Guía del usuario

AWS IAM Identity Center

AWS IAM Identity Center: Guía del usuario

Table of Contents

¿Qué es IAM Identity Center?

AWS IAM Identity Center es el recomendado Servicio de AWS para gestionar el acceso de los usuarios humanos a AWS los recursos. Es un único lugar en el que puede asignar a los usuarios de su plantilla, que también se conocen como workforce identities, acceso uniforme a varias Cuentas de AWS y aplicaciones. El IAM Identity Center se ofrece sin coste adicional.

Con el IAM Identity Center, puede crear o conectar a los usuarios de la fuerza laboral y gestionar de forma centralizada su acceso a todas sus aplicaciones Cuentas de AWS . Puede utilizar permisos para varias cuentas para asignar a los usuarios de personal a Cuentas de AWS. Puede utilizar las asignaciones de aplicaciones para asignar a sus usuarios el acceso a las aplicaciones AWS gestionadas y gestionadas por los clientes.

> **Note**
>
> Aunque se ha retirado el nombre de servicio AWS Single Sign-On, el término inicio de sesión único se sigue utilizando en esta guía para describir el esquema de autenticación que permite a los usuarios iniciar sesión una vez para acceder a múltiples aplicaciones y sitios web.

Capacidades de IAM Identity Center

IAM Identity Center incluye las siguientes capacidades y características principales:

Administración de las identidades de la plantilla

Los usuarios humanos que crean u operan cargas de trabajo también AWS se conocen como usuarios de la fuerza laboral o identidades de la fuerza laboral. Los usuarios de la fuerza laboral son empleados o contratistas a los que usted permite acceder Cuentas de AWS en su organización y en las aplicaciones empresariales internas. Estas personas pueden ser desarrolladores que crean sus sistemas internos y orientados al cliente o usuarios de las aplicaciones y los sistemas de bases de datos internos. Puede crear usuarios y grupos de personal en el Centro de identidades de IAM o conectarse y sincronizarse con un conjunto de usuarios y grupos existente en su propia fuente de identidad para usarlos en todas sus aplicaciones Cuentas de AWS y en todas sus aplicaciones. Para obtener más información, consulte Administre su fuente de identidad.

Administración de instancias de IAM Identity Center

IAM Identity Center admite dos tipos de instancias: las instancias de organización y las instancias de cuenta. La práctica recomendada es usar una instancia de organización. Es la única instancia que le permite administrar el acceso a las aplicaciones Cuentas de AWS y se recomienda para todo uso de producción de las mismas. Se implementa una instancia de organización en la cuenta AWS Organizations de administración y proporciona un punto único desde el que administrar el acceso de los usuarios en todo el AWS entorno.

Las instancias de cuenta están vinculadas al lugar Cuenta de AWS en el que están habilitadas. Utilice las instancias de cuenta del IAM Identity Center únicamente para admitir despliegues aislados de determinadas aplicaciones AWS gestionadas. Para obtener más información, consulte Administración de las instancias de organización y cuenta de IAM Identity Center.

Gestione el acceso a múltiples Cuentas de AWS

Con los permisos para varias cuentas, puede planificar e implementar de forma centralizada los permisos Cuentas de AWS en varias cuentas a la vez sin necesidad de configurar cada una de sus cuentas manualmente. Puede crear permisos basados en funciones laborales habituales o definir permisos personalizados que se adapten a sus necesidades de seguridad. A continuación, puede asignar esos permisos a los usuarios de personal para controlar su acceso a cuentas específicas.

Esta característica opcional solo está disponible para las instancias de organización. Si utiliza la administración de roles de IAM por cuenta en su entorno, ambos sistemas pueden coexistir. Si quiere probar los permisos de varias cuentas, puede empezar por implementar este sistema de forma limitada y, con el tiempo, migrar cada vez una mayor parte de su entorno para utilizar este sistema.

Administración del acceso a las aplicaciones

IAM Identity Center le permite simplificar la administración del acceso a las aplicaciones. Con IAM Identity Center, puede conceder a los usuarios de la plantilla de IAM Identity Center acceso mediante inicio de sesión único a las aplicaciones.

AWS aplicaciones gestionadas

AWS proporciona aplicaciones como Amazon Redshift Amazon Managed Grafana y Amazon Monitron, que se integran con IAM Identity Center. Estas aplicaciones pueden utilizar IAM Identity Center para la autenticación, los servicios de directorio y la propagación de identidades de confianza. Los usuarios se benefician de una experiencia uniforme de inicio de sesión único y, como las aplicaciones comparten una visión común de los usuarios, los

grupos y la pertenencia a los grupos, los usuarios también tienen una experiencia uniforme al compartir los recursos de la aplicación con otros. Puede configurar las aplicaciones AWS gestionadas para que funcionen con el IAM Identity Center directamente desde las consolas de aplicaciones correspondientes o mediante las API.

Aplicaciones administradas por el cliente

Puede conceder a los usuarios de la plantilla de IAM Identity Center acceso mediante inicio de sesión único a las aplicaciones compatibles con la federación de identidades con SAML 2.0. Muchas de las aplicaciones de SAML 2.0 más utilizadas, como Salesforce y Microsoft 365, funcionan con IAM Identity Center y están disponibles en el catálogo de aplicaciones de la consola de IAM Identity Center. Se trata de una característica opcional que puede resultar útil si utiliza este tipo de aplicaciones y crea sus usuarios y grupos en IAM Identity Center o si utiliza Microsoft Active Directory Domain Services como origen de identidad.

Propagación de identidad de confianza en aplicaciones

La propagación de identidades fiable proporciona una experiencia de inicio de sesión único optimizada para los usuarios de herramientas de consulta y aplicaciones de inteligencia empresarial (BI) que necesitan acceder a los datos de los servicios. AWS La administración del acceso a los datos se basa en la identidad del usuario, por lo que los administradores pueden conceder el acceso en función de la pertenencia actual de los usuarios a grupos y usuarios. El acceso de los usuarios a AWS los servicios y otros eventos se registra en registros y eventos específicos del servicio, de modo que CloudTrail los auditores sepan qué acciones han realizado los usuarios y a qué recursos han accedido.

AWS acceda al portal para sus usuarios

El portal de AWS acceso es un portal web sencillo que proporciona a sus usuarios un acceso perfecto a todas sus aplicaciones Cuentas de AWS y aplicaciones asignadas.

Cambio de nombre de IAM Identity Center

El 26 de julio de 2022, se cambió el nombre de AWS Single Sign-On a. AWS IAM Identity Center Para los clientes actuales, la siguiente tabla pretende describir algunos de los cambios de términos más comunes que se han actualizado en esta guía como consecuencia del cambio de nombre.

Término antiguo	Término actual
AWS Usuario de SSO o usuario de SSO	usuario de personal o usuario

Término antiguo	Término actual
AWS Portal de usuario o portal de usuario de SSO	AWS portal de acceso
AWS Aplicaciones integradas en SSO	AWS aplicaciones gestionadas
AWS directorio SSO	Directorio de Identity Center
AWS Almacén de SSO o almacén de identidad es de AWS SSO	Almacén de identidades utilizado de IAM Identity Center

En la siguiente tabla se describen los cambios aplicables en las guías de referencia de usuarios, desarrolladores y de API que también se produjeron como resultado de este cambio de nombre.

Guía anterior	Guía actual
AWS Guía del usuario de inicio de sesión único	Guía del usuario de IAM Identity Center
AWS Guía para desarrolladores de implement ación de SCIM con inicio de sesión único	Guía para desarrolladores de implementación de IAM Identity Center SCIM
AWS Guía de referencia de la API de inicio de sesión único	Referencia de IAM Identity Center API
AWS Guía de referencia de la API de Single Sign-On Identity Store	Referencia de Identity Store API
AWS Guía de referencia de la API OIDC de inicio de sesión único	Referencia de IAM Identity Center OIDC API
AWS Guía de referencia de la API del portal de inicio de sesión único	Referencia de IAM Identity Center Portal API

Los espacios de nombres antiguos siguen siendo los mismos

Los espacios de nombres de `sso` y `identitystore` API, junto con los siguientes espacios de nombres relacionados, permanecen sin cambios por motivos de compatibilidad con versiones anteriores.

- Comandos de la CLI
  - `aws configure sso`
  - `identitystore`
  - `sso`
  - `sso-admin`
  - `sso-oidc`
- Políticas administradas que contienen prefijos de `AWSSSO` y `AWSIdentitySync`
- Puntos de conexión de servicio que contienen `sso` e `identitystore`
- Recursos de AWS CloudFormation contienen prefijos de `AWS::SSO`
- Rol vinculado al servicio que contiene `AWSServiceRoleForSSO`
- URL de consola que contienen `sso` y `singlesignon`
- URL de documentación que contienen `singlesignon`

Habilitar AWS IAM Identity Center

Complete los siguientes pasos para iniciar sesión en la instancia de organización de IAM Identity Center AWS Management Console y habilitarla.

1. Realice una de estas 2 operaciones para iniciar sesión en la AWS Management Console.
   - Nuevo para AWS (usuario root): inicie sesión como propietario de la cuenta; para ello, seleccione Root user e introduzca su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
   - Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
2. Abra la consola de IAM Identity Center
3. En Habilitar IAM Identity Center, seleccione Habilitar con AWS Organizations.
4. Opcional: agregue las etiquetas que desee asociar a esta instancia de organización.
5. Opcional: configure la administración delegada.

> **Note**
>
> Si utiliza un entorno de varias cuentas, le recomendamos que configure la administración delegada. Con la administración delegada, puede limitar el número de personas que necesitan acceder a la cuenta de administración en AWS Organizations. Para obtener más información, consulte Administración delegada.

> **Important**
>
> La capacidad de crear instancias de cuenta de IAM Identity Center está habilitada de forma predeterminada. Las instancias de cuenta de IAM Identity Center incluyen un subconjunto de características disponibles para una instancia de organización. Puede controlar si los usuarios pueden acceder a esta característica mediante una política de control de servicios.

¿Necesita actualizar los firewalls y las puertas de enlace?

Si filtra el acceso a AWS dominios o puntos de enlace de URL específicos mediante una solución de filtrado de contenido web, como firewalls de última generación (NGFW) o Secure Web Gateways (SWG), debe añadir los siguientes dominios o puntos de enlace de URL a las listas de permisos de la solución de filtrado de contenido web. Si lo hace, podrá acceder a su portal de acceso. AWS

- *[Directory ID or alias]*.awsapps.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

Consideraciones para permitir la publicación de dominios y puntos de enlace de URL

Comprenda el impacto de permitir la inclusión de dominios fuera AWS del portal de acceso.

- Para acceder Cuentas de AWS a la AWS Management Console consola del IAM Identity Center y a ella desde su portal de AWS acceso, debe permitir incluir dominios adicionales en la lista. Consulte Solución de problemas en la Guía de introducción para AWS Management Console obtener una lista de AWS Management Console dominios.
- Para acceder a las aplicaciones AWS gestionadas desde su portal de AWS acceso, debe permitir incluir sus dominios respectivos en una lista. Consulte la documentación de servicio correspondiente para obtener orientación.
- Estas listas de permisos cubren AWS los servicios. Si utilizas software externo, como el externo IdPs (por ejemplo, Okta yMicrosoft Entra ID), tendrás que incluir sus dominios en tus listas de permisos.

Ya tiene todo listo para configurar IAM Identity Center. Cuando habilita IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como origen de identidad predeterminado, que es la forma más rápida de empezar a usar IAM Identity Center. Para ver instrucciones, consulte Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center.

Si desea obtener más información sobre cómo funciona IAM Identity Center con Organizations, los orígenes de identidad y los roles de IAM, consulte los siguientes temas.

Temas

Requisitos y consideraciones previos

Los siguientes temas proporcionan información acerca de los requisitos previos y otras consideraciones para configurar IAM Identity Center.

Consideraciones a la hora de elegir un Región de AWS

Puede habilitar una instancia del IAM Identity Center en una sola instancia, compatible con Región de AWS las que prefiera. La elección de una región requiere una evaluación de sus prioridades en función de los casos de uso y las políticas de la empresa. El acceso a las aplicaciones en la nube Cuentas de AWS y a las aplicaciones en la nube desde su centro de identidad de IAM no depende de esta elección; sin embargo, el acceso a las aplicaciones AWS gestionadas y la posibilidad de utilizarlas AWS Managed Microsoft AD como fuente de identidad pueden depender de esta elección. Consulte los puntos finales y las cuotas del Centro de Identidad de AWS IAM en la Referencia general de AWS lista de regiones compatibles con el Centro de Identidad de IAM.

Consideraciones clave para elegir un. Región de AWS

- Ubicación geográfica: si selecciona una región que esté geográficamente más cercana a la mayoría de sus usuarios finales, estos tendrán una latencia de acceso más baja al portal de AWS acceso y a las aplicaciones AWS gestionadas, como Amazon SageMaker Studio.
- Disponibilidad de las aplicaciones AWS AWS administradas: las aplicaciones administradas, como Amazon SageMaker, solo pueden funcionar en las aplicaciones Regiones de AWS que admiten. Habilite el Centro de Identidad de IAM en una región compatible con las aplicaciones

AWS administradas que desee utilizar con él. Muchas aplicaciones AWS gestionadas también pueden funcionar solo en la misma región en la que habilitó el Centro de identidad de IAM.

- Soberanía digital: las normas de soberanía digital o las políticas de la empresa pueden exigir el uso de una determinada Región de AWS. Consulte con el departamento legal de su empresa.
- Fuente de identidad: si utiliza AWS Managed Microsoft AD AD Connector como fuente de identidad, su región de origen debe coincidir con la región Región de AWS en la que habilitó el Centro de identidad de IAM.
- Regiones deshabilitadas de forma predeterminada: AWS originalmente estaban habilitadas todas las nuevas Regiones de AWS para su uso de forma Cuentas de AWS predeterminada, lo que permitía automáticamente a los usuarios crear recursos en cualquier región. Ahora, cuando se AWS añade una nueva región, su uso está deshabilitado de forma predeterminada en todas las cuentas. Si despliega el Centro de identidad de IAM en una región deshabilitada de forma predeterminada, debe habilitar esta región en todas las cuentas para las que desee gestionar el acceso al Centro de identidades de IAM. Esto es obligatorio incluso si no tiene previsto crear ningún recurso en esa región en esas cuentas.

  Puede habilitar una región para las cuentas corrientes de su organización y debe repetir esta acción para las cuentas nuevas que pueda agregar más adelante. Para obtener instrucciones, consulte Habilitar o deshabilitar una región de su organización en la guía del AWS Organizations usuario. Para evitar repetir estos pasos adicionales, puede optar por implementar su centro de identidad de IAM en una región habilitada de forma predeterminada. Como referencia, las siguientes regiones están habilitadas de forma predeterminada:

  - US East (Ohio)
  - Este de EE. UU. (Norte de Virginia)
  - Oeste de EE. UU. (Oregón)
  - Oeste de EE. UU. (Norte de California)
  - Europa (París)
  - América del Sur (São Paulo)
  - Asia-Pacífico (Bombay)
  - Europa (Estocolmo)
  - Asia-Pacífico (Seúl)
  - Asia-Pacífico (Tokio)
  - Europa (Irlanda)
  - Europa (Fráncfort)

- Europa (Londres)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Canadá (centro)
- Asia-Pacífico (Osaka)

- Llamadas entre regiones: en algunas regiones, el Centro de Identidad de IAM puede llamar al Amazon Simple Email Service de una región diferente para enviar correos electrónicos. En estas llamadas entre regiones, el Centro de Identidad de IAM envía determinados atributos de usuario a la otra región. Para obtener más información acerca de las regiones, consulte AWS IAM Identity Center Disponibilidad regional.

Conmutación Regiones de AWS

Para cambiar de región del centro de identidad de IAM, solo tiene que eliminar la instancia actual y crear una nueva en otra región. Si ya ha activado una aplicación AWS gestionada con su instancia actual, debe eliminarla antes de eliminar su centro de identidad de IAM. Debe volver a crear los usuarios, los grupos, los conjuntos de permisos, las aplicaciones y las asignaciones en la nueva instancia. Puede utilizar las API de asignación de cuentas y aplicaciones del IAM Identity Center para obtener una instantánea de la configuración y, a continuación, utilizarla para volver a crear la configuración en una nueva región. Es posible que también necesite volver a crear alguna configuración del IAM Identity Center a través de la consola de administración de la nueva instancia. Para obtener instrucciones sobre cómo eliminar el Centro de identidades de IAM, consulte. Eliminación de la configuración de IAM Identity Center

Cuota de funciones de IAM creadas por el Centro de Identidad de IAM

IAM Identity Center crea roles de IAM para conceder a los usuarios permisos de acceso a los recursos. Cuando asigna un conjunto de permisos, IAM Identity Center crea los roles de IAM controlados por IAM Identity Center correspondientes en cada cuenta y adjunta a esos roles las políticas especificadas en el conjunto de permisos. El Centro de Identidad de IAM gestiona la función y permite que los usuarios autorizados que haya definido la asuman mediante el portal de acceso o. AWS AWS CLI A medida que modifica el conjunto de permisos, IAM Identity Center garantiza que las políticas y los roles de IAM correspondientes se actualicen en consecuencia.

Si ya has configurado tus funciones de IAM Cuenta de AWS, te recomendamos que compruebes si tu cuenta se acerca a la cuota de funciones de IAM. La cuota predeterminada de roles de IAM por cuenta es de 1000 roles. Para obtener más información, consulte Cuotas de objetos de IAM.

Si se acerca a la cuota, considere solicitar un aumento de la cuota. De lo contrario, es posible que tenga problemas con IAM Identity Center al aprovisionar conjuntos de permisos a cuentas que hayan superado la cuota de roles de IAM. Para obtener información sobre cómo solicitar un aumento de cuota, consulte Solicitar un aumento de cuota en la Guía del usuario de Service Quotas.

> **Note**
>
> Si quiere revisar los roles de IAM en una cuenta que ya utiliza IAM Identity Center, es posible que observe que los nombres de rol comienzan por “AWSReservedSSO_”. Se trata de los roles que el servicio de IAM Identity Center ha creado en la cuenta y provienen de la asignación de un conjunto de permisos a la cuenta.

Centro de identidad de IAM y AWS Organizations

AWS Organizations se recomienda, pero no es obligatorio, para su uso con el Centro de identidades de IAM. Si no ha creado una organización, no tiene que hacerlo. Al activar el Centro de Identidad de IAM, elegirá si desea habilitar el servicio con. AWS Organizations Al configurar una organización, la cuenta Cuenta de AWS que la configura se convierte en la cuenta de administración de la organización. El usuario raíz de la Cuenta de AWS es ahora el propietario de la cuenta de administración de la organización. Todas las cuentas adicionales Cuentas de AWS que invite a su organización son cuentas de miembros. La cuenta de administración crea los recursos, las unidades organizativas y las políticas de la organización que administran las cuentas de miembro. La cuenta de administración delega los permisos a las cuentas de miembro.

> **Note**
>
> Le recomendamos que habilite el Centro de Identidad de IAM con AWS Organizations, lo que crea una instancia organizativa del Centro de Identidad de IAM. Nuestra práctica recomendada es una instancia de organización, ya que es compatible con todas las características de IAM Identity Center y proporciona capacidades de administración centralizada. Para obtener más información, consulte Administración de las instancias de organización y cuenta de IAM Identity Center.

Si ya ha configurado el Centro de Identidad de IAM AWS Organizations y lo va a añadir a su organización, asegúrese de que todas las AWS Organizations funciones estén habilitadas. Al crear una organización, las características se habilitan de manera predeterminada. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations .

Para habilitar el Centro de identidades de IAM, debe iniciar sesión en su cuenta de AWS Organizations administración como usuario con credenciales administrativas o como usuario raíz (no se recomienda a menos que no existan otros usuarios administrativos). AWS Management Console No puede activar el Centro de identidades de IAM si ha iniciado sesión con las credenciales administrativas de una cuenta de AWS Organizations miembro. Para obtener más información, consulte Creación y gestión de una AWS organización en la Guía del AWS Organizations usuario.

Confirme sus fuentes de identidad en el Centro de identidades de IAM

Su origen de identidad en IAM Identity Center define dónde se administran sus usuarios y grupos. Después de habilitar IAM Identity Center, asegúrese de que utiliza el origen de identidad que eligió.

Confirmación del origen de identidad

1. Abra la consola de IAM Identity Center
2. En la página del panel de control, debajo de la sección Pasos de configuración recomendados, selecciona Confirma tu fuente de identidad. Para acceder a esta página, también puede seleccionar Configuración y la pestaña Origen de identidad.
3. No tiene que realizar ninguna acción si desea conservar el origen de identidad asignado. Si prefiere cambiarlo, seleccione Acciones y, a continuación, seleccione Cambiar el origen de identidad.

   Puede elegir una de las siguientes opciones como origen de identidad:

   Directorio de Identity Center

   Cuando se habilita IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como origen de identidad predeterminado. Si aún no utiliza otro proveedor de identidades externo, puede comenzar a crear sus usuarios y grupos y asignar su nivel de acceso a sus Cuentas de AWS y aplicaciones. Para ver un tutorial sobre

el uso de este origen de identidad, consulte Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center.

Active Directory

Si ya está gestionando usuarios y grupos en su AWS Managed Microsoft AD directorio mediante AWS Directory Service o en su directorio autogestionadoActive Directory (AD), le recomendamos que conecte ese directorio cuando active IAM Identity Center. No cree ningún usuario ni grupo en el directorio predeterminado de Identity Center. El Centro de identidades de IAM utiliza la conexión proporcionada por el AWS Directory Service para sincronizar la información de usuarios, grupos y miembros del directorio de origen de Active Directory con el almacén de identidades del Centro de identidades de IAM. Para obtener más información, consulte Conexión un directorio Microsoft AD.

> **Note**
>
> IAM Identity Center no admite Simple AD basado en SAMBA4 como origen de identidad.

Proveedor de identidades externo

Para los proveedores de identidad externos (IdPs), como Okta oMicrosoft Entra ID, puede utilizar el Centro de identidades de IAM para autenticar las identidades IdPs mediante el estándar del lenguaje de marcado de aserciones de seguridad (SAML) 2.0. El protocolo SAML no proporciona ninguna forma de consultar al IdP para obtener información sobre los usuarios y los grupos. Debe hacer que IAM Identity Center conozca a esos usuarios y grupos aprovisionándolos en IAM Identity Center. Puede realizar el aprovisionamiento automático (sincronización) de la información de usuarios y grupos desde su IdP a IAM Identity Center mediante el protocolo del sistema de administración de identidades entre dominios (SCIM) v2.0 si su IdP admite SCIM. De lo contrario, puede aprovisionar manualmente los usuarios y grupos; para ello, ingrese manualmente los nombres de usuario, la dirección de correo electrónico y los grupos en IAM Identity Center.

Para obtener instrucciones detalladas sobre cómo configurar su fuente de identidad, consulte. Tutoriales de introducción

> **Note**
>
> Si tiene previsto utilizar un proveedor de identidades externo, tenga en cuenta que el IdP externo, no IAM Identity Center, administra la configuración de la autenticación multifactor (MFA). El uso de MFA en IAM Identity Center no es compatible con dispositivos externos. IdPs Para obtener más información, consulte Solicitar MFA a los usuarios.

El origen de identidad que elija determina dónde busca IAM Identity Center los usuarios y grupos que necesitan acceso con inicio de sesión único. Tras confirmar o cambiar el origen de identidad, creará o especificará un usuario y le asignará permisos administrativos a su Cuenta de AWS.

