Guía del administrador

AWS Supply Chain

AWS Supply Chain: Guía del administrador

Table of Contents

¿Qué es AWS Supply Chain?

AWS Supply Chain es una aplicación de gestión de la cadena de suministro basada en la nube que unifica los datos y proporciona métodos de previsión basados en el aprendizaje automático para mejorar la previsión de la demanda y la visibilidad del inventario, información práctica, colaboración contextual integrada, planificación de la demanda, planificación del suministro, visibilidad de los proveedores de n niveles y gestión de la información sobre sostenibilidad. AWS Supply Chain puede conectarse a sus sistemas actuales de planificación de recursos empresariales (ERP) y de gestión de la cadena de suministro, y utiliza el aprendizaje automático y la IA generativa para transformar e integrar datos dispares en el lago de datos de la cadena de suministro (SCDL). AWS Supply Chain puede mejorar la gestión de riesgos de la cadena de suministro sin necesidad de cambiar de plataforma, pagar licencias por adelantado ni asumir compromisos a largo plazo.

Temas

Navegadores compatibles con AWS Supply Chain

Antes de trabajar con AWS Supply Chain, compruebe que su navegador es compatible con la siguiente tabla.

Navegador	Versiones compatibles
Google Chrome	Tres últimas versiones.
Mozilla Firefox ESR	Las versiones son compatibles hasta su end-of-lifefecha de Firefox. Para obtener más información, consulta el calendario de versiones ESR de Firefox.
Mozilla Firefox	Tres últimas versiones.
Microsoft Edge y Edge Chromium	Versión 84 y posteriores.
Safari	Safari 10 o posterior en macOS.

Idiomas compatibles con AWS Supply Chain

AWS Supply Chain admite los siguientes idiomas:

- English (EE. UU.)
- Inglés (Reino Unido)
- Alemán
- Español
- Francés
- Italiano
- Portugués
- Chino simplificado
- Chino tradicional
- Japonés
- Coreano

Configuración de una AWS cuenta

Utilice esta sección para crear una AWS cuenta y crear un usuario de IAM. Para obtener información sobre las prácticas recomendadas para crear una AWS cuenta, consulte Cómo establecer un AWS entorno de prácticas recomendadas.

Temas

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 implica recibir una llamada telefónica o un mensaje de texto e introducir 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 .

Requisitos previos para usar AWS Supply Chain

Antes de crear una AWS Supply Chain instancia, asegúrate de completar los siguientes pasos:

- Tienes un Cuenta de AWS. Para crear un Cuenta de AWS, consulteConfiguración de una AWS cuenta.
- Asegúrese de que el Centro de identidad de IAM esté activado. Para activar el Centro de Identidad de IAM, consulte Habilitar el Centro de Identidad de IAM.
- Dispone de los permisos administrativos necesarios. Para obtener más información sobre los permisos, consulte Configuración avanzada.
- Debe activarse una instancia del IAM Identity Center en la misma región en la que desea crear la AWS Supply Chain instancia. AWS Supply Chain solo está disponible en las regiones EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), Europa (Fráncfort), Asia Pacífico (Sídney) y Europa (Irlanda).

  Si la AWS Supply Chain instancia no se encuentra en la misma región que la región del Centro de Identidad de IAM, ponte en contacto con nosotros para obtener más ayuda.

- Debe tener al menos un usuario en la instancia del Centro de Identidad de IAM para asignarlo como administrador. AWS Supply Chain Puede conectar su Active Directory al Centro de Identidad de IAM. Para obtener más información, consulte Conectarse a un directorio de Microsoft AD.
- Añada cualquier usuario adicional que necesite acceder AWS Supply Chain al Centro de identidad de IAM.
- Necesita AWS Key Management Service (AWS KMS) para crear una instancia. AWS Supply Chain usa esto AWS KMS key para cifrar todos los datos que ingresan AWS Supply Chain. Para obtener información sobre AWS KMS las claves, consulte Creación de claves.

Empezar con AWS Supply Chain

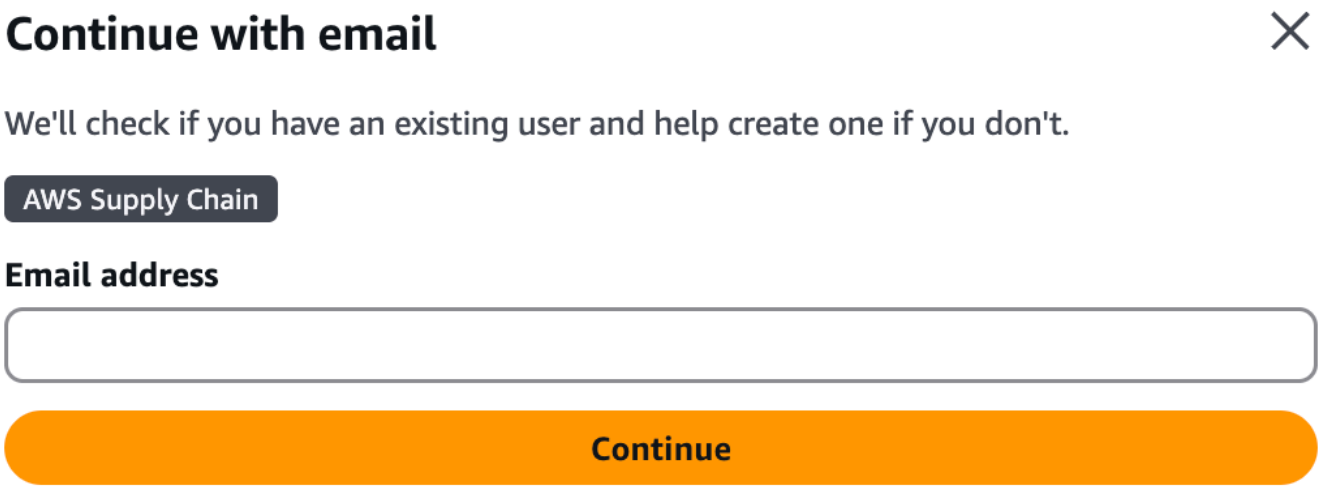
En esta sección, puedes aprender a crear una AWS Supply Chain instancia, conceder roles de permisos de usuario, iniciar sesión en la aplicación AWS Supply Chain web y crear roles de permisos de usuario personalizados. An Cuenta de AWS puede tener hasta 10 AWS Supply Chain instancias activas o en estado de inicialización.

Temas

Paso 1: Asigne un perfil de usuario del IAM Identity Center

Para crear una instancia y utilizar el AWS Supply Chain servicio, debe conectar un perfil de usuario del IAM Identity Center existente o crear uno nuevo.

1. Abra la consola de AWS Supply Chain. También puede buscar «AWS Supply Chain» en la página principal AWS Management Console.
2. Si es necesario, cambia la AWS región seleccionando Seleccionar una región en la parte superior de la consola. Elija su región en la lista desplegable.
3. Selecciona Crear AWS Supply Chain instancia. Aparecerá una notificación.



4. Introduce tu dirección de correo electrónico y selecciona Continuar. iDC verificará si el correo electrónico coincide con un usuario existente.
5. Realice una de las siguientes acciones:

   - Si iDC hace coincidir la dirección de correo electrónico con la de un usuario, selecciona Conectar tu fuente de identidad e incorpora a tu equipo.

     > **Note**
     >
     > Esto se puede usar si su organización tiene una instancia de iDC establecida para la que le gustaría usarla. AWS Supply Chain

   - Si iDC no encuentra ninguna coincidencia con un usuario existente, aparece una notificación de creación de un nuevo usuario. Continúe con el siguiente paso.
6. En la notificación, introduce lo siguiente y, a continuación, selecciona Continuar:

   - Dirección de correo electrónico
   - Nombre
   - Apellido

   iDC crea el usuario automáticamente y lo añade como AWS Supply Chain administrador.
7. Realice una de las siguientes acciones:

   - Para crear una instancia con la configuración estándar, seleccione Crear. Consulte the section called “Usa la configuración estándar”.
   - Para crear una instancia con una configuración personalizada, seleccione Editar en la configuración avanzada. Consulte the section called “Utilice la configuración avanzada”.

Paso 2: Crear una instancia

Al crear una instancia, se AWS Supply Chain establece un entorno específico para la gestión y el análisis de la cadena de suministro. Para configurar una instancia, debe configurar los detalles básicos, establecer los ajustes y definir los permisos de acceso iniciales de los usuarios.

> **Note**
>
> Solo el AWS Management Console administrador puede crear una instancia. El AWS Management Console administrador que crea la AWS Supply Chain instancia debe tener todos los permisos que se indican a continuaciónUso del AWS Supply Chain. Este administrador debe invitar a un usuario de IAM como AWS Supply Chain administrador para que la gestione AWS Supply Chain.

Puede crear una instancia mediante uno de los dos métodos siguientes: configuración estándar o configuración avanzada. La configuración estándar utiliza un proceso automatizado que crea la instancia rápidamente mediante parámetros preestablecidos. La configuración avanzada le permite personalizar la instancia mediante el establecimiento de sus propios parámetros.

