta AWS Organizations de administración y asociarla a su cuenta de License Manager. Para obtener más información, consulte Configuración en AWS License Manager.

Deshabilitación del acceso de confianza con el License Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para inhabilitarlo AWS License Manager como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-manager.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

  Para deshabilitar el uso del acceso de confianza en las suscripciones de Linux:

  ```
  $  aws organizations disable-aws-service-access \
      --service-principal license-manager-linux-subscriptions.amazonaws.com
  ```

- AWS API: D isableAWSService Access

Para habilitar una cuenta de administrador delegado para License Manager

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para License Manager que, de lo contrario, solo pueden ser realizadas por usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión de License Manager.

Para delegar una cuenta de miembro como administrador para License Manager, siga los pasos que se indican en Registro de un administrador delegado en la Guía del usuario de License Manager.

AWS Managed Services Informes de autoservicio (SSR) (AMS) y AWS Organizations

AWS Managed Services (AMS) Los informes de autoservicio (SSR) recopilan datos de varios AWS servicios nativos y proporcionan acceso a los informes sobre las principales ofertas de AMS. SSR proporciona la información que puede utilizar para respaldar las operaciones, la gestión de la configuración, la gestión de activos, la gestión de la seguridad y el cumplimiento.

Tras la integración AWS Organizations, puede activar los informes de autoservicio agregados (SSR). Se trata de una función de AMS que permite a los clientes de Advanced y Accelerate ver sus informes de autoservicio actuales agregados a nivel de organización y en todas las cuentas. Esto le permite ver los indicadores operativos clave, como el cumplimiento de los parches, la cobertura de copias de seguridad y los incidentes en todas las cuentas gestionadas por AMS. AWS Organizations

Utilice la siguiente información como ayuda para integrar los informes de autoservicio AWS Managed Services (SSR) (AMS) con. AWS Organizations

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le permite a AMS realizar operaciones de soporte en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AMS y Organizations, o si elimina la cuenta del miembro de la organización.

- `AWSServiceRoleForManagedServices_SelfServiceReporting`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Las funciones vinculadas al servicio que utiliza AMS otorgan acceso a las siguientes entidades principales de servicio:

- `selfservicereporting.managedservices.amazonaws.com`

Habilitar el acceso confiable con AMS

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable ejecutando un AWS CLI comando de Organizations o llamando a una operación de API de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante Organizations CLI/SDK

Usa los siguientes AWS CLI comandos u operaciones de API para habilitar el acceso a un servicio confiable:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitar AWS Managed Services (AMS) Self-Service Reporting (SSR) como un servicio de confianza para Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal selfservicereporting.managedservices.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: habilite el acceso AWSService

Inhabilitar el acceso de confianza con AMS

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una operación de la API de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Usa los siguientes AWS CLI comandos u operaciones de API para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para deshabilitar AWS Managed Services (AMS) Self-Service Reporting (SSR) como un servicio de confianza para Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal selfservicereporting.managedservices.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: deshabilita el acceso AWSService

Habilitar una cuenta de administrador delegado para AMS

Las cuentas de administrador delegado pueden ver los informes de AMS (como los de parches y copias de seguridad) de todas las cuentas en una única vista agregada en la consola de AMS.

Puede añadir un administrador delegado mediante la consola o la API de AMS, o mediante la operación `RegisterDelegatedAdministrator` CLI o SDK de Organizations.

Deshabilitar un administrador delegado para AMS

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para AMS.

Puede eliminar al administrador delegado mediante la consola o la API de AMS, o mediante la operación `DeregisterDelegatedAdministrator` CLI o SDK de Organizations.

Amazon Macie y AWS Organizations

Amazon Macie es un servicio de privacidad y seguridad de datos completamente administrado que utiliza machine learning y coincidencia de patrones para descubrir, monitorear y ayudar a proteger

sus datos confidenciales en Amazon Simple Storage Service (Amazon S3). Macie automatiza el descubrimiento de datos confidenciales, como la información de identificación personal (PII) y la propiedad intelectual, para proporcionarle una mejor comprensión de los datos que su organización almacena en Amazon S3.

Para obtener más información, consulte Administración de cuentas de Amazon Macie con AWS Organizations en la Guía del usuario de Amazon Macie.

Utilice la siguiente información para ayudarle a integrar Amazon Macie con. AWS Organizations

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado a servicio se crea automáticamente para la cuenta de administrador de Macie delegado de su organización cuando se habilita el acceso de confianza. Este rol permite a Macie realizar operaciones admitidas en las cuentas de la organización.

Puede eliminar o modificar este rol solo si desactiva el acceso de confianza entre Macie y Organizations, o bien si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleRorAmazonMacie`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Macie otorgan acceso a las siguientes entidades de servicio:

- `macie.amazonaws.com`

Habilitar el acceso de confianza con Macie

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de Amazon Macie o la consola de AWS Organizations .

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola de Amazon Macie o herramientas para habilitar la integración con Organizations. Esto permite a Amazon Macie realizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por Amazon Macie. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de Amazon Macie, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la consola Macie

Amazon Macie requiere un acceso confiable AWS Organizations para designar una cuenta de miembro como administrador de Macie de su organización. Si configura un administrador delegado mediante Management Console de Macie, a continuación Macie habilita automáticamente el acceso de confianza para usted.

Para obtener más información, consulte Integración y configuración de una organización en Amazon Macie en laGuía del usuario de Amazon Macie.

Puede habilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitar Amazon Macie como un servicio de confianza en Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal macie.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E Access nableAWSService

Para habilitar una cuenta de administrador delegado para Macie

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y roles de esa cuenta pueden realizar acciones administrativas para Macie que, de lo contrario, solo pueden ser realizadas por usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión de Macie.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations con los siguientes permisos puede configurar una cuenta de miembro como administrador delegado para Macie en la organización:
>
> - `organizations:EnableAWSServiceAccess`
> - `macie:EnableOrganizationAdminAccount`

Para designar una cuenta de miembro como administrador delegado para Macie

Amazon Macie requiere un acceso confiable AWS Organizations para designar una cuenta de miembro como administrador de Macie de su organización. Si configura un administrador delegado mediante Management Console de Macie, a continuación Macie habilita automáticamente el acceso de confianza para usted.

Para obtener más información, consulte https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin.

AWS Marketplace y AWS Organizations

AWS Marketplace es un catálogo digital seleccionado que puede usar para buscar, comprar, implementar y administrar el software, los datos y los servicios de terceros que necesita para crear soluciones y administrar sus negocios.

AWS Marketplace crea y administra las licencias que utiliza AWS License Manager para sus compras en AWS Marketplace. Cuando comparta (concede acceso a) sus licencias con otras cuentas de su organización, AWS Marketplace crea y administra nuevas licencias para esas cuentas.

Para obtener más información, consulte Uso de roles vinculados a servicios en AWS Marketplace en la Guía para comprador de AWS Marketplace .

Utilice la siguiente información para ayudarle a integrarse AWS Marketplace con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le AWS Marketplace permite realizar operaciones de apoyo en las cuentas de su organización.

Puede eliminar o modificar esta función solo si deshabilita el acceso de confianza entre AWS Marketplace y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForMarketplaceLicenseManagement`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza AWS Marketplace otorgan acceso a los siguientes directores de servicio:

- `license-management.marketplace.amazonaws.com`

Habilitar el acceso de confianza con AWS Marketplace

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS Marketplace consola o la consola. AWS Organizations

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Marketplace consola o las herramientas para permitir la integración con Organizations. Esto permite

AWS Marketplace realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Marketplace. Para obtener más información, consulte esta nota.
Si habilitas el acceso confiable mediante la AWS Marketplace consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso confiable mediante la AWS Marketplace consola

Consulte Creación de un rol vinculado a un servicio de AWS Marketplace en la Guía del comprador de AWS Marketplace .

Puede habilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Marketplace.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Marketplace diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Marketplace que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Marketplace como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Deshabilitación del acceso con AWS Marketplace

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede habilitar el acceso confiable mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Marketplace como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

AWS Marketplace Private Marketplace y AWS Organizations

AWS Marketplace es un catálogo digital seleccionado que puede usar para buscar, comprar, implementar y administrar el software, los datos y los servicios de terceros que necesita para crear soluciones y administrar sus negocios. Un mercado privado le ofrece un amplio catálogo de productos disponibles AWS Marketplace, además de un control detallado de dichos productos.

AWS Marketplace Private Marketplace le permite crear varias experiencias de mercado privado asociadas a toda la organización, a una o más cuentas de la organización, cada una con su propio conjunto de productos aprobados. OUs AWS Los administradores también pueden aplicar la marca de la empresa a cada experiencia de mercado privado con el logotipo, los mensajes y la combinación de colores de su empresa o equipo.

Para obtener más información, consulte Using roles to configure Private Marketplace in AWS Marketplace en la Guía del comprador de AWS Marketplace .

Utilice la siguiente información para ayudarle a integrar AWS Marketplace Private Marketplace con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso confiable mediante la consola de Private AWS Marketplace Marketplace. Este rol permite a Private Marketplace llevar a cabo operaciones compatibles en las cuentas de su organización. Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AWS Marketplace Private Marketplace y Organizations y desvincula todas las experiencias de mercado privado de su organización.

Si habilita el acceso de confianza directamente desde la consola de Organizations, CLI o bienSDK, el rol vinculado al servicio no se crea automáticamente.

- `AWSServiceRoleForPrivateMarketplaceAdmin`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Private Marketplace otorgan acceso a las siguientes entidades principales de servicio:

- `private-marketplace.marketplace.amazonaws.com`

Habilitar el acceso de confianza con Private Marketplace

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puedes habilitar el acceso de confianza mediante la consola de AWS Marketplace Private Marketplace o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la consola o las herramientas de AWS Marketplace Private Marketplace para permitir la integración con Organizations. Esto permite a AWS Marketplace Private Marketplace realizar cualquier configuración que necesite, como la creación de los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración con las herramientas que proporciona AWS Marketplace Private Marketplace. Para obtener más información, consulte esta nota.
> Si habilitas el acceso de confianza mediante la consola o las herramientas de AWS Marketplace Private Marketplace, no necesitas completar estos pasos.

Para habilitar el acceso de confianza desde la consola de Private Marketplace

Consulte Getting started with Private Marketplace en la Guía del comprador de AWS Marketplace .

Puedes habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Seleccione AWS Marketplace Private Marketplace en la lista de servicios.

4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso de confianza para AWS Marketplace Private Marketplace, escriba enable para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si solo es el administrador de Private Marketplace AWS Organizations, dígale al administrador de AWS Marketplace Private Marketplace que ahora puede habilitar ese servicio para que funcione AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitar AWS Marketplace Private Marketplace como un servicio de confianza en Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Desactivación del acceso de confianza con Private Marketplace

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para deshabilitar AWS Marketplace Private Marketplace como un servicio de confianza en Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: isableAWSServiceAcceso 3D

Activación de una cuenta de administrador delegado para Private Marketplace

El administrador de la cuenta de administración puede delegar los permisos administrativos de Private Marketplace a una cuenta de miembro designada, conocida como “administrador delegado”. Para registrar una cuenta como administrador delegado en el mercado privado, el administrador de la cuenta de administración debe asegurarse de que el acceso confiable y la función vinculada al servicio estén habilitados, seleccionar Registrar un nuevo administrador, proporcionar el número de AWS cuenta de 12 dígitos y elegir Enviar.

Las cuentas de administración y las cuentas de administrador delegado pueden llevar a cabo tareas administrativas de Private Marketplace, como crear experiencias, actualizar la configuración de marca, asociar o disociar audiencias, agregar o eliminar productos y aprobar o rechazar solicitudes pendientes.

Para configurar un administrador delegado mediante la consola de Private Marketplace, consulte Creating and managing a private marketplace en la Guía del comprador de AWS Marketplace .

También puede configurar un administrador delegado mediante Organizations `RegisterDelegatedAdministrator`API. Para obtener más información, consulte RegisterDelegatedAdministratorla Referencia de comandos de Organizations.

Desactivación de un administrador delegado para Private Marketplace

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para Private Marketplace.

Puede eliminar al administrador delegado mediante la consola de Private Marketplace o API mediante la SDK operación Organizations `DeregisterDelegatedAdministrator` CLI u.

Para deshabilitar la cuenta de Private Marketplace de administrador delegado mediante la consola de Private Marketplace, consulte Creating and managing a private marketplace en la Guía del comprador de AWS Marketplace .

AWS Marketplace panel de información sobre adquisiciones y AWS Organizations

Utiliza el panel de información sobre AWS Marketplace adquisiciones para ver los acuerdos y los datos de análisis de costes de todas las AWS cuentas de su organización. Cuando se integra con Organizations, el panel de información sobre AWS Marketplace adquisiciones escucha los cambios de la organización, como la incorporación de una cuenta a la organización, y agrega datos para sus acuerdos correspondientes a fin de crear sus paneles.

Para obtener más información, consulte Procurement insights en la Guía del comprador de AWS Marketplace .

Utilice la siguiente información para ayudarle a integrar el panel de información sobre AWS Marketplace adquisiciones. AWS Organizations

Políticas administradas y roles vinculados a servicios creados al habilitar la integración

Al activar el panel de información sobre AWS Marketplace adquisiciones, se crean la función `AWSServiceRoleForProcurementInsightsPolicy`vinculada al servicio y la política `AWSServiceRoleForProcurementInsightsPolicy` AWS gestionada.

Activación del acceso de confianza con la información sobre adquisiciones de AWS Marketplace

Al habilitar el acceso confiable, el panel de información sobre AWS Marketplace adquisiciones tiene la capacidad de integrarse con el servicio Organizations del cliente. AWS Marketplace El panel de información sobre adquisiciones escucha los cambios de la organización, como la incorporación de una cuenta a la organización, y agrega datos para sus acuerdos correspondientes a fin de crear sus paneles de control.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la consola del panel de información sobre AWS Marketplace adquisiciones o la consola. AWS Organizations

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la consola o las herramientas del panel de información sobre AWS Marketplace adquisiciones para permitir la integración con Organizations. Esto permite que el panel de información sobre AWS Marketplace adquisiciones realice cualquier configuración que necesite, como la creación de los recursos que necesite el servicio. Siga estos pasos solo si no puede habilitar la integración con las herramientas que proporciona el panel de información sobre AWS Marketplace adquisiciones. Para obtener más información, consulte esta nota.
> Si habilita el acceso confiable mediante la consola o las herramientas del panel de información sobre AWS Marketplace adquisiciones, no necesitará completar estos pasos.

Para permitir un acceso confiable mediante la activación del panel AWS Marketplace de información sobre adquisiciones

Consulte Habilitar el panel de información sobre AWS Marketplace adquisiciones en la Guía del AWS Marketplace comprador.

Para habilitar el acceso de confianza mediante las herramientas de Organizations

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elija Panel de información sobre adquisiciones de AWS Marketplace en la lista de servicios.
4. Elija Habilitar acceso de confianza.

5. En el cuadro de diálogo Habilitar el acceso confiable para la información sobre AWS Marketplace compras, escriba habilitar para confirmar y, a continuación, elija Habilitar el acceso confiable.
6. Si es el administrador de Only AWS Organizations, dígale al administrador del panel de información sobre AWS Marketplace adquisiciones que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitar el panel de información sobre AWS Marketplace adquisiciones como un servicio confiable para Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS APIR: nableAWSServiceAcceso electrónico

Desactivación del acceso de confianza con la información sobre adquisiciones de AWS Marketplace

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para deshabilitar el panel de información sobre AWS Marketplace adquisiciones como un servicio confiable de Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: isableAWSServiceAcceso 3D

Habilitar una cuenta de administrador delegado para obtener información AWS Marketplace sobre las adquisiciones

Para configurar un administrador delegado en la consola de información sobre AWS Marketplace adquisiciones, consulte Registro de administradores delegados> en la Guía del comprador.AWS Marketplace

También puede configurar un administrador delegado mediante Organizations `RegisterDelegatedAdministrator`API. Para obtener más información, consulte RegisterDelegatedAdministratorla Referencia de comandos de Organizations.

Deshabilitar un administrador delegado para obtener información sobre las adquisiciones AWS Marketplace

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para obtener AWS Marketplace información sobre las adquisiciones.

Para eliminar a un administrador delegado a través de la consola de información sobre AWS Marketplace adquisiciones, consulte Anular el registro de administradores delegados en la Guía del comprador.AWS Marketplace

También puede eliminar al administrador delegado mediante la SDK operación Organizations `DeregisterDelegatedAdministrator` CLI u.

AWS Network Manager y AWS Organizations

Network Manager le permite administrar de forma centralizada su AWS Red central de WAN en la nube y su AWS red de Transit Gateway en AWS cuentas, regiones y ubicaciones en las instalaciones. Con el soporte multicuenta, puede crear una única red global para cualquiera de sus AWS cuentas y registrar las puertas de enlace de tránsito de varias cuentas a la red global desde la consola de Network Manager.

Con el acceso de confianza entre Network Manager y Organizations habilitado, los administradores delegados registrados y las cuentas de administración pueden aprovechar el rol vinculado a servicios implementado en las cuentas de miembro para describir los recursos asociados a sus redes globales. Desde la consola de Network Manager, los administradores delegados registrados y las cuentas de administración pueden asumir los roles de IAM personalizados implementados en las cuentas miembro: `CloudWatch-CrossAccountSharingRole` para monitoreo y eventos de múltiples cuentas y `IAMRoleForAWSNetworkManagerCrossAccountResourceAccess` para el acceso del rol de conmutador de consola (para ver y administrar recursos de varias cuentas)

Important

- Recomendamos encarecidamente utilizar la consola de Network Manager para administrar la configuración multicuentas (habilitar/deshabilitar el acceso de confianza y registrar/anular el registro de administradores delegados). La administración de esta configuración desde la consola implementa y administra automáticamente todas las funciones vinculadas a servicios necesarios y los roles de IAM personalizados en las cuentas de miembro necesarias para el acceso multicuenta.
- Cuando habilita el acceso seguro para Network Manager en la consola de Network Manager, esta misma también habilita AWS CloudFormation el servicio StackSets. Network Manager utiliza StackSets para implementar roles de IAM personalizados necesarios para la administración multicuenta.

Para obtener más información sobre la integración de Network Manager con las Organizations, consulte Administrar multicuentas en Network Manager con AWS Organizations en la Guía de usuario de Amazon VPC.

Utilice la siguiente información para obtener ayuda al integrar AWS Network Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Estos roles permiten a Network Manager realizar operaciones compatibles en las cuentas de su organización. Si deshabilita el acceso de confianza, Network Manager no eliminará estos roles de las cuentas de su organización. Puede eliminarlos manualmente desde la consola de IAM.

Cuenta de administración

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

Cuentas de miembros

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Cuando registra una cuenta de miembro como administrador delegado, se crea automáticamente el siguiente rol adicional en la cuenta de administrador delegado:

- `AWSServiceRoleForCloudWatchCrossAccount`

Los principales de servicios utilizados por los roles vinculados a servicios

Los roles vinculados a los servicios solo pueden asumirse por las entidades principales de servicio autorizadas por las relaciones de confianza definidas para el rol.

- Para el `AWSServiceRoleForNetworkManager service-linked` rol, `networkmanager.amazonaws.com` es el único servicio principal que tiene acceso.
- Para el `AWSServiceRoleForCloudFormationStackSetsOrgMember` rol vinculado al servicio, `member.org.stacksets.cloudformation.amazonaws.com` es el único servicio principal que tiene acceso.
- Para el `AWSServiceRoleForCloudFormationStackSetsOrgAdmin` rol vinculado al servicio, `stacksets.cloudformation.amazonaws.com` es el único servicio principal que tiene acceso.

- Para el `AWSServiceRoleForCloudWatchCrossAccount` rol vinculado al servicio, `cloudwatch-crossaccount.amazonaws.com` es el único servicio principal que tiene acceso.

La eliminación de estos roles perjudicará la funcionalidad multicuenta de Network Manager.

Habilitar el acceso de confianza con Network Manager

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo el administrador de la cuenta de administración de Organizations tiene permisos para habilitar el acceso de confianza con otro servicio AWS. Asegúrese de utilizar la consola de Network Manager para habilitar el acceso de confianza y evitar problemas de permisos. Para obtener más información, consulte Gestionar multicuentas en Network Manager con AWS Organizations en la Guía del usuario de Amazon VPC.

Deshabilitar el acceso de confianza con Network Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo el administrador de la cuenta de gestión de Organizations tiene permisos para deshabilitar el acceso de confianza con otro servicio de AWS.

> **Important**
>
> Le recomendamos encarecidamente que use la consola de Network Manager para deshabilitar el acceso de confianza. Si deshabilita el acceso de confianza de cualquier otro modo como, por ejemplo, usando AWS CLI con una API o con la consola AWS CloudFormation, es posible que los StackSets AWS CloudFormation implementados y los roles de IAM personalizados no se eliminen correctamente. Para deshabilitar el acceso de confianza, inicie sesión en la consola de Network Manager.

Habilitar una cuenta de administrador delegado para Network Manager

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y los roles de esa cuenta pueden realizar acciones administrativas para Network Manager

que, de lo contrario, solo podrían realizarlas los usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la de Network Manager.

Para obtener más información sobre cómo designar una cuenta de miembro como administrador delegado de Network Manager en la organización, consulte Registrar un administrador delegador en la Guía del usuario de Amazon VPC.

Amazon Q Developer y AWS Organizations

Amazon Q Developer es un asistente conversacional generativo con inteligencia artificial que puede ayudarlo a comprender, crear, ampliar y operar AWS aplicaciones. También es un generador de código de uso general con tecnología de machine learning que ofrece recomendaciones de código en tiempo real. La versión de suscripción de pago de Amazon Q Developer requiere la integración de Organizations. Para obtener más información, consulta la configuración de Account, IAM Identity Center y Organizations en la guía del usuario de Amazon Q.

Utilice la siguiente información para ayudarle a integrar Amazon Q Developer con AWS Organizations.

Roles vinculados a servicios

El rol vinculado al servicio `AWSServiceRoleForAmazonQDeveloper` permite a Amazon Q Developer llevar a cabo operaciones admitidas en su organización. Cree el rol mediante la consola de Amazon Q Developer o APICLI, como se describe en Crear un rol vinculado a un servicio en la Guía del IAMusuario.

Si usa una cuenta de miembro, puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Amazon Q Developer y Organizations, o si elimina la cuenta de miembro de la organización.

Entidades principales de servicio utilizadas por Amazon Q Developer

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio utilizados por Amazon Q Developer permiten el acceso a las siguientes entidades principales de servicio:

- `q.amazonaws.com`

Activación del acceso de confianza para Amazon Q Developer

Amazon Q Developer Pro utiliza el acceso de confianza para compartir la configuración hecha en la cuenta de administración de Organizations con las cuentas de miembro de la misma organización.

Por ejemplo, el administrador de Amazon Q Developer Pro, que trabaja en la cuenta de administración de Organizations, puede habilitar sugerencias con referencias de código. Si el acceso de confianza está habilitado, las sugerencias con referencias de código también se habilitarán para todas las cuentas de miembro de esa organización.

Solo puede habilitar el acceso de confianza con Amazon Q Developer.

Para habilitar el acceso de confianza para Amazon Q Developer, utilice este procedimiento.

1. En la página Configuración de Amazon Q Developer, en Configuración de las cuentas de miembro, seleccione Editar.
2. En la ventana emergente, seleccione Activar.
3. Seleccione Guardar.

Para obtener más información, consulte Enabling trusted access en la Guía del usuario de Amazon Q Developer.