> **Important**
>
> Si ya administra usuarios y grupos en Active Directory o en un proveedor de identidades (IdP) externo, le recomendamos que considere la posibilidad de conectar esta fuente de identidad al habilitar IAM Identity Center y elegir su fuente de identidad. Esto debe hacerse antes de crear usuarios y grupos en el directorio predeterminado de Identity Center y de realizar cualquier asignación.
>
> Si ya administra usuarios y grupos en una fuente de identidad en IAM Identity Center, cambiar a una fuente de identidad diferente podría eliminar todas las asignaciones de usuarios y grupos que configuró en IAM Identity Center. Si esto ocurre, todos los usuarios, incluido el usuario administrativo del IAM Identity Center, perderán el acceso de inicio de sesión único a sus aplicaciones. Cuentas de AWS Para obtener más información, consulte Consideraciones para cambiar la fuente de identidad.

Tras configurar la fuente de identidad, puede buscar usuarios o grupos para concederles acceso mediante un inicio de sesión único Cuentas de AWS, a las aplicaciones en la nube o a ambas opciones.

Tutoriales de introducción

Puede tener un origen de identidad por organización, por lo que es importante dedicar tiempo a probar las capacidades de cada uno de ellos.

En esta sección, puede elegir uno de los siguientes tutoriales para configurar IAM Identity Center con su origen de identidad preferido, crear un usuario administrativo y configurar conjuntos de permisos para que sus usuarios accedan a los recursos.

Antes de iniciar cualquiera de estos tutoriales, active IAM Identity Center. Para obtener más información, consulte Habilitar AWS IAM Identity Center.

Temas

- Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center
- Uso de Active Directory como origen de identidad
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- Configuración de SAML y SCIM con Google Workspace e IAM Identity Center
- Uso de IAM Identity Center para conectarse a su plataforma de directorios de JumpCloud
- Configuración de SAML y SCIM con Microsoft Entra ID e IAM Identity Center
- Configuración de SAML y SCIM con Okta e IAM Identity Center
- Configuración del aprovisionamiento de SCIM entre OneLogin e IAM Identity Center
- Uso de productos de Ping Identity con IAM Identity Center

Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center

Cuando se habilita IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como origen de identidad predeterminado, así que no tiene que seleccionar uno. Si su organización utiliza otro proveedor de identidad, por ejemplo AWS Directory Service for Microsoft Active DirectoryMicrosoft Entra ID, o si Okta considera la posibilidad de integrar esa fuente de identidad con el Centro de identidades de IAM en lugar de utilizar la configuración predeterminada.

Objetivo

En este tutorial, utilizará el directorio predeterminado como origen de identidad y configurará y probará el acceso de los usuarios. En este escenario, administrará todos los usuarios y grupos en IAM Identity Center. Los usuarios inician sesión a través del portal de AWS acceso. Este tutorial está dirigido a usuarios nuevos AWS o que han estado utilizando IAM para administrar usuarios y grupos. En los siguientes pasos, creará lo siguiente:

- Un usuario administrativo llamado *Nikki Wolf*.
- Un grupo llamado *Equipo de administración*.
- Un conjunto de permisos denominado *AdminAccess*

Para comprobar que todo se ha creado correctamente, debe iniciar sesión y establecer la contraseña del usuario administrativo. Tras completar este tutorial, puede utilizar el usuario administrativo para agregar más usuarios a IAM Identity Center, crear conjuntos de permisos adicionales y configurar el acceso organizativo a las aplicaciones.

Si aún no ha habilitado IAM Identity Center, consulte Habilitar AWS IAM Identity Center.

Antes de empezar

Realice una de estas 2 operaciones para iniciar sesión en la AWS Management Console.

- Nuevo para AWS (usuario root): inicia sesión como propietario de la cuenta; para ello, selecciona el usuario Cuenta de AWS root e introduce tu dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
- Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.

Abra la consola de IAM Identity Center

Paso 1: adición de un usuario

1. En el panel de navegación de IAM Identity Center, seleccione Usuarios y, a continuación, seleccione Agregar usuario.
2. En la página Especificar los detalles del usuario, rellene la siguiente información:
   - Nombre de usuario: para este tutorial, ingrese *nikkiw*.

Al crear los usuarios, seleccione nombres de usuario que sean fáciles de recordar. Sus usuarios deben recordar el nombre de usuario para iniciar sesión en el portal de acceso de AWS y no podrá cambiarlo más adelante.

- Contraseña: seleccione Enviar un correo electrónico a este usuario con las instrucciones de configuración de la contraseña (recomendado).

  Esta opción envía al usuario una dirección de correo electrónico de Amazon Web Services, con el asunto Invitación a unirse al IAM Identity Center (sucesor de AWS Single Sign-On). El correo electrónico proviene de `no-reply@signin.aws` o `no-reply@login.awsapps.com`. Agregue estas direcciones de correo electrónico a su lista de remitentes aprobados.
- Dirección de correo electrónico: ingrese una dirección de correo electrónico del usuario en la que pueda recibir el correo electrónico. A continuación, vuelva a escribirla para confirmarla. Cada usuario debe tener una dirección de correo electrónico única.
- En Nombre, ingrese el nombre del usuario. Para este tutorial, ingrese *`Nikki`*.
- En Apellido, ingrese el apellido del usuario. Para este tutorial, ingrese *`Wolf`*.
- Nombre de visualización: el valor predeterminado es el nombre y apellido del usuario. Si desea cambiar el nombre de visualización, puede ingresar otro nombre. El nombre de visualización está visible en el portal de inicio de sesión y en la lista de usuarios.
- Complete la información opcional si lo desea. No se usa durante este tutorial y puede cambiarla más adelante.

3. Elija Siguiente. Aparece la página Agregar usuario a grupos. Vamos a crear un grupo al que asignarle permisos administrativos en lugar de dárselos directamente a *`Nikki`*.

   Seleccione Crear grupo.

   Se abre una nueva pestaña del navegador para mostrar la página Crear grupo.

   a. En Detalles del grupo, en Nombre del grupo, ingrese un nombre para el grupo. Recomendamos un nombre de grupo que identifique el rol del grupo. Para este tutorial, ingrese *`Equipo de administración`*.

   b. Seleccione Crear grupo.

   c. Cierre la pestaña Grupos del navegador para volver a la pestaña Agregar usuario del navegador.

4. En el área Grupos, seleccione el botón Actualizar. El grupo *Equipo de administración* aparece en la lista.

   Seleccione la casilla de verificación situada junto al ***equipo de administración*** y, a continuación, seleccione Siguiente.

5. En la página Revisar y agregar usuario, confirme lo siguiente:

   - La información principal aparece tal y como quería.
   - En Grupos se muestra el usuario agregado al grupo que ha creado

   Si desea realizar cambios, seleccione Editar. Cuando todos los detalles sean correctos, seleccione Agregar usuario.

   Un mensaje de notificación le informará de que se ha agregado el usuario.

A continuación, agregará permisos administrativos para el grupo *Equipo de administración* para que *Nikki* tenga acceso a los recursos.

Paso 2: adición de permisos administrativos

1. En el panel de navegación del IAM Identity Center, en Permisos para varias cuentas, seleccione Cuentas de AWS.
2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la organización con las cuentas situadas por debajo de ella en la jerarquía. Selecciona la casilla de verificación de tu cuenta de administración y, a continuación, selecciona Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:

   a. En Paso 1: selección de usuarios y grupos, seleccione el grupo *Equipo de administración* que creó. A continuación, elija Next.

   b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.

      i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:

         - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.

- En Política para un conjunto de permisos predefinido, selecciona AdministratorAccess.

Elija Siguiente.

ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

La configuración predeterminada crea un conjunto de permisos denominado *AdministratorAccess*con una duración de sesión establecida en una hora. Puede cambiar el nombre del conjunto de permisos introduciendo un nombre nuevo en el campo Nombre del conjunto de permisos.

iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.

En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.

En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de *AdministratorAccess*permisos que ha creado aparece en la lista. Seleccione la casilla de verificación de ese conjunto de permisos y, a continuación, elija Siguiente.

c. En la página Paso 3: Revisar y enviar las tareas, confirme que el grupo del *equipo de administración* esté seleccionado y que el conjunto de *AdministratorAccess*permisos esté seleccionado y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Volverá a la Cuentas de AWS página. Un mensaje de notificación le informa de que se Cuenta de AWS ha vuelto a aprovisionar y se ha aplicado el conjunto de permisos actualizado.

> ¡Enhorabuena!
>
> Ha configurado correctamente su primer usuario, grupo y conjunto de permisos.

En la siguiente parte de este tutorial, probarás el acceso *de Nikki* iniciando sesión en el portal de AWS acceso con sus credenciales administrativas y configurando su contraseña. Cierre la sesión de la consola.

Paso 3: Probar el acceso de los usuarios

Ahora que *Nikki Wolf* es un usuario de su organización, puede iniciar sesión y acceder a los recursos para los que tiene permiso de acuerdo con su conjunto de permisos. Para comprobar que el usuario está correctamente configurado, en el siguiente paso utilizará las credenciales de *Nikki* para iniciar sesión y configurar su contraseña. Cuando agregó al usuario *Nikki Wolf* en el paso 1, eligió que *Nikki* recibiera un correo electrónico con las instrucciones para configurar la contraseña. Es hora de abrir el correo electrónico y hacer lo siguiente:

1. En el correo electrónico, seleccione el enlace Aceptar la invitación para aceptar la invitación.

   > Note
   >
   > En el correo electrónico también se incluyen el nombre de usuario de *Nikki* y la URL del portal de acceso de AWS que utilizará para iniciar sesión en la organización. Registre esta información para usarla más adelante.

   Accederá a la página Inscríbase a un nuevo usuario, donde podrá configurar la contraseña de *Nikki*.
2. Después de configurar la contraseña de *Nikki*, accederá a la página Inicio de sesión. Ingrese *nikkiw*, seleccione Siguiente y, a continuación, ingrese la contraseña de *Nikki* y seleccione Iniciar sesión.
3. Se abre el portal de AWS acceso y muestra la organización y las aplicaciones a las que puede acceder.

   Seleccione la organización para ampliarla en una lista y, a Cuentas de AWS continuación, seleccione la cuenta para ver las funciones que puede utilizar para acceder a los recursos de la cuenta.

Cada conjunto de permisos tiene dos métodos de administración que puede utilizar: el rol o las claves de acceso.

- Rol, por ejemplo *AdministratorAccess*: abre el AWS Console Home.
- Claves de acceso: proporcionan credenciales que puede usar con el AWS CLI o y el AWS SDK. Incluye la información para usar credenciales de corta duración que se actualizan automáticamente o claves de acceso de corta duración. Para obtener más información, consulte Obtener las credenciales de usuario del IAM Identity Center para el AWS CLI o los SDK AWS.

4. Elija el enlace del rol para iniciar sesión en AWS Console Home.

Has iniciado sesión y has accedido a la AWS Console Home página. Explore la consola y confirme que tiene el acceso que esperaba.

Siguientes pasos

Ahora que ha creado un usuario administrativo en IAM Identity Center, puede hacer lo siguiente:

- Asignar aplicaciones
- Agregar otros usuarios
- Asignar usuarios a las cuentas
- Configurar conjuntos de permisos adicionales

> **Note**
>
> Puede asignar varios conjuntos de permisos al mismo usuario. Para seguir la práctica recomendada de aplicar permisos con privilegios mínimos, después de crear un conjunto de permisos administrativos, cree un conjunto de permisos más restrictivo y asígnelo al mismo usuario. De esta forma, podrá acceder a la suya únicamente Cuenta de AWS con los permisos que necesite, en lugar de con permisos administrativos.

Una vez que los usuarios acepten la invitación para activar su cuenta e inicien sesión en el portal de AWS acceso, los únicos elementos que aparecen en el Cuentas de AWS portal son los roles y las aplicaciones a los que están asignados.

> **Important**
>
> Recomendamos encarecidamente habilitar la autenticación multifactor (MFA) para los usuarios. Para obtener más información, consulte Autenticación multifactor para usuarios de Identity Center.

Uso de Active Directory como origen de identidad

Si administra los usuarios en su directorio de AWS Managed Microsoft AD mediante AWS Directory Service o en su directorio autoadministrado de Active Directory (AD), puede cambiar el origen de identidad de IAM Identity Center para que funcione con esos usuarios. Le recomendamos que considere la posibilidad de conectar este origen de identidad al habilitar IAM Identity Center y elegir el origen de identidad. Hacerlo antes de crear usuarios y grupos en el directorio predeterminado del Identity Center lo ayudará a evitar la configuración adicional que se requiere si cambia el origen de identidad más adelante.

Para utilizar Active Directory como origen de identidad, la configuración debe cumplir los siguientes requisitos previos:

- Si está usando AWS Managed Microsoft AD, debe habilitar IAM Identity Center en la misma Región de AWS donde su directorio de AWS Managed Microsoft AD está configurado. IAM Identity Center almacena los datos de asignación en la misma región que el directorio. Para administrar IAM Identity Center, es posible que deba cambiarse a la región en la que está configurado IAM Identity Center. Además, tenga en cuenta que el portal de acceso de AWS utiliza la misma URL de acceso que su directorio.
- Utilice un Active Directory que resida en la cuenta de administración:

  Debe tener un conector de AD existente o directorio de AWS Managed Microsoft AD configurado en AWS Directory Service, y debe residir dentro de su cuenta de administración de AWS Organizations. Solo puede conectar un directorio de conector de AD o un directorio en AWS Managed Microsoft AD a la vez. Si necesita admitir varios dominios o bosques, utilice AWS Managed Microsoft AD. Para obtener más información, consulte:

  - Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM
  - Conexión de un directorio autoadministrado de Active Directory a IAM Identity Center
- Utilice una instancia de Active Directory que resida en la cuenta de administrador delegado:

Si planea habilitar un administrador delegado de IAM Identity Center y usar Active Directory como origen de identidad de IAM Identity Center, puede usar un conector de AD existente o directorio de AWS Managed Microsoft AD configurado en el directorio de AWS que reside en la cuenta de administrador delegado.

Si decide cambiar la fuente de identidad de IAM Identity Center de cualquier otra fuente a Active Directory, o cambiarla de Active Directory a cualquier otra fuente, el directorio debe residir en (ser propiedad de) la cuenta de miembro administrador delegado de IAM Identity Center, si existe alguna; de lo contrario, debe estar en la cuenta de administración.

En este tutorial se explica la configuración básica para usar Active Directory como origen de identidad de IAM Identity Center.

Paso 1: conexión de Active Directory y especificación de un usuario

Si ya utiliza Active Directory, los siguientes temas lo ayudarán a prepararse para conectar su directorio a IAM Identity Center.

> **Note**
>
> Como práctica recomendada de seguridad, le recomendamos que habilite la autenticación multifactor. Si planea conectar un directorio de AWS Managed Microsoft AD o un directorio autogestionado en Active Directory y no está utilizando RADIUS MFA con AWS Directory Service, active la MFA en IAM Identity Center.

AWS Managed Microsoft AD

1. Revise la guía en Conexión un directorio Microsoft AD.
2. Siga los pasos de Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM.
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en IAM Identity Center. Para obtener más información, consulte Sincronice un usuario administrativo en el IAM Identity Center.

Directorio autogestionado en Active Directory

1. Revise la guía en Conexión un directorio Microsoft AD.
2. Siga los pasos de Conexión de un directorio autoadministrado de Active Directory a IAM Identity Center.
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en IAM Identity Center. Para obtener más información, consulte Sincronice un usuario administrativo en el IAM Identity Center.

Paso 2: sincronización de un usuario administrativo en IAM Identity Center

Tras conectar el directorio al IAM Identity Center, puede especificar el usuario al que quiere conceder permisos administrativos y, a continuación, sincronizar ese usuario del directorio con el IAM Identity Center.

1. Abra la Consola del IAM Identity Center.
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de Administrar sincronización, elija la pestaña Usuarios y, continuación, seleccione Añadir usuarios y grupos.
5. En la pestaña Usuarios, en Usuario, ingrese el nombre de usuario exacto y seleccione Agregar.
6. En Usuarios y grupos añadidos, haga lo siguiente:
    a. Confirme que se ha especificado el usuario a quien desea conceder permisos administrativos.
    b. Seleccione la casilla de verificación situada a la izquierda del nombre de usuario.
    c. Elija Enviar
7. En la página Administrar sincronización, el usuario que especificó aparece en la lista de Ámbito de usuarios sincronizados.
8. En el panel de navegación, seleccione Usuarios.
9. En la página Usuarios, es posible que el usuario que especificó tarde algún tiempo en aparecer en la lista. Seleccione el icono de actualización para actualizar la lista de usuarios.

En este momento, el usuario no tiene acceso a la cuenta de administración. Para configurar el acceso administrativo a esta cuenta, debe crear un conjunto de permisos administrativos y asignar

el usuario a ese conjunto de permisos. Para obtener más información, consulte Crea un conjunto de permisos..

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios de CyberArk Directory Platform a IAM Identity Center. Este aprovisionamiento utiliza el protocolo sistema de administración de identidades entre dominios (SCIM) v2.0. Esta conexión se configura en CyberArk mediante el punto de conexión SCIM y el token de acceso de IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en CyberArk con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y CyberArk.

Esta guía está basada en CyberArk a fecha de agosto de 2021. Los pasos para las versiones más recientes pueden variar. Esta guía contiene algunas notas sobre la configuración de la autenticación de usuarios mediante SAML.

> **Note**
>
> Antes de comenzar a implementar SCIM, le recomendamos que revise las Consideraciones para utilizar el aprovisionamiento automático. A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

Temas

- Requisitos previos
- Consideraciones de SCIM
- Paso 1: habilite el aprovisionamiento en IAM Identity Center
- Paso 2: configure el aprovisionamiento en CyberArk
- (Opcional) Paso 3: configure los atributos de usuario en CyberArk para el control de acceso (ABAC) en IAM Identity Center
- (Opcional) Paso de atributos para el control de acceso

Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Suscripción a CyberArk o prueba gratuita. Para suscribirse a una versión de prueba gratuita, vaya a CyberArk.
- Una cuenta habilitada para IAM Identity Center (gratuita). Para más información, consulte Activar IAM Identity Center.
- Una conexión SAML desde su cuenta de CyberArk a IAM Identity Center, tal y como se describe en la documentación de IAM Identity Center CyberArk.
- Asocie el conector de IAM Identity Center a los roles, usuarios y organizaciones a los que desee permitir el acceso a las Cuentas de AWS.

Consideraciones de SCIM

A continuación, se presentan las consideraciones a tener en cuenta al utilizar la federación de CyberArk para IAM Identity Center:

- Solo los roles asignados en la sección de aprovisionamiento de aplicaciones se sincronizarán con IAM Identity Center.
- El script de aprovisionamiento solo se admite en su estado predeterminado; una vez modificado, el aprovisionamiento de SCIM podría fallar.
  - Solo se puede sincronizar un atributo de número de teléfono y el valor predeterminado es “teléfono del trabajo”.
- Si se cambia la asignación de roles en la aplicación de IAM Identity Center CyberArk, se espera el siguiente comportamiento:
  - Si se cambian los nombres de los roles, no habrá cambios en los nombres de los grupos en IAM Identity Center.
  - Si se cambian los nombres de los grupos, se crearán nuevos grupos en IAM Identity Center y los grupos antiguos permanecerán sin miembros.
- El comportamiento de sincronización y desaprovisionamiento de los usuarios se puede configurar desde la aplicación de IAM Identity Center CyberArk. Asegúrese de configurar el comportamiento correcto para su organización. Estas son las opciones:
  - Sobrescriba (o no) a los usuarios del directorio de Identity Center con el mismo nombre principal.

- Cancele el aprovisionamiento de usuarios de IAM Identity Center cuando se elimine al usuario del rol de CyberArk.
- Cancele el aprovisionamiento de usuarios: deshabilite o elimine.

Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie todos los valores de las opciones siguientes. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
    a. Punto de conexión de SCIM
    b. Token de acceso
5. Elija Close.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes con la aplicación IAM Identity Center de CyberArk. Estos pasos se explican en el procedimiento siguiente.

Paso 2: configure el aprovisionamiento en CyberArk

Utilice el siguiente procedimiento en la aplicación IAM Identity Center CyberArk para habilitar el aprovisionamiento con IAM Identity Center. En este procedimiento se presupone que ya ha añadido la aplicación IAM Identity Center CyberArk a la consola de administración de CyberArk en la sección Aplicaciones web. Si aún no lo ha hecho, consulte los Requisitos previos y complete este procedimiento para configurar el aprovisionamiento de SCIM.

Cómo configurar el aprovisionamiento en CyberArk

1. Abra la aplicación IAM Identity Center CyberArk que agregó como parte de la configuración de SAML CyberArk (Aplicaciones > Aplicación web). Consulte Requisitos previos.
2. Elija la aplicación IAM Identity Center y vaya a la sección Aprovisionamiento.
3. Marque la casilla Habilitar el aprovisionamiento para esta aplicación y elija Live Mode.
4. En el procedimiento anterior, copió el valor del punto de conexión del SCIM de IAM Identity Center. Pegue ese valor en el campo URL del servicio SCIM, en la aplicación IAM Identity Center CyberArk, defina el tipo de autorización como encabezado de autorización. Asegúrese de eliminar la barra inclinada que aparece al final de la URL.
5. Configure el tipo de encabezado como token al portador.
6. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Token al portador de la aplicación IAM Identity Center CyberArk.
7. Haga clic en Verificar para probar y aplicar la configuración.
8. En Opciones de sincronización, elija el comportamiento correcto para el que desee que funcione el aprovisionamiento saliente de CyberArk. Puede optar por sobrescribir (o no) a los usuarios actuales de IAM Identity Center con un nombre principal y un comportamiento de desaprovisionamiento similares.
9. En Asignación de roles, adapte el mapeo de los roles desde CyberArk, en el campo Nombre al grupo de IAM Identity Center, en Grupo de destino.
10. Cuando haya terminado, haga clic en Guardar, en la parte inferior.
11. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios sincronizados de CyberArk aparecerán en la página Usuarios. Estos usuarios ya pueden asignarse a cuentas y conectarse dentro de IAM Identity Center.

(Opcional) Paso 3: configure los atributos de usuario en CyberArk para el control de acceso (ABAC) en IAM Identity Center

Se trata de un procedimiento opcional si CyberArk decide configurar los atributos del Centro de identidades de IAM para gestionar el acceso a sus AWS recursos. Los atributos que defina en CyberArk se transfieren en una aserción de SAML al IAM Identity Center. A continuación, debe crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde CyberArk.

Antes de comenzar con este procedimiento, debe habilitar la característica Atributos para controlar el acceso. Para obtener más información acerca de cómo hacerlo, consulte Habilitación y configuración de atributos para el control de acceso.

Cómo configurar atributos de usuario utilizados en CyberArk para el control de acceso en IAM Identity Center

1. Abra la aplicación IAM Identity Center CyberArk que instaló como parte de la configuración de SAML para CyberArk (Aplicaciones > Aplicaciones web).
2. Vaya a la opción Respuesta SAML.
3. En Atributos, añada los atributos relevantes a la tabla siguiendo la siguiente lógica:
    a. El Nombre del atributo es el nombre del atributo original de CyberArk.
    b. El Valor del atributo es el nombre del atributo que se envía en la aserción SAML a IAM Identity Center.
4. Seleccione Guardar.

(Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica Atributos para controlar el acceso de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

Configuración de SAML y SCIM con Google Workspace e IAM Identity Center

Si su organización Google Workspace lo utiliza, puede integrar sus usuarios y grupos Google Workspace en el Centro de identidades de IAM para darles acceso a AWS los recursos. Puede lograr esta integración cambiando la fuente de identidad del Centro de Identidad de IAM de la fuente de identidad predeterminada del Centro de Identidad de IAM a. Google Workspace

La información de los usuarios de Google Workspace se sincroniza con IAM Identity Center mediante el protocolo del sistema de administración de identidades entre dominios (SCIM) v2.0. Esta conexión se configura en Google Workspace mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador de IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en Google Workspace con los atributos nombrados en IAM Identity Center. Esta asignación vincula los atributos de usuario esperados entre IAM Identity Center y Google Workspace. Para ello, debe configurar Google Workspace como proveedor de identidades de IAM y proveedor de identidades de IAM Identity Center.

Objetivo

Los pasos de este tutorial le ayudarán a establecer la conexión SAML entre y. Google Workspace AWS Más adelante, sincronizará a los usuarios de Google Workspace mediante SCIM. Para comprobar que todo está configurado correctamente, tras completar los pasos de configuración, iniciará sesión como Google Workspace usuario y verificará el acceso a los AWS recursos.
Tenga en cuenta que este tutorial se basa en un entorno de prueba con un directorio de Google Workspace pequeño. No se incluyen las estructuras de directorios, como los grupos y las unidades organizativas. Tras completar este tutorial, sus usuarios podrán acceder al portal de AWS acceso con sus Google Workspace credenciales.

> **Note**
>
> Para suscribirse a una versión de prueba gratuita de Google Workspace, vaya a Google Workspace en el sitio web de Google's.
> Si aún no ha habilitado IAM Identity Center, consulte Habilitar AWS IAM Identity Center.

Consideraciones

- Antes de configurar el aprovisionamiento de SCIM entre el IAM Identity Center Google Workspace y el Centro de Identidad de IAM, le recomendamos que lo revise primero. Consideraciones para utilizar el aprovisionamiento automático
- La sincronización automática de SCIM desde actualmente Google Workspace se limita al aprovisionamiento de usuarios. Por el momento, no se admite el aprovisionamiento automático de grupos. Los grupos se pueden crear manualmente con el comando create-group de AWS CLI Identity Store o la API AWS Identity and Access Management (IAM). CreateGroup Como alternativa, puede utilizar ssosync para sincronizar los Google Workspace usuarios y los grupos en el Centro de identidades de IAM.
- Todos los usuarios de Google Workspace deben tener un valor especificado para Nombre, Apellidos, Nombre de usuario y Nombre de visualización.
- Cada usuario de Google Workspace tiene un único valor por atributo de datos, como la dirección de correo electrónico o el número de teléfono. Los usuarios que tengan varios valores no se sincronizarán. Si hay usuarios que tienen varios valores en sus atributos, elimine los atributos duplicados antes de intentar aprovisionar el usuario en IAM Identity Center. Por ejemplo, solo se puede sincronizar un atributo de número de teléfono. Como el atributo de número de teléfono predeterminado es “teléfono del trabajo”, utilice el atributo “teléfono del trabajo” para almacenar el número de teléfono del usuario, incluso si el número de teléfono del usuario es un teléfono fijo o móvil.
- Los atributos siguen sincronizados si el usuario está deshabilitado en IAM Identity Center, pero sigue activo en Google Workspace.
- Si hay un usuario existente en el directorio de Identity Center con el mismo nombre de usuario y correo electrónico, el usuario se sobrescribirá y sincronizará mediante SCIM from. Google Workspace
- Hay que tener en cuenta otras consideraciones a la hora de cambiar la fuente de identidad. Para obtener más información, consulte the section called “Cómo cambiar de IAM Identity Center a un IdP externo”.

Paso 1Google Workspace: Configurar la aplicación SAML

1. Inicia sesión en la consola Google de administración con una cuenta con privilegios de superadministrador.

2. En el panel de navegación izquierdo de la consola de Google administración, selecciona Aplicaciones y, a continuación, selecciona Aplicaciones web y móviles.
3. En la lista desplegable Añadir aplicación, selecciona Buscar aplicaciones.
4. En el cuadro de búsqueda, escribe Amazon Web Services y, a continuación, selecciona la aplicación Amazon Web Services (SAML) de la lista.
5. En la página Detalles del proveedor de Google identidad: Amazon Web Services, puede realizar una de las siguientes acciones:

   a. Descarga los metadatos del IdP.

   b. Copie la URL del SSO, la URL del ID de la entidad y la información del certificado.

   Necesitará el archivo XML o la información de la URL en el paso 2.
6. Antes de continuar con el siguiente paso en la consola de Google administración, deje esta página abierta y vaya a la consola del IAM Identity Center.

Paso 2: Centro de identidad de IAM yGoogle Workspace: cambiar la fuente de identidad del Centro de identidad de IAM y configurarla Google Workspace como proveedor de identidad de SAML

1. Inicie sesión en la consola del IAM Identity Center con un rol con permisos administrativos.
2. Elija Configuración en el panel de navegación izquierdo.
3. En la página Configuración, seleccione Acciones y, a continuación, seleccione Cambiar el origen de identidad.

   - Si no ha activado el Centro de identidad de IAM, consulte Habilitación de IAM Identity Center para obtener más información. Tras activar el Centro de Identidad de IAM y acceder a él por primera vez, accederá al panel de control, donde podrá seleccionar la fuente de identidad.
4. En la página Elegir el origen de identidad, seleccione Proveedor de identidades externo y, a continuación, seleccione Siguiente.
5. Se abre la página Configurar un proveedor de identidad externo. Para completar esta página y la Google Workspace página del paso 1, deberá completar lo siguiente:

   - En la sección de metadatos del proveedor de identidad de la consola de IAM Identity Center, deberá realizar una de las siguientes acciones:

i. Cargue los metadatos de GoogleSAML como metadatos de SAML del IdP en la consola del IAM Identity Center.

ii. Copie y pegue la URL del GoogleSSO en el campo URL de inicio de sesión del IdP Google, la URL del emisor en el campo URL del emisor del IdP y cargue el certificado como certificado de IdP. Google

6. Tras introducir los Google metadatos en la sección de metadatos del proveedor de identidad de la consola del IAM Identity Center, copie la URL de inicio de sesión del portal de AWS acceso, la URL del Servicio de Consumer Assertion (ACS) de IAM Identity Assertion y la URL del emisor del IAM Identity Center. En el siguiente paso, tendrás que proporcionar estas direcciones URL en la Google consola de administración.
7. Deje la página abierta con la consola del IAM Identity Center y vuelva a la consola de Google administración. Deberías estar en la página de detalles del proveedor de servicios de Amazon Web Services. Seleccione Continuar.
8. En la página de detalles del proveedor de servicios, introduzca los valores de la URL ACS, el ID de entidad y la URL de inicio. Copió estos valores en el paso anterior y se encuentran en la consola del IAM Identity Center.

   - Pegue la URL del Servicio de Consumer Service (ACS) de IAM Identity Center en el campo URL de ACS
   - Pegue la URL del emisor del IAM Identity Center en el campo ID de entidad.
   - Pegue la URL de inicio de sesión del portal de AWS acceso en el campo URL de inicio.
9. En la página de detalles del proveedor de servicios, complete los campos que aparecen debajo del ID de nombre de la siguiente manera:

   - En Name ID format, seleccione EMAIL.
   - En Name ID, seleccione Basic Information > Primary email.
10. Elija Continuar.
11. En la página Asignación de atributos, en Atributos, elija AGREGAR ASIGNACIÓN y, a continuación, configure estos campos en el atributo Google del directorio:

    - Para el atributo de la aplicación **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**, seleccione el campo Información básica, correo electrónico principal entre los Google Directoryatributos.

- Para el atributo de la **`https://aws.amazon.com/SAML/Attributes/Role`** aplicación, seleccione cualquier Google Directoryatributo. Un atributo Google del directorio podría ser Departamento.

12. Seleccione Finish.
13. Vuelva a la consola del IAM Identity Center y seleccione Siguiente. En la página Revisar y confirmar, revise la información y, a continuación, escriba ACCEPT en el espacio correspondiente. Elija Cambiar fuente de identidad.

Ya está preparado para activar la aplicación Amazon Web Services para que sus usuarios puedan aprovisionarse en el IAM Identity Center. Google Workspace

Paso 3Google Workspace: Habilita las aplicaciones

1. Regrese a la Consola de Google administración y a su AWS IAM Identity Center aplicación, que se encuentran en Aplicaciones y Aplicaciones web y móviles.
2. En el panel de acceso de usuario situado junto a Acceso de usuario, seleccione la flecha hacia abajo para ampliar el acceso de usuario y mostrar el panel de estado del servicio.
3. En el panel de estado del servicio, selecciona ACTIVADO para todos y, a continuación, selecciona GUARDAR.

> **Note**
>
> Para ayudar a mantener el principio de privilegios mínimos, le recomendamos que, después de completar este tutorial, cambie el estado del servicio a DESACTIVADO para todos. Solo los usuarios que necesiten acceder a AWS él deben tener el servicio activado. Puede usar grupos o unidades organizativas de Google Workspace para dar acceso a los usuarios a un subconjunto concreto de usuarios.

Paso 4: IAM Identity Center: configure el aprovisionamiento automático del IAM Identity Center

1. Vuelva a la consola de IAM Identity Center.
2. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el

aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.

3. En el cuadro de diálogo de aprovisionamiento automático entrante, copie todos los valores de las opciones siguientes. En el paso 5 de este tutorial, introducirá estos valores para configurar el aprovisionamiento automático. Google Workspace

   - Punto de conexión de SCIM
   - Token de acceso

   > ⚠ Warning
   >
   > Esta es la única vez en la que puede obtener el punto final y el token de acceso del SCIM. Asegúrese de copiar estos valores antes de continuar.

4. Elija Close.

   Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, en el siguiente paso configurará el aprovisionamiento automático en. Google Workspace

Paso 5Google Workspace: Configurar el aprovisionamiento automático

1. Vuelva a la consola de Google administración y a su AWS IAM Identity Center aplicación, que se encuentran en Aplicaciones y Aplicaciones web y móviles. En la sección Aprovisionamiento automático, elija Configurar aprovisionamiento automático.
2. En el procedimiento anterior, copió el valor del token de acceso en la consola del IAM Identity Center. Pegue ese valor en el campo del token de acceso y seleccione Continuar. Además, en el procedimiento anterior, copió el valor del punto final de SCIM en la consola de IAM Identity Center. Pegue ese valor en el campo Endpoint URL. Asegúrese de eliminar la barra inclinada que aparece al final de la URL y elija Continuar.
3. Compruebe que todos los atributos obligatorios de IAM Identity Center (los marcados con un asterisco) estén asignados a los atributos de Google Cloud Directory. Si no es así, haga clic en la flecha hacia abajo y asigne el atributo correspondiente. Elija Continuar.
4. En la sección Alcance del aprovisionamiento, puede elegir un grupo con su Google Workspace directorio para proporcionar acceso a la aplicación Amazon Web Services. Omita este paso y seleccione Continue.

5. En la sección de desaprovisionamiento, puede elegir cómo responder a los diferentes eventos que impidan el acceso a un usuario. Para cada situación, puede especificar el tiempo que debe transcurrir antes de que comience el desaprovisionamiento:

   - en menos de 24 horas
   - después de un día
   - después de siete días
   - después de 30 días

   Cada situación tiene una configuración de tiempo para cuándo suspender el acceso a una cuenta y cuándo eliminarla.

   > **Tip**
   >
   > Configure siempre más tiempo antes de eliminar la cuenta de un usuario que para suspenderla.

6. Seleccione Finalizar. Volverá a la página de la aplicación de Amazon Web Services.
7. En la sección de aprovisionamiento automático, activa el conmutador para cambiarlo de Inactivo a Activo.

   > **Note**
   >
   > El control deslizante de activación está deshabilitado si IAM Identity Center no está activado para los usuarios. Seleccione Acceso de usuario y active la aplicación para activar el control deslizante.

8. En el cuadro de diálogo de confirmación, elija Activar.
9. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. En la página Users se muestran los usuarios de su directorio de Google Workspace que creó SCIM. Si los usuarios aún no aparecen en la lista, es posible que el aprovisionamiento aún esté en proceso. El aprovisionamiento puede tardar hasta 24 horas, aunque en la mayoría de los casos se completa en cuestión de minutos. Asegúrese de actualizar la ventana del navegador cada pocos minutos.

   Seleccione un usuario y consulte sus detalles. La información debe coincidir con la información del directorio. Google Workspace

¡Enhorabuena!

Ha configurado correctamente una conexión SAML entre Google Workspace AWS y ha comprobado que el aprovisionamiento automático funciona. Ahora puede asignar a estos usuarios cuentas y aplicaciones en IAM Identity Center. Para este tutorial, en el siguiente paso designaremos a uno de los usuarios como administrador de IAM Identity Center mediante la concesión de permisos administrativos en la cuenta de administración.

Paso 6: Centro de identidad de IAM: permite a Google Workspace los usuarios acceder a las cuentas

1. Vuelva a la consola del IAM Identity Center. En el panel de navegación del IAM Identity Center, en Permisos para varias cuentas, seleccione Cuentas de AWS.
2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la raíz organizativa con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:

    a. En Paso 1: selección de usuarios y grupos, elija el usuario que realizará la función del trabajo de administrador. A continuación, elija Next.

    b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.

        i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:

        - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
        - En Política para un conjunto de permisos predefinido, elija AdministratorAccess.

        Elija Siguiente.

        ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

        La configuración predeterminada crea un conjunto de permisos denominado *`AdministratorAccess`*con una duración de sesión establecida en una hora.

iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.

iv. En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.

v. En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de *AdministratorAccess*permisos que ha creado aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.

c. En Paso 3: revisión y envío, revise el usuario y el conjunto de permisos seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Volverá a la Cuentas de AWS página. Un mensaje de notificación le informa de que se Cuenta de AWS ha vuelto a aprovisionar y se ha aplicado el conjunto de permisos actualizado. Cuando el usuario inicie sesión, tendrá la opción de elegir el *AdministratorAccess*rol.

> **Note**
>
> La sincronización automática de SCIM Google Workspace solo admite el aprovisionamiento de usuarios. Por el momento, no se admite el aprovisionamiento automático de grupos. No puede crear grupos para los usuarios de Google Workspace mediante la AWS Management Console. Tras aprovisionar a los usuarios, puede crear grupos mediante el comando create-group de AWS CLI Identity Store o la API de IAM. CreateGroup

Paso 7Google Workspace: Confirme Google Workspace el acceso de los usuarios a los recursos AWS

1. Inicie sesión para Google usar una cuenta de usuario de prueba. Para obtener información sobre cómo añadir usuarios aGoogle Workspace, consulte Google Workspacela documentación.

2. Seleccione el icono del lanzador de Google apps (símbolo).
3. Desplácese a la parte inferior de la lista de aplicaciones donde se encuentran las aplicaciones personalizadas de Google Workspace. Se muestran dos aplicaciones: Amazon Web Services y el portal de acceso de AWS .
4. Seleccione la aplicación del portal de acceso de AWS . Ha iniciado sesión en el portal y puede ver el Cuenta de AWS icono. Amplíe ese icono para ver la lista a la Cuentas de AWS que puede acceder el usuario. En este tutorial, solo trabajó con una cuenta, por lo que al expandir el icono solo se muestra una cuenta.

   > **Note**
   >
   > Si selecciona la aplicación Amazon Web Services, recibirá un error de SAML. Esa aplicación se utiliza para los usuarios de Google Workspace que se han aprovisionado como usuarios de IAM y en este tutorial se trata de aprovisionar a sus usuarios de Google Workspace como usuarios de IAM Identity Center.

5. Seleccione la cuenta para ver los conjuntos de permisos disponibles para el usuario. En este tutorial, creó el conjunto de AdministratorAccesspermisos.
6. Junto al conjunto de permisos hay enlaces para el tipo de acceso disponible para ese conjunto de permisos. Cuando creó el conjunto de permisos, especificó que se habilitó el acceso mediante programación y con la Consola de administración, por lo que esas dos opciones están presentes. Seleccione Consola de administración para abrir la AWS Management Console.
7. El usuario ha iniciado sesión en la consola.

(Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica Atributos para controlar el acceso de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
```

```
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

Siguientes pasos

Ahora que ha configurado Google Workspace como proveedor de identidades y ha aprovisionado a usuarios en IAM Identity Center, puede hacer lo siguiente:

- Utilice el comando create-group de AWS CLI Identity Store o la API de IAM CreateGrouppara crear grupos para sus usuarios.

  Los grupos son útiles a la hora de asignar el acceso a las aplicaciones y a ellas. Cuentas de AWS En lugar de asignarlo a cada usuario de manera individual, concede permisos a un grupo. Más adelante, al agregar o eliminar usuarios de un grupo, el usuario obtiene o pierde de forma dinámica el acceso a las cuentas y aplicaciones que haya asignado al grupo.
- Para configurar los permisos en función de los cargos en el trabajo; consulte Create a permission set.

  Los conjuntos de permisos definen el nivel de acceso que tienen los usuarios y grupos en una Cuenta de AWS. Los conjuntos de permisos se almacenan en IAM Identity Center y se pueden aprovisionar a una o varias Cuentas de AWS. Puedes asignar más de un conjunto de permisos a un usuario.

> **Note**
>
> Como administrador de IAM Identity Center, en ocasiones tendrá que sustituir los certificados de IdP antiguos por otros más nuevos. Por ejemplo, debe sustituir un certificado cuando se aproxime la fecha de vencimiento del certificado. El proceso de sustituir un certificado antiguo por uno más nuevo se denomina rotación de certificados. Asegúrese de revisar cómo administrar los certificados de SAML para Google Workspace.

Uso de IAM Identity Center para conectarse a su plataforma de directorios de JumpCloud

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios desde la plataforma de directorios de JumpCloud a IAM Identity Center. Este aprovisionamiento utiliza el protocolo System for Cross-Domain Identity Management (SCIM) v2.0. Esta conexión se configura en JumpCloud mediante el punto de conexión SCIM y el token de acceso de IAM Identity Center. Al configurar la sincronización de SCIM, crea un mapeo de los atributos de usuario en JumpCloud con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y JumpCloud.

Esta guía está basada en JumpCloud a fecha de junio de 2021. Los pasos para las versiones más recientes pueden variar. Esta guía contiene algunas notas sobre la configuración de la autenticación de usuarios mediante SAML.

Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de usuarios y grupos desde JumpCloud a IAM Identity Center mediante el protocolo SCIM.

> **Note**
>
> Antes de comenzar a implementar SCIM, le recomendamos revisar primero las Consideraciones para utilizar el aprovisionamiento automático. A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

Temas

Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Suscripción a JumpCloud o prueba gratuita. Para suscribirse a una versión de prueba gratuita, vaya a JumpCloud.
- Una cuenta habilitada para IAM Identity Center (gratuita). Para más información, consulte Activar IAM Identity Center.
- Una conexión SAML desde su cuenta de JumpCloud al IAM Identity Center, tal y como se describe en la JumpClouddocumentación del IAM Identity Center.
- Asocie el conector del IAM Identity Center a los grupos a los que desee permitir el acceso a las cuentas de AWS.

Consideraciones de SCIM

A continuación, se presentan las consideraciones a tener en cuenta al utilizar la federación de JumpCloud para IAM Identity Center.

- Solo los grupos asociados al AWS conector de inicio de sesión único de JumpCloud se sincronizarán con SCIM.
- Solo se puede sincronizar un atributo de número de teléfono y el valor predeterminado es “teléfono del trabajo”.
- Los usuarios del directorio JumpCloud deben tener su nombre y apellidos configurados para poder sincronizarse con IAM Identity Center mediante SCIM.
- Los atributos siguen sincronizados si el usuario está deshabilitado en IAM Identity Center, pero sigue activo en JumpCloud.
- Si desea activar la sincronización con SCIM únicamente para la información del usuario, desmarque la opción “Habilitar la administración de grupos de usuarios y la pertenencia a grupos” en el conector.
- Si existe un usuario en el directorio de Identity Center con el mismo nombre de usuario y correo electrónico, el usuario se sobrescribirá y sincronizará mediante SCIM desde JumpCloud.

Paso 1: Habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie cada uno de los valores de las siguientes opciones. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
    a. Punto de conexión de SCIM
    b. Token de acceso
5. Elija Close.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes con la aplicación JumpCloud de IAM Identity Center. Estos pasos se explican en el procedimiento siguiente.

Paso 2: Configure el aprovisionamiento en JumpCloud

Utilice el siguiente procedimiento en el conector JumpCloud de IAM Identity Center para habilitar el aprovisionamiento con IAM Identity Center. En este procedimiento se presupone que ya ha añadido la aplicación JumpCloud de IAM Identity Center a la consola de JumpCloud administración del portal. Si aún no lo ha hecho, consulte los Requisitos previos y complete este procedimiento para configurar el aprovisionamiento de SCIM.

Para configurar el aprovisionamiento en JumpCloud

1. Abra el conector JumpCloud de IAM Identity Center que instaló como parte de la configuración SAML para JumpCloud (Autenticación de usuario > IAM Identity Center). Consulte Requisitos previos.

2. Seleccione el conector de IAM Identity Center y, a continuación, elija la tercera pestaña Gestión de identidades.
3. Marque la casilla Habilitar la administración de grupos de usuarios y la pertenencia a grupos en esta aplicación si desea que los grupos se sincronicen con SCIM.
4. Haga clic en Configurar.
5. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL base en el conector de JumpCloud de IAM Identity Center. Asegúrese de eliminar la barra diagonal que aparece al final de la URL.
6. En el procedimiento anterior, copió el valor del Token de acceso en IAM Identity Center. Pegue ese valor en el campo Clave de token en el conector de JumpCloud de IAM Identity Center.
7. Haga clic en Activar para aplicar la configuración.
8. Asegúrese de tener activado un indicador verde junto a Inicio de sesión único activado.
9. Ve a la cuarta pestaña Grupos de usuarios y marca los grupos que deseas aprovisionar con SCIM.
10. Cuando haya terminado, haga clic en Guardar, en la parte inferior.
11. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios sincronizados de JumpCloud aparecerán en la página de Usuarios. Estos usuarios ahora pueden asignarse a cuentas en IAM Identity Center.

(Opcional) Paso 3: Configure los atributos de usuario en JumpCloud para el control de acceso en IAM Identity Center

Este es un procedimiento opcional para JumpCloud, en caso de que quiera configurar atributos para que IAM Identity Center administre el acceso a sus recursos de AWS. Los atributos que defina en JumpCloud se transfieren en una aserción de SAML a IAM Identity Center. A continuación, debe crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde JumpCloud.

Antes de iniciar este procedimiento, abilite primero la característica Atributos para el control de acceso. Para obtener más información acerca de cómo hacerlo, consulte Habilitación y configuración de atributos para el control de acceso.

Para configurar atributos de usuario utilizados en JumpCloud para el control de acceso en IAM Identity Center

1. Abra el conector JumpCloud de IAM Identity Center que instaló como parte de la configuración SAML para JumpCloud (Autenticación de usuario > IAM Identity Center).
2. Elija el conector de IAM Identity Center. A continuación, elija la segunda pestaña para IAM Identity Center.
3. En la parte inferior de esta pestaña está la Asignación de atributos de usuario. Elija Añadir nuevo atributo y, a continuación, haga lo siguiente: debe seguir estos pasos para cada atributo que vaya a añadir para su uso en IAM Identity Center para el control de acceso.

   a. En el campo Nombre del atributo proporcionado por el servicio, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**`.`. Reemplace **`AttributeName`** con el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.

   b. En el campo Nombre del atributo de JumpCloud, elija los atributos de usuario de su directorio de JumpCloud. Por ejemplo, Correo electrónico (trabajo).
4. Seleccione Guardar.