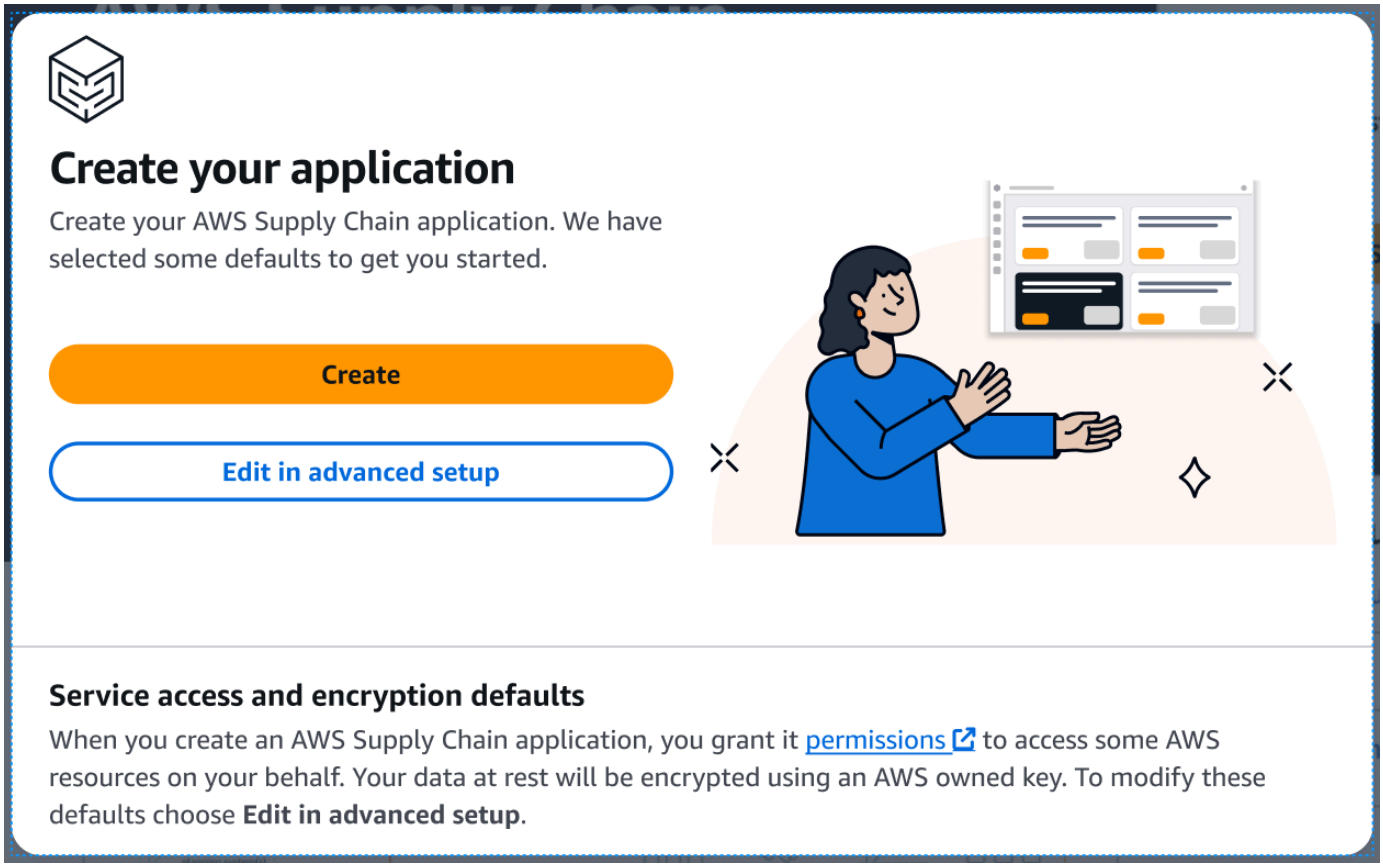
Temas

Usa la configuración estándar

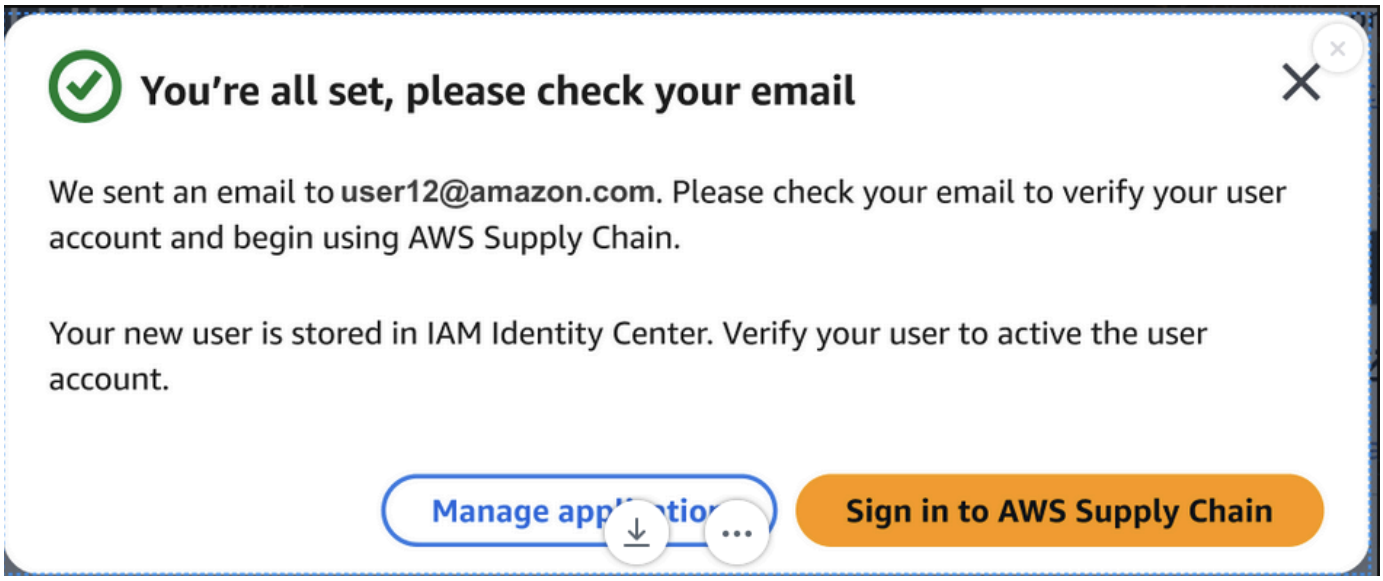
La configuración estándar crea la AWS Supply Chain instancia con la configuración de seguridad y cifrado predeterminada. Las instancias funcionan en regiones AWS geográficas. Para obtener más información sobre las regiones, consulte Regiones y puntos de enlace en la Guía del usuario de IAM y Puntos de enlace regionales en. Referencia general de AWS

Para crear una AWS Supply Chain instancia con una configuración estándar de parámetros preestablecidos, siga estos pasos.

1. Seleccione Crear.

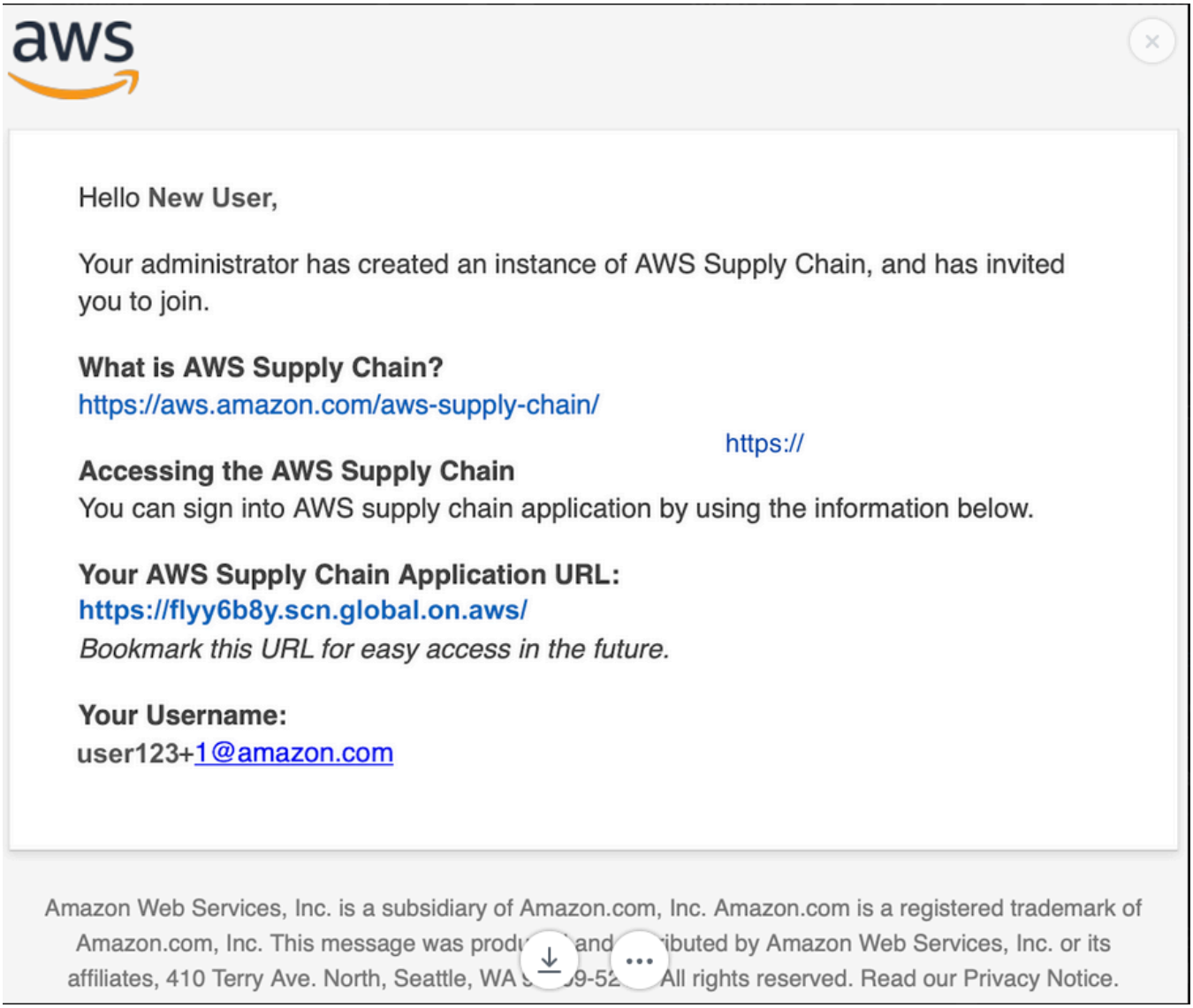


Aparecerá una confirmación.



2. Comprueba si tu correo electrónico contiene lo siguiente:

   - Un correo electrónico del equipo de iDC.
   - Un correo electrónico del equipo de gestión de identidad.

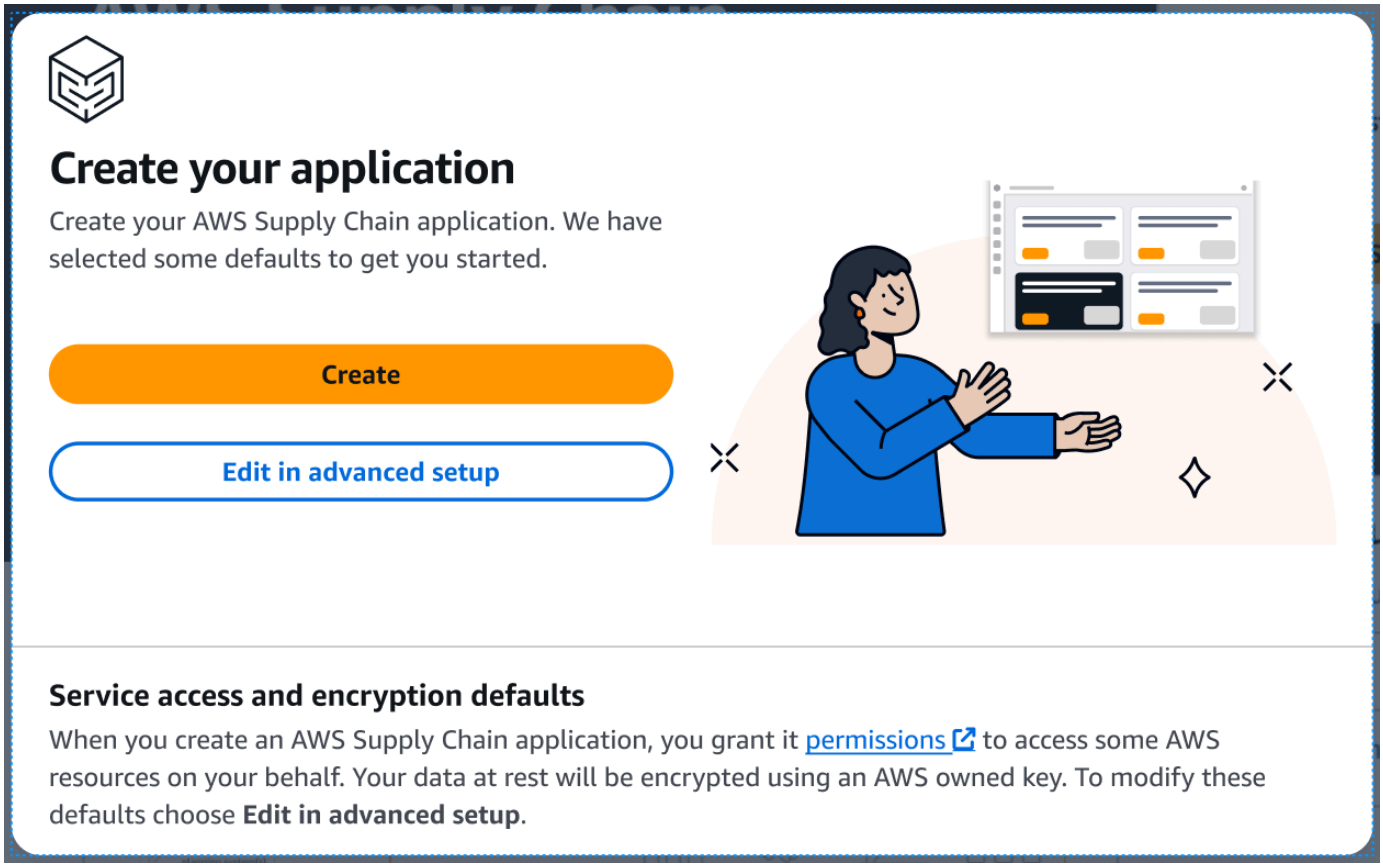


3. Una vez que reciba el correo electrónico de invitación, inicie sesión en AWS Supply Chain. Verthe section called “Inicie sesión en la aplicación AWS Supply Chain web”.