Desactivación del acceso de confianza para Amazon Q Developer

Solo puede deshabilitar el acceso de confianza mediante las herramientas para desarrolladores de Amazon Q.

Para deshabilitar el acceso de confianza para Amazon Q Developer, utilice este procedimiento.

1. En la página Configuración de Amazon Q Developer, en Configuración de las cuentas de miembro, seleccione Editar.
2. En la ventana emergente, seleccione Desactivar.
3. Seleccione Guardar.

Para obtener más información, consulte Enabling trusted access en la Guía del usuario de Amazon Q Developer.

AWS Resource Access Manager y AWS Organizations

AWS Resource Access Manager (AWS RAM) le permite compartir AWS recursos específicos de su propiedad con otros Cuentas de AWS. Es un servicio centralizado que proporciona una experiencia uniforme para compartir diferentes tipos de AWS recursos en varias cuentas.

Para obtener más información al respecto AWS RAM, consulte la Guía AWS RAM del usuario.

Utilice la siguiente información para ayudarle a integrarse AWS Resource Access Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le AWS RAM permite realizar operaciones de apoyo en las cuentas de su organización.

Puede eliminar o modificar esta función solo si deshabilita el acceso de confianza entre AWS RAM y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForResourceAccessManager`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza AWS RAM otorgan acceso a los siguientes directores de servicio:

- `ram.amazonaws.com`

Habilitar el acceso de confianza con AWS RAM

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS Resource Access Manager consola o la consola. AWS Organizations

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Resource Access Manager consola o las herramientas para permitir la integración con Organizations. Esto permite AWS Resource Access Manager realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Resource Access Manager. Para obtener más información, consulte esta nota.
> Si habilitas el acceso confiable mediante la AWS Resource Access Manager consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso confiable mediante la AWS RAM consola o CLI

Consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM .

Puede habilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Resource Access Manager.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Resource Access Manager diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Resource Access Manager que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Resource Access Manager como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Deshabilitación del acceso con AWS RAM

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Puede deshabilitar el acceso de confianza mediante las herramientas AWS Resource Access Manager o las AWS Organizations herramientas.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Resource Access Manager consola o las herramientas para deshabilitar la integración con Organizations. Esto permite AWS Resource Access Manager realizar cualquier limpieza que sea necesaria, como eliminar recursos o acceder a funciones que el servicio ya no necesite. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas por AWS Resource Access Manager.
> Si inhabilitas el acceso de confianza mediante la AWS Resource Access Manager consola o las herramientas, no necesitas completar estos pasos.

Para deshabilitar el acceso de confianza mediante la AWS Resource Access Manager consola o CLI

Consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM .

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Resource Access Manager.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS Resource Access Manager diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Resource Access Manager que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Resource Access Manager como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ram.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Explorador de recursos de AWS y AWS Organizations

Explorador de recursos de AWS es un servicio de búsqueda y descubrimiento de recursos. Con Resource Explorer, puede analizar sus recursos, como las instancias de Amazon Elastic Compute Cloud, las tablas de Amazon Kinesis Data Streams o Amazon DynamoDB, mediante una experiencia similar a la de un motor de búsqueda en Internet. Puede buscar sus recursos mediante metadatos de recursos, como nombres, etiquetas yIDs. Resource Explorer funciona en todas AWS las regiones de su cuenta para simplificar las cargas de trabajo entre regiones.

Al integrar Resource Explorer con Resource Explorer AWS Organizations, puede recopilar pruebas de una fuente más amplia e incluir varias pruebas Cuentas de AWS de su organización en el ámbito de sus evaluaciones.

Utilice la siguiente información para ayudarle a integrarse Explorador de recursos de AWS con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Resource Explorer realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Resource Explorer y Organizations, o si elimina la cuenta de miembro de la organización.

Para obtener más información sobre cómo Resource Explorer utiliza este rol, consulte Uso de roles vinculados a servicios en la Guía del usuario de Explorador de recursos de AWS .

- `AWSServiceRoleForResourceExplorer`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios usados por Resource Explorer conceden acceso a las siguientes entidades de servicio:

- `resource-explorer-2.amazonaws.com`

Para habilitar el acceso de confianza con Explorador de recursos de AWS

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Resource Explorer requiere un acceso confiable AWS Organizations antes de poder designar una cuenta de miembro como administrador delegado de su organización.

Puede habilitar el acceso de confianza mediante la consola de Resource Explorer o la consola de Organizations. Le recomendamos que, siempre que sea posible, utilice la consola o herramientas de Resource Explorer para habilitar la integración con Organizations. Esto permite Explorador de recursos de AWS realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio.

Para habilitar el acceso de confianza desde la consola de Resource Explorer

Para obtener instrucciones sobre cómo habilitar el acceso confiable, consulte Requisitos previos para usar Resource Explorer en la Guía del usuario de Explorador de recursos de AWS .

> **Note**
>
> Si configura un administrador delegado mediante la Explorador de recursos de AWS consola, se le habilitará Explorador de recursos de AWS automáticamente el acceso de confianza.

Puede habilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo Explorador de recursos de AWS como un servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal resource-explorer-2.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Para deshabilitar el acceso de confianza con Resource Explorer

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con Explorador de recursos de AWS.

Puede deshabilitar el acceso de confianza mediante las herramientas Explorador de recursos de AWS o las AWS Organizations herramientas.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la Explorador de recursos de AWS consola o las herramientas para deshabilitar la integración con Organizations. Esto permite Explorador de recursos de AWS realizar cualquier limpieza que sea necesaria, como eliminar recursos o acceder a funciones que el servicio ya no necesite. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas por Explorador de recursos de AWS.
> Si inhabilitas el acceso de confianza mediante la Explorador de recursos de AWS consola o las herramientas, no necesitas completar estos pasos.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo Explorador de recursos de AWS como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

Habilitar una cuenta de administrador delegado para Resource Explorer

Use su cuenta de administrador delegado para crear vistas de recursos de varias cuentas y asignarlas a una unidad organizativa o a toda la organización. Puede compartir vistas de varias cuentas con cualquier cuenta de su organización AWS Resource Access Manager mediante la creación de recursos compartidos.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations con el siguiente permiso puede configurar una cuenta de miembro como administrador delegado para Resource Explorer en la organización: `resource-explorer:RegisterAccount`

Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegada para Resource Explorer, consulte Configuración en la Guía del usuario de Explorador de recursos de AWS .

Si configura un administrador delegado mediante la Explorador de recursos de AWS consola, Resource Explorer le habilitará automáticamente un acceso confiable.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el servicio de la cuenta `resource-explorer-2.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para Resource Explorer

Sólo un administrador de la cuenta de administración de Organizations o de la cuenta de administrador delegado de Resource Explorer puede eliminar una cuenta de administrador delegado para Resource Explorer. Puede deshabilitar el acceso de confianza mediante la SDK operación Organizations `DeregisterDelegatedAdministrator` CLI u.

AWS Security Hub y AWS Organizations

AWS Security Hub le proporciona una visión completa de su estado de seguridad en AWS y le ayuda a comprobar su entorno con los estándares y las prácticas recomendadas del sector de la seguridad.

Security Hub recopila los datos de seguridad de todas su Cuentas de AWS, los Servicios de AWS que utiliza y los productos de socios de terceros compatibles. Lo ayuda a analizar sus tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad.

Cuando utiliza Security Hub y AWS Organizations, puede habilitar automáticamente Security Hub para todas sus cuentas, incluidas las cuentas nuevas a medida que se agregan. Esto aumenta la cobertura de las comprobaciones y hallazgos de Security Hub, lo que proporciona una imagen más completa y precisa de su posición general de seguridad.

Para obtener más información sobre Security Hub, consulte la Guía del usuario de AWS Security Hub.

Utilice la siguiente información para ayudarle a integrar AWS Security Hub con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Security Hub realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Security Hub y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForSecurityHub`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Security Hub otorgan acceso a las siguientes entidades de servicio:

- `securityhub.amazonaws.com`

Habilitación del acceso de confianza Security Hub

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Cuando designa un administrador delegado para Security Hub, Security Hub habilita automáticamente el acceso de confianza para Security Hub en su organización.

Desactivación del acceso de confianza con Security Hub

Para obtener más información sobre los permisos que necesita, consulte Permissions required to disable trusted access en la Guía del usuario de AWS Organizations.

Antes de deshabilitar el acceso de confianza, recomendamos colaborar con el administrador delegado de su organización para deshabilitar Security Hub en las cuentas de miembro y limpiar los recursos de Security Hub en esas cuentas.

Para deshabilitar el acceso de confianza, puede utilizar la consola de AWS Organizations, la API de Organizations o la AWS CLI. Solo un administrador de la cuenta de administración de Organizations puede deshabilitar el acceso de confianza con Security Hub.

Para obtener instrucciones sobre cómo deshabilitar el acceso de confianza con Security Hub, consulte Disabling Security Hub integration with AWS Organizations.

Activación de un administrador delegado para Security Hub

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para Security Hub que, de lo contrario, solo pueden ser realizadas por usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión de Security Hub.

Para obtener información, consulte Designación de una cuenta de administrador de Security Hub en la Guía del usuario de AWS Security Hub.

Para designar una cuenta de miembro como administrador delegado para Security Hub

1. Inicie sesión en Organizations mediante la cuenta de administración de su organización.
2. Lleve a cabo una de las siguientes operaciones:
   - Si su cuenta de administración no tiene habilitado Security Hub, en la consola de Security Hub, elija Ir a Security Hub.
   - Si su cuenta de administración tiene habilitado Security Hub, en la consola de Security Hub, en General, elija Configuración.
3. En Administrador delegado, ingrese el ID de la cuenta.

Desactivación de un administrador delegado para Security Hub

Solo la cuenta de administración de la organización puede eliminar la cuenta de administrador delegado de Security Hub.

Para cambiar al administrador delegado de Security Hub, primero debe eliminar la cuenta de administrador delegado actual y, luego, designar una nueva.

Si utiliza la consola de Security Hub para eliminar al administrador delegado en una región, este se elimina en todas las regiones.

La API de Security Hub solo elimina la cuenta de administrador delegado de Security Hub de la región en la que se emite el comando o la llamada a la API. Debe repetir la acción en las demás regiones.

Si utiliza la API de Organizations para eliminar la cuenta de administrador delegado de Security Hub, se eliminará automáticamente de todas las regiones.

Para obtener instrucciones sobre cómo deshabilitar el administrador delegado de Security Hub, consulte Removing or changing the delegated administrator.

Amazon S3 Storage Lens y AWS Organizations

Al proporcionar a Amazon S3 Storage Lens un acceso confiable a su organización, le permite recopilar y agregar métricas de todos los componentes Cuentas de AWS de su organización. S3 Storage Lens hace esto accediendo a la lista de cuentas que pertenecen a su organización y recopila y analiza las métricas de almacenamiento y uso y actividad de todas ellas.

Para obtener más información, consulte la sección Uso de roles vinculados a servicios para Amazon S3 Storage Lens en la Guía del usuario de Amazon S3 Storage Lens.

Utilice la siguiente información para ayudarle a integrar Amazon S3 Storage Lens con AWS Organizations.

Rol vinculado al servicio creados al habilitar la integración

El siguiente rol vinculado a servicio se crea automáticamente en la cuenta de administrador delegado de su organización cuando se habilita el acceso de confianza y se aplica la configuración de Storage Lens a su organización. Este rol permite a Amazon S3 Storage Lens realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Amazon S3 Storage Lens y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForS3StorageLens`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Amazon S3 Storage Lens otorgan acceso a las siguientes entidades de servicio:

- `storage-lens.s3.amazonaws.com`

Habilitación del acceso de confianza para Amazon S3 Storage Lens

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de Amazon S3 Storage Lens o la consola de AWS Organizations .

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola de Amazon S3 Storage Lens o herramientas para habilitar la integración con Organizations. Esto permite a Amazon S3 Storage Lens realizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por Amazon S3 Storage Lens. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de Amazon S3 Storage Lens, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la consola de Amazon S3

Consulte Habilitación del acceso de confianza para S3 Storage Lens en la Guía del usuario de Amazon Simple Storage Service.

Puede habilitar un acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elija Lente de almacenamiento de Amazon S3 en la lista de servicios.
4. Elija Habilitar acceso de confianza.

5. En el cuadro de diálogo Habilitar el acceso de confianza para Amazon S3 Storage Lens, escriba enable para confirmar y, a continuación, seleccione Enable Trusted Access.
6. Si usted es el administrador de Only AWS Organizations, dígale al administrador de Amazon S3 Storage Lens que ahora puede habilitar ese servicio para que funcione AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitar Amazon S3 Storage Lens como un servicio de confianza en Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS APIR: nableAWSServiceAcceso electrónico

Deshabilitación del acceso de confianza para Amazon S3 Storage Lens

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza con las herramientas Storage Lens de Amazon S3.

Puede deshabilitar el acceso de confianza mediante la consola Amazon S3, la AWS CLI o cualquiera de las AWS SDKs.

Para deshabilitar el acceso de confianza mediante la consola Amazon S3

Consulte Deshabilitación del acceso de confianza para S3 Storage Lens en la Guía del usuario de Amazon Simple Storage Service.

Habilitar una cuenta de administrador delegado para Amazon S3 Storage Lens

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para Amazon S3 Storage Lens que, de lo contrario, solo pueden realizar usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión de Amazon S3 Storage Lens.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations con el siguiente permiso puede configurar una cuenta de miembro como administrador delegado para la Lente de almacenamiento de Amazon S3 en la organización:
> `organizations:RegisterDelegatedAdministrator`
> `organizations:DeregisterDelegatedAdministrator`

Amazon S3 Storage Lens admite un máximo de 5 cuentas de administrador delegado en su organización.

Para designar una cuenta de miembro como administrador delegado para Amazon S3 Storage Lens

Puede registrar un administrador delegado mediante la consola de Amazon S3, la AWS CLI o cualquiera de las AWS SDKs. Para registrar una cuenta de miembro como cuenta de administrador delegado para su organización mediante la consola de Amazon S3, consulte Registro de un administrador delegado para S3 Storage Lens en la Guía del usuario de Amazon Simple Storage Service.

Para anular un registro de un administrador delegado para Amazon S3 Storage Lens

Puede anular el registro de un administrador delegado mediante la consola de Amazon S3, la AWS CLI o cualquiera de las. AWS SDKs Para anular el registro de un administrador delegado mediante la consola de Amazon S3, consulte Anulación del registro de un administrador delegado para S3 Storage Lens en la Guía del usuario de Amazon Simple Storage Service.

AWS Respuesta a incidentes de seguridad y AWS Organizations

AWS Security Incident Response es un servicio de seguridad que brinda asistencia en vivo y asistida por personas las 24 horas del día, los 7 días de la semana, para ayudar a los clientes a responder rápidamente a los incidentes de ciberseguridad, como el robo de credenciales Al integrarse con

Organizations, habilita la cobertura de seguridad para toda su organización. Para obtener más información, consulte Gestión de las cuentas AWS de respuesta a incidentes de seguridad AWS Organizations en la Guía del usuario de respuesta a incidentes de seguridad.

Utilice la siguiente información para ayudarle a integrar AWS Security Incident Response con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

Los siguientes roles vinculados al servicio se crean automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza.

- `AWSServiceRoleForSecurityIncidentResponse`- se utiliza para crear la membresía de Security Incident Response: su suscripción al servicio a través de AWS Organizations.
- `AWSServiceRoleForSecurityIncidentResponse_Triage`- se utiliza únicamente cuando se activa la función de clasificación durante el registro.

Principios de servicio utilizados por Security Incident Response

Las funciones vinculadas al servicio de la sección anterior solo las pueden asumir los directores de servicio autorizados por las relaciones de confianza definidas para el rol. Las funciones vinculadas al servicio que utiliza Security Incident Response permiten el acceso al siguiente director de servicio:

- `security-ir.amazonaws.com`

Permitir un acceso confiable a la respuesta a incidentes de seguridad

Al habilitar un acceso confiable a la respuesta a incidentes de seguridad, el servicio puede realizar un seguimiento de la estructura de su organización y garantizar que todas las cuentas de la organización cuenten con una cobertura activa contra los incidentes de seguridad. También permite que el servicio utilice un rol vinculado al servicio en las cuentas de los miembros para las funciones de clasificación cuando se habilita la función de clasificación.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la consola de respuesta a incidentes de AWS seguridad o la consola. AWS Organizations

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la consola o las herramientas de AWS Security Incident Response para permitir la integración con Organizations. Esto permite a AWS Security Incident Response realizar cualquier configuración que necesite, como la creación de los recursos que necesite el servicio. Siga estos pasos solo si no puede habilitar la integración con las herramientas que proporciona AWS Security Incident Response. Para obtener más información, consulte esta nota. Si habilita el acceso confiable mediante la consola o las herramientas de respuesta a incidentes de AWS seguridad, no necesitará completar estos pasos.

Organizations habilita automáticamente el acceso confiable de la organización cuando utiliza la consola de respuesta a incidentes de seguridad para la configuración y la administración. Si utiliza la respuesta a incidentes CLI de seguridadSDK, debe habilitar manualmente el acceso confiable mediante el nableAWSServiceacceso electrónico API. Para obtener información sobre cómo habilitar el acceso confiable a través de la consola de respuesta a incidentes de seguridad, consulte Habilitar el acceso confiable para la administración de AWS cuentas en la Guía del usuario de respuesta a incidentes de seguridad.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación desde una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Seleccione Respuesta a incidentes de AWS seguridad en la lista de servicios.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso de confianza para la respuesta a incidentes de AWS seguridad, escriba habilitar para confirmar y, a continuación, elija Habilitar el acceso de confianza.

6. Si es el administrador de Only AWS Organizations, dígale al administrador de AWS Security Incident Response que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicio.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitar AWS Security Incident Response como un servicio de confianza en Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal security-ir.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Inhabilitar el acceso de confianza con la respuesta a incidentes de seguridad

Solo un administrador de la cuenta de administración de Organizations puede deshabilitar el acceso de confianza con Security Incident Response.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En el panel de navegación, elija Servicios.
3. Seleccione Respuesta a incidentes de AWS seguridad en la lista de servicios.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de diálogo Deshabilitar el acceso de confianza para la respuesta a incidentes de AWS seguridad, escriba deshabilitar para confirmar y, a continuación, elija Inhabilitar el acceso de confianza.
6. Si solo es el administrador de Security Incident Response AWS Organizations, dígale al administrador de AWS Security Incident Response que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicio o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para deshabilitar AWS Security Incident Response como un servicio de confianza en Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal security-ir.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: isableAWSServiceAcceso 3D

Habilitar una cuenta de administrador delegado para la respuesta a incidentes de seguridad

Al designar una cuenta de miembro como administrador delegado de la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas de respuesta a los incidentes de seguridad que, de otro modo, solo podrían realizar los usuarios o los roles de la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión

de la respuesta a incidentes de seguridad. Para obtener más información, consulte Gestión de las cuentas AWS de respuesta a incidentes de seguridad AWS Organizations en la Guía del usuario de respuesta a incidentes de seguridad.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para la respuesta a incidentes de seguridad en la organización.

Para obtener información sobre cómo configurar un administrador delegado a través de la consola de respuesta a incidentes de seguridad, consulte Designación de una cuenta de administrador de respuesta a incidentes de seguridad delegada en la Guía del usuario de respuesta a incidentes de seguridad.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal security-ir.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el servicio de la cuenta `security-ir.amazonaws.com` como parámetros.

Inhabilitar a un administrador delegado para la respuesta a incidentes de seguridad

> **Important**
>
> Si la membresía se creó desde la cuenta del administrador delegado, anular el registro del administrador delegado es una acción destructiva y provocará una interrupción del servicio. Para volver a registrar DA:

1. Inicie sesión en la consola de respuesta a incidentes de seguridad en https://console.aws.amazon.com/security-ir/ home#/membership/settings
2. Cancela la suscripción desde la consola de servicio. La membresía permanece activa hasta el final del ciclo de facturación.
3. Una vez cancelada la membresía, deshabilite el acceso al servicio a través de la consola de Organizations, CLI oSDK.

Solo un administrador de la cuenta de administración de Organizations puede eliminar a un administrador delegado para Security Incident Response. Puede eliminar el administrador delegado mediante Organizations `DeregisterDelegatedAdministrator` CLI o la SDK operación.

Amazon Security Lake y AWS Organizations

Amazon Security Lake centraliza los datos de seguridad de fuentes en la nube, en las instalaciones y personalizadas en un lago de datos almacenado en su cuenta. Al integrarse con Organizations, puede crear un lago de datos que recopile registros y eventos en todas sus cuentas. Para obtener más información, consulte Administración de varias cuentas con AWS Organizations en la Guía del usuario de Amazon Security Lake.

Utilice la siguiente información para ayudarle a integrar Amazon Security Lake con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando llama al. RegisterDataLakeDelegatedAdministratorAPI Este rol permite a Amazon Security Lake llevar a cabo operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Amazon Security Lake y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForSecurityLake`

⚠ Recomendación: utilice Security Lake RegisterDataLakeDelegatedAdministrator API para permitir que Security Lake acceda a su organización y para registrar al administrador delegado de la organización

Si utiliza Organizations' APIs para registrar un administrador delegado, es posible que las funciones vinculadas al servicio para las organizaciones no se creen correctamente. Para garantizar una funcionalidad completa, utilice Security Lake. APIs

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Amazon Security Lake otorgan acceso a las siguientes entidades principales de servicio:

- `securitylake.amazonaws.com`

Activación del acceso de confianza con Amazon Security Lake

Cuando habilita el acceso de confianza con Security Lake, este puede reaccionar automáticamente a los cambios en la membresía de la organización. El administrador delegado puede habilitar la recopilación de AWS registros de los servicios compatibles en cualquier cuenta de la organización. Para obtener más información, consulte Rol vinculado al servicio para Amazon Security Lake en la guía del usuario de Amazon Security Lake.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede habilitar el acceso confiable mediante las herramientas de Organizations.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elija Amazon Security Lake en la lista de servicios.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso de confianza para Amazon Security Lake, escriba enable para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si solo es el administrador de Amazon Security Lake AWS Organizations, dígale al administrador de Amazon Security Lake que ahora puede habilitar ese servicio para que funcione AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitar Amazon Security Lake como un servicio de confianza en Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Desactivación del acceso de confianza con Amazon Security Lake

Solo un administrador de la cuenta de administración de Organizations puede deshabilitar el acceso de confianza con Amazon Security Lake.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elija Amazon Security Lake en la lista de servicios.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de diálogo Disable Trusted Access for Amazon Security Lake, escriba disable para confirmar y, a continuación, seleccione Disable Trusted Access.
6. Si usted es el administrador de Only AWS Organizations, dígale al administrador de Amazon Security Lake que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para deshabilitar Amazon Security Lake como servicio de confianza en Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal securitylake.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: isableAWSServiceAcceso 3D

Activación de una cuenta de administrador delegado para Amazon Security Lake

El administrador delegado de Amazon Security Lake agrega otras cuentas de la organización como cuentas de miembro. El administrador delegado puede habilitar Amazon Security Lake y configurar los ajustes de Amazon Security Lake para las cuentas de miembro. El administrador delegado puede recopilar registros en una organización en todas AWS las regiones en las que Amazon Security Lake esté activado (independientemente del punto de conexión regional que utilice actualmente).