(Opcional) Pasar atributos para el control de acceso

Si lo desea, puede utilizar la característica Atributos para controlar el acceso de IAM Identity Center para transferir un elemento de `Attribute`con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, para pasar los pares clave-valor de etiquetas de `CostCenter = blue`, utilice el siguiente atributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
```

```
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento de `Attribute` independiente para cada etiqueta.

Configuración de SAML y SCIM con Microsoft Entra ID e IAM Identity Center

AWS IAM Identity Center admite la integración con el lenguaje de marcado para confirmaciones de seguridad (SAML) 2.0, así como el aprovisionamiento automático (sincronización) de la información de usuarios y grupos desde Microsoft Entra ID (antes conocido como Azure Active Directory o Azure AD) a IAM Identity Center mediante el protocolo del sistema de administración de identidades entre dominios (SCIM) 2.0.

Objetivo

En este tutorial, configurará un laboratorio de pruebas y configurará una conexión SAML y el aprovisionamiento de SCIM entre Microsoft Entra ID e IAM Identity Center. Durante los pasos iniciales de preparación, creará un usuario de prueba (Nikki Wolf) tanto en Microsoft Entra ID como en IAM Identity Center que utilizará para probar la conexión SAML en ambas direcciones. Más adelante, como parte de los pasos de SCIM, creará un usuario de prueba diferente (Richard Roe) para comprobar que los nuevos atributos de Microsoft Entra ID se sincronizan con IAM Identity Center según lo previsto.

Requisitos previos

Antes de empezar con este tutorial, primero tendrá que definir lo siguiente:

- Un inquilino de Microsoft Entra ID. Para obtener más información, consulte Inicio rápido: configurar un inquilino en el sitio web de Microsoft.
- Una cuenta habilitada para AWS IAM Identity Center. Para más información, consulte Activar IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.

Paso 1: preparación de su inquilino de Microsoft

En este paso, seguirá las indicaciones para instalar y configurar su aplicación empresarial de AWS IAM Identity Center y asignar el acceso a un usuario de prueba de Microsoft Entra ID recién creado.

Step 1.1 >

Paso 1.1: configuración de la aplicación empresarial de AWS IAM Identity Center en Microsoft Entra ID

En este procedimiento, instalará la aplicación empresarial de AWS IAM Identity Center en Microsoft Entra ID. Necesitará esta aplicación más adelante para configurar su conexión SAML con AWS.

1. Inicie sesión en el Centro de administración de Microsoft Entra como mínimo como administrador de aplicaciones en la nube.
2. Vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione New application.
3. En la página Browse Microsoft Entra Gallery, ingrese **`AWS IAM Identity Center`** en el cuadro de búsqueda.
4. Seleccione AWS IAM Identity Center en el área de resultados.
5. Seleccione Crear.

Step 1.2 >

Paso 1.2: creación de un usuario de prueba en Microsoft Entra ID

Nikki Wolf es el nombre del usuario de prueba de Microsoft Entra ID que creará en este procedimiento.

1. En la consola del Centro de administración de Microsoft Entra, vaya a Identity > Users > All users.
2. Seleccione New user y, a continuación, seleccione Create new user en la parte superior de la pantalla.
3. En User principal name, ingrese **`NikkiWolf`** y, a continuación, seleccione el dominio y la extensión que desee. Por ejemplo, NikkiWolf@*`ejemplo.org`*.
4. En Display name, ingrese **`NikkiWolf`**.
5. En Password, ingrese una contraseña segura o seleccione el icono del ojo para mostrar la contraseña que se generó automáticamente y copie o anote el valor que aparece.
6. Seleccione Properties y, en Name, ingrese **`Nikki`**. En Last name, ingrese **`Wolf`**.
7. Elija Review + create y, a continuación, seleccione Create.

Step 1.3

Paso 1.3: prueba de la experiencia de Nikki antes de asignarle permisos para AWS IAM Identity Center

En este procedimiento, verificará que Nikki puede iniciar sesión correctamente en el portal Mi cuenta de Microsoft.

1. En el mismo navegador, abra una pestaña nueva, vaya a la página de inicio de sesión del portal Mi cuenta e ingrese la dirección de correo electrónico completa de Nikki. Por ejemplo, NikkiWolf@*ejemplo.org*.
2. Cuando se le pida, ingrese la contraseña de Nikki y, a continuación, seleccione Sign in. Si se trata de una contraseña generada automáticamente, se le solicitará que la cambie.
3. En la página Action Required, seleccione Ask later para omitir la solicitud de métodos de seguridad adicionales.
4. En la página My account, en el menú de navegación izquierdo, seleccione My Apps. Tenga en cuenta que, además de los complementos, no se muestra ninguna aplicación en este momento. Agregará una aplicación de AWS IAM Identity Center que aparecerá aquí en un paso posterior.

Step 1.4

Paso 1.4: asignación de permisos a Nikki en Microsoft Entra ID

Ahora que ha comprobado que Nikki puede acceder correctamente al portal Mi cuenta, utilice este procedimiento para asignar su usuario a la aplicación de AWS IAM Identity Center.

1. En la consola del Centro de administración de Microsoft Entra, vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center en la lista.
2. A la izquierda, seleccione Users and groups.
3. Elija Agregar usuario o grupo. Puede ignorar el mensaje que indica que los grupos no están disponibles para su asignación. En este tutorial no se utilizan grupos para las asignaciones.
4. En la página Add Assignment, en Users, seleccione None Selected.
5. Seleccione NikkiWolf y, a continuación, Select.
6. En la página Agregar asignación, elija Asignar. NikkiWolf ahora aparece en la lista de usuarios asignados a la aplicación de AWS IAM Identity Center.

Paso 2: preparación de la cuenta de AWS

En este paso, seguirá las indicaciones para usar IAM Identity Center a fin de configurar los permisos de acceso (mediante un conjunto de permisos), crear manualmente el usuario correspondiente de Nikki Wolf y asignarle los permisos necesarios para administrar los recursos en AWS.

Step 2.1 >

Paso 2.1: creación de un conjunto de permisos de RegionalAdmin en IAM Identity Center

Este conjunto de permisos se utilizará para conceder a Nikki los permisos de cuenta de AWS necesarios para administrar las regiones desde la página Cuenta de la AWS Management Console. De forma predeterminada, todos los demás permisos para ver o administrar cualquier otra información de la cuenta de Nikki están denegados.

1. Abra la consola de IAM Identity Center
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija Crear conjunto de permisos.
4. En la página Seleccionar el tipo de conjunto de permisos, seleccione Conjunto de permisos personalizado y seleccione Siguiente.
5. Seleccione Política insertada para ampliarla y, a continuación, siga estos pasos para crear una política para el conjunto de permisos:
   a. Seleccione Agregar nueva instrucción para crear una instrucción de política.
   b. En Editar instrucción, seleccione Cuenta de la lista y, a continuación, seleccione las siguientes casillas de verificación.
      - **`ListRegions`**
      - **`GetRegionOptStatus`**
      - **`DisableRegion`**
      - **`EnableRegion`**
   c. Junto a Agregar un recurso, elija Agregar.
   d. En la página Agregar recurso, en Tipo de recurso, seleccione Todos los recursos y, a continuación, seleccione Agregar recurso. Compruebe que la política sea similar a la siguiente:

```
{
```

```
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Elija Siguiente.
7. En la página Especificar los detalles del conjunto de permisos, en Nombre de conjunto de permisos, escriba **`RegionalAdmin`** y, a continuación, seleccione Siguiente.
8. En la página Review and create (Revisar y crear), elija Create (Crear). Debería aparecer RegionalAdmin en la lista de conjuntos de permisos.

Step 2.2 >

Paso 2.2: creación del usuario NikkiWolf correspondiente en IAM Identity Center

Como el protocolo SAML no proporciona un mecanismo para consultar el IdP (Microsoft Entra ID) y crear usuarios automáticamente aquí en IAM Identity Center, utilice el siguiente procedimiento para crear manualmente un usuario de IAM Identity Center que refleje los atributos principales del usuario Nikki Wolf en Microsoft Entra ID.

1. Abra la consola de IAM Identity Center.
2. Seleccione Usuarios, Agregar usuario y, a continuación, proporcione la siguiente información:

    a. Nombre de usuario y Dirección de correo electrónico: ingrese la misma dirección **`NikkiWolf@`*`dominiodesuempresa.extensión`*** que utilizó al crear el usuario de Microsoft Entra ID. Por ejemplo, NikkiWolf@*`ejemplo.org`*.

    b. Confirmar dirección de correo electrónico: vuelva a ingresar la dirección de correo electrónico del paso anterior

c. Nombre: ingrese **`Nikki`**.

d. Apellidos: ingrese **`Wolf`**.

e. Nombre de visualización: ingrese **`Nikki Wolf`**.

3. Seleccione Siguiente dos veces, y a continuación, seleccione Agregar usuario.
4. Seleccione Close (Cerrar).

Step 2.3

Paso 2.3: asignación a Nikki del conjunto de permisos de RegionalAdmin en IAM Identity Center

Aquí encontrará la Cuenta de AWS en la que Nikki administrará las regiones y, a continuación, asignará los permisos necesarios para que pueda acceder correctamente al portal de acceso de AWS.

1. Abra la consola de IAM Identity Center
2. En Permisos para varias cuentas, elija Cuentas de AWS.
3. Seleccione la casilla de verificación situada junto al nombre de la cuenta (por ejemplo, *`Entorno aislado`*) donde quiere conceder a Nikki el acceso para administrar las regiones y, a continuación, seleccione Asignar usuarios y grupos.
4. En la página Asignar usuarios y grupos, seleccione la pestaña Usuarios, busque y marque la casilla situada junto a Nikki y, a continuación, seleccione Siguiente.

Paso 3: configuración y prueba de la conexión SAML

En este paso, debe configurar la conexión SAML mediante la aplicación empresarial de AWS IAM Identity Center en Microsoft Entra ID junto con la configuración del IdP externo en IAM Identity Center.

Step 3.1 >

Paso 3.1: recopilación de los metadatos del proveedor de servicios necesarios de IAM Identity Center

En este paso, iniciará el asistente Cambiar el origen de identidad desde la consola de IAM Identity Center y recuperará el archivo de metadatos y la URL de inicio de sesión específica de AWS que deberá ingresar al configurar la conexión con Microsoft Entra ID en el siguiente paso.

1. En la consola de IAM Identity Center, elija Configuración.
2. En la página de Configuraciones, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, elija Cambiar fuente de identidad.
3. En la página Elegir el origen de identidad, seleccione Proveedor de identidades externo y, a continuación, seleccione Siguiente.
4. En la página Configurar un proveedor de identidad externo, en Metadatos del proveedor de servicios, seleccione Descargar el archivo de metadatos para descargarlo en su sistema.
5. En la misma sección, busque el valor de URL de inicio de sesión del portal de acceso de AWS y cópielo. Deberá ingresar este valor en el siguiente paso cuando se le pida.
6. Deje esta página abierta y continúe con el siguiente paso (**`Step 3.2`**) para configurar la aplicación empresarial de AWS IAM Identity Center en Microsoft Entra ID. Más adelante, volverá a esta página para completar el proceso.

Step 3.2 >

Paso 3.2: configuración de la aplicación empresarial de AWS IAM Identity Center en Microsoft Entra ID

Este procedimiento establece la mitad de la conexión SAML en Microsoft mediante los valores del archivo de metadatos y la URL de inicio de sesión que obtuvo en el último paso.

1. En la consola del Centro de administración de Microsoft Entra, vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. A la izquierda, seleccione Single sign-on.
3. En la página Set up Single Sign-On with SAML, seleccione Upload metadata file, seleccione el icono de la carpeta, seleccione el archivo de metadatos del proveedor de servicios que descargó en el paso anterior y, a continuación, seleccione Add.
4. En la página Basic SAML Configuration, compruebe que los valores de Identifier y de Reply URL apuntan ahora a puntos de conexión de AWS que empiezan por `https://<REGION>.signin.aws.amazon.com/platform/saml/`.
5. En Sign on URL (Optional), pegue el valor de URL de inicio de sesión del portal de acceso de AWS que copió en el paso anterior (**`Step 3.1`**), seleccione Save y, a continuación, seleccione X para cerrar la ventana.

6. Si se le pide que pruebe el inicio de sesión único con AWS IAM Identity Center, seleccione No I'll test later. Realizará esta verificación en un paso posterior.
7. En la página Set up Single Sign-On with SAML, en la sección SAML Certificates, junto a Federation Metadata XML, seleccione Download para guardar el archivo de metadatos en el sistema. Deberá cargar este archivo en el siguiente paso cuando se le pida.

Step 3.3 >

Paso 3.3: configuración del IdP externo de Microsoft Entra ID en AWS IAM Identity Center

Aquí volverá al asistente Cambiar el origen de identidad de la consola de IAM Identity Center para completar la segunda mitad de la conexión SAML en AWS.

1. Vuelva a la sesión del navegador que dejó abierta en **`Step 3.1`** en la consola de IAM Identity Center.
2. En la página Configurar un proveedor de identidad externo, en la sección Metadatos del proveedor de identidad, en Metadatos SAML del IdP, pulse el botón Elegir archivo, seleccione el archivo de metadatos del proveedor de identidades que descargó de Microsoft Entra ID en el paso anterior y, a continuación, seleccione Abrir.
3. Elija Siguiente.
4. Cuando haya leído el aviso legal y tenga todo listo para continuar, ingrese **`ACCEPT`**.
5. Seleccione Cambiar el origen de identidad para aplicar los cambios.

Step 3.4 >

Paso 3.4: comprobación de que Nikki se redirige al portal de acceso de AWS

En este procedimiento, probará la conexión SAML; para ello, iniciará sesión en el portal Mi cuenta de Microsoft con las credenciales de Nikki. Cuando se autentique, seleccionará la aplicación de AWS IAM Identity Center que redirigirá a Nikki al portal de acceso de AWS.

1. Vaya a la página de inicio de sesión del portal Mi cuenta e ingrese la dirección de correo electrónico completa de Nikki. Por ejemplo, ***`NikkiWolf`***`@`*`ejemplo.org`*.
2. Cuando se le pida, ingrese la contraseña de Nikki y, a continuación, seleccione Sign in.
3. En la página My account, en el menú de navegación izquierdo, seleccione My Apps.
4. En la página My Apps, seleccione la aplicación denominada AWS IAM Identity Center. Esto debería solicitarle una autenticación adicional.

5. En la página de inicio de sesión de Microsoft, seleccione las credenciales de NikkiWolf. Si se le solicita la autenticación por segunda vez, vuelva a seleccionar las credenciales de NikkiWolf. Esto debería redirigirlo automáticamente al portal de acceso de AWS.

> **Tip**
>
> Si no se le redirige correctamente, compruebe que el valor de URL de inicio de sesión del portal de acceso de AWS que ha ingresado en **`Step 3.2`** coincide con el valor que ha copiado en **`Step 3.1`**.

6. Compruebe que aparece el icono de Cuenta de AWS

.

> **Tip**
>
> Si la página está vacía y no aparece el icono de Cuenta de AWS, confirme que Nikki se haya asignado correctamente al conjunto de permisos de RegionalAdmin (consulte **`Step 2.3`**).

Step 3.5

Paso 3.5: comprobación del nivel de acceso de Nikki para administrar su Cuenta de AWS

En este paso, comprobará el nivel de acceso de Nikki para administrar la configuración regional de su Cuenta de AWS. Nikki solo debe tener los privilegios de administrador suficientes para administrar las regiones desde la página Cuentas.

1. En el portal de acceso de AWS, seleccione el icono de Cuenta de AWS

para ampliar la lista de cuentas. Tras seleccionar el icono, aparecen los nombres de cuenta, los ID de cuenta y las direcciones de correo electrónico asociadas a las cuentas en las que haya definido conjuntos de permisos.

2. Seleccione el nombre de la cuenta (por ejemplo, *`Entorno aislado`*) en la que aplicó el conjunto de permisos (consulte **`Step 2.3`**). Esto ampliará la lista de conjuntos de permisos entre los que Nikki puede elegir para administrar su cuenta.

3. Junto a RegionalAdmin, seleccione Consola de administración para asumir el rol que definió en el conjunto de permisos de RegionalAdmin. Esto le redirige a la página de inicio de la AWS Management Console.
4. En la esquina superior derecha de la consola, seleccione el nombre de cuenta y, a continuación, seleccione Cuenta. El enlace le dirigirá a la página Cuenta. Observe que en todas las demás secciones de esta página aparece un mensaje en el que se indica que no tiene los permisos necesarios para ver ni modificar esos ajustes.
5. En la página Cuenta, desplácese hacia abajo hasta la sección Regiones de AWS. Seleccione la casilla de verificación de cualquier región disponible en la tabla. Tenga en cuenta que Nikki tiene los permisos necesarios para habilitar o deshabilitar la lista de regiones de su cuenta, tal y como estaba previsto.

> ¡Bien hecho!
>
> Los pasos del 1 al 3 lo ayudaron a implementar y probar correctamente la conexión SAML. Ahora, para completar el tutorial, le recomendamos que continúe con el paso 4 para implementar el aprovisionamiento automático.

Paso 4: configuración y comprobación de la sincronización de SCIM

En este paso, configurará el aprovisionamiento automático (sincronización) de la información del usuario desde Microsoft Entra ID a IAM Identity Center mediante el protocolo SCIM v2.0. Esta conexión se configura en el Microsoft Entra ID, mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center.

Al configurar la sincronización de SCIM, crea un mapeo de los atributos de usuario del proveedor en Microsoft Entra ID con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y Microsoft Entra ID.

En los siguientes pasos se explica cómo habilitar el aprovisionamiento automático de usuarios que se encuentran principalmente en Microsoft Entra ID a IAM Identity Center mediante la aplicación de IAM Identity Center en Microsoft Entra ID.

Step 4.1 >

Paso 4.1: creación de un segundo usuario de prueba en Microsoft Entra ID

Con fines de prueba, creará un nuevo usuario (Richard Roe) en Microsoft Entra ID. Más adelante, después de configurar la sincronización con SCIM, comprobará que este usuario y todos los atributos pertinentes se han sincronizado correctamente con IAM Identity Center.

1. En la consola del Centro de administración de Microsoft Entra, vaya a Identity > Users > All users.
2. Seleccione New user y, a continuación, seleccione Create new user en la parte superior de la pantalla.
3. En User principal name, ingrese **`RichRoe`** y, a continuación, seleccione el dominio y la extensión que desee. Por ejemplo, RichRoe@*`ejemplo.org`*.
4. En Display name, ingrese **`RichRoe`**.
5. En Password, ingrese una contraseña segura o seleccione el icono del ojo para mostrar la contraseña que se generó automáticamente y copie o anote el valor que aparece.
6. Seleccione Properties y, a continuación, facilite los siguientes valores:
   - First name: ingrese **`Richard`**.
   - Last name: ingrese **`Roe`**.
   - Job title: ingrese **`Marketing Lead`**.
   - Department: ingrese **`Sales`**.
   - Employee ID: ingrese **`12345`**.
7. Elija Review + create y, a continuación, seleccione Create.

Step 4.2 >

Paso 4.2: habilitación del aprovisionamiento automático en IAM Identity Center

En este procedimiento, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático a IAM Identity Center de los usuarios y grupos que proceden de Microsoft Entra ID.

1. Abra la consola de IAM Identity Center y seleccione Configuración en el panel izquierdo de navegación.
2. En la página Configuración, en la pestaña Origen de identidad, observe que Método de aprovisionamiento está establecido en Manual.
3. Busque el cuadro de información Aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity

Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.

4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie cada uno de los valores de las siguientes opciones. Deberá pegar estos valores en el siguiente paso cuando configure el aprovisionamiento en Microsoft Entra ID.

   a. Punto de conexión de SCIM: por ejemplo, https://scim.*us-east-2*.amazonaws.com/*1111111111-2222-3333-4444-555555555555*/scim/v2/

   b. Token de acceso: seleccione Mostrar token para copiar el valor.

5. Elija Close.
6. En la pestaña Origen de identidad, observe que Método de aprovisionamiento ahora está establecido en SCIM.

Step 4.3 >

Paso 4.3: configuración del aprovisionamiento automático en Microsoft Entra ID

Ahora que ha creado su usuario de prueba RichRoe y ha habilitado SCIM en IAM Identity Center, puede continuar con la configuración de los ajustes de sincronización de SCIM en Microsoft Entra ID.

1. En la consola del Centro de administración de Microsoft Entra, vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. Seleccione Provisioning y, en Manage, vuelva a seleccionar Provisioning.
3. En Provisioning Mode, seleccione Automatic.
4. En Admin Credentials, en Tenant URL, pegue el valor de la URL de Punto de conexión de SCIM que copió anteriormente en **`Step 4.1`**. En Secret Token, pegue el valor de Access token.
5. Elija Test Connection. Debería ver un mensaje que indica que las credenciales probadas se autorizaron correctamente para habilitar el aprovisionamiento.
6. Elija Guardar.
7. En Manage, seleccione Users and groups y, a continuación, seleccione Add user/group.
8. En la página Add Assignment, en Users, seleccione None Selected.
9. Seleccione RichRoe y, a continuación, Select.
10. En la página Agregar asignación, elija Asignar.

11. Seleccione Overview y, a continuación, seleccione Start provisioning.

Step 4.4

Paso 4.4: comprobación de que se ha producido la sincronización

En esta sección, verificará que el usuario de Richard se aprovisionó correctamente y que todos los atributos se muestran en IAM Identity Center.

1. En la consola de IAM Identity Center, seleccione Usuarios.
2. En la página Usuarios, debería aparecer el usuario RichRoe. Observe que, en la columna Creado por, el valor está establecido en SCIM.
3. Seleccione RichRoe y, en Perfil, compruebe que se hayan copiado los siguientes atributos de Microsoft Entra ID.

   - Nombre: **`Richard`**.
   - Apellido: **`Roe`**.
   - Departamento: **`Sales`**.
   - Título: **`Marketing Lead`**.
   - Número de empleado: **`12345`**.

   Ahora que el usuario de Richard se ha creado en IAM Identity Center, puede asignarlo a cualquier conjunto de permisos para controlar el nivel de acceso que tiene a sus recursos de AWS. Por ejemplo, puede asignar RichRoe al conjunto de permisos de **`RegionalAdmin`** que utilizó anteriormente para conceder a Nikki los permisos para administrar las regiones (consulte **`Step 2.3`**) y, a continuación, probar su nivel de acceso mediante **`Step 3.5`**.

> ¡Enhorabuena!
>
> Ha configurado correctamente una conexión SAML entre Microsoft y AWS y ha comprobado que el aprovisionamiento automático funciona para mantener todo sincronizado. Ahora puede aplicar lo aprendido para configurar su entorno de producción de forma más fluida.

Consideraciones que hay que tener en cuenta sobre el uso de SCIM con Microsoft Entra ID en un entorno de producción

Las siguientes son consideraciones importantes sobre Microsoft Entra ID que pueden afectar a la forma en que planea implementar el aprovisionamiento automático con IAM Identity Center en su entorno de producción mediante el protocolo SCIM v2.

> **Note**
>
> Antes de comenzar a implementar SCIM, le recomendamos revisar primero las Consideraciones para utilizar el aprovisionamiento automático.

Atributos para controlar el acceso

Los atributos para el control de acceso se utilizan en las políticas de permisos que determinan quién de su origen de identidad puede acceder a sus recursos de AWS. Si se elimina un atributo de un usuario en Microsoft Entra ID, ese atributo no se eliminará del usuario correspondiente en IAM Identity Center. Se trata de una limitación conocida en Microsoft Entra ID. Si un atributo se cambia a un valor diferente (no vacío) en un usuario, ese cambio se sincronizará con IAM Identity Center.

Agrupación anidada

El servicio de aprovisionamiento de usuarios de Microsoft Entra ID no puede leer ni aprovisionar usuarios en grupos anidados. Solo se pueden leer y aprovisionar los usuarios que sean miembros inmediatos de un grupo asignado explícitamente. Microsoft Entra ID no desglosa de forma recursiva las pertenencias a grupos de usuarios o grupos asignados indirectamente (usuarios o grupos que son miembros de un grupo asignado directamente). Para obtener más información, consulte Ámbito basado en asignaciones en la documentación de Microsoft Entra ID.

Grupos dinámicos

El servicio de aprovisionamiento de usuarios de Microsoft Entra ID puede leer y aprovisionar usuarios en grupos dinámicos. Consulte a continuación un ejemplo que muestra la estructura de usuarios y grupos al utilizar grupos dinámicos y cómo se muestran en IAM Identity Center. Estos usuarios y grupos se aprovisionaron desde Microsoft Entra ID IAM Identity Center mediante SCIM

Por ejemplo, si la Microsoft Entra ID estructura de los grupos dinámicos es la siguiente:

1. Grupo A con los miembros ua1, ua2

2. Grupo B con miembros ub1
3. Grupo C con miembros uc1
4. Grupo K con una regla para incluir a los miembros de los grupos A, B, C
5. Grupo K con una regla para incluir a los miembros de los grupos A, B, C

Una vez que la información del usuario y el grupo se aprovisione desde Microsoft Entra ID a IAM Identity Center a través de SCIM, la estructura será la siguiente:

1. Grupo A con los miembros ua1, ua2
2. Grupo B con miembros ub1
3. Grupo C con miembros uc1
4. Grupo K con miembros ua1, ua2, ub1, uc1
5. Grupo L con miembros ub1, uc1

Cuando configure el aprovisionamiento automático mediante grupos dinámicos, tenga en cuenta las siguientes consideraciones.

- Un grupo dinámico puede incluir un grupo anidado. Sin embargo, el servicio de aprovisionamiento de Microsoft Entra ID no aplana el grupo anidado. Por ejemplo, si tiene la siguiente estructura de Microsoft Entra ID para grupos dinámicos:
  - El grupo A es un elemento principal del grupo B.
  - El grupo A tiene a ua1 como miembro.
  - El grupo B tiene a ub1 como miembro.

El grupo dinámico que incluye al grupo A solo incluirá a los miembros directos del grupo A (es decir, ua1). No incluirá de forma recursiva a los miembros del grupo B.

- Los grupos dinámicos no pueden contener otros grupos dinámicos. Para obtener más información, consulte Limitaciones de vista previa en la documentación de Microsoft Entra ID.

Solución de problemas de SCIM con Microsoft Entra ID

Si tiene problemas con usuarios de Microsoft Entra ID que no se sincronizan con IAM Identity Center, es posible que se deba a un problema de sintaxis que IAM Identity Center ha detectado al agregar un nuevo usuario a IAM Identity Center. Para confirmarlo, consulte los registros de auditoría de

Microsoft Entra ID para ver si hay eventos con errores, como `'Export'`. El motivo del estado de este evento indicará:

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is
 unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

También puede consultar en AWS CloudTrail el evento fallido. Para ello, busque en la consola Event History de CloudTrail con el siguiente filtro:

```
"eventName":"CreateUser"
```

El error del evento CloudTrail indicará lo siguiente:

```
"errorCode": "ValidationException",
        "errorMessage": "Currently list attributes only allow single item“
```

En última instancia, esta excepción significa que uno de los valores transferidos desde Microsoft Entra ID contenía más valores de los previstos. La solución en este caso consiste en revisar los atributos del usuario de Microsoft Entra ID, asegurándose de que ninguno contenga valores duplicados. Un ejemplo habitual de valores duplicados es la presencia de varios valores en los números de contacto, como el número de móvil, trabajo y fax. Aunque son valores independientes, todos se transfieren al IAM Identity Center con el atributo principal phoneNumbers.

Para obtener sugerencias generales acerca de la solución de problemas de SCIM, consulte Resolución de problemas de IAM Identity Center.

Paso 5: (opcional) configuración de ABAC

Ahora que se ha configurado SAML y SCIM, puede optar por configurar el control de acceso basado en atributos (ABAC). El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos basados en atributos.

Con Microsoft Entra ID, puede utilizar uno de los dos métodos siguientes para configurar ABAC para su uso con IAM Identity Center.

Method 1

> Método 1: configuración de atributos de usuario en Microsoft Entra ID para el control de acceso en IAM Identity Center

En el siguiente procedimiento, determinará qué atributos de Microsoft Entra ID debe utilizar IAM Identity Center para administrar el acceso a sus recursos de AWS. Una vez definidos, Microsoft Entra ID envía estos atributos a IAM Identity Center mediante aserciones de SAML. A continuación, tendrás que Crea un conjunto de permisos. en IAM Identity Center para gestionar el acceso en función de los atributos que transferiste desde Microsoft Entra ID.

Antes de comenzar con este procedimiento, primero debes habilitar la característica Atributos para controlar el acceso. Para obtener más información acerca de cómo hacerlo, consulte Habilitación y configuración de atributos para el control de acceso.

1. En la consola del Centro de administración de Microsoft Entra, vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. Elija Single sign-on (Inicio de sesión único).
3. En la sección Attributes & Claims, elija Edit.
4. En la página Attributes & Claims, haga lo siguiente:
    a. Elija Añadir nueva reclamación.
    b. En Nombre, ingrese `AccessControl:`*`AttributeName`*. Replace *`AttributeName`*por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `AccessControl:`**`Department`**.
    c. En Namespace (Espacio de nombres), escriba **`https://aws.amazon.com/SAML/Attributes`**.
    d. En Source (Origen), elija Attribute (Atributo).
    e. En Atributo de origen, utilice la lista desplegable para elegir los atributos del usuario de Microsoft Entra ID. Por ejemplo, `user.`**`department`**.
5. Repita el paso anterior para cada atributo que necesite enviar a IAM Identity Center en la aserción SAML.
6. Seleccione Save.

Method 2

Método 2: configuración de ABAC con IAM Identity Center

Si lo desea, puede utilizar la característica Atributos para controlar el acceso de IAM Identity Center para transferir un elemento de `Attribute`con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**. Este

elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, para pasar los pares clave-valor de etiquetas de `CostCenter = blue`, utilice el siguiente atributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento de `Attribute` independiente para cada etiqueta.

Configuración de SAML y SCIM con Okta e IAM Identity Center

Puede aprovisionar la información de usuarios y grupos desde Okta a IAM Identity Center de forma automática (sincronización) mediante el protocolo del sistema de administración de identidades entre dominios (SCIM) v2.0. Esta conexión se configura en Okta, mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en Okta con los atributos nombrados en IAM Identity Center. Esta asignación vincula los atributos de usuario esperados entre IAM Identity Center y Okta.

Okta admite las siguientes características de aprovisionamiento cuando se conecta al IAM Identity Center a través de SCIM:

- Crear usuarios: los usuarios asignados a la aplicación IAM Identity Center Okta se aprovisionan en IAM Identity Center.
- Actualizar los atributos de usuario: los cambios en los atributos de los usuarios que están asignados a la aplicación IAM Identity Center Okta se actualizan en IAM Identity Center.
- Desactivar usuarios: los usuarios que no están asignados en la aplicación IAM Identity Center Okta están deshabilitados en IAM Identity Center.

- Transferencia de grupos: los grupos (y sus miembros) de Okta se sincronizan con IAM Identity Center.

> **Note**
>
> Para minimizar la sobrecarga administrativa tanto en Okta como en IAM Identity Center, le recomendamos que asigne y transfiera grupos en lugar de usuarios individuales.

Si aún no ha habilitado IAM Identity Center, consulte Habilitar AWS IAM Identity Center.

Objetivo

En este tutorial, seguirá las indicaciones para configurar una conexión SAML con IAM Identity Center en Okta. Más adelante, sincronizará los usuarios desde Okta mediante SCIM. En este escenario, administrará todos los usuarios y grupos en Okta. Los usuarios inician sesión a través del portal de Okta. Para comprobar que todo está configurado correctamente, tras completar los pasos de configuración, iniciará sesión como Okta usuario y verificará el acceso a AWS los recursos.

> **Note**
>
> Puede registrarse para obtener una cuenta de Okta (prueba gratuita) que tenga instalada la aplicación IAM Identity Center de Okta. En el caso de los productos de pago de Okta, es posible que deba confirmar que su licencia de Okta admite la administración del ciclo de vida o capacidades similares que permitan el aprovisionamiento saliente. Estas características pueden ser necesarias para configurar SCIM desde Okta a IAM Identity Center.

Antes de empezar

Antes de configurar el aprovisionamiento de SCIM entre el IAM Identity Center Okta y el IAM, le recomendamos que lo revise primero. Consideraciones para utilizar el aprovisionamiento automático

Confirme los siguientes elementos antes de comenzar:

- Todos los usuarios de Okta deben tener un valor especificado para Nombre, Apellidos, Nombre de usuario y Nombre de visualización.
- Cada usuario de Okta tiene un único valor por atributo de datos, como la dirección de correo electrónico o el número de teléfono. Los usuarios que tengan varios valores no se sincronizarán.

Si hay usuarios que tienen varios valores en sus atributos, elimine los atributos duplicados antes de intentar aprovisionar el usuario en IAM Identity Center. Por ejemplo, solo se puede sincronizar un atributo de número de teléfono. Como el atributo de número de teléfono predeterminado es “teléfono del trabajo”, utilice el atributo “teléfono del trabajo” para almacenar el número de teléfono del usuario, incluso si el número de teléfono del usuario es un teléfono fijo o móvil.

- Si actualiza la dirección de un usuario, debe especificar los valores de la calle, ciudad, estado, código postal y código de país. Si no se especifica ninguno de estos valores para el usuario de Okta en el momento de la sincronización, no se aprovisionará el usuario (ni los cambios que se realicen en él).

> **Note**
>
> Los derechos y los atributos de rol no son compatibles y no se pueden sincronizar con IAM Identity Center.
> Actualmente, no es posible usar el mismo grupo de Okta para la transferencia de tareas y grupos. Para mantener una pertenencia uniforme a los grupos entre Okta e IAM Identity Center, cree un grupo independiente y configúrelo para enviar grupos a IAM Identity Center.

Paso 1: obtención de los metadatos de SAML de su cuenta de Okta

1. Inicie sesión en el Okta admin dashboard, expanda Applications y, a continuación, seleccione Applications.
2. En la página Applications, elija Browse App Catalog (Examinar catálogo de aplicaciones).
3. En el cuadro de búsqueda AWS IAM Identity Center, escriba y seleccione la aplicación para añadir la aplicación IAM Identity Center.
4. Seleccione la pestaña Sign On.
5. En SAML Signing Certificates, seleccione Actions y, a continuación, View IdP Metadata. Se abre una nueva pestaña del navegador en la que se muestra el árbol de documentos de un archivo XML. Seleccione todo el XML de `<md:EntityDescriptor>` a `</md:EntityDescriptor>` y cópielo en un archivo de texto.
6. Guarde el archivo de texto como `metadata.xml`.

Deje el Okta admin dashboard abierto; seguirá usando esa consola en los pasos posteriores.

Paso 2: configuración de Okta como origen de identidad para IAM Identity Center

1. Abra la consola de IAM Identity Center como usuario con privilegios administrativos.
2. Elija Configuración en el panel de navegación izquierdo.
3. En la página Configuración, seleccione Acciones y, a continuación, seleccione Cambiar el origen de identidad.
4. En Elegir la fuente de identidad, seleccione Proveedor de identidades externo y, a continuación, Siguiente.
5. En Configurar un proveedor de identidad externo, haga lo siguiente:

   a. En Metadatos del proveedor de servicios, seleccione Descargar archivo de metadatos para descargar el archivo de metadatos de IAM Identity Center y guardarlo en el sistema. Proporcionará el archivo de metadatos de SAML de IAM Identity Center a Okta más adelante en este tutorial.

      Copie los siguientes elementos en un archivo de texto para acceder a ellos fácilmente:

      - URL del Servicio de consumidor de aserciones (ACS) de IAM Identity Center
      - URL del emisor de IAM Identity Center

      Necesitará estos valores más adelante en este tutorial.

   b. En Metadatos del proveedor de identidad, en IdP SAML meta, selecciona Elegir archivo y, a continuación, selecciona el `metadata.xml` archivo que creaste en el paso anterior.

   c. Elija Siguiente.
6. Cuando haya leído el aviso legal, introduzca ACCEPT para continuar.
7. Elija Cambiar fuente de identidad.

   Deja la AWS consola abierta y seguirás utilizándola en el siguiente paso.
8. Vuelva al Okta admin dashboard y seleccione la pestaña Sign On de la aplicación AWS IAM Identity Center y, a continuación, haga clic en Edit.
9. En Advanced Sign-on Settings, ingrese lo siguiente:

   - En el campo ACS URL, ingrese el valor que ha copiado de URL del Servicio de consumidor de aserciones (ACS) de IAM Identity Center.
   - En Issuer URL, ingrese el valor que ha copiado de URL del emisor de IAM Identity Center.

- En Application username format, seleccione una de las opciones del menú desplegable.

  Asegúrese de que el valor que elija sea único para cada usuario. Para este tutorial, seleccione Okta username.

10. Seleccione Guardar.

Ya tiene todo listo para aprovisionar a usuarios desde Okta en IAM Identity Center. Deje la casilla Okta admin dashboard abierta y vuelva a la consola del IAM Identity Center para continuar con el siguiente paso.

Paso 3: aprovisionamiento de usuarios desde Okta

1. En la consola de IAM Identity Center, en la página Configuración, busque el cuadro de información Aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión de SCIM y el token de acceso.
2. En el cuadro de diálogo Aprovisionamiento automático entrante, copie cada uno de los valores de las siguientes opciones:

   - Punto de conexión de SCIM
   - Token de acceso

   Más adelante en este tutorial, introducirá estos valores para configurar el aprovisionamiento. Okta
3. Elija Close.
4. Vuelva al Okta admin dashboard y acceda a la aplicación IAM Identity Center.
5. En la página de la aplicación IAM Identity Center, seleccione la pestaña Aprovisionamiento y, a continuación, en el menú de navegación de la izquierda, en Configuración, elija Integración.
6. Seleccione Editar y, a continuación, active la casilla de verificación situada junto a Habilitar la integración de la API para activar el aprovisionamiento.
7. Configure Okta con los valores de aprovisionamiento de SCIM de IAM Identity Center que copió anteriormente en este tutorial:

   a. En el campo Base URL, ingrese el valor de Punto de conexión de SCIM. Asegúrese de eliminar la barra inclinada que aparece al final de la URL.

b. En el campo API Token, ingrese el valor de Token de acceso.

8. Elija Verificar credenciales de API para comprobar que las credenciales introducidas son válidas.

   Aparecerá el mensaje AWS IAM Identity Center was verified successfully!.

9. Seleccione Guardar. Se abrirá el área de configuración, con la integración seleccionada.
10. En Configuración, selecciona Ir a la aplicación y, a continuación, selecciona la casilla Habilitar para cada una de las funciones del aprovisionamiento a la aplicación que desees habilitar. Para este tutorial, seleccione todas las opciones.
11. Seleccione Guardar.

Ya tiene todo listo para sincronizar los usuarios desde Okta con IAM Identity Center.

Paso 4: sincronización de los usuarios desde Okta con IAM Identity Center

De forma predeterminada, no hay ningún usuario o grupo asignado a su aplicación IAM Identity Center de Okta. Los grupos de aprovisionamiento aprovisionan a los usuarios que sean miembros del grupo. Complete los siguientes pasos para sincronizar grupos y usuarios con IAM Identity Center.

1. En la página de la aplicación Okta IAM Identity Center, seleccione la pestaña Asignaciones. Puede asignar personas y grupos a la aplicación IAM Identity Center.

   a. Para asignar personas:

      - En la página Assignments, seleccione Assign y, a continuación, seleccione Assign to people.
      - Seleccione los usuarios de Okta que desee que tengan acceso a la aplicación IAM Identity Center. Seleccione Asignar, luego Guardar y volver y, a continuación, seleccione Terminado.

      Esto inicia el proceso de aprovisionamiento de los usuarios en IAM Identity Center.

   b. Para asignar grupos:

      - En la página Assignments, seleccione Assign y, a continuación, seleccione Assign to groups.
      - Seleccione los grupos de Okta que desee que tengan acceso a la aplicación IAM Identity Center. Seleccione Asignar, luego Guardar y volver y, a continuación, seleccione Terminado.

Esto inicia el proceso de aprovisionamiento del usuario o los usuarios en IAM Identity Center.

> **Note**
>
> Es posible que deba especificar más atributos para el grupo si no están presentes en todos los registros de usuario. Los atributos especificados para el grupo anularán cualquier valor de atributo individual.

2. Seleccione la pestaña Transferir grupos. Seleccione el grupo de Okta que contiene todos los grupos que asignó a la aplicación IAM Identity Center. Seleccione Guardar.

   El estado del grupo cambia a Active después de que el grupo y sus miembros se hayan transferido a IAM Identity Center.

3. Vuelva a la pestaña Assignments.

4. Si tiene usuarios que no son miembros de los grupos que ha enviado a IAM Identity Center, agréguelos de forma individual siguiendo estos pasos:

   En la página de tareas, seleccione Asignar y, a continuación, seleccione Asignar a personas.

5. Seleccione los usuarios de Okta que desee que tengan acceso a la aplicación IAM Identity Center. Seleccione Asignar, luego Guardar y volver y, a continuación, seleccione Terminado.

   Esto inicia el proceso de aprovisionamiento de los usuarios individuales en IAM Identity Center.

   > **Note**
   >
   > También puede asignar usuarios y grupos a la AWS IAM Identity Center aplicación desde la página Aplicaciones delOkta admin dashboard. Para ello, seleccione el icono Settings, seleccione Assign to Users o Assign to Groups y, a continuación, especifique el usuario o el grupo.

6. Vuelva a la consola de IAM Identity Center. En el menú de navegación de la izquierda, seleccione Users. Debería ver la lista de usuarios rellenada por sus usuarios de Okta.

¡Enhorabuena!

Ha configurado correctamente una conexión SAML entre Okta AWS y ha comprobado que el aprovisionamiento automático funciona. Ahora puede asignar a estos usuarios cuentas y aplicaciones en IAM Identity Center. Para este tutorial, en el siguiente paso designaremos a uno de los usuarios como administrador de IAM Identity Center mediante la concesión de permisos administrativos en la cuenta de administración.

Paso 5: concesión de acceso a las cuentas a usuarios de Okta

1. En el panel de navegación del IAM Identity Center, en Permisos para varias cuentas, seleccione Cuentas de AWS.
2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la raíz organizativa con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:

    a. En Paso 1: selección de usuarios y grupos, elija el usuario que realizará la función del trabajo de administrador. A continuación, elija Next.

    b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.

        i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:

        - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
        - En Política para un conjunto de permisos predefinido, elija. AdministratorAccess

        Elija Siguiente.

        ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

        La configuración predeterminada crea un conjunto de permisos denominado *`AdministratorAccess`*con una duración de sesión establecida en una hora.

        iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página

Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.

En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.

En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de *AdministratorAccess*permisos que ha creado aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.

c. En Paso 3: revisión y envío, revise el usuario y el conjunto de permisos seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Volverá a la Cuentas de AWS página. Un mensaje de notificación le informa de que se Cuenta de AWS ha vuelto a aprovisionar y se ha aplicado el conjunto de permisos actualizado. Cuando el usuario inicie sesión, tendrá la opción de elegir el rol. *AdministratorAccess*

> **Note**
>
> La sincronización automática de SCIM de Okta solo permite el aprovisionamiento de usuarios; los grupos no se aprovisionan automáticamente. No puede crear grupos para los usuarios de Okta mediante la AWS Management Console. Después de aprovisionar a los usuarios, puede crear grupos mediante una operación de la CLI o la API.

Paso 6: Confirme el acceso de Okta los usuarios a los recursos AWS

1. Inicie sesión en el Okta dashboard con una cuenta de usuario de prueba.
2. En My Apps, seleccione el icono de AWS IAM Identity Center.
3. Ha iniciado sesión en el portal y puede ver el Cuenta de AWS icono. Amplíe ese icono para ver la lista a la Cuentas de AWS que puede acceder el usuario. En este tutorial, solo trabajó con una cuenta, por lo que al expandir el icono solo se muestra una cuenta.

4. Seleccione la cuenta para ver los conjuntos de permisos disponibles para el usuario. En este tutorial, creó el conjunto de AdministratorAccesspermisos.
5. Junto al conjunto de permisos hay enlaces para el tipo de acceso disponible para ese conjunto de permisos. Cuando creó el conjunto de permisos, especificó que se habilitó el acceso mediante programación y con la Consola de administración, por lo que esas dos opciones están presentes. Seleccione Consola de administración para abrir la AWS Management Console.
6. El usuario ha iniciado sesión en la consola.

(Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica Atributos para controlar el acceso de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

Siguientes pasos

Ahora que ha configurado Okta como proveedor de identidades y ha aprovisionado a usuarios en IAM Identity Center, puede hacer lo siguiente:

- Conceda acceso a Cuentas de AWS, consulteAsigne el acceso de los usuarios a Cuentas de AWS.

- Para conceder acceso a las aplicaciones en la nube, consulte Asignar el acceso de los usuarios a las aplicaciones en la consola de IAM Identity Center.
- Para configurar los permisos en función de los cargos en el trabajo; consulte Create a permission set.

Configuración del aprovisionamiento de SCIM entre OneLogin e IAM Identity Center

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de usuarios y grupos desde OneLogin a IAM Identity Center mediante el protocolo System for Cross-Domain Identity Management (SCIM) v2.0. Esta conexión se configura en el OneLogin, mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center. Al configurar la sincronización de SCIM, crea un mapeo de los atributos de usuario en OneLogin con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y OneLogin.

Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de usuarios y grupos desde OneLogin a IAM Identity Center mediante el protocolo SCIM.

> **Note**
>
> Antes de comenzar a implementar SCIM, le recomendamos revisar primero las Consideraciones para utilizar el aprovisionamiento automático.

Temas

Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Una cuenta de OneLogin. Si no tienes una cuenta existente, es posible que puedas obtener una cuenta de prueba gratuita o una cuenta de desarrollador en el OneLoginsitio web.
- Una cuenta habilitada para IAM Identity Center (gratuita). Para más información, consulte Activar IAM Identity Center.
- Una conexión SAML desde su cuenta OneLogin al IAM Identity Center. Para obtener más información, consulte Habilitar el inicio de sesión único entre OneLogin y AWS en el Partner Network Blog de AWS.

Paso 1: Habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie cada uno de los valores de las siguientes opciones. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.

    a. Punto de conexión de SCIM

    b. Token de acceso
5. Elija Close.

Ha configurado el aprovisionamiento en la consola de IAM Identity Center. Ahora debe realizar las tareas restantes mediante la interfaz de usuario OneLogin, tal y como se describe en los siguientes procedimientos.

Paso 2: Configure el aprovisionamiento en OneLogin

Utilice el siguiente procedimiento en el portal de administración de OneLogin para habilitar la integración entre IAM Identity Center y la aplicación IAM Identity Center. Este procedimiento supone que ya ha configurado la aplicación Single Sign-On de AWS en OneLogin para la autenticación SAML. Si aún no ha creado esta conexión SAML, hágalo antes de continuar y, a continuación, vuelva aquí para completar el proceso de aprovisionamiento del SCIM. Para obtener más información para configurar SAML con OneLogin, consulte Habilitar el inicio de sesión único entre OneLogin y AWS en el Partner Network Blog de AWS.

Para configurar el aprovisionamiento en OneLogin

1. Inicie sesión yOneLogin, a continuación, vaya a Aplicaciones > Aplicaciones.
2. En la página Aplicaciones, busque la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center. Elija Configuración en la barra de navegación izquierda.
3. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL base de SCIM en OneLogin. Asegúrese de eliminar la barra diagonal que aparece al final de la URL. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Tokens portadores de SCIM en OneLogin.
4. Junto a Conexión API, haga clic en Habilitar y, a continuación, en Guardar para completar la configuración.
5. En la barra de navegación de la izquierda, elija Proveedores de identidades.
6. Seleccione las casillas de verificación Habilitar el aprovisionamiento, Crear usuario, Eliminar usuario y Actualizar usuario y, a continuación, seleccione Guardar.
7. En la barra de navegación, seleccione Usuarios.
8. Haz clic en Más acciones y selecciona Sincronizar inicios de sesión. Deberías recibir el mensaje Sincronizar usuarios con Single Sign-On de AWS.
9. Vuelva a hacer clic en Más acciones y, a continuación, seleccione Volver a aplicar las asignaciones de derechos. Debería recibir el mensaje Se están reaplicando las asignaciones.
10. En este punto, debería comenzar el proceso de aprovisionamiento. Para confirmarlo, vaya a Actividad > Eventos y supervise el progreso. Los eventos de aprovisionamiento correctos, así como los errores, deberían aparecer en la secuencia de eventos.

11. Para comprobar que todos sus usuarios y grupos se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios sincronizados de OneLogin aparecerán en la página de Usuarios. También puedes ver tus grupos sincronizados en la página Grupos.
12. Para sincronizar automáticamente los cambios de los usuarios con IAM Identity Center, vaya a la página de Aprovisionamiento, busque la sección Requerir la aprobación del administrador antes de realizar esta acción, anule la selección de Crear usuario, Eliminar usuario o Actualizar usuario y haga clic en Guardar.

(Opcional) Paso 3: Configure los atributos de usuario en OneLogin para el control de acceso en IAM Identity Center

Este es un procedimiento opcional para OneLogin, en caso de que quiera configurar atributos para que IAM Identity Center administre el acceso a sus recursos de AWS. Los atributos que defina en OneLogin se transfieren en una aserción de SAML a IAM Identity Center. A continuación, deberá crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde OneLogin.

Antes de comenzar con este procedimiento, primero debes habilitar la característica Atributos para controlar el acceso. Para obtener más información acerca de cómo hacerlo, consulte Habilitación y configuración de atributos para el control de acceso.

Para configurar atributos de usuario utilizados en OneLogin para el control de acceso en IAM Identity Center

1. Inicie sesión yOneLogin, a continuación, vaya a Aplicaciones > Aplicaciones.
2. En la página Aplicaciones, busque la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center. En la barra de navegación izquierda, seleccione y, a continuación, .
3. En la sección Parámetros obligatorios, haga lo siguiente para cada atributo que desee utilizar en IAM Identity Center:

    a. Elija +.

    b. En Nombre del campo, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`** y sustituya **`AttributeName`** por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

c. En Banderas, marque la casilla situada junto a Incluir en la afirmación de SAML y seleccione Guardar.

d. En el campo Valor, usa la lista desplegable para elegir los atributos del usuario de OneLogin. Por ejemplo, Departamento.

4. Seleccione Guardar.

(Opcional) Pasar atributos para el control de acceso

Si lo desea, puede utilizar la característica Atributos para controlar el acceso de IAM Identity Center para transferir un elemento de `Attribute`con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, para pasar los pares clave-valor de etiquetas de `CostCenter = blue`, utilice el siguiente atributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento de `Attribute` independiente para cada etiqueta.

Solución de problemas

La siguiente información puede ayudarle a solucionar algunos problemas comunes que puede encontrarse a la hora de configurar o utilizar la consola de OneLogin.

Los grupos no se aprovisionan en IAM Identity Center

De forma predeterminada, los grupos no se pueden aprovisionar desde OneLogin a IAM Identity Center. Asegúrese de haber activado el aprovisionamiento de grupos para su aplicación de IAM Identity Center en OneLogin. Para ello, inicie sesión en la consola de administración de OneLogin y compruebe que la opción Incluir en el aprovisionamiento de usuarios esté seleccionada en las

propiedades de la aplicación IAM Identity Center (Aplicación IAM Identity Center > Parámetros > Grupos). Para obtener más información sobre cómo crear grupos en OneLogin, incluida la forma de sincronizar los roles de OneLogin como grupos en SCIM, consulte el sitio web de OneLogin.

No se sincroniza nada desde OneLogin a IAM Identity Center, a pesar de que todos los ajustes son correctos

Además de la nota anterior sobre la aprobación del administrador, tendrá que volver a aplicar las asignaciones de derechos para que se apliquen muchos cambios de configuración. Esto se encuentra en Aplicaciones > Aplicaciones > Aplicación IAM Identity Center > Más acciones. Puede ver los detalles y los registros de la mayoría de las acciones en OneLogin, incluidos los eventos de sincronización, en Actividad > Eventos.

He eliminado o desactivado un grupo en OneLogin, pero sigue apareciendo en IAM Identity Center

Actualmente, OneLogin no admite la operación SCIM DELETE para grupos, lo que significa que el grupo sigue existiendo en IAM Identity Center. Por lo tanto, deberá eliminar el grupo directamente de IAM Identity Center para asegurarse de que se eliminen todos los permisos correspondientes en IAM Identity Center para ese grupo.

He eliminado un grupo de IAM Identity Center sin eliminarlo primero de OneLogin y ahora tengo problemas de sincronización entre usuarios y grupos

Para solucionar esta situación, primero asegúrese de no tener ninguna regla o configuración de aprovisionamiento de grupos redundante en OneLogin. Por ejemplo, un grupo asignado directamente a una aplicación junto con una regla que se publica en el mismo grupo. A continuación, elimine los grupos no deseados de IAM Identity Center. Por último, en OneLogin, actualice los derechos (aplicación IAM Identity Center > Aprovisionamiento > Derechos) y, a continuación, vuelva a aplicar las asignaciones de derechos (aplicación IAM Identity Center >Más acciones). Para evitar este problema en el futuro, primero realice el cambio para dejar de aprovisionar el grupo en OneLogin y, a continuación, elimine el grupo de IAM Identity Center.

Uso de productos de Ping Identity con IAM Identity Center

Los siguientes productos de Ping Identity se han probado con IAM Identity Center.

Temas

- PingFederate
- PingOne

PingFederate

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios desde PingFederate por parte de Ping Identity (de ahora en adelante “Ping”) a IAM Identity Center. Este aprovisionamiento utiliza el protocolo System for Cross-Domain Identity Management (SCIM) v2.0. Esta conexión se configura en PingFederate mediante el punto de conexión SCIM y el token de acceso de IAM Identity Center. Al configurar la sincronización de SCIM, crea un mapeo de los atributos de usuario en PingFederate con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y PingFederate.

Esta guía se basa en la versión 10.2 de PingFederate. Los pasos para las versiones más recientes pueden variar. Póngase en contacto con Ping para obtener más información sobre cómo configurar el aprovisionamiento en IAM Identity Center para otras versiones de PingFederate.

Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de usuarios y grupos desde PingFederate a IAM Identity Center mediante el protocolo SCIM.