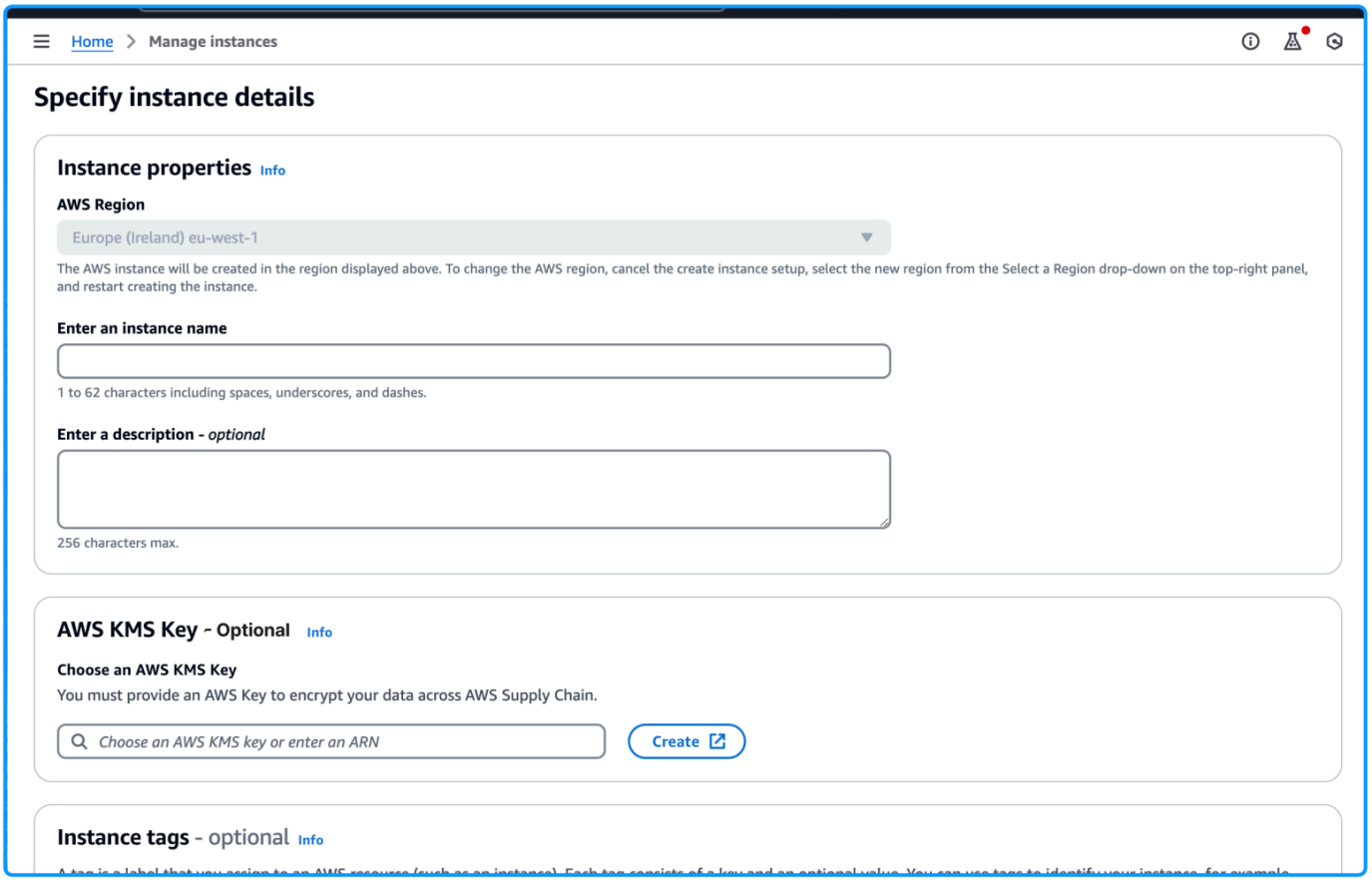
Utilice la configuración avanzada

La configuración avanzada le permite personalizar la instancia mediante el establecimiento de sus propios parámetros. Para crear una AWS Supply Chain instancia mediante una configuración avanzada de parámetros preestablecidos, sigue estos pasos.

1. Seleccione Editar en la configuración avanzada.



Aparecerá la página de propiedades de la instancia.



2. Introduzca lo siguiente en la página de propiedades de la instancia:

   - Nombre: introduzca un nombre de instancia.
   - Descripción: introduce una descripción de la AWS Supply Chain instancia (p. ej., instancia de producción, instancia de prueba, etc.).
   - Clave AWS KMS (opcional): puede elegir usar la AWS KMS clave predeterminada (recomendada) o proporcionar su propia AWS KMS clave. Para obtener más información, consulte the section called “Uso de una AWS KMS clave personalizada”.
   - Etiquetas de instancia: puede añadir etiquetas a la instancia que se puedan utilizar para la identificación. Por ejemplo, puedes añadir una etiqueta para definir el tipo de instancia que vas a crear (p. ej., de producción, de prueba, UAT, etc.).

   > **Note**
   >
   > Si planea usar una conexión de datos S/4 Hana, asegúrese de que la AWS KMS clave que proporcionó tenga la `aws-supply-chain-access` etiqueta con un valor asociado de. `true`

3. Selecciona Crear instancia.
4. (Opcional) Una vez creada la AWS Supply Chain instancia y si decide usar su propia AWS KMS clave bajo AWS KMS clave, actualice su política de KMS para permitir el acceso AWS Supply Chain a su AWS KMS clave.

> **Note**
>
> Sustituya *YourAccountNumber* y *YourInstanceID* por su Cuenta de AWS ID de AWS Supply Chain instancia.

```
 {

    "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
    "Effect": "Allow",
    "Principal":  {
        "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
    },
    "Action":  [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
}
```

Uso de una AWS KMS clave personalizada

Puedes usar tu propia AWS KMS clave al crear instancias. Si desea administrar su propia clave, pero no desea utilizar una clave existente, puede crear una nueva clave.

> **Note**
>
> El uso AWS de una clave propia es la configuración predeterminada recomendada para AWS Supply Chain las instancias.

Usar una AWS KMS clave existente

1. Seleccione Personalizar la configuración de cifrado.
2. Ve a Elegir una AWS KMS clave.
3. Introduce tu clave en el campo correspondiente.
4. Seleccione Update (Actualizar).

Crear una AWS KMS clave

1. Seleccione Crear.
2. Siga los pasos que se indican en Crear una clave de KMS.
3. Actualice la nueva clave con los siguientes permisos.

   - Defina los permisos administrativos clave: déjelos sin marcar
   - Definir los permisos de uso de claves: dejar esta opción sin marcar
   - Actualizar la política clave: edite la política clave y sustitúyala por:

```
{

    "Version": "2012-10-17",
    "Statement":  [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal":  {
                "AWS": "arn:aws:iam::YourAccountNumber:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow access through SecretManager for all principals in the
 account that are authorized to use SecretManager",
            "Effect": "Allow",
            "Principal":  {
                "AWS": "*"
            },
            "Action":  [
                "kms:Encrypt",
                "kms:Decrypt",
```

```
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:CreateGrant",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo"
            ],
            "Resource": "*",
            "Condition":  {
                "StringEquals":  {
                    "kms:ViaService": "secretsmanager.Region.amazonaws.com",
                    "kms:CallerAccount": "YourAccountNumber"
                }
            }
        },
        {
            "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
            "Effect": "Allow",
            "Principal":  {
                "Service": "scn.Region.amazonaws.com"
            },
            "Action":  [
                "kms:Encrypt",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant"
            ],
            "Resource":"*"
        }
    ]
}
```

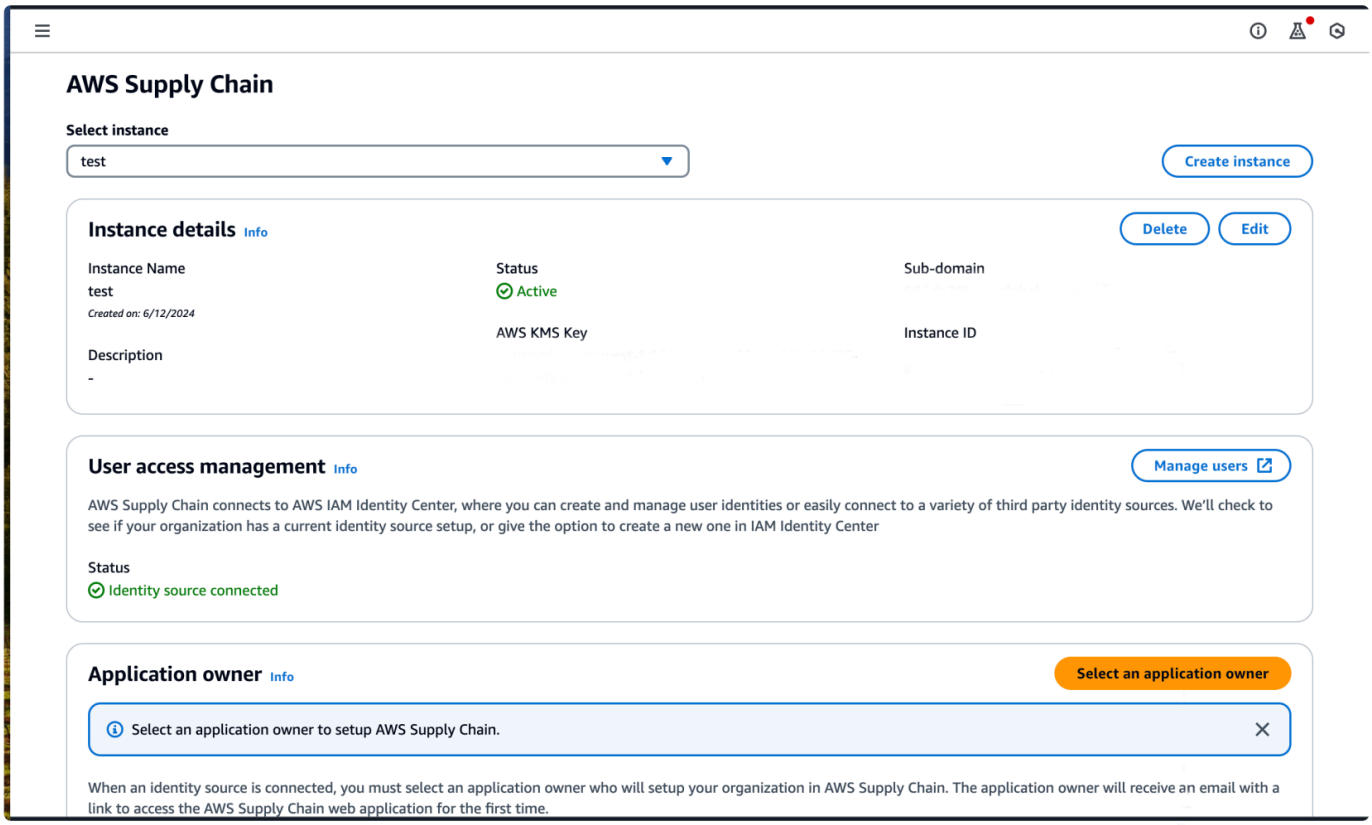
Paso 3: Elige el propietario de AWS Supply Chain la aplicación

Como administrador de AWS la consola, usted elige al propietario de AWS Supply Chain la aplicación para administrar el acceso a la aplicación AWS Supply Chain web. El propietario de

la aplicación AWS Supply Chain puede añadir o eliminar funciones de permisos de usuario en la aplicación web de AWS Supply Chain .

Una vez creada la instancia y conectada una fuente de identidad, siga estos pasos para elegir el propietario de AWS Supply Chain la aplicación.

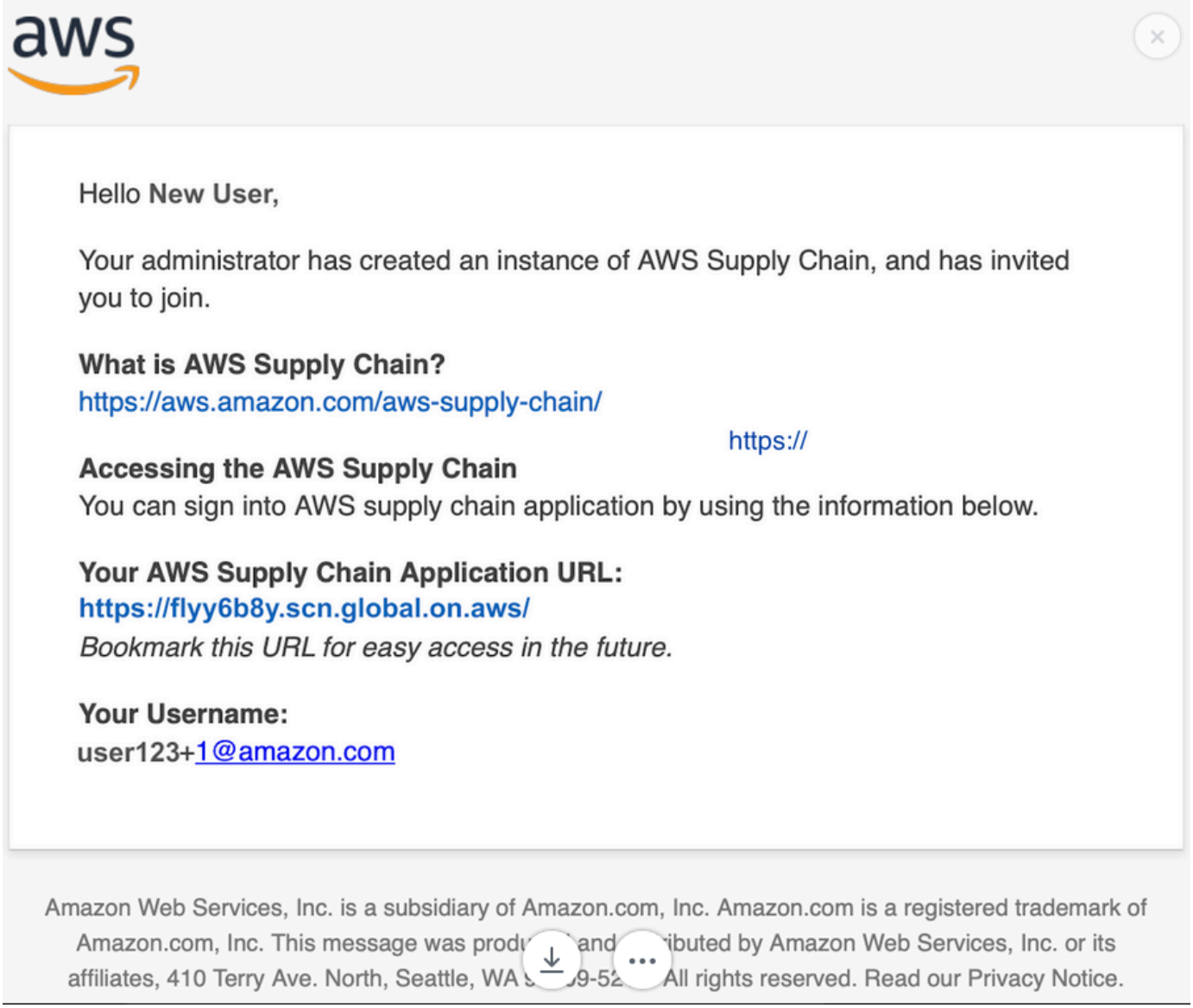
1. Abre el panel de control de la AWS Supply Chain consola.
2. Ve a Seleccionar el propietario de la aplicación y selecciona un usuario como propietario de AWS Supply Chain la aplicación. Los resultados de la búsqueda solo muestran los usuarios que coinciden con los criterios de búsqueda.