También puede configurar el administrador delegado para que añada automáticamente nuevas cuentas en la organización como miembros. El administrador delegado de Amazon Security Lake tiene acceso a los registros y eventos de las cuentas de miembro asociadas. En consecuencia, puede configurar Amazon Security Lake para recopilar datos propiedad de las cuentas de miembro asociadas. También puede conceder permiso a los suscriptores para que consuman los datos que pertenecen a las cuentas asociadas de los miembros.

Para obtener más información, consulte Administración de varias cuentas con AWS Organizations en la Guía del usuario de Amazon Security Lake.

> **Permisos mínimos**
>
> Solo un administrador en la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Amazon Security Lake en la organización.

Puede especificar una cuenta de administrador delegado mediante la consola de Amazon Security Lake, la `CreateDatalakeDelegatedAdmin` API operación Amazon Security Lake o el `create-datalake-delegated-admin` CLI comando. Como alternativa, puede utilizar Organizations `RegisterDelegatedAdministrator` CLI o la SDK operación. Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegado para Amazon Security Lake, consulte

Designating the delegated Security Lake administrator and adding member accounts en la Guía del usuario de Amazon Security Lake.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \ --service-principal securitylake.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el principal de servicio de la cuenta `account.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para Amazon Security Lake

Solo un administrador en la cuenta de administración de Organizations o en la cuenta de administrador delegado de Amazon Security Lake puede eliminar una cuenta de administrador delegado de la organización.

Puede eliminar la cuenta de administrador delegado mediante la `DeregisterDataLakeDelegatedAdministrator` API operación Amazon Security Lake, el `deregister-data-lake-delegated-administrator` CLI comando o mediante Organizations `DeregisterDelegatedAdministrator` CLI o la SDK operación. Para eliminar un administrador delegado mediante Amazon Security Lake, consulte Removing the Amazon Security Lake delegated administrator en la Guía del usuario de Amazon Security Lake.

AWS Service Catalog y AWS Organizations

Service Catalog le permite crear y administrar catálogos de servicios de TI aprobados para su uso en AWS.

La integración de Service Catalog con AWS Organizations simplifica el intercambio de carteras y la copia de productos en una organización. Los administradores de Service Catalog pueden hacer referencia a una organización existente AWS Organizations cuando comparten una cartera y pueden compartir la cartera con cualquier unidad organizativa (OU) de confianza de la estructura de árbol de la organización. Esto elimina la necesidad de compartir la cartera IDs y de que la cuenta receptora

haga referencia manualmente al ID de la cartera al importarla. Las carteras compartidas a través de este mecanismo se enumeran en la cuenta de uso compartido dentro de la vista Cartera importada del administrador en Service Catalog.

Para obtener más información sobre Service Catalog, consulte la Guía del administrador de Service Catalog.

Utilice la siguiente información para ayudarle a integrarse AWS Service Catalog con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

AWS Service Catalog no crea ningún rol vinculado a un servicio como parte de la habilitación del acceso confiable.

Entidades de servicio utilizadas para conceder permisos

Para habilitar el acceso de confianza, debe especificar la siguiente entidad de servicio:

- `servicecatalog.amazonaws.com`

Habilitación del acceso de confianza con Service Catalog

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS Service Catalog consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Service Catalog consola o las herramientas para permitir la integración con Organizations. Esto permite AWS Service Catalog realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Service Catalog. Para obtener más información, consulte esta nota.
> Si habilitas el acceso confiable mediante la AWS Service Catalog consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso confiable mediante Service Catalog CLI o AWS SDK

Llame a uno de los siguientes comandos u operaciones:

- AWS CLI: aws servicecatalog enable-aws-organizations-access
- AWS SDKs::: E Access AWSServiceCatalog nableAWSOrganizations

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en uno de los AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Service Catalog.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Service Catalog diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Service Catalog que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Service Catalog como un servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal servicecatalog.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Desactivar el acceso de confianza con Service Catalog

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Si deshabilita el acceso de confianza AWS Organizations mientras usa Service Catalog, no se eliminan los recursos compartidos actuales, pero le impide crear nuevos recursos compartidos en toda la organización. Los usos compartidos actuales no se sincronizarán con la estructura de su organización si se cambian después de llamar a esta acción.

Para deshabilitar el acceso de confianza mediante el Service Catalog CLI o AWS SDK

Llame a uno de los siguientes comandos u operaciones:

- AWS CLI: aws servicecatalog disable-aws-organizations-access
- AWS SDKs: D Access isableAWSOrganizations

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Service Catalog.
4. Seleccione Deshabilitar el acceso de confianza.

5. En el cuadro de AWS Service Catalog diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Service Catalog que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Service Catalog como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

Service Quotas y AWS Organizations

Service Quotas es un AWS servicio que le permite ver y administrar sus cuotas desde una ubicación central. Las cuotas, también conocidas como límites, son el valor máximo de los recursos, acciones y elementos de su Cuenta de AWS.

Cuando Service Quotas está asociado a AWS Organizations, puede crear una plantilla de solicitud de cuota para solicitar automáticamente los aumentos de cuota al crear las cuentas.

Para obtener más información acerca de Service Quotas, consulte la Guía del usuario de Service Quotas.

Utilice la siguiente información para ayudarle a integrar Service Quotas con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite que Service Quotas realice operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Service Quotas y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForServiceQuotas`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por las Service Quotas otorgan acceso a las siguientes entidades de servicio:

- `servicequotas.amazonaws.com`

Habilitación del acceso de confianza con otros servicios de Service Quotas

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede habilitar el acceso de confianza mediante Service Quotas.

Puede habilitar el acceso de confianza mediante la consola Service Quotas AWS CLI oSDK:

- Para habilitar el acceso de confianza mediante la consola Service Quotas.

  Inicie sesión con su cuenta AWS Organizations de administración y, a continuación, configure la plantilla en la consola de Service Quotas. Para obtener más información, consulte Uso de una plantilla de Service Quotas en la Guía del usuario de Service Quotas.
- Para habilitar el acceso confiable mediante Service Quotas AWS CLI o SDK

  Llame al siguiente comando u operación:
  - AWS CLI: cuotas de servicio de AWS associate-service-quota-template
  - AWS SDKs: AssociateServiceQuotaTemplate

AWS IAM Identity Center y AWS Organizations

AWS IAM Identity Center proporciona acceso de inicio de sesión único para todas sus aplicaciones Cuentas de AWS y las de la nube. Se conecta con Microsoft Active Directory AWS Directory Service para permitir a los usuarios de ese directorio iniciar sesión en un portal de AWS acceso personalizado con sus nombres de usuario y contraseñas de Active Directory existentes. Desde el portal de AWS acceso, los usuarios tienen acceso a todas Cuentas de AWS las aplicaciones en la nube para las que tienen permisos.

Para obtener más información sobre IAM Identity Center, consulte la Guía del AWS IAM Identity Center usuario.

Utilice la siguiente información para ayudarle a integrarse AWS IAM Identity Center con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función permite a IAM Identity Center realizar operaciones de soporte en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre IAM Identity Center y Organizations, o si elimina la cuenta del miembro de la organización.

- `AWSServiceRoleForSSO`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Las funciones vinculadas al servicio que utiliza IAM Identity Center otorgan acceso a los siguientes directores de servicio:

- `sso.amazonaws.com`

Habilitar el acceso confiable con Identity Center IAM

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS IAM Identity Center consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS IAM Identity Center consola o las herramientas para permitir la integración con Organizations. Esto permite AWS IAM Identity Center realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS IAM Identity Center. Para obtener más información, consulte esta nota.
> Si habilitas el acceso confiable mediante la AWS IAM Identity Center consola o las herramientas, no necesitas completar estos pasos.

IAMIdentity Center requiere un acceso confiable AWS Organizations para funcionar. El acceso confiable se habilita al configurar IAM Identity Center. Para obtener más información, consulte Comienzo - Paso 1: Habilitar AWS IAM Identity Center en la Guía del usuario AWS IAM Identity Center .

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS IAM Identity Center.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS IAM Identity Center diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS IAM Identity Center que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS IAM Identity Center como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Deshabilitar el acceso de confianza con IAM Identity Center

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

IAMIdentity Center requiere un acceso confiable AWS Organizations para funcionar. Si deshabilita el acceso de confianza AWS Organizations mientras usa IAM Identity Center, dejará de funcionar porque no podrá acceder a la organización. Los usuarios no pueden usar IAM Identity Center para acceder a las cuentas. Todos los roles que IAM Identity Center cree permanecen, pero el servicio de IAM Identity Center no puede acceder a ellos. Las funciones vinculadas al servicio de IAM Identity Center permanecen. Si vuelve a habilitar el acceso de confianza, IAM Identity Center seguirá funcionando como antes, sin necesidad de volver a configurar el servicio.

Si elimina una cuenta de su organización, IAM Identity Center limpia automáticamente todos los metadatos y los recursos, como su función vinculada al servicio. Una cuenta independiente que se elimina de una organización ya no funciona con Identity Center. IAM

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS IAM Identity Center.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS IAM Identity Center diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS IAM Identity Center que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS IAM Identity Center como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Habilitar una cuenta de administrador delegado para IAM Identity Center

Al designar una cuenta de miembro como administrador delegado de la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para IAM Identity Center que, de otro modo, solo podrían realizar los usuarios o los roles de la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de IAM Identity Center.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado de IAM Identity Center en la organización.

Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegado para IAM Identity Center, consulte Administración delegada en la Guía del AWS IAM Identity Center usuario.

AWS Systems Manager y AWS Organizations

AWS Systems Manager es un conjunto de capacidades que permiten la visibilidad y el control de sus AWS recursos. Las siguientes capacidades de Systems Manager funcionan con Organizations en todas las Cuentas de AWS de su organización:

- Systems Manager Explorer es un panel de operaciones personalizable que proporciona información sobre sus AWS recursos. Puede sincronizar los datos de operaciones Cuentas de AWS en toda la organización mediante Organizations and Systems Manager Explorer. Para obtener más información, consulte el Systems Manager Explorer en la Guía del usuario de AWS Systems Manager .
- Systems Manager Change Manager es un marco empresarial de administración de cambios con el que se pueden solicitar, aprobar, implementar e informar los cambios operativos de la configuración y la infraestructura de la aplicación. Para obtener más información, consulte Cambiar administrador de AWS Systems Manager en la Guía del usuario de AWS Systems Manager .
- Systems Manager OpsCenter proporciona una ubicación central donde los ingenieros de operaciones y los profesionales de TI pueden ver, investigar y resolver los elementos de trabajo operativos (OpsItems) relacionados con AWS los recursos. Cuando se usa OpsCenter con Organizations, permite trabajar OpsItems desde una cuenta de administración (ya sea una cuenta de administración de Organizations o una cuenta de administrador delegado de Systems Manager)

y otra cuenta durante una sola sesión. Una vez configurados, los usuarios pueden realizar los siguientes tipos de acciones:

- Crea, consulta y actualiza OpsItems en otra cuenta.
- Consulta información detallada sobre AWS los recursos que se especifican OpsItems en otra cuenta.
- Inicie los manuales de automatización de Systems Manager para solucionar problemas con los AWS recursos de otra cuenta.

Para obtener más información, consulte AWS Systems Manager OpsCenter en la Guía del usuario de AWS Systems Manager .

- Utilice Quick Setup para configurar rápidamente AWS los servicios y funciones de uso frecuente con las prácticas recomendadas. Para obtener más información, consulte Configuración rápida de AWS Systems Manager en la Guía del usuario de AWS Systems Manager .

  Al registrar una cuenta de administrador AWS Organizations delegado para Systems Manager, puede crear, actualizar, ver y eliminar los gestores de configuración de Quick Setup que se dirigen a las unidades organizativas de una organización. Obtenga más información en Uso de un administrador delegado para una configuración rápida en la Guía del AWS Systems Manager usuario.
- Al configurar la consola integrada para Systems Manager, se introduce una cuenta de administrador delegado. Esta cuenta se utiliza para registrar cuentas de administrador AWS Organizations delegado en Quick Setup CloudFormation StackSets, Explorer y Resource Explorer. Obtenga más información en la Guía del AWS Systems Manager usuario sobre cómo configurar la consola integrada de Systems Manager para una organización.

Utilice la siguiente información para ayudarle a integrarse AWS Systems Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Systems Manager realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Systems Manager y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por Systems Manager otorgan acceso a las siguientes entidades de servicio:

- `ssm.amazonaws.com`

Habilitación del acceso de confianza con Systems Manager

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede habilitar el acceso confiable mediante las herramientas de Organizations.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Systems Manager.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Systems Manager diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Systems Manager que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Systems Manager como un servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: E nableAWSService Access

Deshabilitación del acceso de confianza con Systems Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Systems Manager requiere un acceso confiable AWS Organizations para sincronizar los datos de operaciones Cuentas de AWS en toda la organización. Si deshabilita el acceso de confianza, Systems Manager no puede sincronizar los datos de las operaciones e informa sobre un error.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Systems Manager.
4. Seleccione Deshabilitar el acceso de confianza.
5. En el cuadro de AWS Systems Manager diálogo Deshabilitar el acceso de confianza para, escriba disable para confirmar y, a continuación, seleccione Inhabilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Systems Manager que ahora puede deshabilitar el funcionamiento de ese servicio AWS Organizations mediante la consola de servicios o las herramientas.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Systems Manager como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Para habilitar una cuenta de administrador delegado para Systems Manager

Cuando designa una cuenta de miembro como administrador delegado para la organización, los usuarios y las funciones de esa cuenta pueden realizar acciones administrativas para Systems Manager que, de lo contrario, solo pueden realizar usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la gestión de Systems Manager.

Si utiliza Change Manager en una organización, debe utilizar una cuenta de administrador delegado. Es la Cuenta de AWS que se ha designado como la cuenta para gestionar las plantillas de cambios, las solicitudes de cambio, los manuales de cambios y los flujos de trabajo de aprobación en Change Manager. La cuenta de administrador delegado se encarga de las actividades de cambio en toda la organización. Cuando se configura la organización para utilizar Change Manager, se debe especificar cuál de sus cuentas llevará a cabo este rol. No tiene que ser la cuenta de gestión de la organización. La cuenta de administrador delegado no es necesaria si se utiliza el Administrador de cambios con una sola cuenta.

Para designar una cuenta de miembro como administrador delegado, consulte los siguientes temas en la Guía del usuario de AWS Systems Manager :

- Para Explorer y OpsCenter, consulte Configuración de un administrador delegado.
- Para el Administrador de cambios de Systems Manager, consulte Configuración de una organización y una cuenta delegada para el Administrador de cambios.
- Para una configuración rápida, consulte Registrar un administrador delegado para una configuración rápida.

Desactivación de una cuenta de administrador delegado para Systems Manager

Para anular el registro de un administrador delegado, consulte los siguientes temas de la Guía del usuario:AWS Systems Manager

- Para Explorer y OpsCenter, consulte Anular el registro de un administrador delegado de Explorer.
- Para el Administrador de cambios de Systems Manager, consulte Configuración de una organización y una cuenta delegada para el Administrador de cambios.
- Para una configuración rápida, consulte Anular el registro de un administrador delegado para obtener una configuración rápida.

AWS User Notifications y AWS Organizations

AWS User Notificationses una ubicación central para tus AWS notificaciones.

Tras la integración AWS Organizations, podrá configurar y ver las notificaciones de forma centralizada en todas las cuentas de su organización.

Utilice la siguiente información para ayudarle a integrarse AWS User Notifications con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le Notificaciones de usuario permite realizar operaciones de apoyo en las cuentas de su organización.

Puede eliminar o modificar esta función solo si deshabilita el acceso de confianza entre Notificaciones de usuario y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForAWSUserNotifications`

Para obtener más información, consulte Uso de funciones vinculadas a servicios en la Guía del AWS User Notifications usuario.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza Notificaciones de usuario otorgan acceso a los siguientes directores de servicio:

- `notifications.amazon.com`

Habilitar el acceso de confianza con Notificaciones de usuario

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede habilitar el acceso confiable mediante. AWS User Notifications

Para habilitar el acceso de confianza mediante la Notificaciones de usuario consola, consulte Habilitar la AWS Organizations entrada AWS User Notifications en la Guía del Notificaciones de usuario usuario.

Deshabilitación del acceso con Notificaciones de usuario

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede habilitar el acceso confiable mediante AWS User Notifications.

Para deshabilitar el acceso de confianza mediante la Notificaciones de usuario consola, consulte Habilitar la AWS Organizations entrada AWS User Notifications en la Guía del Notificaciones de usuario usuario.

Habilitar una cuenta de administrador delegado para Notificaciones de usuario

El administrador de la cuenta de administración puede delegar los permisos Notificaciones de usuario administrativos a una cuenta de miembro designada, lo que se denomina administrador delegado. Para registrar una cuenta como administrador delegado para el mercado privado, el administrador de la cuenta de administración debe asegurarse de que el acceso confiable y la función vinculada al servicio estén habilitados, seleccionar Registrar un nuevo administrador, proporcionar el número de AWS cuenta de 12 dígitos y elegir Enviar.

Las cuentas de administración y las cuentas de administrador delegado pueden realizar tareas Notificaciones de usuario administrativas, como crear experiencias, actualizar la configuración de la marca, asociar o disociar audiencias, añadir o eliminar productos y aprobar o rechazar las solicitudes pendientes.

Para configurar un administrador delegado mediante la Notificaciones de usuario consola, consulte Registrar administradores delegados en la Guía del usuario. AWS User NotificationsNotificaciones de usuario

También puede configurar un administrador delegado mediante la API `RegisterDelegatedAdministrator` de Organizations. Para obtener más información, consulte RegisterDelegatedAdministratorla Referencia de comandos de Organizations.

Deshabilitar un administrador delegado para Notificaciones de usuario

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para. Notificaciones de usuario

Puede eliminar el administrador delegado mediante la Notificaciones de usuario consola o la API, o mediante la operación `DeregisterDelegatedAdministrator` CLI o SDK de Organizations.

Para deshabilitar la Notificaciones de usuario cuenta de administrador delegado mediante la Notificaciones de usuario consola, consulte Eliminar administradores delegados AWS User Notifications en la Guía del Notificaciones de usuario usuario.

Políticas de etiquetas y AWS Organizations

Las políticas de etiquetas son un tipo de política AWS Organizations que puede ayudarle a estandarizar las etiquetas en todos los recursos de las cuentas de su organización. Para obtener más información acerca de las políticas de etiquetas, consulte Políticas de etiquetas.

Utilice la siguiente información como ayuda para integrar las políticas de etiquetas. AWS Organizations

Los principales de servicios utilizados por los roles vinculados a servicios

Organizations interactúa con las etiquetas adjuntas a los recursos mediante la siguiente entidad de servicio.

- `tagpolicies.tag.amazonaws.com`

Habilitación del acceso de confianza para las políticas de etiquetas

Puede habilitar el acceso confiable habilitando las políticas de etiquetas en la organización o mediante la AWS Organizations consola.

> **Important**
>
> Le recomendamos encarecidamente que habilite el acceso de confianza mediante políticas de etiquetas. Esto permite a Organizations realizar las tareas de configuración necesarias.

Puede habilitar el acceso de confianza para las políticas de etiquetas habilitando el tipo de política de etiqueta en la consola de AWS Organizations . Para obtener más información, consulte Habilitar un tipo de política.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. Elija políticas de etiquetas en la lista de servicios.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de diálogo Habilitar el acceso de confianza para las políticas de etiquetas, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador de las políticas de etiquetas que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicio.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitar las políticas de etiquetas como un servicio de confianza en Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal tagpolicies.tag.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Deshabilitación del acceso de confianza con políticas de etiquetas

Puede deshabilitar el acceso de confianza a las políticas de etiquetas deshabilitando el tipo de política de etiquetas en la AWS Organizations consola. Para obtener más información, consulte Deshabilitar un tipo de política.

AWS Trusted Advisor y AWS Organizations

AWS Trusted Advisor inspecciona su AWS entorno y hace recomendaciones cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad. Cuando se integra con Organizations, puede recibir los resultados de las Trusted Advisor comprobaciones de todas las cuentas de su organización y descargar informes para ver los resúmenes de las comprobaciones y de los recursos afectados.

Para obtener más información, consulte Vista organizativa para AWS Trusted Advisor en la Guía del usuario de AWS Support .

Usa la siguiente información para ayudarte a integrarte AWS Trusted Advisor con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le Trusted Advisor permite realizar operaciones de apoyo en las cuentas de su organización.

Puede eliminar o modificar esta función solo si deshabilita el acceso de confianza entre Trusted Advisor y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForTrustedAdvisorReporting`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza Trusted Advisor otorgan acceso a los siguientes directores de servicio:

- `reporting.trustedadvisor.amazonaws.com`

Habilitar el acceso de confianza con Trusted Advisor

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede habilitar el acceso confiable mediante. AWS Trusted Advisor

Para habilitar el acceso confiable mediante la Trusted Advisor consola

Consulte Habilitación de la vista organizativa en la Guía del usuario de AWS Support .

Deshabilitación del acceso con Trusted Advisor

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Tras deshabilitar esta función, Trusted Advisor deja de registrar la información de los cheques de todas las demás cuentas de la organización. No puede ver ni descargar informes existentes ni crear informes nuevos.

Puede deshabilitar el acceso de confianza mediante las herramientas AWS Trusted Advisor o las AWS Organizations herramientas.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Trusted Advisor consola o las herramientas para deshabilitar la integración con Organizations. Esto permite AWS Trusted Advisor realizar cualquier limpieza que sea necesaria, como eliminar recursos o acceder a funciones que el servicio ya no necesite. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas por AWS Trusted Advisor.
> Si inhabilitas el acceso de confianza mediante la AWS Trusted Advisor consola o las herramientas, no necesitas completar estos pasos.

Para deshabilitar el acceso de confianza mediante la Trusted Advisor consola

Consulte Deshabilitar la vista organizativa en la Guía del usuario de AWS Support .

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Trusted Advisor como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: D isableAWSService Access

Habilitar una cuenta de administrador delegado para Trusted Advisor

Cuando se designa una cuenta de miembro como administrador delegado de la organización, los usuarios y los roles de la cuenta designada pueden administrar los metadatos de la Cuenta de AWS de otras cuentas de miembro de la organización. Si no habilita una cuenta de administrador delegado, estas tareas solo las puede realizar la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de los detalles de la cuenta.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado de Trusted Advisor la organización.

Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegado Trusted Advisor, consulte Registrar administradores delegados en la Guía del Soporte usuario.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante una AWS CLI o una de las AWS SDKs, puede utilizar los siguientes comandos:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

- AWS SDK: Llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el principal de servicio de la cuenta `account.amazonaws.com` como parámetros.

Deshabilitar un administrador delegado para Trusted Advisor

Puede eliminar al administrador delegado mediante la Trusted Advisor consola o mediante la SDK operación Organizations `DeregisterDelegatedAdministrator` CLI u. Para obtener información sobre cómo deshabilitar la Trusted Advisor cuenta de administrador delegado mediante la Trusted Advisor consola, consulte Anular el registro de administradores delegados en la guía del usuario.Soporte

AWS Well-Architected Tool y AWS Organizations

AWS Well-Architected Tool Esto le ayuda a documentar el estado de sus cargas de trabajo y a compararlas con las mejores prácticas de AWS arquitectura más recientes.

El uso de AWS Well-Architected Tool With Organizations permite AWS Well-Architected Tool tanto a los clientes de Organizations como a los clientes de Organizations simplificar el proceso de compartir AWS Well-Architected Tool recursos con otros miembros de su organización.

Para obtener más información, consulte Cómo compartir los recursos de AWS Well-Architected Tool en la Guía del usuario de AWS Well-Architected Tool .