> **Note**
>
> Antes de comenzar a implementar SCIM, le recomendamos revisar primero las Consideraciones para utilizar el aprovisionamiento automático. A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

Temas

Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Un PingFederate servidor que funcione. Si no tienes una cuenta existente en el server de PingFederate, es posible que puedas obtener una cuenta de prueba gratuita o una cuenta de desarrollador en el sitio web de Ping Identity. La versión de prueba incluye licencias y descargas de software y la documentación asociada.
- Una copia del software IAM Identity Center Connector de PingFederate instalado en su servidor de PingFederate. Para obtener más información sobre cómo obtener este software, consulte IAM Identity Center Connector en el sitio web de Ping Identity.
- Una cuenta habilitada para IAM Identity Center (gratuita). Para más información, consulte Activar IAM Identity Center.
- Una conexión SAML desde su cuenta PingFederate al IAM Identity Center. Para obtener instrucciones sobre cómo configurar esta conexión, consulte la documentación de PingFederate. En resumen, la ruta recomendada es utilizar el conector de IAM Identity Center para configurar el “SSO del navegador” en PingFederate y utilizar las características de “descarga” e “importación” de metadatos en ambos extremos para intercambiar metadatos de SAML entre PingFederate y IAM Identity Center.

Consideraciones adicionales

Las siguientes son consideraciones importantes sobre PingFederate que pueden afectar a la forma en que se implementa el aprovisionamiento con IAM Identity Center.

- Si se elimina un atributo de un usuario en PingFederate, ese atributo no se eliminará del usuario correspondiente en IAM Identity Center. Se trata de una limitación conocida en la implementación del aprovisionador de PingFederate’s. Si un atributo se cambia a un valor diferente (no vacío) en un usuario, ese cambio se sincronizará con IAM Identity Center.

Paso 1: Habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.

3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie cada uno de los valores de las siguientes opciones. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
   a. Punto de conexión de SCIM
   b. Token de acceso
5. Elija Close.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes mediante la consola administrativa de PingFederate. Los pasos se describen en el siguiente procedimiento.

Paso 2: Configure el aprovisionamiento en PingFederate

Utilice el siguiente procedimiento en el portal de administración de PingFederate para habilitar la integración entre IAM Identity Center y la aplicación IAM Identity Center. En este procedimiento, se presupone que ya ha instalado el software del conector de IAM Identity Center. Si aún no lo ha hecho, consulte los Requisitos previos y complete este procedimiento para configurar el aprovisionamiento de SCIM.

> **Important**
>
> Si su servidor de PingFederate no se ha configurado previamente para el aprovisionamiento de SCIM saliente, es posible que deba realizar un cambio en el archivo de configuración para habilitar el aprovisionamiento. Para obtener más información, consulte la Documentación de Ping. En resumen, debe modificar la configuración de `pf.provisioner.mode` del archivo pingfederate-<version>/pingfederate/bin/run.properties a un valor distinto al `OFF` (que es el predeterminado) y reiniciar el servidor si se está ejecutando actualmente. Por ejemplo, puede optar por utilizar `STANDALONE` si actualmente no tiene una configuración de alta disponibilidad con PingFederate.

Para configurar el aprovisionamiento en PingFederate

1. Inicie sesión en la consola administrativa de PingFederate.
2. Seleccione Aplicaciones en la parte superior de la página y, a continuación, haga clic en SP Connections.
3. Localice la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center y haga clic en el nombre de la conexión.
4. Seleccione el tipo de conexión en los encabezados de navegación oscuros situados en la parte superior de la página. Debería ver que el SSO del navegador ya estaba seleccionado en su configuración anterior de SAML. Si no es así, primero debe completar esos pasos antes de continuar.
5. Seleccione la casilla de verificación Aprovisionamiento saliente, elija IAM Identity Center Cloud Connector como tipo y haga clic en Guardar. Si IAM Identity CenterCloud Connector no aparece como opción, asegúrese de haber instalado IAM Identity Center Cloud Connector y de haber reiniciado el servidor de PingFederate.
6. Haga clic en Siguiente varias veces hasta llegar a la página Aprovisionamiento saliente y, a continuación, haga clic en el botón Configurar aprovisionamiento.
7. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL de SCIM en la consola de PingFederate. Asegúrese de eliminar la barra diagonal que aparece al final de la URL. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Token de acceso en la consola de PingFederate. Haga clic en Guardar.
8. En la página Configuración del canal (Configurar canal), haga clic en Crear.
9. Introduzca un Nombre del canal para este nuevo canal de aprovisionamiento (por ejemplo **`AWSIAMIdentityCenterchannel`**) y haga clic en Siguiente.
10. En la página Origen, elija el almacén de datos activo que desee utilizar para la conexión al IAM Identity Center y haga clic en Siguiente.

> **Note**
>
> Si aún no ha configurado un origen de datos, deberá hacerlo ahora. Consulte la documentación del producto de Ping para obtener información sobre cómo elegir y configurar un origen de datos en PingFederate.

11. En la página Configuración de origen, confirme que todos los valores son correctos para la instalación y, a continuación, haga clic en Siguiente.
12. En la página Ubicación de origen, introduzca la configuración adecuada para su origen de datos y, a continuación, haga clic en Siguiente. Por ejemplo, si utiliza Active Directory como directorio LDAP:

    a. Introduzca el DN base de su bosque de AD (por ejemplo, **`DC=myforest,DC=mydomain,DC=com`**).

    b. En Usuarios **>** DN de grupo, especifique un único grupo que contenga todos los usuarios que desee aprovisionar al IAM Identity Center. Si no existe ese grupo único, créelo en AD, vuelva a esta configuración y, a continuación, introduzca el DN correspondiente.

    c. Especifique si desea buscar subgrupos (Búsqueda anidada) y cualquier filtro LDAP necesario.

    d. En Usuarios **>** DN de grupo, especifique un único grupo que contenga todos los usuarios que desee aprovisionar al IAM Identity Center. En muchos casos, puede ser el mismo DN que especificó en la sección Usuarios. Introduzca los valores Búsqueda anidada y Filtro según sea necesario.
13. En la página Asignación de atributos, asegúrese de lo siguiente y, a continuación, haga clic en Siguiente:

    a. El campo userName debe asignarse a un atributo con formato de correo electrónico (user@domain.com). También debe coincidir con el valor que el usuario utilizará para iniciar sesión en Ping. Este valor, a su vez, se rellena en la notificación del `nameId` de SAML durante la autenticación federada y se utiliza para hacer coincidir con el usuario de IAM Identity Center. Por ejemplo, cuando utilice Active Directory, puede optar por especificar el `UserPrincipalName` como userName.

    b. Los demás campos con un sufijo * deben asignarse a atributos que no sean nulos para los usuarios.
14. En la página Activación y resumen, defina el estado del canal como Activo para que la sincronización comience inmediatamente después de guardar la configuración.
15. Confirme que todos los valores de configuración de la página son correctos y haga clic en Listo.
16. En la página Administrar canales, haga clic en Guardar.
17. En este punto, comienza el aprovisionamiento. Para confirmar la actividad, puede ver el archivo provisioner.log, que se encuentra de forma predeterminada en el directorio de pingfederate-<version>/pingfederate/log de su servidor de PingFederate.

18. Para comprobar que los usuarios y los grupos se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios sincronizados de PingFederate aparecerán en la página de Usuarios. También puedes ver tus grupos sincronizados en la página Grupos.

(Opcional) Paso 3: Configurar los atributos de usuario en PingFed erate para el control de acceso en IAM Identity Center

Este es un procedimiento opcional para PingFederate, en caso de que quiera configurar atributos para que IAM Identity Center administre el acceso a sus recursos de AWS. Los atributos que defina en PingFederate se transfieren en una aserción de SAML a IAM Identity Center. A continuación, deberá crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde PingFederate.

Antes de comenzar con este procedimiento, primero debes habilitar la característica Atributos para controlar el acceso. Para obtener más información acerca de cómo hacerlo, consulte Habilitación y configuración de atributos para el control de acceso.

Para configurar atributos de usuario utilizados en PingFederate para el control de acceso en IAM Identity Center

1. Inicie sesión en la consola administrativa de PingFederate.
2. Seleccione Aplicaciones en la parte superior de la página y, a continuación, haga clic en SP Connections.
3. Localice la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center y haga clic en el nombre de la conexión.
4. Seleccione el tipo de conexión en los encabezados de navegación oscuros situados en la parte superior de la página. A continuación, haga clic en Configurar el SSO del navegador.
5. En la página Configurar el SSO del navegador, seleccione Creación de aserciones y, a continuación, haga clic en Configurar creación de aserciones.
6. En la página Configurar la creación de aserciones, elija Contrato de atributos.
7. En la página Contrato de atributos, en la sección Ampliar el contrato, añada un nuevo atributo siguiendo estos pasos:

    a. En el cuadro de texto, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**, sustituya **`AttributeName`** por el nombre del atributo

que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

b. En Formato de nombre de atributo, elija urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

c. Elija Añadir, y a continuación, elija Siguiente.

8. En la página de asignación de fuentes de autenticación, elija la instancia de adaptador configurada con su aplicación.

9. En la página Cumplimiento del contrato de atributo, elija el origen (almacén de datos) y el valor (atributo del almacén de datos) para el contrato de atributo `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

> **Note**
>
> Si aún no ha configurado un origen de datos, deberá hacerlo ahora. Consulte la documentación del producto de Ping para obtener información sobre cómo elegir y configurar un origen de datos en PingFederate.

10. Haga clic en Siguiente varias veces hasta llegar a la página de activación y resumen y, a continuación, haga clic en Guardar.

(Opcional) Pasar atributos para el control de acceso

Si lo desea, puede utilizar la característica Atributos para controlar el acceso de IAM Identity Center para transferir un elemento de `Attribute`con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, para pasar los pares clave-valor de etiquetas de `CostCenter = blue`, utilice el siguiente atributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento de `Attribute` independiente para cada etiqueta.

PingOne

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios desde PingOne por parte de Ping Identity (de ahora en adelante “Ping”) a IAM Identity Center. Este aprovisionamiento utiliza el protocolo System for Cross-Domain Identity Management (SCIM) v2.0. Esta conexión se configura en PingOne mediante el punto de conexión SCIM y el token de acceso de IAM Identity Center. Al configurar la sincronización de SCIM, crea un mapeo de los atributos de usuario en PingOne con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y PingOne.

Esta guía está basada en PingOne a fecha de octubre de 2020. Los pasos para las versiones más recientes pueden variar. Póngase en contacto con Ping para obtener más información sobre cómo configurar el aprovisionamiento en IAM Identity Center para otras versiones de PingOne. Esta guía contiene algunas notas sobre la configuración de la autenticación de usuarios mediante SAML.

Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de usuarios desde PingOne a IAM Identity Center mediante el protocolo SCIM.

> **Note**
>
> Antes de comenzar a implementar SCIM, le recomendamos revisar primero las Consideraciones para utilizar el aprovisionamiento automático. A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

Temas

Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- Una suscripción o una prueba gratuita de PingOne, con funciones de autenticación federada y aprovisionamiento. Para obtener más información acerca de cómo obtener una prueba gratuita, consulte el sitio web de Ping Identity.
- Una cuenta habilitada para IAM Identity Center (gratuita). Para más información, consulte Activar IAM Identity Center.
- La aplicación IAM Identity Center de PingOne se agregó a su portal de administración de PingOne. Puede obtener la aplicación IAM Identity Center de PingOne en el catálogo de aplicaciones de PingOne. Para obtener información general, consulte Añadir una aplicación desde el catálogo de aplicaciones del sitio web de Ping Identity.
- Una conexión SAML desde su cuenta de PingOne a IAM Identity Center. Una vez que la aplicación IAM Identity Center de PingOne se haya agregado a su portal de administración de PingOne, debe usarla para configurar una conexión SAML desde su instancia de PingOne a IAM Identity Center. Utilice las características de “descarga” e “importación” de metadatos en ambos extremos para intercambiar metadatos de SAML entre PingOne y IAM Identity Center. Para obtener instrucciones sobre cómo configurar esta conexión, consulte la documentación de PingOne.

Consideraciones adicionales

Las siguientes son consideraciones importantes sobre PingOne que pueden afectar a la forma en que se implementa el aprovisionamiento con IAM Identity Center.

- A partir de octubre de 2020, PingOne no admite el aprovisionamiento de grupos a través de SCIM. Póngase en contacto con Ping para obtener la información más reciente sobre el apoyo grupal en SCIM para PingOne.
- Los usuarios pueden seguir aprovisionándose desde PingOne después de deshabilitar el aprovisionamiento en el portal de administración de PingOne. Si necesita finalizar el aprovisionamiento inmediatamente, elimine el token portador del SCIM correspondiente o desactívelo en IAM Identity Center de Aprovisionamiento estático.
- Si se elimina un atributo de un usuario en PingOne, ese atributo no se eliminará del usuario correspondiente en IAM Identity Center. Se trata de una limitación conocida en la implementación del aprovisionador de PingOne’s. Si se modifica un atributo, el cambio se sincronizará con IAM Identity Center.

- Las siguientes son notas importantes sobre la configuración de SAML en PingOne:
  - IAM Identity Center solo es compatible con `emailaddress` como formato de `NameId`. Esto significa que debe elegir un atributo de usuario que sea único en su directorio de PingOne, que no sea nulo y que tenga el formato de correo electrónico/UPN (por ejemplo, user@domain.com) para la asignación de SAML_SUBJECT en PingOne. El correo electrónico (trabajo) es un valor razonable para probar las configuraciones con el directorio integrado de PingOne.
  - Es posible que los usuarios que ingresen PingOne con una dirección de correo electrónico que contenga un carácter + no puedan iniciar sesión en IAM Identity Center debido a errores como `'SAML_215'` o `'Invalid input'`. Para solucionar este problema, en PingOne, seleccione la opción Avanzada para la asignación de SAML_SUBJECT en las asignaciones de atributos. A continuación, defina el formato de ID de nombre para enviarlo a SP: para urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress en el menú desplegable.

Paso 1: Habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie cada uno de los valores de las siguientes opciones. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
   a. Punto de conexión de SCIM
   b. Token de acceso
5. Elija Close.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes con la aplicación PingOne de IAM Identity Center. Estos pasos se explican en el procedimiento siguiente.

Paso 2: Configure el aprovisionamiento en PingOne

Utilice el siguiente procedimiento en la aplicación PingOne de IAM Identity Center para habilitar el aprovisionamiento con IAM Identity Center. En este procedimiento se presupone que ya ha añadido la aplicación PingOne de IAM Identity Center a la consola de PingOne administración del portal. Si aún no lo ha hecho, consulte los Requisitos previos y complete este procedimiento para configurar el aprovisionamiento de SCIM.

Para configurar el aprovisionamiento en PingOne

1. Abra la aplicación de PingOne de IAM Identity Center que instaló como parte de la configuración de SAML para PingOne (Aplicaciones > Mis aplicaciones). Consulte Requisitos previos.
2. Desplácese hasta el final de la página. En Aprovisionamiento de usuarios, elija el enlace completo para acceder a la configuración de aprovisionamiento de usuarios de su conexión.
3. En la página de instrucciones de aprovisionamiento, seleccione Continuar con el siguiente paso.
4. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL de SCIM de la aplicación PingOne de IAM Identity Center. Asegúrese de eliminar la barra diagonal que aparece al final de la URL. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo ACCESS_TOKEN en la aplicación de PingOne de IAM Identity Center.
5. Para REMOVE_ACTION, elija Desactivado o Eliminado (consulte el texto de descripción de la página para obtener más información).
6. En la página de asignación de atributos, elija un valor para usarlo en la afirmación SAML_SUBJECT (`NameId`), siguiendo las instrucciones de Consideraciones adicionales que aparecen anteriormente en esta página. A continuación elija Continuar con el paso siguiente.
7. En la página Personalización de la aplicación de PingOne: IAM Identity Center, realice los cambios de personalización que desee (opcional) y haga clic en Continuar con el siguiente paso.
8. En la página Acceso grupal, seleccione los grupos que contienen los usuarios que desea habilitar para el aprovisionamiento y el inicio de sesión único en IAM Identity Center. Elija Continuar con el paso siguiente.
9. Desplácese hasta el final de la página y seleccione Finalizar para iniciar el aprovisionamiento.

10. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Los usuarios sincronizados de PingOne aparecerán en la página de Usuarios. Estos usuarios ahora pueden asignarse a cuentas en IAM Identity Center.

    Recuerde que PingOne no admite el aprovisionamiento de grupos o la pertenencia a grupos a través de SCIM. Póngase en contacto con la asistencia de Ping para obtener más información.

(Opcional) Paso 3: Configure los atributos de usuario en PingOne para el control de acceso en IAM Identity Center

Este es un procedimiento opcional para PingOne, en caso de que quiera configurar atributos para que IAM Identity Center administre el acceso a sus recursos de AWS. Los atributos que defina en PingOne se transfieren en una aserción de SAML a IAM Identity Center. A continuación, debe crear un conjunto de permisos en IAM Identity Center para administrar el acceso en función de los atributos que transfirió desde PingOne.

Antes de comenzar con este procedimiento, primero debes habilitar la característica Atributos para controlar el acceso. Para obtener más información acerca de cómo hacerlo, consulte Habilitación y configuración de atributos para el control de acceso.

Para configurar atributos de usuario utilizados en PingOne para el control de acceso en IAM Identity Center

1. Abra la aplicación de PingOne de IAM Identity Center que instaló como parte de la configuración de SAML para PingOne (Aplicaciones > Mis aplicaciones).
2. Elija Editar y, a continuación, elija Continuar con el siguiente paso hasta llegar a la página Asignaciones de atributos.
3. En la página Asignaciones de atributos, elija Añadir nuevo atributo y, a continuación, haga lo siguiente. Debe realizar estos pasos para cada atributo que vaya a añadir para su uso en IAM Identity Center para el control de acceso.

    a. En el campo Atributo de la aplicación, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`*. Sustituya *`AttributeName`* por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.

b. En el campo Nombre del atributo de , elija los atributos de usuario de su directorio de PingOne. Por ejemplo, Correo electrónico (trabajo).

4. Elija Siguiente y, a continuación, elija Terminar.

(Opcional) Pasar atributos para el control de acceso

Si lo desea, puede utilizar la característica Atributos para controlar el acceso de IAM Identity Center para transferir un elemento de `Attribute`con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte Transferencia de etiquetas de sesión en AWS STS en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, para pasar los pares clave-valor de etiquetas de `CostCenter = blue`, utilice el siguiente atributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento de `Attribute` independiente para cada etiqueta.

Introducción a las tareas habituales en IAM Identity Center

Si es un usuario nuevo de IAM Identity Center, el flujo de trabajo básico para empezar a utilizar el servicio es el siguiente:

1. Inicie sesión en la consola de su cuenta de administración si utiliza una instancia de organización del IAM Identity Center o en la suya Cuenta de AWS si utiliza una instancia de cuenta del IAM Identity Center y vaya a la consola del IAM Identity Center.
2. Seleccione el directorio que utiliza para almacenar las identidades de sus usuarios y grupos en la consola de IAM Identity Center. IAM Identity Center le proporciona un directorio predeterminado que puede utilizar para configurar el acceso de los usuarios. Si prefiere utilizar otro origen de identidad, puede conectar su instancia de Active Directory o un proveedor de identidades externo.
3. En el caso de las instancias de organización, asigne el acceso de los usuarios a las Cuentas de AWS; para ello, seleccione las cuentas de su organización y, a continuación, seleccione los usuarios o grupos del directorio y los permisos que desea concederles.
4. Ofrezca a los usuarios acceso a las aplicaciones de la siguiente manera:
   a. Configure las aplicaciones de SAML 2.0 administradas por el cliente; para ello, elija una de las aplicaciones preintegradas del catálogo de aplicaciones o agregue su propia aplicación de SAML 2.0.
   b. Configure las propiedades de la aplicación.
   c. Asigne a los usuarios acceso a la aplicación. Se recomienda asignar el acceso de los usuarios mediante la pertenencia a grupos en lugar de agregar permisos de usuario individuales. Con los grupos puede conceder o denegar permisos para grupos de usuarios en lugar de asignar esos permisos a cada individuo. Si un usuario se muda a una organización diferente, simplemente muévalo a un grupo diferente. Así el usuario recibirá automáticamente los permisos necesarios para la nueva organización.
5. Si utiliza el directorio predeterminado del Centro de identidades de IAM, indique a sus usuarios cómo iniciar sesión en el portal de acceso. AWS Los nuevos usuarios del Centro de Identidad de IAM deben activar sus credenciales de usuario antes de poder utilizarlas para iniciar sesión en el portal de AWS acceso. Para obtener más información, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario

Los temas de esta sección lo ayudarán a familiarizarse con las tareas habituales que se realizan después de finalizar la configuración inicial de IAM Identity Center.

Si aún no ha habilitado IAM Identity Center, consulte Habilitar AWS IAM Identity Center.

Temas

Crea un conjunto de permisos.

Los conjuntos de permisos se guardan en IAM Identity Center y definen el nivel de acceso que tienen los usuarios y grupos en una cuenta Cuenta de AWS. El primer conjunto de permisos que cree es el conjunto de permisos administrativos. Si completó uno de los Tutoriales de introducción, ya creó su conjunto de permisos administrativos. Utilice este procedimiento para crear conjuntos de permisos, tal y como se describe en el tema Managed Policies de AWS para funciones de trabajo de la Guía del usuario de IAM.

1. Realice una de estas 2 operaciones para iniciar sesión en la AWS Management Console.
   - Nuevo para AWS (usuario root): inicie sesión como propietario de la cuenta; para ello, seleccione Root user e introduzca su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
   - Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
2. Abra la consola del IAM Identity Center.
3. En el panel de navegación del IAM Identity Center, en Permisos multicuenta, seleccione Conjuntos de permisos.
4. Elija Crear conjunto de permisos.
   a. En la página Seleccione el tipo de conjunto de permisos, en la sección Tipo de conjunto de permisos, elija Conjunto de permisos predefinido.
   b. En la sección Política para el conjunto de permisos predefinido, seleccione una de las siguientes opciones:

- AdministratorAccess
- Facturación
- DatabaseAdministrator
- DataScientist
- NetworkAdministrator
- PowerUserAccess
- ReadOnlyAccess
- SecurityAudit
- SupportUser
- SystemAdministrator
- ViewOnlyAccess

5. En la página Especificar detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente. La configuración predeterminada limita la sesión a una hora.
6. En la página Revisar y crear confirme lo siguiente:

    1. Para el paso 1: seleccione el tipo de conjunto de permisos, muestra el tipo de conjunto de permisos que eligió.
    2. En el paso 2: Definir los detalles del conjunto de permisos, muestra el nombre del conjunto de permisos que ha elegido.
    3. Seleccione Crear.

Creación de un conjunto de permisos que aplique los permisos de privilegio mínimo

Para seguir la práctica recomendada de aplicar permisos con privilegios mínimos, después de crear un conjunto de permisos administrativos, cree un conjunto de permisos más restrictivo y asígnelo a uno o más usuarios. Los conjuntos de permisos creados en el procedimiento anterior proporcionan un punto de partida para evaluar la cantidad de acceso a los recursos que necesitan los usuarios. Para cambiar a permisos de privilegios mínimos, puede ejecutar el Analizador de acceso de IAM para supervisar las entidades principales con las políticas administradas por AWS . Después de saber qué permisos utilizan, puede escribir una política personalizada o generar una política con solo los permisos necesarios para su equipo.

Con IAM Identity Center, puede asignar varios conjuntos de permisos al mismo usuario. A su usuario administrativo también se le deben asignar conjuntos de permisos adicionales y más restrictivos. De esta forma, podrán acceder a usted únicamente Cuenta de AWS con los permisos necesarios, en lugar de utilizar siempre sus permisos administrativos.

Por ejemplo, si es desarrollador, después de crear su usuario administrativo en IAM Identity Center, puede crear un nuevo conjunto de permisos que conceda permisos de `PowerUserAccess` y, a continuación, asignarse ese conjunto de permisos a usted. A diferencia del conjunto de permisos administrativos, que utiliza `AdministratorAccess` permisos, el conjunto de `PowerUserAccess` permisos no permite gestionar los usuarios y grupos de IAM. Al iniciar sesión en el AWS portal de acceso para acceder a su AWS cuenta, puede elegir `PowerUserAccess` no `AdministratorAccess` realizar las tareas de desarrollo en la cuenta.

Tenga en cuenta las siguientes consideraciones:

- Para empezar rápidamente a crear un conjunto de permisos más restrictivo, utilice un conjunto de permisos predefinido en lugar de uno personalizado.

  Con un conjunto de permisos predefinido, que utiliza permisos predefinidos, puede elegir una única política AWS gestionada de una lista de políticas disponibles. Cada política otorga un nivel específico de acceso a AWS los servicios y recursos o permisos para una función laboral común. Para obtener información sobre cada una de estas políticas, consulte Políticas administradas de AWS para funciones de trabajo.
- Puede configurar la duración de la sesión de un conjunto de permisos para controlar el tiempo que un usuario permanece registrado en una Cuenta de AWS.

  Cuando los usuarios se federan Cuenta de AWS y utilizan la consola de AWS gestión o la interfaz de línea de AWS comandos (AWS CLI), IAM Identity Center utiliza la configuración de duración de la sesión del conjunto de permisos para controlar la duración de la sesión. De forma predeterminada, el valor de Duración de la sesión, que determina el tiempo que un usuario puede iniciar sesión Cuenta de AWS antes de AWS cerrar la sesión del usuario, se establece en una hora. Puede especificar un valor máximo de 12 horas. Para obtener más información, consulte Definir la duración de la sesión.
- También puede configurar la duración de la sesión del portal de AWS acceso para controlar el tiempo que un usuario de la fuerza laboral permanece conectado al portal.

  De forma predeterminada, el valor de Duración máxima de la sesión, que determina el tiempo que un usuario de Workforce puede iniciar sesión en el portal de AWS acceso antes de tener

que volver a autenticarse, es de ocho horas. Puede especificar un valor máximo de 90 días. Para obtener más información, consulte Configure la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center.

- Cuando inicie sesión en el portal de AWS acceso, elija el rol que proporciona los permisos con privilegios mínimos.

  Cada conjunto de permisos que cree y asigne a su usuario aparece como un rol disponible en el AWS portal de acceso. Cuando inicie sesión en el portal en calidad de ese usuario, elija el rol que corresponda al conjunto de permisos más restrictivo que pueda usar para realizar tareas en la cuenta, en lugar de `AdministratorAccess`.

- Puede agregar otros usuarios a IAM Identity Center y asignar conjuntos de permisos nuevos o existentes a esos usuarios.

  Para obtener información, consulte Asigne el Cuenta de AWS acceso a los grupos.

Asigne el Cuenta de AWS acceso a un usuario del Centro de Identidad de IAM

Para configurar el Cuenta de AWS acceso de un usuario del Centro de Identidad de IAM, debe asignar el usuario al conjunto de permisos Cuenta de AWS y.