3. (Opcional) Seleccione Ir al centro de identidad de IAM para añadir más usuarios. Para obtener más información sobre cómo añadir usuarios, consulte Administrar su fuente de identidad en la Guía del usuario de AWS IAM Identity Center y, para obtener más información sobre las funciones de permisos de usuario, consulte Funciones de permisos de usuario.

> **Note**
>
> Solo puede añadir un usuario a la vez desde la AWS Supply Chain consola. No puede añadir un grupo como propietario de la aplicación en AWS Supply Chain.

4. Selecciona Enviar invitación. Se envía un correo electrónico al administrador de la aplicación web. Una vez que el administrador de la aplicación web reciba el correo electrónico de invitación, podrá seleccionar la URL de la aplicación e iniciar sesión en AWS Supply Chain.



En el panel de control de la AWS Supply Chain consola, verá al usuario en la lista Propietario de la aplicación.

Elija Administrar en AWS Supply Chain para añadir y eliminar usuarios de la aplicación AWS Supply Chain web

Inicie sesión en la aplicación AWS Supply Chain web

Como AWS Supply Chain administrador, debería haber recibido una invitación por correo electrónico a la aplicación AWS Supply Chain web.

1. Puede elegir el enlace en el correo electrónico o en el panel de la consola de AWS Supply Chain , en Subdominio, y elegir URL web.

   Aparece la página de inicio de sesión de la aplicación web de AWS Supply Chain.
2. Introduzca las credenciales de usuario del AWS IAM Identity Center y seleccione Iniciar sesión.

   > **Note**
   >
   > Solo se le pedirá que complete los perfiles de su cuenta y organización cuando inicie sesión por primera vez.
3. En la página Complete su perfil, introduzca su Cargo y Zona horaria. Elija Siguiente.
4. En la página Vamos a añadir la información de su organización, introduzca el Nombre de la organización y elija la Ubicación de la sede central. Opcionalmente, puede agregar un logotipo de la empresa. Elija Siguiente.
5. En la página AWS Supply Chain Configure sus compañeros de equipo en , seleccione los usuarios que desee que tengan acceso a la aplicación web de AWS Supply Chain . Elija Invitar a usuarios. Para obtener información sobre las funciones AWS Supply Chain de permisos de usuario, consulteAdministrar las funciones de permisos de usuario.
6. Si desea agregar usuarios más adelante, puede elegir Omitir por ahora.

   Aparece la página de Incorporación completada.
7. Cada usuario que haya agregado recibirá un mensaje de correo electrónico con un enlace a él AWS Supply Chain, o bien puede seleccionar Copiar el enlace y enviarlo a los usuarios.
8. Seleccione Ir a la página de inicio para ver el panel de AWS Supply Chain .

Uso del AWS Supply Chain

AWS Supply Chain es una aplicación basada en la nube que le ayuda a obtener visibilidad de la red de su cadena de suministro, a tomar decisiones informadas con rapidez y a mejorar la resiliencia de la cadena de suministro. Con AWS Supply Chain ella, puede conectar fuentes de datos dispares, generar información mediante el aprendizaje automático y colaborar con equipos internos y socios externos. En esta sección se explican algunas de las funciones AWS Supply Chain básicas.

Temas

Uso de AWS Supply Chain la consola

El uso de la consola es la forma más sencilla de administrar los recursos y las configuraciones del servicio. La consola proporciona una interfaz web intuitiva en la que puede ver, crear, modificar y supervisar sus recursos. En esta sección, se muestra cómo acceder a la consola y navegar por ella para realizar tareas de administración habituales.

> **Note**
>
> Si su AWS cuenta es una cuenta de miembro de una AWS organización e incluye una política de control de servicios (SCP), asegúrese de que la SCP de la organización conceda los siguientes permisos a la cuenta de miembro. Si los siguientes permisos no están incluidos en la política SCP de la organización, no se podrá crear la AWS Supply Chain instancia.

Para acceder a la AWS Supply Chain consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS Supply Chain recursos de su cuenta 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.

El administrador de la consola necesita los siguientes permisos para crear y actualizar correctamente las instancias de AWS Supply Chain .

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "scn:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "s3:GetObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:CreateBucket",
    "s3:PutBucketVersioning",
    "s3:PutBucketObjectLockConfiguration",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketPolicy",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketPublicAccessBlock",
    "s3:DeleteObject",
    "s3:ListAllMyBuckets",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketNotification",
    "s3:PutAccountPublicAccessBlock",
    "s3:PutBucketLogging",
    "s3:PutBucketTagging"
   ],
   "Resource": "arn:aws:s3:::aws-supply-chain-*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "cloudtrail:CreateTrail",
    "cloudtrail:PutEventSelectors",
    "cloudtrail:GetEventSelectors",
```

```
    "cloudtrail:StartLogging"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "events:DescribeRule",
    "events:PutRule",
    "events:PutTargets"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "chime:CreateAppInstance",
    "chime:DeleteAppInstance",
    "chime:PutAppInstanceRetentionSettings",
    "chime:TagResource"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "cloudwatch:PutMetricData",
    "cloudwatch:Describe*",
    "cloudwatch:Get*",
    "cloudwatch:List*"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "organizations:CreateOrganization",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:EnableAWSServiceAccess",
    "organizations:ListDelegatedAdministrators"
   ],
   "Resource": "*",
   "Effect": "Allow"
```

```
  },
  {
   "Action": [
    "kms:CreateGrant",
    "kms:RetireGrant",
    "kms:DescribeKey"
   ],
   "Resource": key_arn,
   "Effect": "Allow"
  },
  {
   "Action": [
    "kms:ListAliases"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "iam:CreateRole",
    "iam:CreatePolicy",
    "iam:GetRole",
    "iam:PutRolePolicy",
    "iam:AttachRolePolicy",
    "iam:CreateServiceLinkedRole"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "sso:AssociateDirectory",
    "sso:AssociateProfile",
    "sso:CreateApplication",
    "sso:CreateApplicationAssignment",
    "sso:CreateInstance",
    "sso:CreateManagedApplicationInstance",
    "sso:DeleteApplication",
    "sso:DeleteApplicationAssignment",
    "sso:DeleteManagedApplicationInstance",
    "sso:DescribeApplication",
    "sso:DescribeDirectories",
    "sso:DescribeInstance",
    "sso:DescribeRegisteredRegions",
```