Utilice la siguiente información para ayudarle a integrarse AWS Well-Architected Tool con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le AWS WA Tool permite realizar operaciones de apoyo en las cuentas de su organización.

Puede eliminar o modificar esta función solo si deshabilita el acceso de confianza entre AWS WA Tool y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForWellArchitected`

La política de roles de servicio es `AWSWellArchitectedOrganizationsServiceRolePolicy`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza AWS WA Tool otorgan acceso a los siguientes directores de servicio:

- `wellarchitected.amazonaws.com`

Habilitar el acceso de confianza con AWS WA Tool

Permite actualizar AWS WA Tool para reflejar los cambios jerárquicos en una organización.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso confiable mediante la AWS Well-Architected Tool consola o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Well-Architected Tool consola o las herramientas para permitir la integración con Organizations. Esto permite AWS Well-Architected Tool realizar cualquier configuración que necesite, como crear los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración utilizando las herramientas proporcionadas por AWS Well-Architected Tool. Para obtener más información, consulte esta nota.

Si habilitas el acceso confiable mediante la AWS Well-Architected Tool consola o las herramientas, no necesitas completar estos pasos.

Para habilitar el acceso confiable mediante la AWS WA Tool consola

Consulte Compartir sus AWS Well-Architected Tool recursos en la Guía AWS Well-Architected Tool del usuario.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una API operación en una de las AWS SDKs.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como IAM usuario, asumir un IAM rol o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En el panel de navegación, elija Servicios.
3. En la lista de servicios, elija AWS Well-Architected Tool.
4. Elija Habilitar acceso de confianza.
5. En el cuadro de AWS Well-Architected Tool diálogo Habilitar el acceso de confianza para, escriba habilitar para confirmar y, a continuación, seleccione Habilitar el acceso de confianza.
6. Si es el administrador de Only AWS Organizations, dígale al administrador AWS Well-Architected Tool que ahora puede habilitar el funcionamiento de ese servicio AWS Organizations desde la consola de servicios.

AWS CLI, AWS API

Para habilitar el acceso a servicios confiables mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para habilitar el acceso a los servicios de confianza:

- AWS CLI: enable-aws-service-access

  Ejecute el siguiente comando para habilitarlo AWS Well-Architected Tool como un servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal wellarchitected.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: E nableAWSService Access

Deshabilitación del acceso con AWS WA Tool

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Puede deshabilitar el acceso confiable mediante las herramientas AWS Well-Architected Tool o las AWS Organizations herramientas.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS Well-Architected Tool consola o las herramientas para deshabilitar la integración con Organizations. Esto permite AWS Well-Architected Tool realizar cualquier limpieza que sea necesaria, como eliminar recursos o acceder a funciones que el servicio ya no necesite. Continúe con estos pasos solo si no puede deshabilitar la integración utilizando las herramientas proporcionadas por AWS Well-Architected Tool.
> Si inhabilitas el acceso de confianza mediante la AWS Well-Architected Tool consola o las herramientas, no necesitas completar estos pasos.

Para deshabilitar el acceso de confianza mediante la AWS WA Tool consola

Consulte Compartir sus AWS Well-Architected Tool recursos en la Guía AWS Well-Architected Tool del usuario.

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para inhabilitarlo AWS Well-Architected Tool como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: D isableAWSService Access

Amazon VPC IP Address Manager (IPAM) y AWS Organizations

Amazon VPC IP Address Manager (IPAM) es una VPC función que le facilita la planificación, el seguimiento y la supervisión de las direcciones IP de sus AWS cargas de trabajo.

Su uso AWS Organizations le permite monitorear el uso de direcciones IP en toda su organización y compartir grupos de direcciones IP entre las cuentas de los miembros.

Para obtener más información, consulta Integrate IPAM with AWS Organizations en la Guía del VPC IPAM usuario de Amazon.

Utilice la siguiente información para ayudarle a integrar Amazon VPC IP Address Manager (IPAM) con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

La siguiente función vinculada al servicio se crea automáticamente en la cuenta de administración de su organización y en la cuenta de cada miembro al realizar la integración IPAM mediante AWS Organizations la IPAM consola o mediante IPAM la de ella. `EnableIpamOrganizationAdminAccount` API

- `AWSServiceRoleForIPAM`

Para obtener más información, consulte Funciones vinculadas a servicios IPAM en la Guía del VPCIPAMusuario de Amazon.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de IPAM conceden acceso a las siguientes entidades de servicio:

- `ipam.amazonaws.com`

Para habilitar el acceso de confianza con IPAM

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

> **Note**
>
> Cuando designa un administrador delegado, IPAM se habilita automáticamente un acceso confiable IPAM para su organización.
> IPAMrequiere un acceso AWS Organizations de confianza antes de poder designar una cuenta de miembro como administrador delegado de este servicio para su organización.

Puede habilitar el acceso de confianza utilizando únicamente las herramientas de Amazon VPC IP Address Manager (IPAM).

Si lo integras IPAM AWS Organizations con la IPAM consola o con la IPAM `EnableIpamOrganizationAdminAccount`API, concedes automáticamente un acceso confiable aIPAM. Al conceder un acceso de confianza, se crea el rol vinculado al servicio `AWS ServiceRoleForIPAM` en la cuenta de administración y en todas las cuentas de los miembros de la organización. IPAMutiliza la función vinculada al servicio para supervisar los recursos de EC2 red CIDRs asociados a la organización y almacenar las métricas relacionadas con los recursos de red de IPAM Amazon. CloudWatch Para obtener más información, consulte Funciones vinculadas a servicios IPAM en la Guía del VPCIPAMusuario de Amazon.

Para obtener instrucciones sobre cómo habilitar el acceso confiable, consulta Integrate IPAM with AWS Organizations en la Guía del VPC IPAM usuario de Amazon.

> **Note**
>
> No puede habilitar el acceso confiable IPAM mediante la AWS Organizations consola o con el `EnableAWSServiceAccess`API.

Para deshabilitar el acceso de confianza con IPAM

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza IPAM mediante el AWS Organizations `disable-aws-service-access`API.

Para obtener información sobre cómo deshabilitar los permisos de la IPAM cuenta y eliminar el rol vinculado al servicio, consulte Roles vinculados al servicio en IPAM la Guía del usuario de Amazon. VPC IPAM

Puede deshabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una API operación de Organizations en uno de los AWS SDKs.

AWS CLI, AWS API

Para deshabilitar el acceso a servicios de confianza mediante OrganizationsCLI/SDK

Utilice los siguientes AWS CLI comandos u API operaciones para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Ejecute el siguiente comando para deshabilitar Amazon VPC IP Address Manager (IPAM) como un servicio de confianza en Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: isableAWSServiceAcceso 3D

Habilitar una cuenta de administrador delegado para IPAM

La cuenta de administrador delegado IPAM es responsable de crear los grupos de direcciones IP IPAM y de administrar y supervisar el uso de las direcciones IP en la organización y compartir los grupos de direcciones IP entre las cuentas de los miembros. Para obtener más información, consulta Integrate IPAM with AWS Organizations en la Guía del VPC IPAM usuario de Amazon.

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado paraIPAM.

Puede especificar una cuenta de administrador delegado desde la IPAM consola o mediante. `enable-ipam-organization-admin-account` API Para obtener más información, consulte enable-ipam-organization-admin-account en la Referencia de AWS AWS CLI comandos.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para IPAM en la organización

Para configurar un administrador delegado mediante la IPAM consola, consulte Integrar IPAM con AWS Organizations en la Guía del VPC IPAM usuario de Amazon.

Desactivación de un administrador delegado para IPAM

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para. IPAM

Para eliminar a un administrador delegado mediante la AWS AWS CLI, consulte disable-ipam-organization-admin-account en la AWS AWS CLI Referencia de comandos.

Para deshabilitar la IPAM cuenta de administrador delegado mediante la IPAM consola, consulta Integrate IPAM with AWS Organizations en la Guía del VPC IPAM usuario de Amazon.

Analizador de accesibilidad de Amazon VPC y AWS Organizations

El Analizador de accesibilidad es una herramienta de análisis de configuración que le permite realizar pruebas de conectividad entre un recurso de origen y un recurso de destino en las nubes privadas virtuales (VPC).

El uso de AWS Organizations junto con el Analizador de accesibilidad le permite trazar rutas a través de las cuentas de sus organizaciones.

Para obtener más información, consulte Manage delegated administrator accounts in Reachability Analyzer en la Guía del usuario de Analizador de accesibilidad.

Utilice la siguiente información para ayudarle a integrar el analizador de accesibilidad con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite al Analizador de accesibilidad realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si desactiva el acceso de confianza entre el Analizador de accesibilidad y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForReachabilityAnalyzer`

Para obtener más información, consulte Cross-account analyses for Reachability Analyzer (Análisis entre cuentas para el Analizador de accesibilidad) en la Reachability Analyzer user guide (Guía del usuario del analizador de accesibilidad).

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios utilizados por el Analizador de accesibilidad otorgan acceso a las siguientes entidades de servicio:

- `reachabilityanalyzer.networkinsights.amazonaws.com`

Para habilitar el acceso de confianza con el Analizador de accesibilidad

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Al designar un administrador delegado para el Analizador de accesibilidad, se habilita automáticamente el acceso de confianza para el Analizador de accesibilidad de su organización.

El Analizador de accesibilidad requiere acceso de confianza a AWS Organizations para que se pueda designar una cuenta de miembro que sea el administrador delegado de este servicio para la organización.

Important

- Puede habilitar el acceso de confianza mediante la consola del Analizador de accesibilidad o la consola de Organizations. No obstante, le recomendamos encarecidamente que utilice la consola del Analizador de accesibilidad o la API de `EnableMultiAccountAnalysisForAwsOrganization` para permitir la integración con Organizations. Esto permite al Analizador de accesibilidad realizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio.
- Conceder acceso de confianza crea el rol vinculado a servicio `AWSServiceRoleForReachabilityAnalyzer` en la cuenta de administración y en todas las cuentas de miembro de la organización. El Analizador de accesibilidad utiliza la función vinculada al servicio para permitir a la dirección y al administrador delegado ejecutar análisis de conectividad entre cualquier recurso de la organización. El Analizador de accesibilidad es capaz de tomar instantáneas de los elementos de red de las cuentas de una organización para responder a consultas de conectividad.
- Para obtener más información e instrucciones sobre cómo habilitar el acceso de confianza a través del Analizador de accesibilidad, consulte Cross-account analyses for Reachability Analyzer (Análisis de cuentas cruzadas para el Analizador de accesibilidad) en la Reachability Analyzer user guide (Guía del usuario del Analizador de accesibilidad).

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de Analizador de accesibilidad de VPC, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.

3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **enable** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador del Analizador de accesibilidad que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar el Analizador de accesibilidad como servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal reachabilityanalyzer.networkinsights.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Para desactivar el acceso de confianza mediante el Analizador de accesibilidad

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Puede desactivar el acceso de confianza mediante la consola del Analizador de accesibilidad (recomedado) o la consola de Organizations. Para desactivar el acceso de confianza mediante la consola del Analizador de accesibilidad, consulte Cross-account analyses for Reachability Analyzer (Análisis de cuentas cruzadas para el Analizador de accesibilidad) en la Reachability Analyzer user guide (Guía del usuario del Analizador de accesibilidad).

Para habilitar una cuenta de administrador delegado para el Analizador de accesibilidad

La cuenta de administrador delegado puede ejecutar análisis de conectividad en cualquiera de los recursos de la organización. Para obtener más información, consulte Integración del Analizador de accesibilidad con AWS Organizations en la Guía del usuario del Analizador de accesibilidad.

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para el Analizador de accesibilidad.

Puede especificar una cuenta de administrador delegado desde la consola del Analizador de accesibilidad o mediante la API `RegisterDelegatedAdministrator`. Para obtener más información, consulte RegisterDelegatedAdministrator en la Organizations Command Reference (Referencia de comandos de Organizations).

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para el Analizador de accesibilidad en la organización

Para configurar un administrador delegado mediante la consola del Analizador de accesibilidad, consulte Integración del Analizador de accesibilidad con AWS Organizations en la Guía del usuario del Analizador de accesibilidad.

Desactivación de un administrador delegado para el Analizador de accesibilidad

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para el Analizador de accesibilidad.

Puede eliminar el administrador delegado mediante la consola o la API del Analizador de accesibilidad, o bien mediante la operación `DeregisterDelegatedAdministrator` de la CLI de Organizations o el SDK.

Para desactivar la cuenta de administrador delegado del Analizador de accesibilidad mediante la consola del Analizador de accesibilidad, consulte Cross-account analyses for Reachability Analyzer (Análisis de cuentas cruzadas para el Analizador de accesibilidad) en la Reachability Analyzer user guide (Guía del usuario del Analizador de accesibilidad).

Administrador delegado de los Servicios de AWS que funcionan con Organizations

Le recomendamos que utilice la cuenta de administración de AWS Organizations y sus usuarios y roles únicamente para las tareas que deba realizar dicha cuenta. También le recomendamos que almacene sus recursos de AWS en otras cuentas de miembros de la organización y los mantenga fuera de la cuenta de administración. Esto se debe a que las características de seguridad, como las políticas de control de servicios (SCP) de las organizaciones, no restringen ni los usuarios ni los roles de la cuenta de administración. Separar los recursos de su cuenta de administración también lo ayudará a comprender los cargos de sus facturas.

Muchos Servicios de AWS que se integran con Organizations le permiten reducir el uso de la cuenta de administración. Estos servicios le permiten registrar una o más cuentas de miembros como administradores que pueden administrar todas las cuentas de la organización utilizadas en el servicio. Estas cuentas se denominan administradores delegados para ese servicio específico. Al registrar una cuenta de miembro como administrador delegado de un servicio de AWS, permite que esa cuenta tenga algunos permisos administrativos para ese servicio, así como permisos para las acciones de solo lectura de la organización.

Antes de registrar una cuenta como administrador delegado de un servicio:

- Confirme que el servicio es compatible con los administradores delegados. Consulte la tabla de Servicios de AWS que puedes usar con AWS Organizations para obtener información sobre los servicios que admiten a los administradores delegados.
- Habilite el acceso de confianza para ese servicio.

> **Note**
>
> Para obtener información sobre cómo habilitar un servicio para un administrador delegado, consulte la tabla de Servicios de AWS que puedes usar con AWS Organizations y seleccione el enlace Más información de la columna Admite administradores delegados de ese servicio.

Permisos concedidos a cuentas de administrador delegado

Cada cuenta de administrador delegado específica de un servicio tiene permisos concedidos por ese servicio. Para obtener más información, consulte la tabla Servicios de AWS que puedes usar con

AWS Organizations y seleccione el enlace Más información en la columna Admite administradores delegados de ese servicio.

Una cuenta de administrador delegado también tiene estos permisos de solo lectura:

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`

Estos permisos le permiten ver, pero no cambiar, los siguientes elementos de la consola:

- Estructura de la organización, todas las cuentas y unidades organizativas y políticas organizativas
- Pertenencias
- Todas las cuentas y unidades organizativas.
- Políticas organizativas

Seguridad en AWS Organizations

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de cumplimiento a los que se aplica AWS Organizations, consulte Servicios de AWS Alcance by Compliance Program.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Organizations. En los siguientes temas, se le mostrará cómo configurar Organizations para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a usar otros Servicios de AWS que le ayuden a monitorear y proteger los recursos de su Organización.

Temas

- AWS PrivateLink para AWS Organizations
- Identity and Access Management para AWS Organizations
- Inicio de sesión y supervisión AWS Organizations
- Validación de conformidad en AWS Organizations
- Resiliencia en AWS Organizations
- Seguridad de la infraestructura en AWS Organizations

AWS PrivateLink para AWS Organizations

Con AWS PrivateLink for AWS Organizations, puede acceder al AWS Organizations servicio desde la Nube Privada Virtual (VPC) sin tener que cruzar la Internet pública.

Amazon VPC le permite lanzar AWS recursos en una red virtual personalizada. Puede utilizar una VPC para controlar la configuración de red, como el intervalo de direcciones IP, las subredes, las tablas de enrutamiento y las puertas de enlace de red. Para obtener más información VPCs, consulte la Guía del usuario de Amazon VPC.

Para conectar su Amazon VPC AWS Organizations, primero debe definir un punto de enlace de la VPC de interfaz (puntos de enlace de interfaz). Los puntos finales de la interfaz están representados por una o más interfaces de red elásticas (ENIs) a las que se les asignan direcciones IP privadas desde las subredes de la VPC. Las solicitudes de su VPC a puntos de enlace a AWS Organizations través de la interfaz permanecen en la red de Amazon.

Para obtener información general sobre los puntos de enlace de la interfaz, consulte Acceder a un AWS servicio mediante un punto de enlace de VPC de interfaz en la Guía del usuario de Amazon VPC.

Temas

- Limitaciones y restricciones de la forma AWS PrivateLinkAWS Organizations
- Creación de un punto final de VPC para AWS Organizations
- Creación de una política de punto de conexión de VPC para AWS Organizations

Limitaciones y restricciones de la forma AWS PrivateLinkAWS Organizations

Se aplican limitaciones de VPC a AWS PrivateLink . AWS Organizations Para obtener más información, consulte Acceder a un AWS servicio mediante un punto final de VPC de interfaz y AWS PrivateLink cuotas en la Guía del usuario de Amazon VPC. Además, se aplican las siguientes restricciones:

- Solo está disponible en la región `us-east-1`.
- No admite seguridad de la capa de transporte (TLS) 1.1

Creación de un punto final de VPC para AWS Organizations

Puede crear un AWS Organizations punto de conexión en su VPC mediante la consola de Amazon VPC, el AWS Command Line Interface () o.AWS CLI AWS CloudFormation

Para obtener información sobre cómo crear y configurar un punto de conexión mediante la consola de Amazon VPC o la AWS CLI, consulte Crear un punto de enlace de VPC en la Guía del usuario de Amazon VPC. Para obtener información sobre cómo crear y configurar un punto final mediante AWS CloudFormation, consulte el VPCEndpoint recurso AWS:EC2::: en la Guía del AWS CloudFormation usuario.

Al crear un AWS Organizations punto final, utilice lo siguiente como nombre del servicio:

```
com.amazonaws.us-east-1.organizations
```

Si necesita módulos criptográficos validados por FIPS 140-2 para acceder AWS, utilice el siguiente nombre de servicio AWS Organizations FIPS:

```
com.amazonaws.us-east-1.organizations-fips
```

Creación de una política de punto de conexión de VPC para AWS Organizations

Puede vincular una política de punto de conexión con su punto de conexión de VPC que controla el acceso a Organizations. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Controlar el acceso a los puntos de conexión de la VPC mediante políticas de puntos de conexión en la Guía de usuario de Amazon VPC.

Ejemplo: Política de punto de conexión de VPC para acciones de AWS Organizations

```
{
   "Statement":[
      {
```

```
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

Identity and Access Management para AWS Organizations

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (iniciar sesión) y autorizado (tiene permisos) para utilizar recursos de Organizations. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- ¿Cómo AWS Organizations funciona con IAM
- Administrar los permisos de acceso de una organización con AWS Organizations
- Ejemplos de políticas basadas en identidades de AWS Organizations
- Ejemplos de políticas basadas en recursos para AWS Organizations
- AWS políticas gestionadas para AWS Organizations
- Control de acceso basado en atributos con etiquetas para AWS Organizations
- Solución de problemas de AWS Organizations identidad y acceso

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Organizations.

Usuario de servicio: si utiliza el servicio de Organizations para llevar a cabo su trabajo, su administrador le proporcionará las credenciales y los permisos que necesite. A medida que utilice más características de Organizations para llevar a cabo su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una característica de Organizations, consulte Solución de problemas de AWS Organizations identidad y acceso.

Administrador de servicio: si está a cargo de los recursos de Organizations de su empresa, probablemente tenga acceso completo a Organizations. Su trabajo consiste en determinar a qué características y recursos de Organizations deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo puede utilizar su empresa IAM con Organizations, consulte ¿Cómo AWS Organizations funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más información sobre cómo escribir políticas para administrar el acceso a Organizations. Para consultar ejemplos de políticas basadas en identidades de Organizations que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidades de AWS Organizations.

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus

credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios empresarial, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulta Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puedes crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué

puedes acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .

- Permisos de usuario de IAM temporales: un usuario de IAM puedes asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puedes utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulta Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puedes asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué

condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades puedes clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas puedes establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puedes conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud

cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Organizations funciona con IAM

Antes de utilizar IAM para administrar el acceso a Organizations, conozca qué características de IAM se pueden utilizar con Organizations.

Característica de IAM	Compatible con Organizations
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	No
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan las Organizaciones y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades para Organizations

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para Organizations

Para ver ejemplos de políticas basadas en identidades de Organizations, consulte Ejemplos de políticas basadas en identidades de AWS Organizations.

Políticas basadas en recursos de Organizations

Compatibilidad con las políticas basadas en recursos: sí

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS,

el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

El servicio de Organizations solo admite un tipo de política basada en recursos denominada política de delegación basada en recursos, que especifica qué cuenta de miembro puede llevar a cabo acciones con las políticas. Puede agregar varias declaraciones en la política para denotar distintos conjuntos de permisos para las cuentas de los miembros.

Para obtener más información, consulte Administrador delegado para AWS Organizations.

Ejemplos de políticas basadas en recursos de Organizations

Para ver ejemplos de políticas basadas en recursos de Organizations, consulte Ejemplos de políticas basadas en recursos para AWS Organizations.

Acciones de política para Organizations

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puedes utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Organizations, consulte Actions defined by AWS Organizations en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Organizations utilizan el siguiente prefijo antes de la acción:

```
organizations
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "organizations:action1",
      "organizations:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidades de Organizations, consulte Ejemplos de políticas basadas en identidades de AWS Organizations.

Recursos de políticas para Organizations

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de Organizations y sus tipos ARNs, consulte los recursos definidos por AWS Organizations en la Referencia de autorización de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Organizations.

Para ver ejemplos de políticas basadas en identidades de Organizations, consulte Ejemplos de políticas basadas en identidades de AWS Organizations.

Claves de condición de política de Organizations

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Organizations, consulte Condition keys for AWS Organizations en la Referencia de autorizaciones de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Organizations.

Para ver ejemplos de políticas basadas en identidades de Organizations, consulte Ejemplos de políticas basadas en identidades de AWS Organizations.

ACLs en Organizations

Soportes ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Organizations

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulta Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Organizations

Compatible con el uso de credenciales temporales: no

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes

AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para Organizations

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

Roles de servicio para Organizations

Compatibilidad con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Organizations. Edite los roles de servicio solo cuando Organizations proporcione orientación para hacerlo.

Roles vinculados a servicios para Organizations

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Administrar los permisos de acceso de una organización con AWS Organizations

Todos los AWS recursos, incluidas las raíces OUs, las cuentas y las políticas de una organización, son propiedad de un Cuenta de AWS, y los permisos para crear un recurso o acceder a ellos se rigen por las políticas de permisos. Para una organización, su cuenta de administración posee todos los recursos. El administrador de una cuenta puede controlar el acceso a AWS los recursos adjuntando políticas de permisos a las identidades de IAM (usuarios, grupos y roles).

> **Note**
>
> Un administrador de la cuenta (o usuario administrador) es un usuario con permisos de administrador. Para obtener más información, consulte las prácticas recomendadas de seguridad en IAM en la AWS Account Management Guía de referencia.

Cuando concede permisos, decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas desea permitir en esos recursos.