1. Realice una de estas 2 operaciones para iniciar sesión en la AWS Management Console.

   - Nuevo para AWS (usuario raíz): inicie sesión como propietario de la cuenta; para ello, seleccione el usuario raíz e introduzca su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
   - Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.

2. Abra la consola de IAM Identity Center.
3. En el panel de navegación, en Permisos para varias cuentas, elijaCuentas de AWS.
4. En la página de Cuentas de AWS, se muestra una lista de su organización en forma de árbol. Seleccione la casilla de verificación situada junto a la casilla Cuenta de AWS a la que desee asignar el acceso. Si desea configurar el acceso administrativo para IAM Identity Center, seleccione la casilla de verificación situada junto a la cuenta de administración.
5. Seleccione Asignar usuarios o grupos.

6. Para el paso 1: seleccionar usuarios y grupos, en la página Asignar usuarios y grupos al «***Cuenta de AWS nombre***», haga lo siguiente:

   1. En la pestaña Usuarios, seleccione el usuario a quien desea conceder permisos administrativos.

      Para filtrar los resultados, escriba el nombre del usuario que desea en el cuadro de búsqueda.

   2. Tras confirmar que se haya seleccionado el usuario correcto, seleccione Siguiente.

7. En el paso 2: seleccionar conjuntos de permisos, en la página Asignar conjuntos de permisos a «***Cuenta de AWS nombrar***», en Conjuntos de permisos, seleccione un conjunto de permisos para definir el nivel de acceso que tienen los usuarios y los grupos a este conjunto Cuenta de AWS.

8. Elija Siguiente.

9. Para el paso 3: Revisar y enviar, en la página Revisar y enviar las tareas a «***Cuenta de AWS nombrar***», haga lo siguiente:

   1. Revise el usuario y el conjunto de permisos seleccionados.

   2. Tras confirmar que el usuario correcto está asignado al conjunto de permisos, seleccione Enviar.

      > **Important**
      >
      > El proceso de asignación de usuarios puede tardar unos minutos en completarse. Es importante que deje esta página abierta hasta que se complete el proceso correctamente.

10. Si se aplica alguna de las siguientes condiciones, siga los pasos que se indican en Solicitar MFA a los usuarios para habilitar la MFA en IAM Identity Center:

    - Está utilizando el directorio predeterminado del Identity Center como origen e de identidad.
    - Utiliza un AWS Managed Microsoft AD directorio o un directorio autoadministrado en Active Directory como fuente de identidad y no usa RADIUS AWS Directory Service MFA con.

> **Note**
>
> Si utiliza un proveedor de identidad externo, tenga en cuenta que el IdP externo, no el IAM Identity Center, administra la configuración de MFA. No se admite el uso de MFA en el Centro de identidad de IAM para uso externo. IdPs

Al configurar el acceso a la cuenta para el usuario administrativo, del IAM Identity Center crea el rol de IAM correspondiente. Esta función, que está controlada por el Centro de Identidad de IAM, se crea en el lugar correspondiente Cuenta de AWS y las políticas especificadas en el conjunto de permisos se adjuntan a la función.

Inicie sesión en el portal de AWS acceso con sus credenciales del Centro de Identidad de IAM

El portal de AWS acceso proporciona a los usuarios del IAM Identity Center un acceso de inicio de sesión único a todas sus aplicaciones Cuentas de AWS y aplicaciones asignadas a través de un portal web.

Complete los siguientes pasos para confirmar que el usuario del Centro de Identidad de IAM puede iniciar sesión en el portal de acceso y AWS acceder al. Cuenta de AWS

1. Realice una de estas 2 operaciones para iniciar sesión en la AWS Management Console.
   - Nuevo para AWS (usuario root): inicie sesión como propietario de la cuenta; para ello, seleccione el usuario root e introduzca su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
   - Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM y selecciona un rol de administrador.
2. Abra la consola de IAM Identity Center
3. En el panel de navegación, elija Panel.
4. En la página del panel de control, en el resumen de la configuración, selecciona la URL del portal de AWS acceso.
5. Inicie sesión mediante cualquiera de las siguientes opciones:

- Si utiliza Active Directory o un proveedor de identidades (IdP) externo como origen de identidad, inicie sesión con las credenciales del usuario de Active Directory o IdP.
- Si utiliza el directorio predeterminado de Identity Center como origen de identidad, inicie sesión con el nombre de usuario que especificó al crear el usuario y la nueva contraseña que especificó para el usuario.

1. En la pestaña Cuentas, localiza la tuya Cuenta de AWS y amplíala.
2. Se mostrarán los roles que tiene disponibles. Por ejemplo, si tiene asignados tanto el conjunto de AdministratorAccesspermisos como el conjunto de permisos de facturación, esas funciones se muestran en el portal de AWS acceso. Seleccione el nombre del rol de IAM que desee usar para la sesión.
3. Si se le redirige a la consola AWS de administración, ha terminado correctamente de configurar el acceso a Cuenta de AWS.

> **Note**
>
> Si no ve Cuentas de AWS en la lista, es probable que aún no se le haya asignado al usuario un conjunto de permisos para esa cuenta. Para obtener instrucciones sobre cómo asignar usuarios a un conjunto de permisos, consulte Asigne el acceso de los usuarios a Cuentas de AWS.

Ahora que ha confirmado que puede iniciar sesión con las credenciales del Centro de Identidad de IAM, cambie al navegador que utilizó para iniciar sesión AWS Management Console y cierre la sesión con sus credenciales de usuario raíz o de usuario de IAM.

> **Important**
>
> Le recomendamos encarecidamente que utilice las credenciales del usuario administrativo del Centro de Identidad de IAM al iniciar sesión en el portal de AWS acceso para realizar tareas administrativas en lugar de utilizar las credenciales del usuario raíz o del usuario de IAM. Proteja las credenciales del usuario raíz y utilícelas sólo para las tareas que el usuario raíz pueda realizar. Para permitir que otros usuarios accedan a sus cuentas y aplicaciones, y para administrar IAM Identity Center, cree y asigne conjuntos de permisos únicamente a través de IAM Identity Center.

Asigne el Cuenta de AWS acceso a los grupos

Una vez que haya creado un usuario administrativo en el Centro de identidades de IAM y creado conjuntos de permisos adicionales que pueda utilizar para realizar tareas con los permisos menos privilegiados, podrá proporcionar acceso a sus Cuentas de AWS grupos de usuarios.

Se recomienda asignar el acceso directamente a grupos en lugar de a usuarios individuales. Por ejemplo, si crea grupos y conjuntos de permisos basados en unidades organizativas, si un usuario cambia a una unidad organizativa diferente, simplemente tiene que mover a ese usuario a un grupo diferente y, automáticamente, recibirá los permisos necesarios para la nueva unidad organizativa y perderá los permisos de la unidad organizativa anterior.

Para asignar el acceso a un grupo de usuarios a Cuentas de AWS

1. Abra la consola de IAM Identity Center

   > **Note**
   >
   > Si su fuente de identidad es, AWS Managed Microsoft AD asegúrese de que la consola del IAM Identity Center utilice la región en la que se encuentra su AWS Managed Microsoft AD directorio antes de pasar al siguiente paso.

2. En el panel de navegación, en Permisos para varias cuentas, elijaCuentas de AWS.
3. En la página Cuentas de AWS, aparece una lista de su organización en forma de árbol. Seleccione la casilla de verificación situada junto a una o varias de Cuentas de AWS las que desee asignar el acceso de inicio de sesión único.

   > **Note**
   >
   > Puedes seleccionar hasta 10 Cuentas de AWS por conjunto de permisos.

4. Seleccione Asignar usuarios o grupos.
5. En Paso 1: selección de usuarios y grupos, en la página Asignar usuarios y grupos a “***nombre-de-cuenta-de-AWS***”, seleccione la pestaña Grupos y, a continuación, elija uno o más grupos.

   Para filtrar los resultados, escriba el nombre del grupo que desea en el cuadro de búsqueda.

   Para mostrar los grupos que ha seleccionado, seleccione el triángulo lateral situado junto a Usuarios y grupos seleccionados.

Tras confirmar que se hayan seleccionado los grupos correctos, seleccione Siguiente.

6. En Paso 2: selección de conjuntos de permisos, en la página Asignar conjuntos de permisos a "***nombre-de-cuenta-de-AWS***", seleccione uno o varios conjuntos de permisos

> **Note**
>
> Si no creó el conjunto de permisos que desea antes de iniciar este procedimiento, seleccione Crear conjunto de permisos y siga los pasos que se indican en Crea un conjunto de permisos.. Tras crear los conjuntos de permisos que desea aplicar, en la consola de IAM Identity Center, vuelva a las Cuentas de AWS y siga las instrucciones hasta llegar al paso 2: seleccionar conjuntos de permisos. Cuando llegue a este paso, seleccione los nuevos conjuntos de permisos que ha creado y continúe con el siguiente paso de este procedimiento.

Tras confirmar que se haya seleccionado los conjuntos de permisos correctos, seleccione Siguiente.

7. Para el Paso 3: Revisar y enviar, en la página Revisar y enviar las tareas a "***AWS-nombre-de-cuenta***", haga lo siguiente:

   1. Revise los grupos y los conjuntos de permisos seleccionados.
   2. Tras confirmar que se hayan seleccionado los grupos y los conjuntos de permisos correctos, seleccione Enviar.

> **Important**
>
> El proceso de asignación de grupos puede tardar unos minutos en completarse. Es importante que deje esta página abierta hasta que se complete el proceso correctamente.

> **Note**
>
> Es posible que deba conceder permisos a los usuarios o grupos para operar en la cuenta AWS Organizations de administración. Como se trata de una cuenta con muchos privilegios, las restricciones de seguridad adicionales requieren que tengas

la FullAccess política de IAM o permisos equivalentes antes de poder configurarla. Estas restricciones de seguridad adicionales no son obligatorias para ninguna de las cuentas de los miembros de su AWS organización.

Como alternativa, puede utilizar AWS CloudFormation para crear y asignar conjuntos de permisos y asignar usuarios a esos conjuntos de permisos. A continuación, los usuarios pueden iniciar sesión en el portal de acceso de AWS o utilizar los comandos de la AWS Command Line Interface (AWS CLI).

Configuración del acceso mediante inicio de sesión único a las aplicaciones

El IAM Identity Center admite dos tipos de aplicaciones: aplicaciones AWS administradas y aplicaciones administradas por el cliente.

AWS las aplicaciones gestionadas se configuran directamente desde las consolas de aplicaciones correspondientes o mediante las API de las aplicaciones.

Debe agregar las aplicaciones administradas por el cliente a la consola de IAM Identity Center y configurarlas con los metadatos correspondientes tanto para IAM Identity Center como para el proveedor de servicios. Puede elegir entre un catálogo de aplicaciones de uso común compatibles con SAML 2.0 o puede configurar sus propias aplicaciones de SAML 2.0 o aplicaciones de OAuth 2.0.

Los pasos de configuración para configurar el acceso mediante inicio de sesión único a las aplicaciones varían según el tipo de aplicación.

Configure una aplicación AWS gestionada

AWS las aplicaciones gestionadas, como Amazon Managed Grafana y Amazon Monitron, se integran con IAM Identity Center y pueden usarlo para servicios de autenticación y directorio. Para configurar una aplicación AWS gestionada para que funcione con el Centro de Identidad de IAM, debe configurarla directamente desde la consola para el servicio correspondiente o debe utilizar las API de la aplicación.

Configuración de una aplicación del catálogo de aplicaciones

Puede seleccionar una aplicación de SAML 2.0 de un catálogo de aplicaciones de uso frecuente en la consola de IAM Identity Center. Utilice este procedimiento para configurar una relación de confianza de SAML 2.0 entre IAM Identity Center y el proveedor de servicios de la aplicación.

Para configurar una aplicación del catálogo de aplicaciones

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, elija Deseo seleccionar una aplicación del catálogo.
6. En Catálogo de aplicaciones, empiece a escribir el nombre de la aplicación que desea agregar en el cuadro de búsqueda.
7. Elija el nombre de la aplicación en la lista cuando aparezca en los resultados de la búsqueda y, a continuación, seleccione Siguiente.
8. En la página Configurar aplicación, los campos Nombre de visualización y Descripción se rellenan automáticamente con los detalles correspondientes de la aplicación. Puede modificar esta información.
9. En Metadatos de IAM Identity Center, haga lo siguiente:

    a. En a Archivo de metadatos del SAML de IAM Identity Center, elija Descargar para descargar los metadatos del proveedor de identidad.

    b. En el a Certificado de IAM Identity Center, elija Descargar certificado para descargar el certificado del proveedor de identidad.

    > **Note**
    >
    > Necesitará estos archivos más tarde al configurar la aplicación desde el sitio web del proveedor de servicios. Siga las instrucciones de dicho proveedor.

10. (Opcional) En Propiedades de la aplicación, puede especificar URL de inicio de aplicación, Estado de retransmisión y Duración de la sesión. Para obtener más información, consulte Configuración de las propiedades de la aplicación en la consola de IAM Identity Center.

11. En Metadatos de la aplicación, realice una de las siguientes acciones:

    a. Si tiene un archivo de metadatos, seleccione Cargar archivo de metadatos de SAML de la aplicación. A continuación, seleccione Elegir archivo para buscar y seleccionar el archivo de metadatos.

    b. Si no tiene un archivo de metadatos, elija Escribir manualmente los valores de los metadatos y, a continuación, proporcione los valores de URL de ACS de la aplicación y Audiencia de SAML de la aplicación.

12. Seleccione Submit (Enviar). Accederá a la página de detalles de la aplicación que acaba de añadir.

Configuración de su propia aplicación de SAML 2.0

Utilice este procedimiento para configurar su propia relación de confianza de SAML 2.0 entre IAM Identity Center y su propio proveedor de servicios de la aplicación de SAML 2.0. Antes de comenzar este procedimiento, asegúrese de que dispone del certificado y del archivo de intercambio de metadatos del proveedor de servicios para que pueda completar la configuración de la relación de confianza.

Para configurar su propia aplicación de SAML 2.0

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, seleccione Tengo una aplicación que quiero configurar.
6. En Tipo de aplicación, seleccione SAML 2.0.
7. Elija Siguiente.
8. En la página Configurar aplicación, en Configurar aplicación, introduzca un nombre para mostrar para la aplicación, por ejemplo **`MyApp`**. Escriba una descripción en Descripción.
9. En Metadatos de IAM Identity Center, haga lo siguiente:

    a. En a Archivo de metadatos del SAML de IAM Identity Center, elija Descargar para descargar los metadatos del proveedor de identidad.

b. Junto a Certificado de IAM Identity Center, seleccione Descargar para descargar el certificado del proveedor de identidades.

> **Note**
>
> Necesitará estos archivos más tarde al configurar la aplicación personalizada desde el sitio web del proveedor de servicios.

10. (Opcional) En Propiedades de la aplicación, también puede especificar los valores de URL de inicio de aplicación, Estado de retransmisión y Duración de la sesión. Para obtener más información, consulte Configuración de las propiedades de la aplicación en la consola de IAM Identity Center.
11. En Metadatos de la aplicación, elija Escribir manualmente los valores de los metadatos. A continuación, proporcione valores para la URL de ACS de la aplicación y la audiencia de SAML de la aplicación.
12. Seleccione Submit (Enviar). Accederá a la página de detalles de la aplicación que acaba de añadir.

Una vez configuradas las aplicaciones, los usuarios pueden acceder a ellas desde su portal de AWS acceso en función de los permisos que haya asignado.

Si tienes aplicaciones gestionadas por el cliente que admiten OAuth 2.0 y tus usuarios necesitan acceder a los AWS servicios desde estas aplicaciones, puedes utilizar la propagación de identidades fiable. Con una propagación de identidad fiable, un usuario puede iniciar sesión en una aplicación y esa aplicación puede transmitir la identidad de los usuarios en las solicitudes de acceso a los datos de los servicios. AWS Para obtener más información, consulte Uso de la propagación de identidades de confianza con aplicaciones administradas por el cliente.

Para obtener más información acerca de los tipos de aplicación admitidos, consulte Administración del acceso a las aplicaciones.

Vea las asignaciones de usuarios y grupos

Puede ver quién tiene acceso a qué en el Centro de identidades de IAM desde las páginas Usuarios y Grupos. Utilice este procedimiento para ver el nivel de acceso que tienen los usuarios a AWS las cuentas, los conjuntos de permisos, las aplicaciones y los grupos.

1. Abra la consola de IAM Identity Center
2. Elija Usuarios o grupos en función de si desea editar un grupo de usuarios o un usuario que se asignó individualmente.
3. Elija un usuario o grupo de la lista.
4. Elija si desea ver las asignaciones de cuentas, las asignaciones de aplicaciones o las asignaciones grupales:

   - AWS asignaciones de cuentas y conjuntos de permisos
     1. Elija la pestaña Accounts.
     2. Seleccione una cuenta de la lista para ver las asignaciones de conjuntos de permisos de usuarios y grupos.
     3. Seleccione el conjunto de permisos que desee ver para ver los detalles de las políticas y las asignaciones.
   - Asignaciones de aplicaciones
     1. Seleccione la pestaña Aplicaciones para ver qué aplicaciones están asignadas a un usuario o grupo.
     2. Seleccione una aplicación de la lista para ver los detalles de la asignación.
   - Agrupa las tareas
     1. En la página Usuarios, seleccione la pestaña Grupos.
     2. Seleccione un grupo para ver las asignaciones grupales de un usuario.

Administración de las instancias de organización y cuenta de IAM Identity Center

Una instancia es una implementación única de IAM Identity Center. Hay dos tipos de instancias disponibles para IAM Identity Center: las instancias de organización y las instancias de cuenta.

Cuenta de AWS tipos que pueden habilitar IAM Identity Center

Para habilitar el Centro de identidades de IAM, inicie sesión en AWS Management Console el con una de las siguientes credenciales, en función del tipo de instancia que desee crear:

- Su cuenta AWS Organizations de administración (recomendada): necesaria para crear una instancia organizativa del IAM Identity Center. Utilice una instancia de organización para los permisos de varias cuentas y las asignaciones de aplicaciones en toda la organización.
- Su cuenta de AWS Organizations miembro: utilícela para crear una instancia de cuenta del IAM Identity Center para permitir la asignación de solicitudes dentro de esa cuenta de miembro. En una organización pueden existir una o más cuentas con una instancia de nivel de miembro.
- Una instancia independiente Cuenta de AWS: se utiliza para crear una instancia de organización o una instancia de cuenta del IAM Identity Center. La versión independiente Cuenta de AWS no está gestionada por. AWS Organizations Solo se puede asociar una instancia del Centro de Identidad de IAM a una instancia independiente Cuenta de AWS y puede utilizarla para las asignaciones de aplicaciones dentro de esa instancia independiente. Cuenta de AWS

Capability	Instancia en la cuenta de AWS Organizations administración (recomendada)	Instancia en una cuenta de miembro	Instancia en una instancia independiente Cuenta de AWS
Administración de usuarios	 S	 S	 Sí
AWS portal de acceso para acceder con un solo inicio de sesión	 S	 S	 Sí

Capability	Instancia en la cuenta de AWS Organizations administración (recomendada)	Instancia en una cuenta de miembro	Instancia en una instancia independiente Cuenta de AWS
a sus aplicaciones gestionadas AWS			
Aplicaciones gestionadas por el cliente de OAuth 2.0 (OIDC)	 S	 S	 Sí
Permisos para varias cuentas	 S	 N	 No
AWS portal de acceso para acceder con un solo inicio de sesión a su Cuentas de AWS	 S	 N	 No
aplicaciones SAML 2.0 administradas por el cliente	 S	 N	 No
El administrador delegado puede administrar la instancia	 S	 N	 No

Temas

- Instancias de organización de IAM Identity Center
- Instancias de cuenta de IAM Identity Center
- Habilite las instancias de cuentas en la consola de IAM Identity Center
- Control de la creación de instancias de cuenta con políticas de control de servicio

- Creación de una instancia de cuenta de IAM Identity Center

Instancias de organización de IAM Identity Center

Al activar el Centro de Identidad de IAM junto con AWS Organizations, se crea una instancia organizativa del Centro de Identidad de IAM. La instancia de organización debe estar habilitada en su cuenta de administración y puede administrar de forma centralizada el acceso de los usuarios y grupos con una sola instancia de organización. Solo puede tener una instancia de organización para cada cuenta de administración de AWS Organizations.

Si habilitó IAM Identity Center antes del 15 de noviembre de 2023, tiene una instancia de organización de IAM Identity Center.

Cuándo usar una instancia de organización

Las instancias de organización son el método principal para activar IAM Identity Center y, en la mayoría de los casos, se recomienda usar una instancia de organización. Las instancias de organización ofrecen los siguientes beneficios:

- Support para todas las funciones de IAM Identity Center, incluida la gestión de permisos para varios Cuentas de AWS miembros de su organización y la asignación del acceso a las aplicaciones gestionadas por los clientes.
- Reducción de la cantidad de puntos de administración: una instancia de organización tiene un único punto de administración, que es la cuenta de administración. Le recomendamos que habilite una instancia de organización en lugar de una instancia de cuenta para reducir la cantidad de puntos de administración.
- Controle la creación de instancias de cuentas: puede controlar si las cuentas de los miembros de su organización pueden crear instancias de cuentas, siempre y cuando no haya implementado una instancia del IAM Identity Center en su organización en una región habilitada (esta opción está desactivada de Región de AWS forma predeterminada).

Instancias de cuenta de IAM Identity Center

Con una instancia de cuenta de IAM Identity Center, puede implementar aplicaciones AWS gestionadas compatibles y aplicaciones gestionadas por clientes basadas en el OIDC. Las instancias de cuentas permiten el despliegue aislado de aplicaciones en una sola aplicación Cuenta de AWS,

aprovechando las funciones del portal de acceso e identidad de los empleados de IAM Identity Center.

Las instancias de cuenta están vinculadas a una sola cuenta Cuenta de AWS y se utilizan únicamente para gestionar el acceso de usuarios y grupos a las aplicaciones compatibles de la misma cuenta y. Región de AWS Está limitado a una instancia de cuenta por Cuenta de AWS. Puede crear una instancia de cuenta a partir de cualquiera de las siguientes opciones:

- Una cuenta de miembro en AWS Organizations.
- Una cuenta independiente Cuenta de AWS que no está gestionada por AWS Organizations.

Restricciones de disponibilidad de las cuentas de los miembros

Puede implementar una instancia de cuenta en una cuenta de miembro de una organización si se cumplen las siguientes condiciones:

- No tenías una instancia de IAM Identity Center implementada en tu organización antes del 15 de noviembre de 2023.
- Ya tienes una instancia del Centro de Identidad de IAM implementada en tu organización antes del 15 de noviembre de 2023 y tu administrador ha habilitado las cuentas de los miembros para crear instancias de cuentas del Centro de Identidad de IAM.
- Su administrador no ha creado una política de control de servicios que impida que las cuentas de los miembros creen instancias de cuentas.
- A pesar de todo, todavía no tienes una instancia del Centro de Identidad de Región de AWS IAM en esta misma cuenta.
- Está trabajando en un Región de AWS lugar en el que el Centro de Identidad de IAM no está disponible. Para obtener información acerca de las regiones, consulte AWS IAM Identity Center Disponibilidad regional.

Temas

- Cuándo usar las instancias de cuenta
- Consideraciones sobre las instancias de cuenta
- AWS aplicaciones administradas que admiten instancias de cuentas

Cuándo usar las instancias de cuenta

En la mayoría de los casos, se recomienda usar una instancia de organización. Las instancias de cuenta solo se deben usar si se da una de las siguientes situaciones:

- Desea realizar una prueba temporal de una aplicación AWS gestionada compatible para determinar si la aplicación se adapta a las necesidades de su empresa.
- No tiene previsto adoptar el IAM Identity Center en toda su organización, pero quiere dar soporte a una o más aplicaciones AWS gestionadas.
- Tiene una instancia organizativa de IAM Identity Center, pero desea implementar una aplicación AWS gestionada compatible en un conjunto aislado de usuarios que son distintos de los usuarios de la instancia de su organización.

> **Important**
>
> Si piensa utilizar IAM Identity Center para admitir aplicaciones en varias cuentas, cree una instancia de organización y no utilice instancias de cuenta.

Consideraciones sobre las instancias de cuenta

Una instancia de cuenta está diseñada para casos de uso especializados y ofrece un subconjunto de características disponibles para una instancia de organización. Tenga en cuenta lo siguiente antes de crear una instancia de cuenta:

- Las instancias de cuentas no admiten conjuntos de permisos y, por lo tanto, no admiten el acceso a Cuentas de AWS ellos.
- No puede convertir una instancia de cuenta en una instancia de organización.
- No puede fusionar una instancia de cuenta con una instancia de organización.
- Solo instancias de cuentas de AWS aplicaciones gestionadas soporte seleccionadas.
- Utilice instancias de cuenta para usuarios aislados que utilizarán las aplicaciones en una sola cuenta y durante la vida útil de las aplicaciones utilizadas.
- Las aplicaciones que están asociadas a una instancia de cuenta deben permanecer asociadas a la instancia de cuenta hasta que elimine la aplicación y sus recursos.
- La instancia de una cuenta debe permanecer en el Cuenta de AWS lugar donde se creó.

AWS aplicaciones administradas que admiten instancias de cuentas

Consulte AWS aplicaciones gestionadas para saber qué aplicaciones AWS gestionadas son compatibles con las instancias de cuentas de IAM Identity Center. Compruebe la disponibilidad de la creación de instancias de cuentas con su aplicación AWS gestionada.

Habilite las instancias de cuentas en la consola de IAM Identity Center

Si activó el Centro de Identidad de IAM antes del 15 de noviembre de 2023, tiene una instancia organizativa del Centro de Identidad de IAM y la posibilidad de que las cuentas de los miembros creen instancias de cuentas está deshabilitada de forma predeterminada. Puede elegir si las cuentas de miembros pueden crear instancias de cuenta mediante la habilitación de la característica de instancias de cuenta en la AWS Management Console.

> **Note**
>
> Las cuentas de los miembros pueden crear una instancia de cuenta siempre que no hayas implementado una instancia del Centro de Identidad de IAM en tu organización en una región habilitada (Región de AWS que está deshabilitada de forma predeterminada), independientemente de la fecha de despliegue. Cualquier instancia organizativa de IAM Identity Center que se implemente de forma opcional Región de AWS impedirá la creación de instancias de cuentas. Para obtener información acerca de las regiones, consulte AWS IAM Identity Center Disponibilidad regional.

Para habilitar la creación de instancias de cuentas por parte de las cuentas de miembros de su organización

1. Abra la consola de IAM Identity Center
2. Seleccione Configuración y, a continuación, seleccione la pestaña Administración.
3. En la sección Instancias de cuenta de IAM Identity Center, seleccione Habilitar instancias de cuenta de IAM Identity Center.
4. En el cuadro de diálogo Habilitar instancias de cuenta de IAM Identity Center, confirme que desea permitir que las cuentas de miembros de su organización creen instancias de cuenta; para ello, seleccione Habilitar.

> **Important**
>
> La activación de las instancias de cuentas del Centro de Identidad de IAM para las cuentas de los miembros es una operación que se realiza una sola vez. Esto significa que esta operación no se puede revertir. Una vez habilitada, puedes limitar la creación de instancias de cuentas mediante la creación de una política de control de servicios (SCP). Para obtener instrucciones, consulte Controlar la creación de instancias de cuentas con las políticas de control de servicios.

Control de la creación de instancias de cuenta con políticas de control de servicio

Los usuarios pueden crear una instancia del Centro de Identidad de IAM vinculada a una única instancia Cuenta de AWS, denominada instancia de cuenta del Centro de Identidad de IAM. Puede controlar la creación de instancias de cuenta con políticas de control de servicio (SCP).

1. Abra la consola de IAM Identity Center
2. En el panel de control, en la sección Administración central, seleccione el botón Impedir instancias de cuentas.
3. En el cuadro de diálogo Asociar una SCP para impedir la creación de nuevas instancias de cuenta, se le ofrecerá una SCP. Cópiela y pulse el botón Ir al panel de control de SCP. Se le dirigirá a la consola de AWS Organizations para crear la SCP o asociarla como una instrucción a una SCP existente.

   Las políticas de control de servicios son una característica de. AWS Organizations Para obtener instrucciones sobre cómo conectar una SCP, consulte Asociar y desasociar políticas de control de servicios en la Guía del usuario de AWS Organizations .

En lugar de impedir la creación de instancias de cuentas, puede limitar la creación de instancias de cuentas a una instancia específica Cuenta de AWS de su organización:

Example : SCP para controlar la creación de instancias

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