```
    "sso:DescribeTrusts",
    "sso:DisassociateProfile",
    "sso:GetManagedApplicationInstance",
    "sso:GetPeregrineStatus",
    "sso:GetProfile",
    "sso:GetSharedSsoConfiguration",
    "sso:GetSsoConfiguration",
    "sso:GetSSOStatus",
    "sso:ListApplicationAssignments",
    "sso:ListApplicationTemplates",
    "sso:ListDirectoryAssociations",
    "sso:ListInstances",
    "sso:ListProfileAssociations",
    "sso:ListProfiles",
    "sso:PutApplicationAuthenticationMethod",
    "sso:PutApplicationGrant",
    "sso:RegisterRegion",
    "sso:SearchDirectoryGroups",
    "sso:SearchDirectoryUsers",
    "sso:SearchGroups",
    "sso:SearchUsers",
    "sso:StartPeregrine",
    "sso:StartSSO",
    "sso:UpdateSsoConfiguration",
    "sso-directory:SearchUsers"
   ],
   "Resource": "*",
   "Effect": "Allow"
  }
 ]
}
```

*key_arn*especifica la clave que quieres usar para la AWS Supply Chain instancia. Para conocer las prácticas recomendadas y restringir el acceso únicamente a las claves que desee utilizar AWS Supply Chain, consulte Especificar las claves de KMS en las declaraciones de política de IAM. Para representar todas las claves de KMS, utilice únicamente un carácter comodín («*»).

Actualizando tu perfil

Puede actualizar su cuenta y el perfil de su organización en cualquier momento en la aplicación AWS Supply Chain web.

Actualización del perfil de cuenta

Para actualizar el perfil de tu cuenta, sigue estos pasos.

1. En el panel de control de la aplicación AWS Supply Chain web, en el panel de navegación izquierdo, selecciona el icono de Configuración.
2. Seleccione Perfil de la cuenta.

   Aparece la página Perfil de la cuenta.
3. Actualice la información de la cuenta y elija Guardar.

Actualización del perfil de su organización

Para actualizar el perfil de la organización, sigue estos pasos.

1. En el panel de control de la aplicación AWS Supply Chain web, en el panel de navegación izquierdo, selecciona el icono de Configuración.
2. Elija Organización y, a continuación, elija Perfil de la organización.

   Aparece la página Perfil de la organización.
3. Actualice el Logotipo o la Ubicación de la sede central de la organización y, a continuación, seleccione Guardar.

Administrar las funciones de permisos de usuario

Como AWS Supply Chain administrador, puede usar las funciones de permisos de usuario predeterminadas o crear funciones de permisos personalizadas. AWS Supply Chain tiene los siguientes roles de permisos de usuario predeterminados:

- Administrador: acceso para crear, ver y administrar todos los datos y permisos de usuario.
- Analista de datos: acceso para crear, ver y administrar todas las conexiones de datos.
- Gestor de inventario: acceso para crear, ver y gestionar la información.
- Planificador de la demanda: permite crear, ver y gestionar previsiones, anulaciones y publicar planes de demanda.
- Administrador de datos de socios: acceso para administrar y ver los socios, administrar y ver las solicitudes de datos y ver los datos de sostenibilidad.

- Planificador de suministros: acceso para administrar y ver los planes de suministro.

> **Note**
>
> Como AWS Supply Chain administrador, antes de añadir usuarios, tenga en cuenta lo siguiente:
>
> - Cada rol de permisos de usuario predeterminado se define con un conjunto de permisos. Puede agregar usuarios a los roles de permisos de usuario predeterminados o crear roles de permisos personalizados.
> - A un usuario solo se le puede asignar un rol de permisos de usuario.
> - Los roles de permisos de usuario predeterminados no se pueden editar.
> - Al editar un rol de permisos personalizado que ha creado, se actualizan los permisos de todos los usuarios del rol de permisos personalizado.
> - Al eliminar un rol de permiso personalizado que haya creado, todos los usuarios del rol de permiso personalizado perderán el acceso a él AWS Supply Chain.
> - No se admite la adición de grupos en AWS Supply Chain.

Temas

Añadir usuarios

Como AWS Supply Chain administrador, puede añadir usuarios para acceder a la aplicación AWS Supply Chain web. Primero hay que añadir los usuarios al Centro de Identidad de IAM (iDC) y, a continuación, se pueden añadir a ellos. AWS Supply Chain Para obtener más información sobre cómo añadir usuarios a iDC, consulte Asignar el acceso de los usuarios.

Una vez que se hayan agregado los usuarios a iDC, siga estos pasos para agregar un usuario.

1. Seleccione el icono de configuración en el AWS Supply Chain panel de control.

2. Seleccione Usuarios y permisos.
3. Seleccione Usuarios, Usuarios. Aparece la página Administrar usuarios.
4. Seleccione Añadir nuevo usuario. Aparece la página Añadir usuario.
5. Seleccione el usuario en el menú desplegable Agregar usuario (s).
6. Seleccione el rol para el usuario en el menú desplegable Seleccionar rol.
7. Seleccione Añadir.

Actualización de permisos de usuario

Para actualizar el rol de permiso de usuario para los AWS Supply Chain usuarios actuales, sigue estos pasos.

1. En el AWS Supply Chain panel de control, en el panel de navegación izquierdo, selecciona el icono de Configuración.
2. Seleccione Permisos y, a continuación, seleccione Usuarios.

   Aparece la página Administrar usuarios.
3. En la página Administrar usuarios, selecciona el usuario o grupo para el que quieres actualizar el rol de permisos de usuario y, en el menú desplegable del rol de permisos, selecciona uno de los roles de permisos.

   > **Note**
   >
   > El panel de AWS Supply Chain se personaliza en función de los permisos de rol que asigne. Para obtener más información, consulte Creación de roles de permisos de usuario personalizados.
4. Seleccione Guardar.

Eliminación de usuarios

Como AWS Supply Chain administrador, puede eliminar usuarios de la aplicación AWS Supply Chain web. Siga estos pasos para eliminar usuarios.

1. En el AWS Supply Chain panel de control, en el panel de navegación izquierdo, selecciona el icono de Configuración.

2. Seleccione Permisos y, a continuación, seleccione Usuarios.

   Aparece la página Administrar usuarios.

3. En la página Administrar usuarios, seleccione el usuario que desee eliminar y elija el icono Eliminar.

Creación de roles de permisos de usuario personalizados

Además de los roles de permisos de usuario predeterminados, puede crear roles de permisos de usuario personalizados para incluir varios roles de permisos y añadir ubicaciones y productos específicos. Siga estos pasos para crear nuevos roles de permisos.

1. En el AWS Supply Chain panel de control, en el panel de navegación izquierdo, selecciona el icono de Configuración. Seleccione Permisos y, a continuación, Roles de permisos.

   Aparece la página Roles de permisos.

2. Elija Crear nuevo rol.
3. En la página Administrar el rol de permisos, en Nombre del rol, introduzca un nombre.
4. Mueva el control deslizante para seleccionar el rol de permisos de usuario.

   - Administrar: al asignar a los usuarios el permiso de administración, los usuarios pueden agregar, editar y administrar información.
   - Ver: al asignar a los usuarios el permiso de visualización, los usuarios solo pueden ver la información actual.

5.
   > **Note**
   >
   > Solo puede elegir los productos y las ubicaciones en Acceso a ubicaciones y Acceso a productos si la instancia está conectada a un origen de datos. Por ejemplo, puede crear un usuario administrador personalizado solo para administrar los aguacates en la ubicación de Seattle, o un usuario de Insight solo para administrar la información sobre los aguacates en la ubicación de Seattle.

   En Acceso a ubicaciones, busque las regiones mientras escribe en la barra de búsqueda y seleccione las regiones.

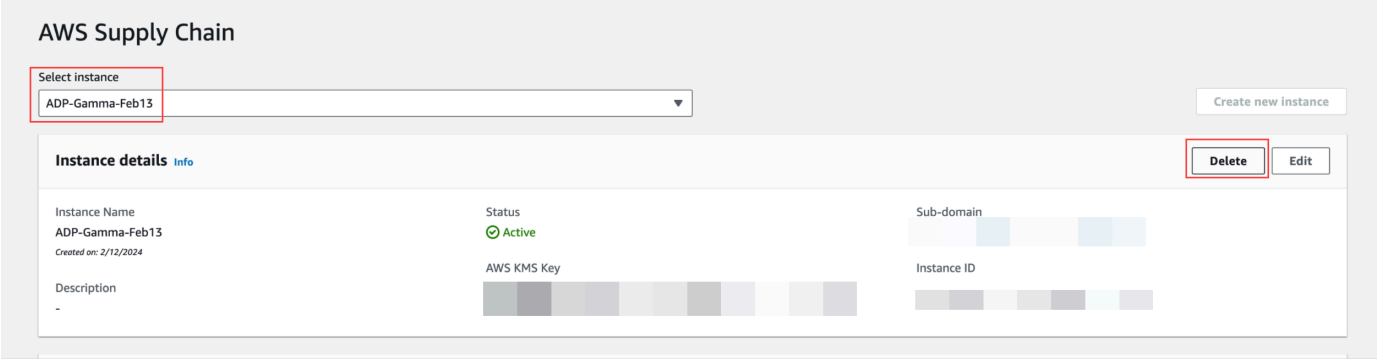
6. En Acceso a productos, busque los productos mientras escribe en la barra de búsqueda y seleccione los productos.
7. Seleccione Guardar.

Eliminación de una instancia

Para eliminar una instancia, sigue estos pasos.

> **Note**
>
> Al eliminar una instancia, la información del bucket de Amazon S3 no se elimina automáticamente.

1. Abre la AWS Supply Chain consola enhttps://console.aws.amazon.com/scn/home.
2. En el panel de la AWS Supply Chain consola, en el menú desplegable, selecciona la instancia que quieres eliminar.



3. Elija Eliminar.
4. En la página Eliminar AWS Supply Chain instancia, en Confirmación, escriba **`delete`** para confirmar que desea eliminar la instancia.
5. Elija Eliminar. Se inicia la eliminación de la instancia y, una vez eliminada, verá un mensaje de confirmación.

> **Note**
>
> Una vez eliminada la instancia, la información relacionada con Amazon Q in AWS Supply Chain se eliminará automáticamente.

Seguridad en AWS Supply Chain

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para AWS cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted y AWS. 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. Nube de AWS AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos 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 conformidad aplicables AWS Supply Chain, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad AWS Servicios incluidos .
- Seguridad en la nube: la Servicio de AWS que utilice determinará su responsabilidad. También es responsable de otros factores, incluida la confidencialidad de sus datos, sus requisitos y la legislación y los reglamentos vigentes.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando utiliza AWS Supply Chain. En los temas siguientes, se muestra cómo configurarlo AWS Supply Chain para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayuden a supervisar y proteger sus AWS Supply Chain recursos.

Temas

Protección de datos en AWS Supply Chain

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Supply Chain. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS Supply Chain o Servicios de AWS utiliza la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos

de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Datos administrados por AWS Supply Chain

Para limitar los datos a los que pueden acceder los usuarios autorizados de una instancia de la cadena de AWS suministro específica, los datos que se encuentran en la cadena de AWS suministro se segregan por su ID de AWS cuenta y su ID de instancia de cadena AWS de suministro.

AWS La cadena de suministro gestiona una variedad de datos de la cadena de suministro, como la información del usuario, la información extraída del conector de datos y los detalles del inventario.

Preferencia de exclusión

Es posible que usemos y almacenemos su contenido procesado por AWS Supply Chain, tal y como se indica en las condiciones de servicio de AWS. Si desea AWS Supply Chain excluirse del uso o almacenamiento de su contenido, puede crear una política de exclusión en AWS Organizations. Para obtener más información sobre la creación de una política de exclusión, consulte la sintaxis y los ejemplos de la política de exclusión de los servicios de IA.

Cifrado en reposo

Los datos de contacto clasificados como PII, o los datos que representan el contenido del cliente, incluido el contenido utilizado en Amazon Q para su almacenamiento AWS Supply Chain, AWS Supply Chain se cifran en reposo (es decir, antes de colocarlos, almacenarlos o guardarlos en un disco) con una clave limitada en el tiempo y específica de la AWS Supply Chain instancia.

El cifrado del lado del servidor de Amazon S3 se utiliza para cifrar todos los datos de la consola y de las aplicaciones web con una clave de datos de AWS Key Management Service que es única para cada cuenta de cliente. Para obtener más información AWS KMS keys, consulte ¿Qué es? AWS Key Management Service en la Guía para AWS Key Management Service desarrolladores.

> **Note**
>
> AWS Supply Chain Las funciones Supply Planning y N-Tier Visibility no admiten el cifrado data-at-rest con el KMS-CMK suministrado.

Cifrado en tránsito

Los datos, incluido el contenido utilizado en Amazon Q para AWS Supply Chain intercambiarlos con AWS Supply Chain, están protegidos en tránsito entre el navegador web del usuario y AWS Supply Chain mediante el cifrado TLS estándar del sector.

Administración de claves

AWS Supply Chain es compatible parcialmente con KMS-CMK.

Para obtener información sobre la actualización de la clave de AWS KMS AWS Supply Chain, consultePaso 2: Crear una instancia.

Privacidad del tráfico entre redes

> **Note**
>
> AWS Supply Chain no es compatible PrivateLink.

Un punto final de nube privada virtual (VPC) para AWS Supply Chain es una entidad lógica dentro de una VPC que solo permite la conectividad a. AWS Supply Chain La VPC enruta las solicitudes AWS Supply Chain y redirige las respuestas a la VPC. Para obtener más información, consulte VPC Endpoints en la Guía del usuario de VPC.

¿Cómo se utilizan AWS Supply Chain las subvenciones en AWS KMS

AWS Supply Chain requiere una concesión para utilizar la clave gestionada por el cliente.

AWS Supply Chain crea varias concesiones utilizando la AWS KMS clave que se transfiere durante la CreateInstanceoperación. AWS Supply Chain crea una subvención en tu nombre enviando CreateGrantlas solicitudes a AWS KMS. Las subvenciones AWS KMS se utilizan para dar AWS Supply Chain acceso a la AWS KMS clave de la cuenta de un cliente.

> **Note**
>
> AWS Supply Chain utiliza su propio mecanismo de autorización. Una vez que se agrega un usuario a la lista AWS Supply Chain, no se puede denegar la inclusión del mismo usuario en la lista mediante la AWS KMS política.

AWS Supply Chain usa la concesión para lo siguiente:

- Para enviar GenerateDataKeysolicitudes AWS KMS para cifrar los datos almacenados en su instancia.
- Para enviar solicitudes de descifrado a para AWS KMS leer los datos cifrados asociados a la instancia.
- Para añadir DescribeKeyy RetireGrantpermisos a fin de mantener tus datos protegidos cuando los envíes a otros AWS servicios, como Amazon Forecast. CreateGrant

Puede revocar el acceso a la concesión o eliminar el acceso del servicio a la clave administrada por el cliente en cualquier momento. Si lo haces, AWS Supply Chain no podrás acceder a ninguno de los datos cifrados por la clave gestionada por el cliente, lo que afectará a las operaciones que dependen de esos datos.

Supervisar el cifrado para AWS Supply Chain

Los siguientes ejemplos son AWS CloudTrail eventos para y `Decrypt` para `Encrypt` monitorear las operaciones de KMS solicitadas AWS Supply Chain para acceder a los datos cifrados por la clave administrada por el cliente: `GenerateDataKey`

Encrypt


```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
    "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
    },
```

```
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

GenerateDataKey

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:s3:arn": "arn:aws:s3:::test/rawEvent/bf6666c1-111-48aaca-b6b0-
dsadsadsa3432423/noFlowName/scn.data.inboundorder/20240306_223934_536"
        },
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "keySpec": "AES_222"
```

```
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Decrypt

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
```

```
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Acceso AWS Supply Chain mediante un punto final de interfaz (AWS PrivateLink)

Puede usarlo AWS PrivateLink para crear una conexión privada entre su VPC y. AWS Supply Chain Puede acceder AWS Supply Chain como si estuviera en su VPC, sin el uso de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect una conexión. Las instancias de la VPC no necesitan direcciones IP públicas para acceder a AWS Supply Chain.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a AWS Supply Chain.

Para obtener más información, consulte Acceso Servicios de AWS directo AWS PrivateLink en la AWS PrivateLink Guía.

Consideraciones sobre AWS Supply Chain

Antes de configurar un punto final de interfaz para AWS Supply Chain, consulte las consideraciones de la AWS PrivateLink guía.

AWS Supply Chain permite realizar llamadas a todas sus acciones de API a través del punto final de la interfaz.

Cree un punto final de interfaz para AWS Supply Chain

Puede crear un punto final de interfaz para AWS Supply Chain usar la consola de Amazon VPC o AWS Command Line Interface ()AWS CLI. Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Cree un punto final de interfaz para AWS Supply Chain usar el siguiente nombre de servicio:

```
com.amazonaws.region.scn
```

Si habilita DNS privado para el punto de conexión de interfaz, puede realizar solicitudes a la API para AWS Supply Chain usando su nombre de DNS predeterminado para la región. Por ejemplo, *scn*.*region*.amazonaws.com.

Creación de una política de puntos de conexión para el punto de conexión de interfaz

Una política de punto de conexión es un recurso de IAM que puede adjuntar al punto de conexión de su interfaz. La política de punto final predeterminada permite el acceso total a AWS Supply Chain través del punto final de la interfaz. Para controlar el acceso permitido AWS Supply Chain desde su VPC, adjunte una política de punto final personalizada al punto final de la interfaz.