De forma predeterminada, los usuarios, grupos y roles de IAM no tienen permisos. Como administrador de la cuenta de administración de una organización, puede realizar tareas administrativas o delegar permisos de administrador a otros usuarios o funciones de IAM en la cuenta de administración. Para ello, asocia una política de permisos de IAM a un usuario, grupo o rol de IAM. De forma predeterminada, un usuario no tiene ningún permiso; esto recibe el nombre

de denegación implícita. La política invalida la denegación implícita con un permiso explícito que especifica las acciones que puede realizar el usuario y los recursos que puede utilizar en las acciones. Si los permisos se conceden a un rol, los usuarios de otras cuentas de la organización pueden asumir ese rol.

AWS Organizations recursos y operaciones

En esta sección se analiza cómo AWS Organizations los conceptos se corresponden con sus conceptos equivalentes a la IAM.

Recursos

En AWS Organizations, puede controlar el acceso a los siguientes recursos:

- La raíz y la OUs que componen la estructura jerárquica de una organización
- Las cuentas que son miembros de la organización
- Las políticas que adjunta a las entidades de la organización
- Los protocolos que usa para cambiar el estado de la organización

Cada uno de esos recursos tiene un único nombre de recurso de Amazon (ARN) asociado. El acceso a un recurso se controla especificando su ARN en el elemento `Resource` de una política de permisos de IAM. Para obtener una lista completa de los formatos de ARN de los recursos que se utilizan AWS Organizations, consulte Tipos de recursos definidos AWS Organizations en la Referencia de autorización de servicio.

Operaciones

AWS proporciona un conjunto de operaciones para trabajar con los recursos de una organización. Estas operaciones le permiten realizar tareas como crear, mostrar, modificar y eliminar recursos y obtener acceso a su contenido. A la mayoría de las operaciones se puede hacer referencia en el elemento `Action` de una política de IAM para controlar quién puede utilizar dicha operación. Para obtener una lista de las operaciones de AWS Organizations que pueden utilizarse como permisos en una política de IAM, consulte Actions defined by organizations en la Referencia de autorización de servicios.

Al combinar un elemento `Action` y un elemento `Resource` en el elemento `Statement` de una política de permisos, puede controlar exactamente qué recursos de ese conjunto concreto de acciones se pueden usar.

Claves de condición

AWS proporciona claves de condición que puede consultar para proporcionar un control más detallado sobre determinadas acciones. Puede hacer referencia a estas claves de condición en el elemento `Condition` de una política de IAM para especificar las circunstancias adicionales que se deben cumplir para que se aplique la instrucción.

Las siguientes claves de condición son especialmente útiles en AWS Organizations:

- `aws:PrincipalOrgID` - simplifica la especificación del elemento `Principal` en una política basada en recursos. Esta clave global ofrece una alternativa a enumerar todas IDs las cuentas Cuentas de AWS de una organización. En lugar de mostrar todas las cuentas de la organización, puede especificar el ID de organización en el elemento `Condition`.

  > **Note**
  >
  > Esta condición global también se aplica a la cuenta de administración de una organización.

  Para obtener más información, consulte la descripción de `PrincipalOrgID` en Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.
- `aws:PrincipalOrgPaths` - Utiliza esta clave de condición para hacer coincidir los miembros de una raíz de organización específica, una unidad organizativa o sus secundarias. La clave de condición `aws:PrincipalOrgPaths` vuelve como verdadera cuando el elemento principal (usuario raíz, usuario o rol de IAM) que realiza la solicitud se encuentra en la ruta de la organización especificada. Una ruta es una representación textual de la estructura de una AWS Organizations entidad. Para obtener más información sobre las rutas, consulte Comprender la ruta de la AWS Organizations entidad en la Guía del usuario de IAM. Para obtener más información sobre el uso de esta clave de condición, consulte aws: PrincipalOrgPaths en la Guía del usuario de IAM.

  Por ejemplo, el siguiente elemento de condición coincide con los miembros de cualquiera de las dos organizaciones OUs de la misma organización.

```
        "Condition": {
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
                    "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
```

```
                ]
            }
        }
```

- `organizations:PolicyType` - Puede utilizar esta clave de condición para restringir las operaciones de API relacionadas con la política de Organizations para que funcionen únicamente en políticas de Organizations del tipo especificado. Puede aplicar esta clave de condición a cualquier instrucción de política que incluya una acción que interactúe con las políticas de Organizations.

  Puede utilizar los siguientes valores con esta clave de condición:

  - `SERVICE_CONTROL_POLICY`
  - `RESOURCE_CONTROL_POLICY`
  - `DECLARATIVE_POLICY_EC2`
  - `BACKUP_POLICY`
  - `TAG_POLICY`
  - `CHATBOT_POLICY`
  - `AISERVICES_OPT_OUT_POLICY`

  Por ejemplo, la siguiente política de ejemplo permite al usuario realizar cualquier operación de Organizations. Sin embargo, si el usuario realiza una operación que toma un argumento de política, la operación solo se permite si la política especificada es una política de etiquetado. La operación produce un error si el usuario especifica cualquier otro tipo de política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
```

```
}
```

- `organizations:ServicePrincipal`— Disponible como condición si utiliza las operaciones Habilitar el AWSService acceso o Deshabilitar el AWSService acceso para habilitar o deshabilitar el acceso de confianza con otros AWS servicios. Puede utilizar `organizations:ServicePrincipal` para limitar las solicitudes que esas operaciones realizan a una lista de nombres de principal de servicio aprobados.

  Por ejemplo, la siguiente política permite al usuario especificar únicamente AWS Firewall Manager cuándo habilitar o deshabilitar el acceso de confianza con AWS Organizations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

Para ver una lista de todas las claves de AWS Organizations condición específicas que se pueden usar como permisos en una política de IAM, consulte las claves de condición de la Referencia de AWS Organizations autorización de servicios.

Titularidad de los recursos

Cuenta de AWS Es propietario de los recursos que se crean en la cuenta, independientemente de quién los haya creado. En concreto, el propietario del recurso es el Cuenta de AWS de la entidad principal (es decir, el usuario raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud de

creación de recursos. En el caso de una organización, siempre es la cuenta de administración. No puede llamar a la mayoría de las operaciones que crean o tiene acceso a los recursos de la organización desde las cuentas de miembro. Los siguientes ejemplos ilustran cómo funciona:

- Si utiliza las credenciales de cuenta raíz de su cuenta de administración para crear una unidad organizativa, su cuenta de administración será la propietaria del recurso. (En AWS Organizations, el recurso es la OU).
- Si crea un usuario de IAM en su cuenta de administración y le concede permisos para crear unidades organizativas, este puede crearlas. Sin embargo, la cuenta de administración, a la que pertenece el usuario, es la propietaria del recurso de unidad organizativa.
- Si crea un rol de IAM en su cuenta de administración con permisos para crear unidades organizativas, cualquier persona puede asumir el rol y crearlos. La cuenta de administración, a la que pertenece el rol (y no el usuario que lo asume), es la propietaria del recurso de unidad organizativa.

Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

> **Note**
>
> En esta sección se analiza el uso de la IAM en el contexto de AWS Organizations. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte la Guía del usuario de IAM. Para obtener información acerca de la sintaxis y las descripciones de las políticas de IAM, consulte Referencia de políticas JSON de IAM en la Guía del usuario de IAM.

Las políticas que se asocian a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM). Las políticas que se asocian a un recurso se denominan políticas basadas en recursos. AWS Organizations solamente admite las políticas basadas en identidades (políticas de IAM).

Temas

- Políticas basadas en permiso de identidades (políticas de IAM)
- Políticas basadas en recursos

Políticas basadas en permiso de identidades (políticas de IAM)

Puede adjuntar políticas a las identidades de IAM para permitir que esas identidades realicen operaciones en AWS los recursos. Por ejemplo, puede hacer lo siguiente:

- Adjunte una política de permisos a un usuario o grupo de su cuenta: para conceder a un usuario permisos para crear un AWS Organizations recurso, como una política de control de servicios (SCP) o una OU, puede adjuntar una política de permisos a un usuario o grupo al que pertenezca el usuario. El usuario o grupo debe estar en la organización de la cuenta de administración.
- Asociar una política de permisos a un rol (conceder permisos entre cuentas): puede asociar una política de permisos basada en la identidad a un rol de IAM para conceder acceso entre cuentas a una organización. Por ejemplo, el administrador de la cuenta de administración puede crear un rol para conceder permisos entre cuentas a un usuario de una cuenta de miembro de la siguiente manera:
  1. El administrador de la cuenta de administración crea un rol de IAM y asocia una política de permisos al rol, que concede permisos a los recursos de la organización.
  2. El administrador de la cuenta de administración asocia una política de confianza al rol, que identifica el ID de la cuenta de miembro como la entidad `Principal`, la cual puede asumir el rol.
  3. El administrador de la cuenta de miembro puede delegar entonces permisos para asumir el rol a cualquier usuario de la cuenta de miembro. Esto permite a los usuarios de la cuenta de miembro crear o tener acceso a los recursos de la cuenta de administración y la organización. El principal de la política de confianza también puede ser el principal de un AWS servicio si quieres conceder permisos a un AWS servicio para que asuma esa función.

  Para obtener más información sobre el uso de IAM para delegar permisos, consulte Administración de accesos en la Guía del usuario de IAM.

A continuación se ofrecen ejemplos de políticas que permite a un usuario realizar la acción `CreateAccount` en su organización.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
         "Effect":"Allow",
         "Action":[
```

```
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

También puede facilitar un ARN parcial en el elemento `Resource` de la política para indicar el tipo de recurso.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

También puede denegar la creación de cuentas que no incluyan etiquetas específicas en la cuenta que se está creando.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/key":"value"
            }
         }
      }
   ]
}
```

Para obtener más información acerca de los usuarios, los grupos, los roles y los permisos, consulte Identidades de IAM (usuarios, grupos y roles) en la Guía del usuario de IAM.

Políticas basadas en recursos

Algunos servicios, como Amazon S3, admiten políticas de permisos basadas en recursos. Por ejemplo, puede adjuntar una política a un bucket de Amazon S3 para gestionar los permisos de acceso a ese bucket. AWS Organizations actualmente no admite políticas basadas en recursos.

Especificación de elementos de política: acciones, condiciones, efectos y recursos

Para cada AWS Organizations recurso, el servicio define un conjunto de operaciones o acciones de la API que pueden interactuar con ese recurso o manipularlo de alguna manera. Para conceder permisos para estas operaciones, AWS Organizations define un conjunto de acciones que puede especificar en una política. Por ejemplo, para el recurso OU, AWS Organizations define acciones como las siguientes:

- `AttachPolicy` y `DetachPolicy`
- `CreateOrganizationalUnit` y `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` y `DescribeOrganizationalUnit`

En algunos casos, la ejecución de una operación de la API podría requerir permisos para más de una acción y podría necesitar permisos para más de un recurso.

A continuación se indican los aspectos más básicos que puede utilizar en una política de permisos de IAM:

- Action - Puede utilizar esta palabra clave para identificar las operaciones (acciones) que desea permitir o denegar. Por ejemplo, según lo especificado`Effect`, `organizations:CreateAccount` permite o deniega al usuario los permisos para realizar la AWS Organizations `CreateAccount` operación. Para obtener más información, consulte Elementos de política JSON de IAM: Action en la Guía del usuario de IAM.
- Resource - Utilice esta palabra clave para especificar el ARN del recurso al que se aplica la instrucción de la política. Para obtener más información, consulte Elementos de política JSON de IAM: Resource en la Guía del usuario de IAM.
- Condition - Utilice esta palabra clave para especificar condiciones adicionales que se deben cumplir para que la instrucción de política sea aplicable. `Condition` suele especificar circunstancias adicionales que deben estar definidas como "true" para que la política coincida.

Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Effect - Puede utilizar esta palabra clave para especificar si la instrucción de la política permite o deniega la acción en el recurso. Si no concede acceso de forma explícita (o permite) un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso; de esta forma, se asegurará de que un usuario no pueda realizar la acción especificada en el recurso especificado, incluso si otra política otorga acceso. Para obtener más información, consulte Elementos de política JSON de IAM: Effect en la Guía del usuario de IAM.
- Principal: en las políticas basadas en la identidad (políticas de IAM), el usuario al que se asocia esta política es de forma automática e implícita la entidad principal. En el caso de las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad para la que desea recibir los permisos (solo se aplica a las políticas basadas en recursos). AWS Organizations actualmente solo admite políticas basadas en la identidad, no en políticas basadas en recursos.

Para obtener más información acerca de la sintaxis y las descripciones de las políticas de IAM, consulte Referencia de políticas JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de AWS Organizations

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Organizations. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Organizations, incluido el ARNs formato de cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de AWS Organizations la Referencia de autorización de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Organizations

- Cómo permitir a los usuarios consultar sus propios permisos
- Conceder permisos completos de administrador a un usuario
- Conceder acceso limitado por acciones
- Concesión de acceso a recursos específicos
- Concesión de la capacidad de habilitar el acceso de confianza a entidades principales de servicio limitadas

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Organizations de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas

nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de Organizations

Para acceder a la AWS Organizations consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Organizations en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de Organizations, adjunte también la política de `AWSOrganizationsFullAccess`Organizations o `AWSOrganizationsReadOnlyAccess` AWS gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

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

```
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Conceder permisos completos de administrador a un usuario

Puede crear una política de IAM que conceda todos los permisos de AWS Organizations administrador a un usuario de IAM de su organización. Para ello, puede usar el editor de políticas JSON en la consola de IAM.

Utilización del editor de política de JSON para la creación de una política

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en. https://console.aws.amazon.com/iam/
2. En el panel de navegación de la izquierda, elija Políticas.

Si es la primera vez que elige Políticas, aparecerá la página Welcome to Managed Policies (Bienvenido a políticas administradas). Elija Comenzar.

3. En la parte superior de la página, seleccione Crear política.
4. En la sección Editor de políticas, seleccione la opción JSON.
5. Ingrese el siguiente documento de política JSON:

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

6. Elija Next (Siguiente).

> **Note**
>
> Puede alternar entre las opciones Visual y JSON del editor en todo momento. No obstante, si realiza cambios o selecciona Siguiente en la opción Visual del editor, es posible que IAM reestructure la política, con el fin de optimizarla para el editor visual. Para obtener más información, consulte Reestructuración de política en la Guía del usuario de IAM.

7. En la página Revisar y crear, introduzca el Nombre de la política y la Descripción (opcional) para la política que está creando. Revise los Permisos definidos en esta política para ver los permisos que concede la política.
8. Elija Crear política para guardar la nueva política.

Para obtener más información sobre la creación de una política de IAM, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Conceder acceso limitado por acciones

Si desea conceder permisos limitados en lugar de todos los permisos, puede crear una política que muestre los permisos individuales que desea permitir en el elemento `Action` de la política de

permisos de IAM. Tal y como se muestra en el siguiente ejemplo, puede utilizar caracteres comodín (*) para conceder solo los permisos `Describe*` y `List*`, que básicamente proporcionan acceso de solo lectura a la organización.

> **Note**
>
> En una política de control de servicios (SCP), el carácter comodín (*) de un elemento `Action` únicamente puede aparecer solo o al final de la cadena. No puede aparecer al principio o en el medio de la cadena. Por lo tanto, `"servicename:action*"` es válido, pero `"servicename:*action"` ambos no `"servicename:some*action"` son válidos en SCPs.

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

Para obtener una lista de todos los permisos que se pueden asignar en una política de IAM, consulte Acciones definidas por AWS Organizations en la Referencia de autorización de servicios.

Concesión de acceso a recursos específicos

Además de restringir el acceso a acciones específicas, puede restringir el acceso a entidades específicas de la organización. Los elementos `Resource` de los ejemplos en las secciones anteriores especifican el carácter comodín ("*"), que significa "cualquier recurso al que la acción tenga acceso." En su lugar, puede sustituir el "*" por el Nombre de recurso de Amazon (ARN) de las entidades específicas a las que desea permitir el acceso.

Ejemplo: Conceder permisos a una sola unidad organizativa

La primera instrucción de la siguiente política concede acceso de lectura a un usuario de IAM en toda la organización, pero la segunda instrucción permite al usuario realizar acciones administrativas

de AWS Organizations solo en una unidad organizativa especificada (OU). Esto no se extiende a ningún niño OUs. No se concede acceso a la facturación. Tenga en cuenta que esto no le da acceso administrativo a Cuentas de AWS la unidad organizativa. Solo concede permisos para realizar AWS Organizations operaciones en las cuentas de la OU especificada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-
<organizationalUnitId>"
    }
  ]
}
```

Puede obtener el IDs correspondiente a la OU y a la organización desde la AWS Organizations consola o llamando al `List*` APIs. El usuario o grupo al que aplica esta política puede realizar cualquier acción (`"organizations:*"`) en cualquier entidad que esté directamente incluida en la unidad organizativa especificada. La unidad organizativa se identifica por el Nombre de recurso de Amazon (ARN).

Para obtener más información sobre los ARNs distintos recursos, consulte los tipos de recursos definidos AWS Organizations en la Referencia de autorización de servicios.

Concesión de la capacidad de habilitar el acceso de confianza a entidades principales de servicio limitadas

Puede utilizar el elemento `Condition` de una instrucción de política para limitar aún más las circunstancias donde se debe aplicar dicha declaración de política.

Ejemplo: Concesión de permisos para habilitar el acceso de confianza a un servicio especificado

La siguiente instrucción muestra cómo se puede restringir la capacidad de habilitar el acceso de confianza únicamente a los servicios especificados. Si el usuario intenta llamar a la API con una entidad de servicio diferente a la utilizada AWS IAM Identity Center, esta política no coincide y se deniega la solicitud:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

Para obtener más información sobre los ARNs distintos recursos, consulta los tipos de recursos definidos AWS Organizations en la Referencia de autorización de servicios.

Ejemplos de políticas basadas en recursos para AWS Organizations

Los siguientes ejemplos de código muestran cómo se pueden utilizar las políticas de delegación basadas en recursos. Para obtener más información, consulte Administrador delegado para AWS Organizations.

Temas

- Ejemplo: ver la organización OUs, las cuentas y las políticas
- Ejemplo: Crear, leer, actualizar y eliminar políticas
- Ejemplo: Etiquetar y desetiquetar políticas
- Ejemplo: Vincular políticas a una sola unidad organizativa o cuenta
- Ejemplo: Permisos consolidados para administrar las políticas de copia de seguridad de una organización

Ejemplo: ver la organización OUs, las cuentas y las políticas

Antes de delegar la administración de las políticas, debes delegar los permisos para navegar por la estructura de una organización y ver las unidades organizativas (OUs), las cuentas y las políticas asociadas a ellas.

En este ejemplo se muestra cómo puede incluir estos permisos en su política de delegación basada en los recursos para la cuenta del miembro,. *AccountId*

> **Important**
>
> Es aconsejable que incluya permisos solo para las acciones mínimas requeridas como se muestra en el ejemplo, aunque es posible delegar cualquier acción de solo lectura de Organizaciones utilizando esta política.

Este ejemplo de política de delegación otorga los permisos necesarios para completar las acciones mediante programación desde la API o. AWS AWS CLI Para utilizar esta política de delegación, sustituya el texto del AWS marcador de posición por su *AccountId* propia información. A continuación, siga las instrucciones indicadas en Administrador delegado para AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Ejemplo: Crear, leer, actualizar y eliminar políticas

Puede crear una política de delegación basada en recursos que permita a la cuenta de administración delegar acciones `create`, `read`, `update` y `delete` para cualquier tipo de política. En este ejemplo se muestra cómo puede delegar estas acciones para las políticas de control de servicios en la cuenta del miembro,*`MemberAccountId`*. Los dos recursos que se muestran en el ejemplo permiten el acceso a las políticas de control de servicios AWS gestionados y gestionados por el cliente, respectivamente.

> **Important**
>
> Esta política permite que los administradores delegados lleven a cabo las acciones especificadas en las políticas creadas por cualquier cuenta de la organización, incluida la cuenta de administración.
> No permite a los administradores delegados vincular ni desvincular políticas porque no incluye los permisos necesarios para llevar a cabo las acciones `organizations:AttachPolicy` y `organizations:DetachPolicy`.

En este ejemplo, la política de delegación otorga los permisos necesarios para completar las acciones mediante programación desde la AWS API o. AWS CLI Sustituya el texto AWS del marcador de posición por *`MemberAccountIdManagementAccountId`*, y por su *`OrganizationId`* propia información. A continuación, siga las instrucciones indicadas en Administrador delegado para AWS Organizations.

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

```
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "SERVICE_CONTROL_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingMinimalActionsForSCPs",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:DescribePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
service_control_policy/*",
```

```
        "arn:aws:organizations::aws:policy/service_control_policy/*"
      ]
    }
  ]
}
```

Ejemplo: Etiquetar y desetiquetar políticas

En este ejemplo se muestra cómo podría crear una política de delegación basada en recursos que permita a los administradores delegados etiquetar o desetiquetar las políticas de copia de seguridad. Otorga los permisos necesarios para completar las acciones mediante programación desde la AWS API o. AWS CLI

Para utilizar esta política de delegación, sustituya el texto del AWS marcador de posición por *`MemberAccountId`* y por su propia *`OrganizationId`* información. *`ManagementAccountId`* A continuación, siga las instrucciones indicadas en Administrador delegado para AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingTaggingBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:TagResource",
        "organizations:UntagResource"
      ],
      "Resource": "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
    }
  ]
}
```

Ejemplo: Vincular políticas a una sola unidad organizativa o cuenta

En este ejemplo, se muestra cómo se puede crear una política de delegación basada en recursos que permita a los administradores delegados `attach` o `detach` las políticas de Organizations de una unidad organizativa (OU) o cuenta específicas. Antes de delegar estas acciones, debe delegar los permisos para navegar por la estructura de una organización y ver las cuentas que contiene. Para obtener más información, consulte Ejemplo: ver la organización OUs, las cuentas y las políticas

Important

- Si bien esta política permite adjuntar o separar políticas de la unidad organizativa o cuenta especificada, no incluye ni a los hijos ni a las cuentas OUs subordinadas a menores. OUs
- Esta política permite que los administradores delegados realicen las acciones especificadas en las políticas creadas por cualquier cuenta de la organización, incluida la cuenta de administración.

Este ejemplo de política de delegación otorga los permisos necesarios para completar las acciones mediante programación desde la API o. AWS AWS CLI Para usar esta política de delegación, sustituya el texto del AWS marcador de posición por *MemberAccountId* *ManagementAccountIdOrganizationId*, y por su propia *TargetAccountId* información. A continuación, siga las instrucciones indicadas en Administrador delegado para AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AttachDetachPoliciesSpecifiedAccountOU",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
```

```
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/ou-OUId",
        "arn:aws:organizations::ManagementAccountId:account/
o-OrganizationId/TargetAccountId",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

Para delegar la vinculación y desvinculación de políticas de cualquier OU o cuenta de la organización, sustituya el recurso del ejemplo anterior por los siguientes recursos:

```
"Resource": [
    "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/
*"
]
```

Ejemplo: Permisos consolidados para administrar las políticas de copia de seguridad de una organización

En este ejemplo se muestra cómo se puede crear una política de delegación basada en recursos que permita a la cuenta de administración delegar todos los permisos necesarios para administrar las políticas de copia de seguridad dentro de la organización, incluidas `create`, `read`, `update` y acciones `delete`, así como acciones de `attach` y `detach` política.

> **Important**
>
> Esta política permite que los administradores delegados realicen las acciones especificadas en las políticas creadas por cualquier cuenta de la organización, incluida la cuenta de administración.

Este ejemplo de política de delegación otorga los permisos necesarios para completar las acciones mediante programación desde la AWS API o. AWS CLI Para usar esta política

de delegación, sustituya el texto del AWS marcador de posición por *MemberAccountId* *ManagementAccountIdOrganizationId*, y por su propia *RootId* información. A continuación, siga las instrucciones indicadas en Administrador delegado para AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
            "organizations:DescribeOrganization",
            "organizations:DescribeOrganizationalUnit",
            "organizations:DescribeAccount",
            "organizations:ListRoots",
            "organizations:ListOrganizationalUnitsForParent",
            "organizations:ListParents",
            "organizations:ListChildren",
            "organizations:ListAccounts",
            "organizations:ListAccountsForParent",
            "organizations:ListTagsForResource"
        ],
      "Resource": "*"
    },
    {
      "Sid": "DelegatingNecessaryDescribeListActionsForSpecificPolicyType",
      "Effect": "Allow",
      "Principal": {
            "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
            "organizations:DescribePolicy",
            "organizations:DescribeEffectivePolicy",
            "organizations:ListPolicies",
            "organizations:ListPoliciesForTarget",
            "organizations:ListTargetsForPolicy"
      ],
      "Resource": "*",
      "Condition": {
            "StringLikeIfExists": {
```

```
                "organizations:PolicyType": "BACKUP_POLICY"
            }
      }
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
      "AWS": "arn:aws:iam::MemberAccountId:root"
    },
      "Action": [
            "organizations:CreatePolicy",
            "organizations:UpdatePolicy",
            "organizations:DeletePolicy",
            "organizations:AttachPolicy",
            "organizations:DetachPolicy",
            "organizations:EnablePolicyType",
            "organizations:DisablePolicyType"
      ],
      "Resource": [
            "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/
r-RootId",
            "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
            "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
            "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ],
      "Condition": {
            "StringLikeIfExists": {
                "organizations:PolicyType": "BACKUP_POLICY"
            }
      }
    }
  ]
}
```

AWS políticas gestionadas para AWS Organizations

En esta sección, se identifican las políticas AWS administradas que se proporcionan para administrar la organización. No puede modificar ni eliminar una política AWS gestionada, pero puede adjuntarla o desvincularla a las entidades de su organización según sea necesario.