Una política de punto de conexión especifica la siguiente información:

- Los principales que pueden realizar acciones (Cuentas de AWS usuarios de IAM y funciones de IAM)
- Las acciones que se pueden realizar
- Los recursos en los que se pueden realizar las acciones

Para obtener más información, consulte Control del acceso a los servicios con políticas de punto de conexión en la Guía del usuario de AWS PrivateLink .

Ejemplo: política de puntos finales de VPC para acciones AWS Supply Chain

A continuación, se muestra un ejemplo de una política de un punto de conexión personalizada. Cuando se asocia con un punto de conexión, esta política concede acceso a las acciones de AWS Supply Chain mostradas para todas las entidades principales en todos los recursos.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [

            "scn:action-1",
            "scn:action-2",
            "scn:action-3"

         ],
         "Resource":"*"
      }
   ]
}
```

IAM para AWS Supply Chain

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Supply Chain La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS Supply Chain

Usuario del servicio: si utiliza el AWS Supply Chain servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS Supply Chain funciones para realizar 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 en AWS Supply Chain, consulte Solución de problemas de identidad y acceso AWS Supply Chain.

Administrador de servicios: si estás a cargo de AWS Supply Chain los recursos de tu empresa, probablemente tengas acceso total a ellos AWS Supply Chain. Su trabajo consiste en determinar a qué AWS Supply Chain funciones y recursos 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 su empresa puede utilizar la IAM AWS Supply Chain, consulte¿Cómo AWS Supply Chain funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS Supply Chain. Para ver ejemplos de políticas AWS Supply Chain basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en identidades de AWS Supply Chain

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus 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 (IAM Identity Center), 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, asumes 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 de su empresa, 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 administrar 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 Supply Chain funciona con IAM

Antes de utilizar IAM para gestionar el acceso AWS Supply Chain, infórmese sobre las funciones de IAM disponibles para su uso. AWS Supply Chain

Funciones de IAM que puede utilizar con AWS Supply Chain

Característica de IAM	AWS Supply Chain soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	No

Para obtener una visión general de cómo AWS Supply Chain funcionan 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 la identidad para AWS Supply Chain

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 la identidad para AWS Supply Chain

Para ver ejemplos de políticas AWS Supply Chain basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS Supply Chain

Políticas basadas en recursos dentro de AWS Supply Chain

Admite políticas basadas en recursos: no

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

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.

Acciones políticas para AWS Supply Chain

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.

Las acciones políticas AWS Supply Chain utilizan el siguiente prefijo antes de la acción:

```
scn
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "scn:action1",
      "scn:action2"
         ]
```

Para ver ejemplos de políticas AWS Supply Chain basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS Supply Chain

Recursos de políticas para AWS Supply Chain

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 ejemplos de políticas AWS Supply Chain basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS Supply Chain

Claves de condición de la política para AWS Supply Chain

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 ejemplos de políticas AWS Supply Chain basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS Supply Chain

Uso de credenciales temporales con AWS Supply Chain

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida información sobre cuáles 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 AWS Supply Chain

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWSél, se le 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 AWS Supply Chain

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 puede interrumpir AWS Supply Chain la funcionalidad. Edite las funciones de servicio solo cuando se AWS Supply Chain proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AWS Supply Chain

Compatibilidad con roles vinculados al servicio: no

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 obtener más información acerca de cómo crear o administrar roles vinculados a servicios, consulte 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.

Ejemplos de políticas basadas en identidades de AWS Supply Chain

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar AWS Supply Chain recursos. Tampoco pueden realizar tareas mediante la Consola de administración de AWS, la Interfaz de la línea de comandos de AWS (AWS CLI) o la API de AWS. 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 puede añadir las políticas de IAM a roles y los usuarios pueden 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 en la Guía del usuario de IAM.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS Supply Chain recursos de tu cuenta, acceder a ellos o eliminarlos. 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.

Solución de problemas de identidad y acceso AWS Supply Chain

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con un AWS Supply Chain IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AWS Supply Chain
- No estoy autorizado a realizar lo siguiente: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Supply Chain recursos

No estoy autorizado a realizar ninguna acción en AWS Supply Chain

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

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 `scn:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 scn:GetWidget on resource: my-example-widget
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-widget`* mediante la acción `scn:`*`GetWidget`*.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS Supply Chain.

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 realizar una acción en AWS Supply Chain. 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 mis AWS Supply Chain recursos

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 respaldan políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS Supply Chain es compatible con estas funciones, consulte. ¿Cómo AWS Supply Chain 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 usuario de su propiedad Cuenta de AWS en la 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.

AWS políticas gestionadas para AWS Supply Chain

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSSupply ChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess proporciona a los usuarios AWS Supply Chain federados acceso a la AWS Supply Chain aplicación, incluidos los permisos necesarios para realizar acciones dentro de la AWS Supply Chain aplicación. La política proporciona permisos administrativos a los usuarios y grupos del Centro de Identidad de IAM y está asociada a un rol creado AWS Supply Chain por usted. No debe adjuntar la AWSSupply ChainFederationAdminAccess política a ninguna otra entidad de IAM.

Si bien esta política proporciona todos los permisos de acceso AWS Supply Chain mediante los permisos scn: *, el AWS Supply Chain rol determina tus permisos. El AWS Supply Chain rol solo incluye los permisos necesarios y no tiene permisos de administrador APIs.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `Chime`— Proporciona acceso para crear o eliminar usuarios en Amazon Chime AppInstance; brinda acceso para administrar el canal, los miembros del canal y los moderadores; brinda acceso para enviar mensajes al canal. Las operaciones de Chime se centran en las instancias de aplicaciones etiquetadas con la palabra «ID». SCNInstance
- `AWS IAM Identity Center (AWS SSO)`— Proporciona los permisos necesarios para asociar y desasociar perfiles de usuario, enumerar las asociaciones de perfiles, enumerar las asignaciones de aplicaciones, describir la aplicación, describir la instancia y obtener la configuración de las asignaciones de aplicaciones en el IAM Identity Center.

- `AppFlow`: proporciona acceso para crear, actualizar y eliminar perfiles de conexión; proporciona acceso para crear, actualizar, eliminar, iniciar y detener flujos; proporciona acceso para etiquetar y desetiquetar flujos y describir registros de flujo.
- `Amazon S3`: proporciona acceso a una lista de todos los buckets. Proporciona GetBucketLocation, GetBucketPolicy PutObject GetObject, y ListBucket acceso a los depósitos con el recurso arn arn:aws:s3::: -*. aws-supply-chain-data
- `SecretsManager`: proporciona acceso a la creación de secretos y a la actualización de la política de secretos.
- `KMS`— Proporciona AppFlow al servicio Amazon el acceso a las claves de la lista y a los alias de las claves. Proporciona DescribeKey claves CreateGrant de ListGrants KMS etiquetadas con el valor clave-valor aws-suply-chain-access: true y permite crear secretos y actualizar la política de secretos.

  Los permisos (kms: ListKeys, kms: ListAliases, kms: GenerateDataKey y kms:Decrypt) no están restringidos a Amazon AppFlow y se pueden conceder a cualquier AWS KMS clave de tu cuenta.

Para ver los permisos de esta política, consulta la. AWSSupplyChainFederationAdminAccess AWS Management Console

AWS Supply Chain actualizaciones de las políticas AWS gestionadas

En la siguiente tabla se enumeran los detalles sobre las actualizaciones de las políticas AWS administradas AWS Supply Chain desde que este servicio comenzó a realizar un seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS Supply Chain documento.

Cambio	Descripción	Fecha
AWSSupplyChainFederationAdminAccess: política actualizada	AWS Supply Chain actualizó la política gestionada para permitir a los usuarios federados acceder a ListApplicationAssignments DescribeApplication DescribeInstance,	10 de diciembre de 2024

Cambio	Descripción	Fecha
	y a GetApplicationAssignmentConfiguration las operaciones del Centro de Identidad de IAM.	
AWSSupplyChainFederationAdminAccess: política actualizada	AWS Supply Chain actualizó la política gestionada para permitir a los usuarios federados acceder a ListProfileAssociations las operaciones del Centro de Identidad de IAM.	1 de noviembre de 2023
AWSSupplyChainFederationAdminAccess: política actualizada	AWS Supply Chain se actualizó la política gestionada para permitir a los usuarios federados acceder al depósito de S3 dedicado PutObject y a las GetObject operaciones del mismo con el recurso arn arn:aws:s3: ::aws-supply-chain-data-*.	21 de septiembre de 2023
AWSSupplyChainFederationAdminAccess: política nueva	AWS Supply Chain agregó una nueva política para permitir a los usuarios federados acceder a la aplicación. AWS Supply Chain Esto incluye los permisos necesarios para realizar acciones dentro de la aplicación AWS Supply Chain .	1 de marzo de 2023

Cambio	Descripción	Fecha
AWS Supply Chain comenzó a rastrear los cambios	AWS Supply Chain comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	1 de marzo de 2023

Validación de conformidad para AWS Supply Chain

Los auditores externos evalúan la seguridad y el cumplimiento AWS Supply Chain como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de Servicios de AWS los programas de cumplimiento específicos, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS los servicios incluidos . Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros con AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad en materia de cumplimiento cuando los AWS Supply Chain utiliza 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:

- Guías de inicio rápido de seguridad y conformidad : estas guías de implementación analizan consideraciones sobre arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS .
- Documento técnico sobre cómo diseñar una arquitectura basada en la seguridad y el cumplimiento de la HIPAA: en este documento técnico se describe cómo pueden utilizar las empresas para crear aplicaciones que cumplan con la HIPAA. AWS
- AWS Recursos de cumplimiento Recursos de de trabajo y guías puede aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config : evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.

- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interna AWS para ayudarle a comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Supply Chain

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente. Estas zonas están conectadas con redes con baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre Regiones de AWS las zonas de disponibilidad, consulte Infraestructura AWS global.

Además de la infraestructura AWS global, AWS Supply Chain ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos.

Registro y supervisión AWS Supply Chain

El registro y la supervisión son una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de la cadena de AWS suministro y del resto de sus AWS soluciones. AWS proporciona la herramienta de AWS CloudTrail monitoreo para vigilar la cadena de AWS suministro, informar cuando algo anda mal y tomar medidas automáticas cuando sea apropiado.

> **Note**
>
> APIs las llamadas solo desde la AWS Supply Chain consola se capturan AWS CloudTrail.

AWS CloudTrail captura las llamadas a la API y otros eventos relacionados que realiza la Cuenta de AWS o que se realizan en nombre de esta. Además, entrega los archivos de registro a un bucket de Amazon S3 especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que estas se realizaron. Puedes ver los eventos de la cadena AWS de suministro en scn.amazonaws.com. Para obtener más información, consulte la AWS CloudTrail Guía del usuario de .

> **Note**
>
> Tenga en cuenta lo siguiente con: AWS Supply Chain
>
> - Cuando invitas a usuarios que no tienen acceso a AWS Supply Chain ella, estos usuarios no reciben información en las notificaciones que reciben de la aplicación web. Los usuarios invitados reciben una notificación por correo electrónico con un enlace a la aplicación web. Solo pueden iniciar sesión y ver el contenido de la notificación si tienen los permisos de usuario necesarios.
> - Todos los usuarios con o sin permisos de usuario para una información de Insights concreta pueden ver los mensajes de chat de Insights.
> - Como administrador de la aplicación, cuando añada usuarios a la AWS Supply Chain instancia, estos tendrán acceso a AWS KMS key. Puede administrar los permisos de usuario para añadir o eliminar usuarios. Para obtener más información sobre los permisos de usuario, consulte Administrar las funciones de permisos de usuario.

AWS Supply Chain eventos de datos en CloudTrail

> **Note**
>
> Las aplicaciones web que AWS Supply Chain aplicación web APIs se APIs enumeran a continuación aparecen en los eventos de datos de CloudTrail.

Los eventos de datos proporcionan información sobre las operaciones de recursos realizadas en o dentro de un recurso (por ejemplo, leer o escribir en un objeto de Amazon S3). Se denominan también operaciones del plano de datos. Los eventos de datos suelen ser actividades de gran volumen. De forma predeterminada, CloudTrail no registra los eventos de datos. El historial de CloudTrail eventos no registra los eventos de datos.

Se aplican cargos adicionales a los eventos de datos. Para obtener más información sobre CloudTrail los precios, consulta AWS CloudTrail Precios.

Puede registrar eventos de datos para los tipos de AWS Supply Chain recursos mediante la CloudTrail consola o las operaciones de la CloudTrail API. AWS CLI

- Para registrar eventos de datos mediante la CloudTrail consola, cree un almacén de datos de rutas o eventos para registrar eventos de datos, o actualice un banco de datos de seguimiento o evento existente para registrar eventos de datos.

  1. Para registrar eventos de datos, elija Eventos de datos.
  2. En la lista Tipo de evento de datos, elija el tipo de recurso en el que desea registrar los eventos de datos.
  3. Elija la plantilla de selector de registro que desea usar. Puede registrar todos los eventos de datos del tipo de recurso, registre todos los eventos `readOnly`, registre todos los eventos `writeOnly` o cree una plantilla de selector de registro personalizada para filtrar por los campos `readOnly`, `eventName` y `resources.ARN`.

- Para registrar eventos de datos mediante el AWS CLI, configure el `--advanced-event-selectors` parámetro para que el `eventCategory` campo sea igual al valor del tipo de recurso `Data` y el `resources.type` campo igual al valor del tipo de recurso. Puede agregar condiciones para filtrar los valores de los campos `readOnly`, `eventName` y `resources.ARN`.
  - Para configurar una ruta para registrar eventos de datos, ejecute el put-event-selectorscomando Para obtener más información, consulte Registro de eventos de datos para registros de seguimiento en la AWS CLI.
  - Para configurar un almacén de datos de eventos para registrar eventos de datos, ejecute el create-event-data-storecomando para crear un nuevo banco de datos de eventos para registrar eventos de datos, o ejecute el update-event-data-storecomando para actualizar un banco de datos de eventos existente. Para obtener más información, consulte Registro de eventos de datos para almacenes de datos de eventos con la AWS CLI.

*Puede configurar selectores de eventos avanzados para filtrar según los campos `eventName`, `readOnly` y `resources.ARN` y así registrar solo los eventos que son importantes para usted. Para obtener más información sobre estos campos, consulte AdvancedFieldSelector.

AWS Supply Chain eventos de gestión en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se realizan en los recursos de su AWS cuenta. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

AWS Supply Chain registra todas las operaciones del plano de control CloudTrail como eventos de administración.

AWS Supply Chain aplicación web APIs

Las AWS Supply Chain aplicaciones que APIs aparecen en esta sección las invocan en nombre de los usuarios federados. No APIs están visibles en los CloudTrail registros y no se incluyen en el documento de referencia de autorización del servicio; consulte AWS Supply Chain. El acceso a ellos lo APIs controlan AWS Supply Chain las aplicaciones en función de los permisos de los roles de usuario federados. No debe intentar controlar el acceso a ellas APIs para evitar interrumpir las aplicaciones. AWS Supply Chain

Roles de usuario

APIs Los siguientes elementos se utilizan para administrar los usuarios, las funciones de los usuarios, las notificaciones de los usuarios y los mensajes de chat. AWS Supply Chain

```
scn:AddMembersToResourceBasedChat
scn:AssignGalaxyRoleToUser
scn:AssociateUser
scn:BatchGetUsers
scn:BatchMarkNotificationAsDelivered
scn:CreateRole
scn:DeleteRole
scn:DescribeChatForUser
scn:GetAccessDetailConfig
scn:GetChatPreferencesForUser
scn:GetMessagingSessionConnectionDetails
scn:GetNotificationsPreference
scn:GetOrCreateChimeUser
scn:GetOrCreateResourceBasedChat
scn:GetOrCreateUserBasedChat
scn:GetOrganizationInfo
scn:GetResourceBasedChatArn
scn:GetUserDetails
scn:ListChatMembers
scn:ListChatMessages
scn:ListChatModerators
scn:ListChats
scn:ListRoles
scn:ListUserNotifications
scn:ListUsersWithRole
scn:MarkNotificationAsDelivered
```

```
scn:MarkNotificationAsRead
scn:RemoveMemberFromResourceBasedChat
scn:RemoveUser
scn:SearchChimeUsers
scn:SearchUsers
scn:SendChatMessage
scn:SetNotificationsPreference
scn:UpdateChatPreferencesForUser
scn:UpdateChatReadMarker
scn:UpdateOrganizationInfo
scn:UpdateRole
scn:UpdateUser
```

Lago de datos

APIs Los siguientes se utilizan para crear y administrar flujos de datos y conexiones en el lago de datos.

```
scn:CreateConnection
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSapODataConnection
scn:CreateUpdateDatasetSchemaJob
scn:DeleteConnection
scn:DeleteDataflow
scn:DeleteExtractFlows
scn:DeleteSapODataConnection
scn:describeDatasetGroup
scn:DescribeDataset
scn:DescribeJob
scn:GetConnection
scn:GetCreateExtractFlowsStatus
scn:GetDataflow
scn:ListConnections
scn:ListCustomerFiles
scn:ListDataflows
```

```
scn:ListDataflowStats
scn:ListDatasets
scn:UpdateConnection
scn:UpdateDataflow
scn:UpdateExtractFlow
```

Información

La aplicación Insights utiliza lo siguiente APIs para gestionar los filtros, las listas de seguimiento y ver los cambios en el inventario.

```
scn:AddModeratorToResourceBasedChat
scn:ComputePostRebalancedQuantities
scn:ComputePostRebalancedQuantitiesV1
scn:CreateInsightFilter
scn:CreateInsightSubscription
scn:DeleteInsightFilter
scn:DeleteInsightSubscription
scn:GetInsightLineItem
scn:GetInsightSubscription
scn:GetInstanceAttribute
scn:GetInstanceRequiredDatasetAvailabilityStatus
scn:GetKpiData
scn:GetModelEndpointStatus
scn:GetPIVForProduct
scn:GetPIVForSite
scn:GetPIVForSiteAndProduct
scn:GetPIVForSitesAndProducts
scn:GetProducts
scn:GetProductSummaryAggregates
scn:GetSites
scn:GetSiteSummaryAggregates
scn:IsUserAuthorizedForInsightLineItem
scn:ListCustomAttributeValues
scn:ListGeographiesAsGalaxyAdmin
scn:ListInsightFilters
scn:ListInsightLineItems
scn:ListInsightSubscriptions
scn:ListInventoryQuantityAggregates
```

```
scn:ListInventoryRisksBySiteAndProduct
scn:ListInventorySummariesBySite
scn:ListPIVProductsBySite
scn:ListProductHierarchiesAsGalaxyAdmin
scn:ListProducts
scn:ListProductsAsGalaxyAdmin
scn:ListSites
scn:ListUsers
scn:PotentiallyComputeThenListRebalancingOptionsForInsightLineItem
scn:RegisterInstanceAttribute
scn:UpdateInsightFilter
scn:UpdateInsightLineItemStatus
scn:UpdateInsightSubscription
scn:UpdateRebalancingOptionStatus
scn:UpdateRebalancingOptionStatusV1
```

Planificación de la demanda

APIs Los siguientes elementos se utilizan AWS Supply Chain para crear y gestionar previsiones, planes de demanda o libros de trabajo.

```
scn:AssociateDatasetWithWorkbook
scn:CreateBaselineForecast
scn:CreateDemandPlan
scn:CreateDemandPlanningCycle
scn:CreateDemandPlanningDatasetExportJob
scn:CreateDerivedForecast
scn:CreateWorkbook
scn:DeleteDemandForecastConfig
scn:DeleteDemandPlanningCycle
scn:DeleteDerivedForecast
scn:DeleteWorkbook
scn:DescribeBaselineForecast
scn:DescribeDemandPlanningCycleAccuracyJob
scn:DescribeDerivedForecast
scn:DescribePlanningCycle
scn:DescribeWorkbook
scn:DisassociatePlanningCycle
scn:GetDemandForecastConfig
```

```
scn:GetDemandPlan
scn:GetDemandPlanningCycle
scn:GetDemandPlanningCycleAccuracy
scn:GetDemandPlanningDatasetJob
scn:ListDemandPlans
scn:ListDerivedForecasts
scn:ListForecastingJobs
scn:ListPlanningCycles
scn:ListWorkbooks
scn:PublishDemandPlan
scn:PutDemandForecastConfig
scn:StartDemandPlanningCycleAccuracyJob
scn:StartForecastingJob
scn:UpdateDemandPlan
scn:UpdateDemandPlanningCycleMetadata
scn:UpdateWorkbook
```

Planificación del suministro

APIs Los siguientes se utilizan AWS Supply Chain para crear y gestionar planes de suministro.

```
scn:CreateReplenishmentPipeline
scn:GetReplenishmentPipeline
scn:UpdateReplenishmentPipeline
scn:ListReplenishmentPipelinesByInstance
scn:GetInstanceReplenishmentConfig
scn:CreateBacktest
scn:CreateReplenishmentReviewInstanceConfig
scn:GetReplenishmentReviewInstanceConfig
scn:ListReplenishmentVendors
scn:GetExceptionsSupplyInsightsStatistics
scn:GetPorSupplyInsightsStatistics
scn:GetPlanToPOConversionAnalytics
scn:GetPurchasePlanStatistics
scn:ListPlanExceptions
scn:ListPurchaseOrderRequestLines
scn:UpdatePurchaseOrderRequestLines
scn:ListBomPurchasePlans
scn:ListBomProductionPlans
```

```
scn:ListBomTransferPlans
scn:ListBomInsights
scn:ListBomProcesses
scn:ExportBomPlans
scn:GetBomPlanSummary
scn:GetDashboardAnalytics
scn:GetPurchaseOrderRequestExplanation
scn:ListBomSupplyPlan
scn:GetBomPlanRecordDetails
scn:GetBomPlanSummaryAnalytics
scn:ListBomPurchaseOrders
scn:ListBomTransferOrders
scn:ListBomProductionOrders
scn:ExportAllExplodedBoms
scn:ExportBillOfMaterials
scn:ExportInventoryPolicy
scn:ExportProductionProcess
scn:ExportSourcingRule
scn:ExportTransportationLane
scn:ExportVendorLeadTime
scn:ImportBillOfMaterials
scn:ImportInventoryPolicy
scn:ImportProductionProcess
scn:ImportSourcingRule
scn:ImportTransportationLane
scn:ImportVendorLeadTime
```

Amazon Q en AWS Supply Chain

Lo siguiente APIs se utiliza en Amazon Q en AWS Supply Chain.

```
scn:GetQMessage
scn:ListQMessages
scn:PutQMessageFeedback
scn:SendQMessage
scn:GetQEnablementStatus
scn:UpdateQEnablementStatus
```

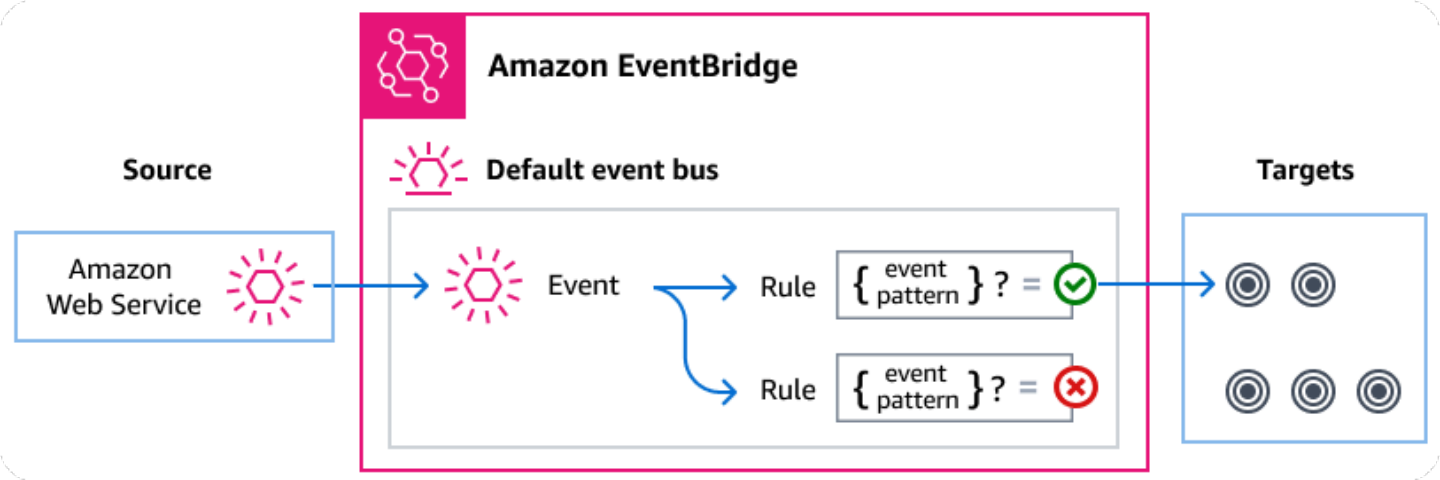
Gestión de AWS Supply Chain eventos mediante Amazon EventBridge

Con EventBridgeél, puede automatizar otros servicios para responder a los cambios en el estado de ejecución de un flujo de trabajo Step Functions estándar.

Amazon EventBridge es un servicio sin servidor que utiliza eventos para conectar los componentes de la aplicación, lo que facilita la creación de aplicaciones escalables basadas en eventos. La arquitectura basada en eventos es un estilo de creación de sistemas de software de acoplamiento flexible que funcionan juntos emitiendo eventos y respondiendo a ellos. Los eventos representan un cambio en un recurso o entorno.

Así es como funciona:

Como ocurre con muchos AWS servicios, AWS Supply Chain genera y envía eventos al bus de eventos EventBridge predeterminado. (El bus de eventos predeterminado se aprovisiona automáticamente en todas las AWS cuentas). Un bus de eventos es un enrutador que recibe eventos y los envía a cero o más destinos u objetivos. Las reglas que se especifican al bus de eventos evalúan los eventos a medida que llegan. Cada regla comprueba si un evento coincide con el patrón de evento de la regla. Si el evento coincide, el bus de eventos envía el evento a los destinos especificados.



Temas

- AWS Supply Chain eventos
- Entregar AWS Supply Chain eventos mediante reglas EventBridge
- AWS Supply Chain referencia detallada de eventos

AWS Supply Chain eventos

AWS Supply Chain envía automáticamente los siguientes eventos al bus de EventBridge eventos predeterminado. Los eventos que coinciden con el patrón de eventos de una regla se envían a los destinos especificados de forma periódica. Es posible que los eventos se entreguen fuera de servicio.

Para obtener más información, consulte Eventos de EventBridge en la Guía del usuario de Amazon EventBridge .

Tipo de detalle del evento	Descripción
Cambio de estado de integración de datos de la cadena de suministro de AWS	Muestra el estado de cada archivo ingerido. AWS Supply Chain

Entregar AWS Supply Chain eventos mediante reglas EventBridge

Para que el bus de eventos EventBridge predeterminado envíe AWS Supply Chain eventos a un destino, debe crear una regla. Cada regla contiene un patrón de eventos que EventBridge coincide con cada evento recibido en el bus de eventos. Si los datos del evento coinciden con el patrón de eventos especificado, EventBridge envía ese evento a los objetivos de la regla.

Para obtener instrucciones detalladas sobre cómo crear reglas de bus de eventos, consulte Creación de reglas que reaccionan a eventos en la Guía del usuario de EventBridge .

Crear un patrón de eventos que coincida con AWS Supply Chain los eventos

Cada patrón de eventos es un objeto JSON que contiene:

- Un atributo `source` que identifica el servicio que envía el evento. Para AWS Supply Chain los eventos, la fuente es`aws.supplychain`.
- (Opcional): un atributo `detail-type` que contiene una matriz de los tipos de eventos que deben coincidir.
- (Opcional): un atributo `detail` que contiene cualquier otro dato de evento con el que coincidir.

Por ejemplo, el siguiente patrón de eventos coincide con todos los `AWS Supply Chain Data Integration Status Change` eventos de AWS Supply Chain:

```
{
  "source": ["aws.supplychain"],
  "detail-type": ["AWS Supply Chain Data Integration Status Change"]
}
```

Para obtener más información sobre la escritura de los patrones de eventos, consulte Patrones de eventos en la Guía del usuario de EventBridge .

AWS Supply Chain referencia detallada de eventos

Todos los eventos de los AWS servicios tienen un conjunto común de campos que contienen metadatos sobre el evento, como el AWS servicio que es el origen del evento, la hora en que se generó el evento, la cuenta y la región en las que tuvo lugar el evento, etc. Para ver las definiciones de estos campos generales, consulte Referencia de estructura de eventos en la Guía del usuario de Amazon EventBridge .

Además, cada evento tiene un campo `detail` que contiene datos específicos de ese evento en particular. La siguiente referencia define los campos de detalle para los distintos eventos de AWS Supply Chain .

Cuando se utilice EventBridge para seleccionar y gestionar AWS Supply Chain eventos, es útil tener en cuenta lo siguiente:

- El `source` campo para todos los eventos de AWS Supply Chain está establecido en`aws.supplychain`.
- El campo `detail-type` especifica el tipo de evento.

  Por ejemplo, `AWS Supply Chain Data Integration Status Change`.
- El campo `detail` contiene los datos específicos de ese evento en particular.

Para obtener más información sobre cómo construir patrones de eventos que permitan que las reglas coincidan con los eventos de AWS Supply Chain , consulte Patrones de eventos en la Guía del usuario de Amazon EventBridge .

Para obtener más información sobre los eventos y cómo EventBridge los procesa, consulte Amazon EventBridge los eventos en la Guía del Amazon EventBridge usuario.

Cambio de estado de integración de datos de la cadena de suministro de AWS

A continuación se muestra un ejemplo del `AWS Supply Chain Data Integration Status Change event` evento.

```
{
    "version": "0",
    "id": "instanceID",
    "detail-type": "AWS Supply Chain Data Integration Status Change",
    "source": "aws.supplychain",
    "account": "acccountID",
    "time": "2024-03-30T12:26:13Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "version": "1.0",
        "instanceId": "instanceID",
        "flowArn": "arn:aws:scn:region:acccountID:instance/instanceID/data-integration-
flows/flowname",
        "flowExecutionId": "flowExecutionId",
        "status": "IN_PROGRESS",
        "startTime": "2024-03-30T12:26:13Z",
        "endTime": "",
        "message": "",
        "sourceType": "S3",
        "sourceInfo": {
            "s3Source": {
                "bucketName": "aws-supply-chain-data-instanceID",
                "key": "flowname"
            }
        }
    }
}
```

`endTime`solo está disponible cuando el estado es error o éxito.

Cuotas para AWS Supply Chain

Cuenta de AWS Tiene cuotas predeterminadas, antes denominadas límites, para cada una de ellas Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región. Puede solicitar un aumento de las cuotas de los recursos que estén configuradas en el nivel de su cuenta. Para obtener más información sobre las cuotas a nivel de cuenta, consulta la siguiente tabla.

Para ver las cuotas AWS Supply Chain, abra la consola Service Quotas. En el panel de navegación, elija servicios de AWS y seleccione AWS Supply Chain.

Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si la cuota aún no se encuentra disponible en Service Quotas, utilice el formulario de aumento del límite.

Cuenta de AWS Tiene las siguientes cuotas relacionadas con AWS Supply Chain.

Recurso	Predeterminado	Ajustable
Número de instancias **Note** Puede crear hasta 10 instancias en una AWS cuenta.	10	No
Número de buckets de Amazon S3	100	No
Invitaciones activas y pendientes en una cuenta AWS	30	Sí
Solicitudes de datos dentro de una AWS cuenta	4.000	Sí
Líneas de Insights por lista de seguimiento	1 000	No

Recurso	Predeterminado	Ajustable
Listas de seguimiento de Insights por instancia dentro de una cuenta AWS	1 000	Sí
Listas de seguimiento de Insights por usuario de una cuenta AWS	100	Sí
La integración de datos fluye por instancia dentro de una cuenta AWS	100	No
Espacios de nombres de conjuntos de datos personalizados por instancia dentro de una cuenta AWS	20	Sí
Conjuntos de datos por espacio de nombres de conjunto de datos personalizado por instancia dentro de una cuenta AWS	250	Sí
Conjuntos de datos en el espacio de nombres de conjunto de datos predeterminado por instancia dentro de una cuenta AWS	1 000	No

Preguntas frecuentes (FAQs)

La siguiente información puede ayudarle a solucionar problemas habituales relacionados con la activación del Centro de identidades de IAM.

Pregunta	Respuesta
¿Por qué es necesaria la integración del Centro de Identidad de IAM?	El centro de identidad de IAM es la función de IAM que gestiona la sincronización de las fuentes de identidad. El centro de identidad de IAM es la fuente de identidad de la instancia . AWS Supply Chain Debe configurar el IAM Identity Center para configurar la AWS consola y la aplicación AWS Supply Chain web. Para obtener más información sobre el Centro de Identidad de IAM, consulte Habilitar el Centro de Identidad de AWS IAM en la Guía del AWS IAM Identity Center usuario.
¿Para qué utilizar una instancia de organizac ión del IAM Identity Center? AWS Supply Chain	Al crear una instancia de organización, puede habilitar el acceso al Centro de Identidad de IAM en todas las AWS cuentas. Por ejemplo, si su centro de identidad de IAM no está habilitad o en la misma AWS cuenta que la cuenta de la AWS Supply Chain instancia. Para obtener más información sobre las ventajas de crear una instancia organizativa del IAM Identity Center, consulte Organizar las instancias del IAM Identity Center en la Guía del AWS IAM Identity Center usuario.
¿Para qué se necesitan los privilegios de administrador delegado? AWS Supply Chain	No es necesario tener un administrador delegado para utilizarlos, AWS Supply Chain pero se recomienda que la configuración de una AWS organización restrinja el acceso a la cuenta de administración de la organización y administre el Centro de Identidad de IAM. Para

Pregunta	Respuesta
	obtener más información, consulte Delegated adminsitrotor for Organizations. AWS . Al crear una instancia de organización, asegúrese de que la cuenta que se utilizará para crear una AWS Supply Chain instancia forme parte de la misma organización que la cuenta del IAM Identity Center. Asegúrese de que los permisos necesarios estén habilitados para crear una instancia y de que pueda crear una AWS Supply Chain instancia en la misma región que la cuenta del IAM Identity Center. Para obtener información sobre los permisos necesarios para crear una AWS Supply Chain instancia, consulteEmpezar con AWS Supply Chain.

AWS apoyo

Si es administrador y necesita ponerse en contacto con el servicio de asistencia AWS Supply Chain, elija una de las siguientes opciones:

- Si tiene una Soporte cuenta, vaya al Support Center y envíe un ticket.
- Abra la AWS Management Console y elija Cadena de suministro de AWS , Asistencia, Crear caso.

Es conveniente facilitar la siguiente información:

- El AWS ID/ARN de su instancia de cadena de suministro.
- Su región. AWS
- Una descripción detallada del problema.

Historial de documentos de la Guía AWS Supply Chain del administrador

En la siguiente tabla se describen las versiones de la documentación de AWS Supply Chain.

Cambio	Descripción	Fecha
AWS Supply Chain Cuotas actualizadas	Se actualizaron las cuotas de tu AWS cuenta relacionadas con AWS Supply Chain.	12 de mayo de 2025
Política AWS gestionada actualizada	AWS Supply Chain se actualizó la política gestionada para permitir a los usuarios federados acceder a ListApplicationAssignments DescribeApplication DescribeInstance, y a GetApplicationAssignmentConfiguration las operaciones del Centro de Identidad de IAM.	10 de diciembre de 2024
Actualización de la política de KMS	Se actualizó la política de KMS AWS Supply Chain para permitir el acceso a su AWS KMS clave.	18 de marzo de 2024
PrivateLink soporte	Puede acceder AWS Supply Chain mediante un punto final de interfaz (AWS PrivateLink).	26 de febrero de 2024
Adición de grupos	Los usuarios deben formar parte de un grupo del Centro de identidades de IAM para poder acceder a AWS Supply Chain.	14 de noviembre de 2023

Política AWS gestionada actualizada	AWS Supply Chain se actualizó la política gestionada para permitir a los usuarios federados acceder a ListProfileAssociations las operaciones del IAM Identity Center.	1 de noviembre de 2023
Política gestionada actualizada AWS	AWS Supply Chain actualizó la política administrada para permitir a los usuarios federados acceder al bucket dedicado de Amazon S3 PutObject y a las GetObject operaciones en él con el recurso arn arn:aws:s3: ::aws-supply- chain-data-*.	21 de septiembre de 2023
Información actualizada sobre la compatibilidad en las regiones	AWS Supply Chain La planificación de la demanda ahora también es compatible con la región de Asia Pacífico (Sídney).	12 de septiembre de 2023
Utilice AWS la consola para suscribirse y excluirse AWS Supply Chain	AWS Supply Chain los usuarios ahora pueden usar la AWS consola para suscribirse y AWS Supply Chain excluirse del uso o almacenamiento de su contenido en AWS Organizations.	7 de septiembre de 2023
Información actualizada sobre las regiones compatibles	AWS Supply Chain ahora también es compatible con la región de Asia Pacífico (Sídney) y la región de Europa (Irlanda).	19 de julio de 2023

Información actualizada sobre cómo ponerse en contacto con AWS Support y crear una instancia	AWS Supply Chain los usuarios ahora pueden ponerse en contacto con AWS Support para obtener ayuda y actualizar el contenido sobre cómo crear una instancia.	3 de abril de 2023
Se agregó una política AWS administrada	AWS Supply Chain agregó una nueva política para permitir a los usuarios federados acceder a la aplicación AWS Supply Chain, incluidos los permisos necesarios para realizar acciones dentro de la aplicació n AWS Supply Chain.	1 de marzo de 2023
Versión inicial	Versión inicial de la Guía del AWS Supply Chain administr ador.	29 de noviembre de 2022

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.