AWS Organizations políticas administradas para su uso con AWS Identity and Access Management () IAM

Una política IAM gestionada es proporcionada y mantenida por AWS. Una política administrada proporciona permisos para tareas comunes que puede asignar a sus usuarios adjuntando la política administrada al IAM usuario u objeto de rol correspondiente. No es necesario que redacte la política usted mismo y, cuando la AWS actualice según corresponda para admitir nuevos servicios, se beneficiará de la actualización de forma automática e inmediata. Puedes ver la lista de políticas AWS administradas en la página Políticas de la IAM consola. Use el menú de Filtrar políticas para seleccionar AWS administrado.

Puede usar estas políticas administradas para conceder permisos a los usuarios de su organización.

AWS política gestionada: AWSOrganizationsFullAccess

Proporciona todos los permisos necesarios para crear y administrar completamente una organización.

Consulte la política: `AWSOrganizationsFullAccess`.

AWS política gestionada: AWSOrganizationsReadOnlyAccess

Proporciona acceso de solo lectura a la información acerca de la organización. No permite al usuario realizar ningún cambio.

Consulte la política: `AWSOrganizationsReadOnlyAccess`.

AWS política gestionada: DeclarativePoliciesEC2Report

El rol AWSServiceRoleForDeclarativePoliciesEC2Reportvinculado al servicio utiliza esta política para poder describir los estados de los atributos de las cuentas de los miembros.

Consulte la política: DeclarativePoliciesEC2Report.

Actualizaciones de las políticas AWS gestionadas por Organizations

La siguiente tabla detalla las actualizaciones de las políticas AWS administradas desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase al RSS feed de la página del historial del AWS Organizations documento.

Cambio	Descripción	Fecha
Nueva política gestionada - DeclarativePoliciesEC2Report	Se agregó la `DeclarativePoliciesEC2Report` política para habilitar la funcionalidad del rol AWSServiceRoleForDeclarativePoliciesEC2Report vinculado al servicio.	22 de noviembre de 2024
AWSOrganizationsReadOnlyAccess— se actualizó para permitir API los permisos de cuenta necesarios para ver la dirección de correo electrónico de un usuario raíz.	Organizations ha agregado la acción `account:GetPrimaryEmail` a fin de permitir el acceso para ver la dirección de correo electrónico del usuario raíz de cualquier cuenta de miembro de una organización y la acción `account:GetRegionOptStatus` a fin de permitir el acceso para ver las regiones habilitadas para cualquier cuenta de miembro de una organización.	6 de junio de 2024
AWSOrganizationsFullAccess— actualizado para incluir `Sid` elementos que describen la declaración de política.	Organizations ha agregado elementos `Sid` para la política administrada `AWSOrganizationsFullAccess` .	6 de febrero de 2024
AWSOrganizationsReadOnlyAccess— actualizado para incluir `Sid` elementos que describen la declaración de política.	Organizations ha agregado elementos `Sid` para la política administrada `AWSOrganizationsReadOnlyAccess` .	6 de febrero de 2024
AWSOrganizationsFullAccess— actualizado para permitir API los permisos de cuenta necesarios para activarlos o desactivarlos Regiones de AWS a través de la consola de Organizations.	Organizations ha añadido las acciones `account:ListRegions` , `account:EnableRegion` y `account:DisableRegion` a la política para permitir el acceso de	22 de diciembre de 2022

Cambio	Descripción	Fecha
	escritura para habilitar o desactivar Regiones para una cuenta.	
AWSOrganizationsReadOnlyAccess— actualizado para permitir los API permisos de cuenta necesario s para publicar en bolsa a Regiones de AWS través de la consola de Organizations.	Organizations ha añadido la acción `account:ListRegions` a la política para permitir el acceso a la visualización de Regiones para una cuenta.	22 de diciembre de 2022
AWSOrganizationsFullAccess— actualizado para permitir API los permisos de cuenta necesarios para añadir o editar los contactos de la cuenta a través de la consola de Organizations.	Se han agregado las acciones `account:GetContactInformation` y `account:PutContactInformation` a la política para permitir el acceso de escritura para modificar los contactos de una cuenta en Organizations.	21 de octubre de 2022
AWSOrganizationsReadOnlyAccess— actualizado para permitir API los permisos de cuenta necesarios para ver los contactos de la cuenta a través de la consola de Organizations.	Se ha agregado la acción `account:GetContactInformation` a la política para permitir el acceso para ver los contactos de una cuenta en Organizations.	21 de octubre de 2022
AWSOrganizationsFullAccess— actualizado para permitir la creación de una organización.	Organizations agregó el permiso `CreateServiceLinkedRole` a la política para habilitar la creación del rol vinculado al servicio necesario para crear una organización. El permiso está restringido a la creación de un rol que solo puede ser utilizado por el servicio `organizations.amazonaws.com`	24 de agosto de 2022

Cambio	Descripción	Fecha
AWSOrganizationsFullAccess— actualizado para permitir API los permisos de cuenta necesarios para añadir, editar o eliminar contactos alternativos de la cuenta a través de la consola de Organizations.	Las Organizations han agregado el `account:GetAlternateContact` , `account:DeleteAlternateContact` , `account:PutAlternateContact` de acciones de la política para habilitar el acceso de escritura para modificar contactos alternativos de una cuenta.	7 de febrero de 2022
AWSOrganizationsReadOnlyAccess— actualizado para permitir API los permisos de cuenta necesarios para ver los contactos alternativos de la cuenta a través de la consola de Organizations.	Las Organizations han agregado el `account:GetAlternateContact` de acción de la política para permitir el acceso para ver contactos alternativos de una cuenta.	7 de febrero de 2022

AWS Organizations políticas de control de servicios gestionados

Las políticas de control de servicios (SCPs) son similares a las políticas de IAM permisos, pero son una característica AWS Organizations más queIAM. Se utiliza SCPs para especificar los permisos máximos para las entidades afectadas. Puedes adjuntarlos SCPs a las raíces, las unidades organizativas (OUs) o las cuentas de tu organización. Puede crear su propia política o bien usar las políticas que IAM define. Puede consultar la lista de políticas de su organización en la página Políticas de la consola de Organizations.

> **Important**
>
> Cada raíz, unidad organizativa y cuenta debe tener al menos una SCP adjunta en todo momento.

Nombre de la política	Descripción	ARN
FullAWSAccess	Proporciona acceso a las cuentas de los miembros desde la cuenta de AWS Organizations administración.	arn:aws:organizations: :aws: -F policy/service_control_policy/p ullAWSAccess

Control de acceso basado en atributos con etiquetas para AWS Organizations

El Control de acceso basado en atributos le permite usar atributos administrados por el administrador, como etiquetas adjuntas tanto a recursos AWS como identidades AWS para controlar el acceso a esos recursos. Por ejemplo, puede especificar que un usuario pueda tener acceso a un recurso cuando tanto el usuario como el recurso tengan el mismo valor para una determinada etiqueta.

Los recursos etiquetables AWS Organizations incluyen Cuentas de AWS, el nodo raíz, las unidades organizativas o políticas de la organización. Al adjuntar etiquetas a recursos de Organizations, puede utilizar esas etiquetas para controlar quién puede tener acceso a esos recursos. Esto se hace agregando elementos `Condition` a sus instrucciones de permisos de política de AWS Identity and Access Management (IAM) que comprueban si ciertas claves de etiqueta y valores están presentes antes de permitir la acción. Esto le permite crear una política de IAM que efectivamente dice "Permitir al usuario administrar solo aquellas OU que tienen una etiqueta con una clave `X` y un valor `Y`" o "Permitir al usuario gestionar solo aquellas OU que están etiquetadas con una clave `Z` que tiene el mismo valor que la clave de la etiqueta adjunta del usuario `Z`".

Puede basar sus pruebas `Condition` en diferentes tipos de referencias de etiquetas en una política de IAM.

- Comprobación de las etiquetas que se asocian a los recursos especificados en la solicitud
- Comprobación de las etiquetas que se asocian al usuario o rol de IAM que realiza la solicitud
- Compruebe las etiquetas que se incluyen como parámetros en la solicitud

Para obtener más información sobre el uso de etiquetas para el control de acceso en las políticas, consulte Controlar el acceso a y para los usuarios y roles de IAM utilizando etiquetas de recursos.

Para obtener la sintaxis completa de las políticas de permisos de IAM, consulte la Referencia de políticas JSON de IAM

Comprobación de las etiquetas que se asocian a los recursos especificados en la solicitud

Cuando realiza una solicitud mediante el comando AWS Management Console, el AWS Command Line Interface (AWS CLI), o uno de las SDK de AWS, especifique a qué recursos desea acceder con esa solicitud. Ya sea que esté intentando enumerar los recursos disponibles de un tipo determinado, leer un recurso o escribir, modificar o actualizar un recurso, especifique el recurso al que se tendrá acceso como parámetro en la solicitud. Dichas solicitudes están controladas por las políticas de permisos de IAM que se adjuntan a los usuarios y roles. En estas políticas, puede comparar las etiquetas adjuntas al recurso solicitado y elegir permitir o denegar el acceso en función de las claves y valores de dichas etiquetas.

Para verificar una etiqueta adjunta al recurso, haga referencia a la etiqueta en un elemento `Condition` al anteponer el nombre de la clave de la etiqueta con la siguiente cadena: `aws:ResourceTag/`

Por ejemplo, la siguiente política de ejemplo permite al usuario o rol realizar cualquier AWS Organizations operación a menos que ese recurso tenga una etiqueta con la clave `department` y el valor `security`. Si esa clave y valor están presentes, entonces la política deniega explícitamente la operación `UntagResource`.

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

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
```

```
                }
            }
        }
    ]
}
```

Para obtener más información acerca de cómo utilizar este elemento, consulte Control del acceso a los recursos y aws:ResourceTag en la Guía del usuario de IAM.

Comprobación de las etiquetas que se asocian al usuario o rol de IAM que realiza la solicitud

Puede controlar qué puede hacer la persona que realiza la solicitud (entidad principal) en función de las etiquetas que se asocian al usuario o rol de IAM. Para ello, utilice la clave de condición `aws:PrincipalTag/`*`key-name`* para especificar qué etiqueta y valor se deben adjuntar al usuario o rol que llama.

En el siguiente ejemplo se muestra cómo permitir una acción solo cuando la etiqueta especificada (`cost-center`) tiene el mismo valor tanto en la entidad que llama a la operación como en el recurso al que tiene acceso la operación. En este ejemplo, el usuario que llama puede iniciar y detener una instancia de Amazon EC2 solo si la instancia está etiquetada con el mismo valor `cost-center` como usuario.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

Para obtener más información acerca de cómo utilizar este elemento, consulte Control del acceso a los recursos IAM y `aws:PrincipalTag` en la Guía del usuario de IAM.

Compruebe las etiquetas que se incluyen como parámetros en la solicitud

Varias operaciones le permiten especificar etiquetas como parte de la solicitud. Por ejemplo, al crear un recurso, puede especificar las etiquetas que se adjuntan al nuevo recurso. Puede especificar un elemento `Condition` que utiliza `aws:TagKeys` para permitir o denegar la operación en función de si se incluye una clave de etiqueta específica o un conjunto de claves en la solicitud. A este operador de comparación no le importa qué valor contiene la etiqueta. Solo comprueba si está presente una etiqueta con la clave especificada.

Para comprobar la clave de etiqueta, o una lista de claves, especifique un elemento `Condition` con la sintaxis siguiente:

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

Puede utilizar `ForAllValues:` para prefaciar al operador de comparación para asegurarse de que todas las claves de la solicitud deben coincidir con una de las claves especificadas en la política. Por ejemplo, la siguiente política de muestra permite cualquier operación de Organizations solo si todas las etiquetas presentes son un subconjunto de tres etiquetas en esta política.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

De manera alternativa, puede utilizar `ForAnyValue:` para prefaciar un operador de comparación para asegurarse de que al menos una de las claves de la solicitud deben coincidir con una de las claves especificadas en la política. Por ejemplo, la siguiente política permite cualquier operación

de Organizations solo si al menos una de las claves de etiqueta especificadas está presente en la solicitud.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
            }
        }
    }
}
```

Varias operaciones le permiten especificar etiquetas en la solicitud. Por ejemplo, al crear un recurso, puede especificar las etiquetas que se adjuntan al nuevo recurso. Puede comparar un par clave-valor de etiqueta en la política con un par clave-valor incluido en la solicitud. Para ello, haga referencia a la etiqueta en un elemento `Condition` al anteponer el nombre de la clave de la etiqueta con la siguiente cadena: `aws:RequestTag/`*`key-name`* y, a continuación, especifique el valor de etiqueta que debe estar presente.

Por ejemplo, la siguiente política de muestra deniega cualquier solicitud del usuario o rol para crear un Cuenta de AWS donde a la solicitud le falta el `costcenter`, o proporciona esa etiqueta con un valor distinto de `1`, `2`, o bien `3`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
```

```
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

Para obtener más información sobre el uso de estos elementos, consulte aws:TagKeys y aws:RequestTag en la Guía del usuario de IAM.

Solución de problemas de AWS Organizations identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando se trabaja con Organizations e IAM.

Temas

- No tengo autorización para llevar a cabo una acción en Organizations.
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a los recursos de mi Organización

No tengo autorización para llevar a cabo una acción en Organizations.

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `organizations:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 organizations:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `organizations:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no cuenta con autorización para llevar a cabo la acción `iam:PassRole`, las políticas se deben actualizar para permitir transferir un rol a Organizations.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para llevar a cabo una acción en Organizations. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a los recursos de mi Organización

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes especificar una persona de confianza para

que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede utilizar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Organizations admite estas características, consulte ¿Cómo AWS Organizations funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Inicio de sesión y supervisión AWS Organizations

Como práctica recomendada, debe monitorear su organización para asegurarse de que los cambios queden registrados. Esto le ayuda a garantizar que se pueda investigar cualquier cambio inesperado y revertir los cambios no deseados. AWS Organizations actualmente admite dos Servicios de AWS que le permiten supervisar su organización y la actividad que se lleva a cabo en ella.

Temas

- Registrar las llamadas a la API con AWS CloudTrail for AWS Organizations
- Amazon EventBridge y AWS Organizations

Registrar las llamadas a la API con AWS CloudTrail for AWS Organizations

AWS Organizations está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, rol o AWS servicio en AWS Organizations. CloudTrail captura todas las llamadas a la API AWS Organizations como eventos, incluidas las llamadas desde la AWS

Organizations consola y desde las llamadas de código a AWS Organizations APIs. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Organizations. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar el destinatario de la solicitud AWS Organizations, la dirección IP desde la que se realizó, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulta la Guía AWS CloudTrail del usuario.

> **Important**
>
> Puede ver toda la CloudTrail información AWS Organizations solo en la región EE. UU. Este (Virginia del Norte). Si no ves tu AWS Organizations actividad en la CloudTrail consola, configura la consola en EE.UU. Este (Virginia del Norte) mediante el menú de la esquina superior derecha. Si realizas consultas CloudTrail con las herramientas AWS CLI o el SDK, dirige la consulta al punto final de EE. UU. Este (Virginia del Norte).

AWS Organizations información en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS Organizations, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de AWS Organizations, cree un registro de seguimiento. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Cuando el CloudTrail registro está activado en su cuenta Cuenta de AWS, las llamadas a la API realizadas a AWS Organizations las acciones se registran en los archivos de CloudTrail registro, donde se escriben junto con otros registros de AWS servicio. Puede configurar otros Servicios de AWS para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail

Todas AWS Organizations las acciones se registran CloudTrail y se documentan en la referencia de la AWS Organizations API. Por ejemplo, las llamadas a `CreateAccount` (incluido el `CreateAccountResult` evento) y `InviteAccountToOrganization` generan entradas en los archivos de CloudTrail registro. `ListHandshakesForAccount` `CreatePolicy`

Cada entrada de registro contiene información sobre quién generó la solicitud. La información de identidad del usuario en la entrada de registro le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario de IAM
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol de IAM o un usuario federado.
- Si la solicitud la realizó otro AWS servicio

Para obtener más información, consulte el Elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de AWS Organizations registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una única solicitud de cualquier origen e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etcétera. Los archivos de registro de CloudTrail no son un rastro de la pila ordenada de las llamadas a la API públicas, por lo que no aparecen en ningún orden específico.

Ejemplos de entradas de registro: CloseAccount

El siguiente ejemplo muestra una entrada de CloudTrail registro para una `CloseAccount` llamada de ejemplo que se genera cuando se llama a la API y el flujo de trabajo para cerrar la cuenta comienza a procesarse en segundo plano.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro para una `CloseAccountResult` llamada una vez finalizado correctamente el flujo de trabajo en segundo plano para cerrar la cuenta.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
```

```
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

Ejemplos de entradas de registro: CreateAccount

El siguiente ejemplo muestra una entrada de CloudTrail registro para una `CreateAccount` llamada de ejemplo que se genera cuando se llama a la API y el flujo de trabajo para crear la cuenta comienza a procesarse en segundo plano.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
```

```
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro para una `CreateAccount` llamada una vez finalizado correctamente el flujo de trabajo en segundo plano para crear la cuenta.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
```

```
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que se genera después de que un flujo de trabajo en `CreateAccount` segundo plano no pueda crear la cuenta.

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
```

```
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

Ejemplo de entrada de registro: CreateOrganizationalUnit

El siguiente ejemplo muestra una entrada de CloudTrail registro para un ejemplo de `CreateOrganizationalUnit` llamada.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
```

```
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Ejemplo de entrada de registro: InviteAccountToOrganization

El siguiente ejemplo muestra una entrada de CloudTrail registro para un ejemplo de `InviteAccountToOrganization` llamada.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
        }
    },
```

```
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
```

```
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Ejemplo de entrada de registro: AttachPolicy

El siguiente ejemplo muestra una entrada de CloudTrail registro para un ejemplo de `AttachPolicy` llamada. La respuesta indica que la llamada ha dado un error porque el tipo de política solicitado no está habilitado en la raíz donde se ha intentado adjuntar la solicitud.

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
```

```
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Amazon EventBridge y AWS Organizations

AWS Organizations puede trabajar con Amazon EventBridge, anteriormente Amazon CloudWatch Events, para generar eventos cuando se producen acciones especificadas por el administrador en una organización. Por ejemplo, por la sensibilidad de ese tipo de acciones, la mayoría de los administradores desean que se les advierta cada vez que alguien crea una nueva cuenta en la organización o que un administrador de una cuenta de miembro intenta salir de la organización. Puede configurar EventBridge reglas que busquen estas acciones y, a continuación, envíen los eventos generados a objetivos definidos por el administrador. El objetivo puede ser un tema de Amazon SNS que envíe un correo electrónico o un mensaje de texto a sus suscriptores. O bien una función AWS Lambda creada para registrar los detalles de la acción, de modo que pueda revisarlos más adelante.

Para ver un tutorial que muestra cómo habilitar la supervisión de EventBridge las actividades clave de su organización, consulte. Tutorial: Supervisa los cambios importantes en tu organización con Amazon EventBridge

> **Important**
>
> Actualmente, solo AWS Organizations se aloja en la región EE.UU. Este (Virginia del Norte) (aunque está disponible en todo el mundo). Para llevar a cabo los pasos de este tutorial, debe configurar AWS Management Console para usar esa región.

Para obtener más información EventBridge, incluido cómo configurarlo y habilitarlo, consulta la Guía del EventBridge usuario de Amazon.

Validación de conformidad en AWS Organizations

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Organizations

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte la Infraestructura global de AWS.

Seguridad de la infraestructura en AWS Organizations

Como se trata de un servicio administrado, AWS Organizations está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWSprotege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para obtener acceso a Organizations a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más

información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Solución de problemas AWS Organizations

Si tiene problemas al trabajar con él AWS Organizations, consulte los temas de esta sección.

Solución de problemas generales

Utilice esta información como ayuda para diagnosticar y solucionar problemas de acceso denegado u otros problemas comunes que puedan surgir al trabajar con ellos. AWS Organizations

Temas

- Recibo un mensaje de «acceso denegado» cuando hago una solicitud a AWS Organizations
- Aparece un mensaje de “acceso denegado” al realizar una solicitud con credenciales de seguridad temporales
- Obtengo un mensaje de "acceso denegado" cuando intento dejar una organización como cuenta de miembro o eliminar una cuenta de miembro como cuenta de administración.
- Obtengo un mensaje de "cuota superada" cuando intento agregar una cuenta a mi organización
- Aparece un mensaje que indica que "esta operación requiere un periodo de espera" al añadir o eliminar cuentas
- Obtengo un mensaje de "organización todavía inicializando" cuando intento añadir una cuenta a mi organización
- Aparece el mensaje "Invitations are disabled" cuando intento invitar a una cuenta a mi organización.
- Los cambios que realizo no están siempre visibles inmediatamente

Recibo un mensaje de «acceso denegado» cuando hago una solicitud a AWS Organizations

- Compruebe que tiene permisos para llamar a la acción y a los recursos que ha solicitado. Un administrador debe conceder permisos asociando una política de IAM a su usuario, grupo o rol. Si las declaraciones de política que otorgan esos permisos incluyen alguna condición, como time-of-day restricciones de dirección IP, también debes cumplir esos requisitos al enviar la solicitud. Para obtener más información sobre cómo consultar o modificar políticas de un usuario, grupo o rol consulte Trabajo con políticas en la Guía del usuario de IAM.

- Si va a firmar las solicitudes de la API manualmente (sin utilizarlas AWS SDKs), compruebe que ha firmado correctamente la solicitud.

Aparece un mensaje de “acceso denegado” al realizar una solicitud con credenciales de seguridad temporales

- Compruebe que el usuario o la función de que está utilizando para realizar la solicitud tiene los permisos adecuados. Los permisos de credenciales de seguridad temporales se obtienen de un usuario o una función de y, por tanto, se limitan a los concedidos al usuario o la función de . Para obtener más información sobre cómo se determinan los permisos de las credenciales de seguridad temporales, consulte Controlar los permisos para credenciales de seguridad temporarias en la Guía del usuario de IAM.
- Compruebe que las solicitudes se han firmado correctamente y que la solicitud tiene el formato correcto. Para obtener más información, consulte la documentación del kit de herramientas del SDK que elija o Cómo usar credenciales de seguridad temporales para solicitar acceso a AWS los recursos en la Guía del usuario de IAM.
- Compruebe que sus credenciales de seguridad temporales no hayan caducado. Para obtener más información, consulte Solicitud de credenciales de seguridad temporales en la Guía del usuario de IAM.

Obtengo un mensaje de "acceso denegado" cuando intento dejar una organización como cuenta de miembro o eliminar una cuenta de miembro como cuenta de administración.

- Puede eliminar una cuenta de miembro solo después de habilitar el acceso de usuario de IAM Acceder facturación en la cuenta de miembro. Para obtener más información, consulte Activación del acceso a la consola de Billing and Cost Management en la Guía del usuario de AWS Billing .
- Puede eliminar una cuenta de su organización solo si la cuenta tiene la información que necesita para funcionar como cuenta independiente. Cuando creas una cuenta en una organización mediante la AWS Organizations consola, la API o AWS CLI los comandos, esa información no se recopila automáticamente. Si desea crear una cuenta independiente, debe aceptar el acuerdo de AWS cliente, elegir un plan de soporte, proporcionar y verificar la información de contacto requerida y proporcionar un método de pago actual. AWS utiliza el método de pago para cobrar por cualquier AWS actividad facturable (no de nivel AWS gratuito) que se produzca mientras la

cuenta no esté vinculada a una organización. Para obtener más información, consulte Salir de una organización desde una cuenta de miembro con AWS Organizations.

Obtengo un mensaje de "cuota superada" cuando intento agregar una cuenta a mi organización

Existe un número máximo de cuentas que puede tener en una organización. Las cuentas eliminadas o cerradas también se tienen en cuenta en esta cuota.

Una invitación de unión se contabiliza para el número máximo de cuentas de la organización. La cuenta se devuelve si la cuenta invitada rechaza la invitación, la cuenta de administración cancela la invitación o la invitación caduca.

- Antes de cerrar o eliminar una Cuenta de AWS, elimínala de tu organización para que no se siga descontando de tu cuota.
- Para obtener más información sobre cómo solicitar un aumento de cuotas, consulte Valores mínimos y máximos.

Aparece un mensaje que indica que "esta operación requiere un periodo de espera" al añadir o eliminar cuentas

Algunas acciones requieren un periodo de espera. Por ejemplo, no se puede eliminar inmediatamente cuentas recién creadas. Vuelva a intentarlo en unos días. Si tiene problemas con las cuotas de la cuenta al agregar o eliminar cuentas, consulte Valores mínimos y máximos para obtener información sobre cómo solicitar un aumento de cuota.

Obtengo un mensaje de "organización todavía inicializando" cuando intento añadir una cuenta a mi organización

Si recibe este error y ha pasado más de una hora desde que se creó la organización, póngase en contacto con AWS Support.

Aparece el mensaje "Invitations are disabled" cuando intento invitar a una cuenta a mi organización.

Esto sucede cuando habilita todas las características en la organización. Esta operación puede tardar algún tiempo y requiere que todas las cuentas de miembro respondan. Hasta que se complete la operación, no podrá invitar a nuevas cuentas a unirse a la organización.

Los cambios que realizo no están siempre visibles inmediatamente

Al ser un servicio al que se obtiene acceso a través de equipos de centros de datos de todo el mundo, AWS Organizations utiliza un modelo de computación distribuida llamado consistencia final. Cualquier cambio que realices AWS Organizations tarda en ser visible desde todos los puntos de enlace posibles. Parte del retraso se debe al tiempo que se tarda en enviar los datos de un servidor a otro o de una zona de replicación a otra. AWS Organizations también utiliza el almacenamiento en caché para mejorar el rendimiento, pero en algunos casos esto puede aumentar el tiempo. Es posible que el cambio no sea visible hasta que se agoten los datos previamente almacenados.

Diseñe sus aplicaciones globales teniendo en cuenta estos posibles retrasos y asegúrese de que funcionan según lo previsto, incluso cuando un cambio realizado en una ubicación no está visible inmediatamente en otra ubicación.

Para obtener más información sobre cómo esto afecta a otras Servicios de AWS personas, consulta los siguientes recursos:

- Administración de la consistencia de los datos en la Guía para desarrolladores de bases de datos Amazon Redshift
- Modelo de consistencia de datos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service
- Garantizar la coherencia al utilizar Amazon S3 y Amazon Elastic MapReduce para los flujos de trabajo de ETL en el blog sobre AWS big data
- EC2 Coherencia eventual en la referencia de la EC2 API de Amazon.

Llamar a la API mediante solicitudes de consulta HTTP

Esta sección contiene información general sobre el uso de la API de consulta para AWS Organizations. Para obtener más información acerca de las operaciones y los errores de la API, consulte la Referencia de API AWS Organizations.

> **Note**
>
> En lugar de realizar llamadas directas a la API de AWS Organizations Query, puede utilizar una de las AWS SDKs. AWS SDKs Constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas (Java, Ruby, .NET, iOS, Android y más). SDKs Proporcionan una forma cómoda de crear un acceso programático a AWS Organizations y AWS. Por ejemplo, se SDKs encargan de tareas como firmar criptográficamente las solicitudes, gestionar los errores y volver a intentar las solicitudes automáticamente. Para obtener información sobre AWS SDKs, incluido cómo descargarlos e instalarlos, consulte Herramientas para Amazon Web Services.

La API de consulta AWS Organizations le permite llamar a las acciones de servicio. Las solicitudes de la API de consulta son solicitudes HTTPS que deben contener un `Action` parámetro que indique la operación que se va a realizar. AWS Organizations admite las solicitudes GET y POST para todas las operaciones. Es decir, la API no requiere que use GET para algunas acciones y POST para otras. Sin embargo, las solicitudes GET están sujetas a las limitaciones de tamaño de una URL. Aunque este límite depende del navegador, suele ser de 2048 bytes. Por lo tanto, para las solicitudes de la API de consultas que requieran tamaños más grandes, debe utilizar una solicitud POST.

La respuesta es un documento XML. Para obtener más información acerca de la respuesta, consulte las páginas de cada acción en la Referencia de API AWS Organizations.

Temas

- puntos de conexión
- HTTPS obligatorio
- Firmar solicitudes de API AWS Organizations

puntos de conexión

AWS Organizations tiene un único punto final de API global que está alojado en la región EE.UU. Este (Norte de Virginia).

Para obtener más información sobre AWS los puntos de enlace y las regiones de todos los servicios, consulte los puntos de enlace regionales en. Referencia general de AWS

HTTPS obligatorio

Dado que la API de consultas devuelve información confidencial como, por ejemplo, credenciales de seguridad, debe usar HTTPS para cifrar todas las solicitudes de la API.

Firmar solicitudes de API AWS Organizations

Las solicitudes deben firmarse con un ID de clave de acceso y una clave de acceso secreta. Te recomendamos encarecidamente que no utilices tus Usuario raíz de la cuenta de AWS credenciales para el trabajo diario AWS Organizations. Puede utilizar las credenciales de un usuario o rol.

Para firmar tus solicitudes de API, debes usar la versión 4 de AWS Signature. Para obtener información sobre el uso de la versión 4 de Signature, consulte Firmar las solicitudes de AWS API en la Guía del usuario de IAM.

AWS Organizations no es compatible con versiones anteriores, como la versión 2 de Signature.

Para obtener más información, consulte los siguientes temas:

- AWS Credenciales de seguridad: proporciona información general sobre los tipos de credenciales que puede utilizar para acceder AWS.
- Prácticas recomendadas de seguridad en IAM: ofrece sugerencias para usar el servicio de IAM para ayudar a proteger sus AWS recursos, incluidos los de. AWS Organizations
- Credenciales temporales de seguridad en IAM: describe cómo crear y utilizar las credenciales temporales de seguridad.

Ejemplos de código para organizaciones que utilizan AWS SDKs

Los siguientes ejemplos de código muestran cómo utilizar Organizations con un kit de desarrollo de AWS software (SDK).

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Las acciones muestran cómo llamar a las funciones de servicio individuales y es posible verlas en contexto en los escenarios relacionados.

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulteSe usa AWS Organizations con un SDK AWS. En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

Ejemplos de código

- Ejemplos básicos para las organizaciones que utilizan AWS SDKs
  - Actions for Organizations que utilizan AWS SDKs
    - AttachPolicyÚselo con un AWS SDK o CLI
    - CreateAccountÚselo con una AWS SDK o CLI
    - CreateOrganizationÚselo con una AWS SDK o CLI
    - CreateOrganizationalUnitÚselo con una AWS SDK o CLI
    - CreatePolicyÚselo con una AWS SDK o CLI
    - DeleteOrganizationÚselo con una AWS SDK o CLI
    - DeleteOrganizationalUnitÚselo con una AWS SDK o CLI
    - DeletePolicyÚselo con una AWS SDK o CLI
    - DescribePolicyÚselo con una AWS SDK o CLI
    - DetachPolicyÚselo con una AWS SDK o CLI
    - ListAccountsÚselo con una AWS SDK o CLI
    - ListOrganizationalUnitsForParentÚselo con una AWS SDK o CLI
    - ListPoliciesÚselo con una AWS SDK o CLI

Ejemplos básicos para las organizaciones que utilizan AWS SDKs

Los siguientes ejemplos de código muestran cómo utilizar los conceptos básicos de AWS Organizations with AWS SDKs.

Ejemplos

- Actions for Organizations que utilizan AWS SDKs
  - AttachPolicyÚselo con un AWS SDK o CLI
  - CreateAccountÚselo con una AWS SDK o CLI
  - CreateOrganizationÚselo con una AWS SDK o CLI
  - CreateOrganizationalUnitÚselo con una AWS SDK o CLI
  - CreatePolicyÚselo con una AWS SDK o CLI
  - DeleteOrganizationÚselo con una AWS SDK o CLI
  - DeleteOrganizationalUnitÚselo con una AWS SDK o CLI
  - DeletePolicyÚselo con una AWS SDK o CLI
  - DescribePolicyÚselo con una AWS SDK o CLI
  - DetachPolicyÚselo con una AWS SDK o CLI
  - ListAccountsÚselo con una AWS SDK o CLI
  - ListOrganizationalUnitsForParentÚselo con una AWS SDK o CLI
  - ListPoliciesÚselo con una AWS SDK o CLI

Actions for Organizations que utilizan AWS SDKs

Los siguientes ejemplos de código muestran cómo realizar acciones individuales de Organizations con AWS SDKs. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para obtener una lista completa, consulta la AWS Organizations APIReferencia.

Ejemplos

- AttachPolicyÚselo con un AWS SDK o CLI
- CreateAccountÚselo con una AWS SDK o CLI
- CreateOrganizationÚselo con una AWS SDK o CLI

- CreateOrganizationalUnitÚselo con una AWS SDK o CLI
- CreatePolicyÚselo con una AWS SDK o CLI
- DeleteOrganizationÚselo con una AWS SDK o CLI
- DeleteOrganizationalUnitÚselo con una AWS SDK o CLI
- DeletePolicyÚselo con una AWS SDK o CLI
- DescribePolicyÚselo con una AWS SDK o CLI
- DetachPolicyÚselo con una AWS SDK o CLI
- ListAccountsÚselo con una AWS SDK o CLI
- ListOrganizationalUnitsForParentÚselo con una AWS SDK o CLI
- ListPoliciesÚselo con una AWS SDK o CLI

`AttachPolicy`Úselo con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `AttachPolicy`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
```

```
        /// <summary>
        /// Initializes the Organizations client object and then calls the
        /// AttachPolicyAsync method to attach the policy to the root
        /// organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new AttachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- Para API obtener más información, consulte AttachPolicyla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Asociación de una política a un nodo raíz, unidad organizativa o cuenta

Ejemplo 1

El siguiente ejemplo muestra cómo adjuntar una política de control de servicios (SCP) a una unidad organizativa:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

Ejemplo 2

El siguiente ejemplo de código muestra cómo adjuntar una política de control de servicio directamente a una cuenta:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- Para API obtener más información, consulte AttachPolicyla Referencia de AWS CLI comandos.

Python

SDKpara Python (Boto3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
```

```
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- Para API obtener más información, consulte AttachPolicyla AWS SDKreferencia de Python (Boto3). API

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulte. Se usa AWS Organizations con un SDK AWS En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`CreateAccount`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateAccount`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
```

```
    /// </summary>
    public class CreateAccount
    {
        /// <summary>
        /// Initializes an Organizations client object and uses it to create
        /// the new account with the name specified in accountName.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var accountName = "ExampleAccount";
            var email = "someone@example.com";

            var request = new CreateAccountRequest
            {
                AccountName = accountName,
                Email = email,
            };

            var response = await client.CreateAccountAsync(request);
            var status = response.CreateAccountStatus;

            Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
        }
    }
```

- Para API obtener más información, consulte CreateAccountla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Creación de una cuenta de miembro que forme parte automáticamente de la organización

En el siguiente ejemplo se muestra cómo crear una cuenta de miembro en una organización. La cuenta de miembro se configura con el nombre Production Account y la dirección de correo electrónico susan@example.com. Organizations crea automáticamente un IAM rol con el nombre predeterminado de OrganizationAccountAccessRole porque el roleName

parámetro no está especificado. Además, la configuración que permite a IAM los usuarios o roles con permisos suficientes acceder a los datos de facturación de la cuenta se establece en el valor predeterminado de ALLOW porque el IamUserAccessToBilling parámetro no está especificado. Organizations envía automáticamente a Susan un correo electrónico de AWS bienvenida a:

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

La salida incluye un objeto de solicitud que muestra que el estado ahora es `IN_PROGRESS`:

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Más adelante, puede consultar el estado actual de la solicitud proporcionando el valor de respuesta Id al describe-create-account-status comando como valor del create-account-request-id parámetro.

Para obtener más información, consulte Crear una AWS cuenta en su organización en la Guía del AWS usuario de Organizations.

- Para API obtener más información, consulte CreateAccountla Referencia de AWS CLI comandos.

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulteSe usa AWS Organizations con un SDK AWS. En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`CreateOrganization`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateOrganization`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
public class CreateOrganization
{
    /// <summary>
    /// Creates an Organizations client object and then uses it to create
    /// a new organization with the default user as the administrator, and
    /// then displays information about the new organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
        {
            FeatureSet = "ALL",
        });

        Organization newOrg = response.Organization;

        Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
    }
}
```

- Para API obtener más información, consulte CreateOrganizationla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Ejemplo 1: Creación de una nueva organización

Bill quiere crear una organización con las credenciales de la cuenta 111111111111. En el siguiente ejemplo se muestra que la cuenta se convierte en la cuenta maestra de la nueva organización. Puesto que no especifica un conjunto de características, la nueva organización tiene habilitadas todas las características de forma predeterminada y las políticas de control de servicios están habilitadas en la raíz.

```
aws organizations create-organization
```

El resultado incluye un objeto de organización con detalles sobre la nueva organización:

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

Ejemplo 2: Creación de una nueva organización con solo las características de facturación consolidada habilitadas

En el siguiente ejemplo se crea una organización que solo admite las características de facturación consolidada:

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

El resultado incluye un objeto de organización con detalles sobre la nueva organización:

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

Para obtener más información, consulte Creación de una organización en la Guía del usuario de AWS Organizations.

- Para API obtener más información, consulte CreateOrganizationla Referencia de AWS CLI comandos.

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulteSe usa AWS Organizations con un SDK AWS. En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`CreateOrganizationalUnit`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateOrganizationalUnit`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
            Name = orgUnitName,
            ParentId = "r-0000",
        };

        var response = await client.CreateOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
```

```
                Console.WriteLine($"Successfully created organizational unit:
 {orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
 {response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- Para API obtener más información, consulte CreateOrganizationalUnitla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Creación de una unidad organizativa en raíz o UO principal

En el siguiente ejemplo se muestra cómo crear una unidad organizativa que se denomina AccountingOU:

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

El resultado incluye un organizationalUnit objeto con detalles sobre la nueva unidad organizativa:

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- Para API obtener más información, consulte CreateOrganizationalUnitla Referencia de AWS CLI comandos.

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulteSe usa AWS Organizations con un SDK AWS. En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`CreatePolicy`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreatePolicy`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations Policy.
/// </summary>
public class CreatePolicy
{
    /// <summary>
    /// Initializes the AWS Organizations client object, uses it to
    /// create a new Organizations Policy, and then displays information
    /// about the newly created Policy.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyContent = "{" +
            "   \"Version\": \"2012-10-17\"," +
```

```
                " \"Statement\" : [{" +
                    " \"Action\" : [\"s3:*\"]," +
                    " \"Effect\" : \"Allow\"," +
                    " \"Resource\" : \"*\"" +
                "}]" +
            "}";

            try
            {
                var response = await client.CreatePolicyAsync(new
CreatePolicyRequest
                {
                    Content = policyContent,
                    Description = "Enables admins of attached accounts to
delegate all Amazon S3 permissions",
                    Name = "AllowAllS3Actions",
                    Type = "SERVICE_CONTROL_POLICY",
                });

                Policy policy = response.Policy;
                Console.WriteLine($"{policy.PolicySummary.Name} has the following
content: {policy.Content}");
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }
    }
```

- Para API obtener más información, consulte CreatePolicyla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Ejemplo 1: Para crear una política con un archivo fuente de texto para la JSON política

El siguiente ejemplo muestra cómo crear una política de control de servicios (SCP) denominada`AllowAllS3Actions`. El contenido de la política se extrae de un archivo del equipo local denominado `policy.json`.

```
aws organizations create-policy --content file://policy.json --
name AllowAllS3Actions, --type SERVICE_CONTROL_POLICY --description "Allows
 delegation of all S3 actions"
```

La salida incluye un objeto de política con detalles sobre la nueva política:

```
{
        "Policy": {
                "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource\":[\"*\"]}]}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::o-exampleorgid:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Allows delegation of all S3 actions",
                        "Name": "AllowAllS3Actions",
                        "Type":"SERVICE_CONTROL_POLICY"
                }
        }
}
```

Ejemplo 2: Para crear una política con una JSON política como parámetro

El siguiente ejemplo muestra cómo crearlaSCP, esta vez incrustando el contenido de la política en forma de JSON cadena en el parámetro. La cadena debe aplicar una secuencia de escape con barras diagonales antes de las comillas dobles para garantizar que se traten como literales en el parámetro, que a su vez queda rodeado de comillas dobles:

```
aws organizations create-policy --content "{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource
\":[\"*\"]}]}" --name AllowAllS3Actions --type SERVICE_CONTROL_POLICY --
description "Allows delegation of all S3 actions"
```

Para obtener más información sobre la creación y el uso de políticas en su organización, consulte Administración de políticas de la organización en la Guía del usuario de AWS Organizations.

- Para API obtener más información, consulte CreatePolicyla Referencia de AWS CLI comandos.

Python

SDKpara Python (Boto3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def create_policy(name, description, content, policy_type, orgs_client):
    """
    Creates a policy.

    :param name: The name of the policy.
    :param description: The description of the policy.
    :param content: The policy content as a dict. This is converted to JSON
 before
                    it is sent to AWS. The specific format depends on the policy
 type.
    :param policy_type: The type of the policy.
    :param orgs_client: The Boto3 Organizations client.
    :return: The newly created policy.
    """
    try:
        response = orgs_client.create_policy(
            Name=name,
            Description=description,
            Content=json.dumps(content),
            Type=policy_type,
        )
        policy = response["Policy"]
        logger.info("Created policy %s.", name)
    except ClientError:
        logger.exception("Couldn't create policy %s.", name)
        raise
    else:
        return policy
```

- Para API obtener más información, consulte CreatePolicyla AWS SDKreferencia de Python (Boto3). API

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulte. Se usa AWS Organizations con un SDK AWS En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`DeleteOrganization`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteOrganization`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
{
    /// <summary>
    /// Initializes the Organizations client and then calls
    /// DeleteOrganizationAsync to delete the organization.
    /// </summary>
```

```
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- Para API obtener más información, consulte DeleteOrganizationla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Eliminación de una organización

En el siguiente ejemplo se muestra cómo eliminar una organización. Para realizar esta operación, debe ser administrador de la cuenta maestra de la organización. En el ejemplo se supone que previamente eliminaste todas las cuentas y políticas de los miembros de la organización: OUs

```
aws organizations delete-organization
```

- Para API obtener más información, consulte DeleteOrganizationla Referencia de AWS CLI comandos.

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulteSe usa AWS Organizations con un SDK AWS. En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`DeleteOrganizationalUnit`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteOrganizationalUnit`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-00000000";

        var request = new DeleteOrganizationalUnitRequest
        {
```

```
                OrganizationalUnitId = orgUnitId,
            };

            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- Para API obtener más información, consulte DeleteOrganizationalUnitla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Eliminación de una unidad organizativa

En el ejemplo siguiente se muestra cómo se elimina una OU. En el ejemplo se supone que anteriormente se eliminaron todas las cuentas y otras OUs de la OU:

```
aws organizations delete-organizational-unit --organizational-unit-id ou-
examplerootid111-exampleouid111
```

- Para API obtener más información, consulte DeleteOrganizationalUnitla Referencia de AWS CLI comandos.

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulteSe usa AWS Organizations con un SDK AWS. En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`DeletePolicy`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeletePolicy`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);
```

```
            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted Policy: {policyId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete Policy: {policyId}.");
            }
        }
    }
```

- Para API obtener más información, consulte DeletePolicyla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Eliminación de una política

En el siguiente ejemplo se muestra cómo eliminar una política de una organización. En el ejemplo se asume que anteriormente se ha desvinculado la política de todas las entidades:

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- Para API obtener más información, consulte DeletePolicyla Referencia de AWS CLI comandos.

Python

SDKpara Python (Boto3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- Para API obtener más información, consulte DeletePolicyla AWS SDKreferencia de Python (Boto3). API

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulte. Se usa AWS Organizations con un SDK AWS En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`DescribePolicy`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DescribePolicy`.

CLI

AWS CLI

Obtención de información acerca de una política

En el siguiente ejemplo se muestra cómo solicitar información acerca de una política:

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

El resultado incluye un objeto de política que contiene detalles acerca de la política:

```
{
```

```
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- Para API obtener más información, consulte DescribePolicyla Referencia de AWS CLI comandos.

Python

SDKpara Python (Boto3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
```

```
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- Para API obtener más información, consulte DescribePolicyla AWS SDKreferencia de Python (Boto3). API

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulte. Se usa AWS Organizations con un SDK AWS En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`DetachPolicy`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DetachPolicy`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
```

```
    {
        /// <summary>
        /// Initializes the Organizations client object and uses it to call
        /// DetachPolicyAsync to detach the policy.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new DetachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- Para API obtener más información, consulte DetachPolicyla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Desasociación de una política de un nodo raíz, unidad organizativa o cuenta

En el siguiente ejemplo se muestra cómo desasociar una política de una unidad organizativa:

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- Para API obtener más información, consulte DetachPolicyla Referencia de AWS CLI comandos.

Python

SDKpara Python (Boto3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- Para API obtener más información, consulte DetachPolicyla AWS SDKreferencia de Python (Boto3). API

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulte. Se usa AWS Organizations con un SDK AWS En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`ListAccounts`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `ListAccounts`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Uses the AWS Organizations service to list the accounts associated
/// with the default account.
/// </summary>
public class ListAccounts
{
    /// <summary>
    /// Creates the Organizations client and then calls its
    /// ListAccountsAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var request = new ListAccountsRequest
        {
            MaxResults = 5,
        };
```

```
            var response = new ListAccountsResponse();
            try
            {
                do
                {
                    response = await client.ListAccountsAsync(request);
                    response.Accounts.ForEach(a => DisplayAccounts(a));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations account.
        /// </summary>
        /// <param name="account">An Organizations account for which to display
        /// information on the console.</param>
        private static void DisplayAccounts(Account account)
        {
            string accountInfo = $"{account.Id}
{account.Name}\t{account.Status}";

            Console.WriteLine(accountInfo);
        }
    }
```

- Para API obtener más información, consulte ListAccountsla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Recuperación de una lista de todas las cuentas de una organización

En el siguiente ejemplo se muestra cómo solicitar una lista de las cuentas de una organización:

```
aws organizations list-accounts
```

La salida incluye una lista de objetos de resumen de cuenta.

```
{
        "Accounts": [
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481830215.45,
                        "Id": "111111111111",
                        "Name": "Master Account",
                        "Email": "bill@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/222222222222",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835741.044,
                        "Id": "222222222222",
                        "Name": "Production Account",
                        "Email": "alice@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835795.536,
                        "Id": "333333333333",
                        "Name": "Development Account",
                        "Email": "juan@example.com",
```

```
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835812.143,
                        "Id": "444444444444",
                        "Name": "Test Account",
                        "Email": "anika@example.com",
                        "Status": "ACTIVE"
                }
        ]
}
```

- Para API obtener más información, consulte ListAccountsla Referencia de AWS CLI comandos.

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulteSe usa AWS Organizations con un SDK AWS. En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`ListOrganizationalUnitsForParent`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `ListOrganizationalUnitsForParent`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;
```

```
    /// <summary>
    /// Lists the AWS Organizations organizational units that belong to an
    /// organization.
    /// </summary>
    public class ListOrganizationalUnitsForParent
    {
        /// <summary>
        /// Initializes the Organizations client object and then uses it to
        /// call the ListOrganizationalUnitsForParentAsync method to retrieve
        /// the list of organizational units.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var parentId = "r-0000";

            var request = new ListOrganizationalUnitsForParentRequest
            {
                ParentId = parentId,
                MaxResults = 5,
            };

            var response = new ListOrganizationalUnitsForParentResponse();
            try
            {
                do
                {
                    response = await
client.ListOrganizationalUnitsForParentAsync(request);
                    response.OrganizationalUnits.ForEach(u =>
DisplayOrganizationalUnit(u));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
```

```
            }
        }

        /// <summary>
        /// Displays information about an Organizations organizational unit.
        /// </summary>
        /// <param name="unit">The OrganizationalUnit for which to display
        /// information.</param>
        public static void DisplayOrganizationalUnit(OrganizationalUnit unit)
        {
            string accountInfo = $"{unit.Id} {unit.Name}\t{unit.Arn}";

            Console.WriteLine(accountInfo);
        }
    }
```

- Para API obtener más información, consulte ListOrganizationalUnitsForParentla AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Para recuperar una lista de OUs las unidades organizativas o raíz principales

El siguiente ejemplo muestra cómo obtener una lista de OUs en una raíz específica:

```
aws organizations list-organizational-units-for-parent --parent-id r-
examplerootid111
```

El resultado muestra que la raíz especificada contiene dos OUs y muestra los detalles de cada una:

```
{
        "OrganizationalUnits": [
                {
                        "Name": "AccountingDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid111"
                },
```

```
                {
                        "Name": "ProductionDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid222"
                }
        ]
}
```

- Para API obtener más información, consulte ListOrganizationalUnitsForParentla Referencia de AWS CLI comandos.

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulteSe usa AWS Organizations con un SDK AWS. En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

`ListPolicies`Úselo con una AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `ListPolicies`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
```

```
        /// Initializes an Organizations client object, and then calls its
        /// ListPoliciesAsync method.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            // The value for the Filter parameter is required and must must be
            // one of the following:
            //     AISERVICES_OPT_OUT_POLICY
            //     BACKUP_POLICY
            //     SERVICE_CONTROL_POLICY
            //     TAG_POLICY
            var request = new ListPoliciesRequest
            {
                Filter = "SERVICE_CONTROL_POLICY",
                MaxResults = 5,
            };

            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
```

```
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
 {policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- Para API obtener más información, consulte ListPolicies la AWS SDK for .NET APIReferencia.

CLI

AWS CLI

Recuperación de una lista de todas las políticas de una organización de un tipo determinado

El siguiente ejemplo muestra cómo obtener una lista deSCPs, tal como se especifica en el parámetro de filtro:

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

La salida incluye una lista de políticas con información resumida:

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
```

```
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
                }
        ]
}
```

- Para API obtener más información, consulte ListPoliciesla Referencia de AWS CLI comandos.

Python

SDKpara Python (Boto3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
```

```
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- Para API obtener más información, consulte ListPoliciesla AWS SDKreferencia de Python (Boto3). API

Para obtener una lista completa de guías para AWS SDK desarrolladores y ejemplos de código, consulte. Se usa AWS Organizations con un SDK AWS En este tema también se incluye información sobre cómo empezar y detalles sobre SDK las versiones anteriores.

Historial de documentos para AWS Organizations

En la tabla siguiente se describen las actualizaciones principales de la documentación de AWS Organizations.

- Versión de API: 2016-11-28
- Última actualización de la documentación: 24 de enero de 2025

Cambio	Descripción	Fecha
Integración de las organizaciones con AWS User Notifications	Puede integrarlo Notificaciones de usuario AWS Organizations para configurar y ver las notificaciones de forma centralizada en todas las cuentas de su organización.	24 de enero de 2025
Integración de las organizaciones con AWS Managed Services (AMS) Self-Service Reporting (SSR)	Puede integrar AMS SSR AWS Organizations para habilitar los informes de autoservicio agregados (SSR). Se trata de una función de AMS que permite a los clientes de Advanced y Accelerate ver sus informes de autoservicio existentes agregados a nivel de organización y en todas las cuentas.	21 de enero de 2025
Se agregaron políticas declarativas	Puede utilizar políticas declarativas para declarar y aplicar de forma centralizada las configuraciones deseadas para una determinada escala	1 de diciembre de 2024

	Servicio de AWS en toda la organización. Una vez conectada, la configuración siempre se mantiene cuando el servicio agrega nuevas funciones o APIs.	
Nueva política AWS gestionada	Se agregó la `DeclarativePoliciesEC2Report` política para habilitar la funcionalidad de la función vinculada al declarative-policies-ec servicio 2.amazonaws.com.	22 de noviembre de 2024
Políticas de copia de seguridad actualizadas	AWS Backup policies actualizó la clave `selections` de política para incluir una clave de `conditions` política y agregó una nueva clave de `resources` política al esquema. Con el nuevo esquema, tiene más flexibilidad en la selección de recursos para sus políticas de respaldo.	14 de noviembre de 2024

Administración de forma centralizada el acceso raíz a las cuentas de los miembros	Ahora puede administrar las credenciales de los usuarios raíz privilegiados en todas las cuentas de los miembros de AWS Organizations con acceso raíz centralizado. Proteja de forma centralizada las credenciales de usuario raíz de su Cuentas de AWS sistema gestionado AWS Organizations para eliminar e impedir la recuperación de las credenciales de los usuarios raíz y el acceso a escala.	14 de noviembre de 2024
Se agregaron políticas de control de recursos () RCPs	Puede utilizar las políticas de control de recursos (RCPs) para controlar el número máximo de permisos disponibles para los recursos de una organización.	13 de noviembre de 2024
Se agregaron políticas de chatbot	Puede usar las políticas de chatbot para controlar el acceso a las cuentas de su organización desde aplicaciones de chat como Slack y Microsoft Teams.	26 de septiembre de 2024

Actualizaciones de contenido basadas en escenarios	La AWS Organizations documentación se actualizó a lo largo de toda la guía para que estuviera más orientada a los escenarios y se reorganizó el contenido para mejorar la legibilidad y la detección. Si tiene comentarios sobre estos cambios, use el botón Enviar comentarios en la parte inferior de la página.	4 de septiembre de 2024
Nuevo tema de exclusión de todos los servicios de IA	Se agregó documentación sobre cómo excluirse de todos los servicios de IA compatibles. AWS	16 de agosto de 2024
Organizations ahora admite 10 000 cuentas en una organización	Ahora puede administrar hasta 10 000 cuentas de miembro en una organización, lo que duplica el límite anterior de 5000 cuentas. Si tiene un requisito válido y una necesidad empresarial, puede solicitar y obtener la aprobación de una cuota de 10 000 cuentas sin necesidad de comprobar el límite de servicio por parte de Organizations u otros Servicios de AWS integrados.	14 de agosto de 2024
Nuevo tema de migración de cuentas	Se agregó documentación sobre cómo migrar una cuenta de una organización a otra.	1 de agosto de 2024

Políticas de copia de seguridad actualizadas	AWS Backup las políticas ahora admiten los archivos de instantáneas de Amazon Elastic Block Store (Amazon EBS). Para ver ejemplos actualizados, consulte Updating a backup policy y Backup policy syntax and examples.	9 de julio de 2024
Se actualizó la AWSOrganizations ReadOnlyAccess política administrada	Se agregó la `account:GetPrimaryEmail` acción a la AWSOrganizations ReadOnlyAccess política que permite acceder a la dirección de correo electrónico del usuario raíz de cualquier cuenta de miembro de una organización y se agregó la `account:GetRegionOptStatus` acción para permitir el acceso a las regiones habilitadas para cualquier cuenta de miembro de una organización.	6 de junio de 2024
Nuevo tema de actualización de la dirección de correo electrónico del usuario raíz	Organizations ahora ofrece la capacidad de actualizar de forma centralizada la dirección de correo electrónico del usuario raíz de cualquier cuenta de miembro de una organización.	6 de junio de 2024

Declaraciones de políticas actualizadas	Se agregaron nuevos `Sid` elementos a las declaraciones de políticas AWS Organizations gestionadas.	6 de febrero de 2024
Nuevo tema de cierre de cuentas de administración	Se agregaron enlaces a consideraciones y pasos detallados que explican cómo cerrar una cuenta de administración.	1 de febrero de 2024
Prácticas recomendadas actualizadas	Se agregó nueva información a la sección de prácticas recomendadas para ayudar a alinearse con las prácticas recomendadas de IAM.	12 de junio de 2023
Se actualizaron AWSOrganizations FullAccess y AWSOrganizations ReadOnlyAccess gestionaron las políticas	Ambas políticas administradas se actualizaron para permitir el acceso de escritura o lectura a los contactos de las cuentas.	21 de octubre de 2022
Se actualizó la política AWSOrganizations FullAccess gestionada	La política administrada se actualizó para permitir la creación de una organización agregando el permiso necesario para crear el rol vinculado al servicio que necesita una organización nueva.	24 de agosto de 2022

Capacidad de cierre de cuentas de las organizaciones desde la AWS Organizations consola	Las entidades principales de la cuenta de administración pueden cerrar cuentas de miembro desde la consola de AWS Organizations y proteger las cuentas de los miembros del cierre accidental mediante el uso de las políticas de IAM.	29 de marzo de 2022
Anuncio actualizado para actualizar contactos alternativos con la consola de AWS Organizations	Organizations ahora ofrece la posibilidad de actualizar contactos alternativos para las cuentas de su organización mediante la AWS Organizations consola. Anuncie la nueva capacidad y señale a la referencia de administración de cuentas para obtener instrucciones.	8 de febrero de 2022
Actualizaciones de políticas administradas por Organizations: Actualización de una política existente	Se actualizaron AWSOrganizations FullAccess y AWSOrganizations ReadOnlyAccess gestionaron las políticas para permitir los permisos de API de la cuenta necesarios para actualizar o ver los contactos alternativos de la cuenta a través de la AWS Organizations consola.	7 de febrero de 2022

Integración de las organizaciones con Amazon DevOps Guru	Puede integrar Amazon DevOps Guru AWS Organizations para supervisar el estado de las aplicaciones de forma integral en todas las cuentas de su organización y obtener información valiosa.	3 de enero de 2022
Integración de Organizations con Amazon Detective	Puede integrar Amazon Detective AWS Organizations para garantizar que su gráfico de comportamiento de detective proporcione visibilidad de la actividad de todas las cuentas de su organización.	16 de diciembre de 2021
La integración de Organizations con AWS Config ahora admite la agregación de datos multicuenta y multirregión.	Puede utilizar una cuenta de administrador delegada para agregar la configuración de recursos y los datos de conformidad de todas las cuentas de miembros de su organización. Para obtener más información, consulte Acumulación de datos de varias cuentas y regiones en la Guía del desarrollador de AWS Config .	16 de junio de 2021

La integración de las organizaciones con AWS Firewall Manager ahora incluye soporte para un administrador delegado	Ahora puede designar una cuenta de miembro de su organización para que sea el administrador de Firewall Manager de toda la organización. Esto permite una mejor separación de los permisos de la cuenta de administración de la organización.	30 de abril de 2021
Las políticas de copia de seguridad de Organizations ahora admiten la copia de seguridad continua	Puede utilizar la función de copias de seguridad AWS Backup continuas con las políticas de copias de seguridad de su organización.	10 de marzo de 2021
La integración de las organizaciones con AWS CloudFormation StackSets ahora incluye soporte para un administrador delegado	Ahora puede designar una cuenta de miembro de su organización para que sea la AWS CloudFormation StackSets administradora de toda la organización. Esto permite una mejor separación de los permisos de la cuenta de administración de la organización.	18 de febrero de 2021
Continúe invitando cuentas mientras habilita todas las características	AWS actualizó el proceso para habilitar todas las funciones de una organización. Ahora puede seguir invitando a nuevas cuentas a unirse a su organización mientras espera a que las cuentas existentes respondan a sus invitaciones.	3 de febrero de 2021

Introduce la versión 2.0 de la AWS Organizations consola	AWS introdujo una nueva versión de la AWS consola. Toda la documentación se ha actualizado para reflejar la nueva forma de realizar las tareas.	21 de enero de 2021
Organizations ahora admite la integración con AWS Marketplace	Ahora puede AWS Marketplace compartir más fácilmente sus licencias de software entre todas las cuentas de su organización.	3 de diciembre de 2020
Organizations ahora admite la integración con Amazon S3 Lens	Amazon S3 Lens admite el acceso de confianza y el administrador delegado con Organizations. Para obtener información detallada, consulte Amazon S3 Storage Lens en la Guía del usuario de Amazon Simple Storage Service.	18 de noviembre de 2020
Copias de seguridad entre cuentas	Cuando utiliza políticas de copia de seguridad para realizar copias de seguridad de los recursos de su organización, ahora puede almacenar copias de las copias de seguridad Cuentas de AWS en otras partes de la organización.	18 de noviembre de 2020

Regiones de AWS en China ahora el soporte AWS Resource Access Manager como servicio confiable de Organizations	Ahora puede usar AWS RAM funciones que se integran con Organizations como un servicio confiable cuando usa Organizations y AWS RAM en China.	18 de noviembre de 2020
Organizations ahora admite la integración con AWS Security Hub	Puede habilitar Security Hub en todas las cuentas de su organización y designar una de las cuentas de miembro de su organización como la cuenta de administrador delegada para Security Hub.	12 de noviembre de 2020
Se ha cambiado el nombre de la cuenta maestra	AWS Organizations cambió el nombre de la «cuenta maestra» a «cuenta de administración». Solo se ha cambiado el nombre, no se cambia su funcionalidad.	20 de octubre de 2020
Sección Nuevas prácticas recomendadas y temas	Se ha añadido una nueva sección para las prácticas recomendadas de AWS Organizations. La nueva sección incluye temas que tratan las prácticas recomendadas para los usuarios raíz de cuentas de administración y cuentas de miembro y administración de contraseñas.	6 de octubre de 2020

Se ha agregado nueva sección de prácticas recomendadas y dos primeras páginas	Hay una nueva sección para temas que describen las prácticas recomendadas para AWS Organizations. Esta actualización incluye un tema sobre prácticas recomendadas para la cuenta de administración de una organización y un tema sobre prácticas recomendadas para cuentas de miembro.	2 de octubre de 2020
Las políticas de respaldo de las organizaciones ahora admiten respaldos consistentes con las aplicaciones en EC2 instancias de Windows mediante VSS (Volume Shadow Copy Service)	Las políticas de copia de seguridad admiten una nueva sección `advanced_backup_settings` “. La primera entrada de esta nueva sección es una configuración `ec2` llamada `WindowsVSS` que puede habilitar o desactivar. Para obtener más información, consulte Creación de una copia de seguridad de Windows habilitada para VSS en la Guía para desarrolladores de AWS Backup .	24 de septiembre de 2020

Organizations apoya tag-on-create y controla el acceso por etiquetas	Puede agregar etiquetas a los recursos de Organizations cuando los crea. Puede usar Políticas de etiquetas para estandarizar el uso de etiquetas en los recursos de Organizations. Puede usar Políticas de IAM para restringir el acceso solo a los recursos que tienen claves de etiqueta y valores especificados.	15 de septiembre de 2020
Añadido AWS Health como un servicio de confianza	Puede agregar AWS Health eventos en todas las cuentas de su organización.	4 de agosto de 2020
Políticas de exclusión de servicios de inteligencia artificial (IA)	Puede utilizar las políticas de exclusión de los servicios de IA para controlar si los servicios de AWS IA pueden almacenar y utilizar el contenido de los clientes procesado por esos servicios (contenido de IA) para el desarrollo y la mejora continua de los servicios y tecnologías de AWS IA.	8 de julio de 2020
Se agregaron políticas de respaldo e integración con AWS Backup	Puede usar las políticas de copia de seguridad para crear y aplicar políticas de copia de seguridad en todas las cuentas de su organización.	24 de junio de 2020

Compatibilidad con la administración delegada del Analizador de acceso de IAM	Permite delegar el acceso administrativo de Access Analyzer de su organización en una cuenta de miembro designada.	30 de marzo de 2020
Integración con AWS CloudFormation StackSets	Puede crear un conjunto de pilas administradas por servicios para implementar instancias de pila en cuentas administradas por AWS Organizations.	11 de febrero de 2020
Integración con Compute Optimizer	Compute Optimizer se ha agregado como un servicio que puede funcionar con las cuentas de su organización.	4 de febrero de 2020
Políticas de etiquetas	Puede utilizar las políticas de etiquetas para ayudar a estandarizar las etiquetas en todos los recursos en las cuentas de su organización.	26 de noviembre de 2019
Integración con Systems Manager	Puede sincronizar los datos de operaciones de toda Cuentas de AWS la organización en Systems Manager Explorer.	26 de noviembre de 2019
leyes: PrincipalOrgPaths	La nueva clave de condición global comprueba la AWS Organizations ruta del usuario de IAM, el rol de IAM o el usuario Cuenta de AWS raíz que realiza la solicitud.	20 de noviembre de 2019

Integración con las reglas AWS Config	Puede utilizar las operaciones de la AWS Config API para gestionar AWS Config las reglas Cuentas de AWS en toda la organización.	8 de julio de 2019
Nuevo servicio para el acceso de confianza	Service Quotas se ha añadido como un servicio que puede funcionar con las cuentas de su organización.	24 de junio de 2019
Integración con la Torre AWS de Control	AWS Control Tower se agregó como un servicio que puede funcionar con las cuentas de su organización.	24 de junio de 2019
Integración con AWS Identity and Access Management	IAM proporciona los datos del servicio a los que se accedió por última vez para las entidades de su organización (la raíz de la organización y las cuentas). OUs Puede usar estos datos para restringir el acceso únicamente a los Servicios de AWS que necesite.	20 de junio de 2019
Etiquetado de cuentas	Puede aplicar etiquetas a su organización y eliminar estas etiquetas, así como ver las etiquetas de una cuenta de su organización.	6 de junio de 2019

Los recursos, las condiciones y el `NotAction` elemento de las políticas de control de servicios (SCPs)	Ahora puede especificar los recursos, las condiciones y el `NotAction` elemento SCPs para denegar el acceso a todas las cuentas de su organización o unidad organizativa (OU).	25 de marzo de 2019
Servicios nuevos para el acceso de confianza	AWS License Manager y Service Catalog se han agregado como servicios que pueden funcionar con las cuentas de su organización.	21 de diciembre de 2018
Servicios nuevos para el acceso de confianza	AWS CloudTrail y AWS RAM se han agregado como servicios que pueden funcionar con las cuentas de su organización.	4 de diciembre de 2018
Nuevo servicio para el acceso de confianza	AWS Directory Service agregado como un servicio que puede funcionar con las cuentas de su organización.	25 de septiembre de 2018
Verificación de dirección de correo electrónico	Para poder invitar a cuentas existentes a su organizac ión, debe verificar que es el propietario de la dirección de correo electrónico asociada a la cuenta de administración.	20 de septiembre de 2018
CreateAccount notifications	`CreateAccount` las notificac iones se publican en los CloudTrail registros de la cuenta de administración.	28 de junio de 2018

Nuevo servicio para el acceso de confianza	AWS Artifact se agrega como un servicio que puede funcionar con las cuentas de su organización.	20 de junio de 2018
Servicios nuevos para el acceso de confianza	AWS Config y AWS Firewall Manager se agregan como servicios que pueden funcionar con las cuentas de su organización.	18 de abril de 2018
Acceso de servicios de confianza	Ahora puede habilitar o deshabilitar el acceso Servicios de AWS para seleccionar las cuentas de su organización para que funcionen. IAM Identity Center es el primer servicio de confianza compatible.	29 de marzo de 2018
Ahora la eliminación de cuentas es un servicio autónomo	Ahora puede eliminar las cuentas que se crearon desde dentro AWS Organizations sin ponerse en contacto con ellas AWS Support.	19 de diciembre de 2017
Se agregó soporte para el nuevo servicio AWS IAM Identity Center	AWS Organizations ahora admite la integración con AWS IAM Identity Center (IAM Identity Center).	7 de diciembre de 2017

AWS agregó un rol vinculado al servicio a todas las cuentas de la organización	Se agrega un nombre `AWSServiceRoleForOrganizations` de rol vinculado a un servicio a todas las cuentas de una organización para permitir la integración entre ellas. AWS Organizations Servicios de AWS	11 de octubre de 2017
A partir de ahora, puede eliminar cuentas creadas	Los clientes ya pueden eliminar cuentas creadas en su organización con ayuda de AWS Support.	15 de junio de 2017
Lanzamiento del servicio	Versión inicial de la AWS Organizations documentación que acompañó al lanzamiento del nuevo servicio.	17 de febrero de 2017

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.