```
    "Statement" : [
        {
            "Sid": "DenyMemberAccountInstances",
            "Effect": "Deny",
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
        }
    ]
}
```

Creación de una instancia de cuenta de IAM Identity Center

Las instancias de organización son el método principal y recomendado para activar IAM Identity Center. Asegúrese de que su caso de uso admita la creación de una instancia de cuenta y de que conozca las consideraciones que hay que tener en cuenta.

Creación de una instancia de cuenta a partir de una cuenta de miembro de la organización o de una Cuenta de AWS independiente

1. Realice una de estas 2 operaciones para iniciar sesión en la AWS Management Console.
   - Nuevo para AWS (usuario root): inicia sesión como propietario de la cuenta; para ello, selecciona Usuario root e introduce tu dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
   - Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
2. Abra la consola de IAM Identity Center.
3. En Activar el IAM Identity Center, seleccione Activar.
4. Seleccione Continuar creando la instancia de cuenta y seleccione Continuar.

> **Note**
>
> Si existe una instancia de organización de IAM Identity Center, asegúrese de que su caso de uso requiera su propia instancia de cuenta de IAM Identity Center. Si no es así, seleccione Cancelar y usar la instancia de la organización.

5. Opcional. Agregue las etiquetas que desee asociar a esta instancia de cuenta.

Una notificación en la consola indica que se ha creado correctamente una instancia de cuenta e incluye el ID de la instancia. Puede asignar un nombre a la instancia en Resumen de configuración.

> **Note**
>
> De forma predeterminada, la autenticación multifactor (MFA) está habilitada para las instancias de cuenta. Se pedirá a los usuarios que inicien sesión con la MFA cuando cambien de dispositivo, navegador o ubicación. Como práctica recomendada de seguridad, aconsejamos que utilice la MFA para las identidades de la plantilla. Información sobre Administrar dispositivos MFA en el IAM Identity Center.

Las funciones de administración, como la confirmación de la fuente de identidad, el ajuste de la configuración de autenticación multifactorial y la adición de aplicaciones AWS administradas, deben completarse en la consola del IAM Identity Center.

Autenticación

Un usuario inicia sesión en el portal de AWS acceso con su nombre de usuario. Cuando lo hace, IAM Identity Center redirige la solicitud al servicio de autenticación de IAM Identity Center en función del directorio asociado a la dirección de correo electrónico del usuario. Una vez autenticados, los usuarios tienen acceso de inicio de sesión único a cualquiera de las AWS cuentas y aplicaciones de terceros (software-as-a-service SaaS) que aparecen en el portal sin necesidad de solicitar más datos de inicio de sesión. Esto significa que los usuarios ya no necesitan realizar un seguimiento de las credenciales de varias cuentas para las distintas AWS aplicaciones asignadas que utilizan a diario.

Sesiones de autenticación

El Centro de Identidad de IAM mantiene dos tipos de sesiones de autenticación: una para representar el inicio de sesión de los usuarios en el Centro de Identidad de IAM y otra para representar el acceso de los usuarios a las aplicaciones AWS gestionadas, como Amazon SageMaker Studio o Amazon Managed Grafana. Cada vez que un usuario inicia sesión en IAM Identity Center, se crea una sesión de inicio de sesión durante el tiempo configurado en IAM Identity Center, que puede ser de hasta 90 días. Para obtener más información, consulte Gestione la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center. Cada vez que el usuario accede a una aplicación, la sesión de inicio de sesión de IAM Identity Center se utiliza para obtener una sesión de aplicación de IAM Identity Center para esa aplicación. Las sesiones de las aplicaciones de IAM Identity Center tienen una duración actualizable de 1 hora, es decir, las sesiones de aplicaciones de IAM Identity Center se actualizan automáticamente cada hora, siempre que la sesión de inicio de sesión en IAM Identity Center de la que se obtuvieron esas sesiones siga siendo válida. Cuando el usuario utiliza el Centro de identidad de IAM para acceder a la AWS Management Console CLI, la sesión de inicio de sesión del Centro de identidad de IAM se utiliza para obtener una sesión de IAM, tal como se especifica en el conjunto de permisos del Centro de identidad de IAM correspondiente (más específicamente, el Centro de identidad de IAM asume una función de IAM, que administra el Centro de identidad de IAM, en la cuenta de destino).

Al deshabilitar o eliminar un usuario de IAM Identity Center, se impedirá inmediatamente que ese usuario inicie sesión para crear nuevas sesiones de inicio de sesión en IAM Identity Center. Las sesiones de inicio de sesión en IAM Identity Center se almacenan en caché durante una hora, lo que significa que si deshabilita o elimina a un usuario mientras tiene una sesión de inicio de sesión activa

en IAM Identity Center, su sesión de inicio de sesión actual continuará durante una hora, en función de cuándo se actualizó la sesión de inicio de sesión por última vez. Durante este tiempo, el usuario puede iniciar nuevas sesiones de aplicación de IAM Identity Center y de rol de IAM.

Cuando caduque la sesión de inicio de sesión en IAM Identity Center, el usuario ya no podrá iniciar nuevas sesiones de aplicación o de rol de IAM en IAM Identity Center. Sin embargo, las sesiones de aplicación de IAM Identity Center también se pueden almacenar en caché durante un máximo de una hora, de modo que el usuario puede conservar el acceso a una aplicación durante un máximo de una hora después de que haya expirado la sesión de inicio de sesión en IAM Identity Center. Todas las sesiones de rol de IAM existentes continuarán en función de la duración configurada en el conjunto de permisos de IAM Identity Center (configurable por el administrador; hasta 12 horas).

En la siguiente tabla se resumen estos comportamientos:

Experiencia de usuario y comportamiento del sistema	Tiempo transcurrido desde la desactivación/ eliminación del usuario
El usuario ya no puede iniciar sesión en IAM Identity Center; no puede obtener una nueva sesión de inicio de sesión en IAM Identity Center	Ninguno (con efecto inmediato)
El usuario ya no puede iniciar nuevas sesiones de aplicaciones o de rol de IAM a través de IAM Identity Center	Hasta 1 hora
El usuario ya no puede acceder a ninguna aplicación (se terminan todas las sesiones de la aplicación)	Hasta 2 horas (hasta 1 hora para que caduque la sesión de inicio de sesión de IAM Identity Center y hasta 1 hora para que caduque la sesión de la aplicación de IAM Identity Center)
El usuario ya no puede acceder a ninguno de ellos a través del Centro de Identidad de IAM Cuentas de AWS	Hasta 13 horas (hasta 1 hora si caduca la sesión de inicio de sesión en IAM Identity Center y hasta 12 horas más si la sesión de rol de IAM configurada por el administrador se ajusta a la configuración de duración de sesión de IAM Identity Center para el conjunto de permisos)

Para obtener más información acerca de las sesiones, consulte Definir la duración de la sesión.

Administración de las identidades de la plantilla

AWS Identity and Access Management (IAM) ayuda a gestionar de forma segura las identidades y el acceso a los servicios y recursos de AWS. Como servicio de IAM, AWS IAM Identity Center es donde puede crear o conectar las identidades de su personal de AWS una sola vez y gestionar el acceso de forma centralizada a sus múltiples Cuentas de AWS y aplicaciones.

Para los clientes del centro de identidades IAM, no hay cambios en la forma de gestionar de forma centralizada el acceso a múltiples Cuentas de AWS o aplicaciones. Para los nuevos clientes del centro de identidades IAM, puede configurar el centro de identidades IAM de forma flexible para que se ejecute junto con la gestión de acceso única de Cuenta de AWS o sustituyéndola mediante IAM.

Temas

Casos de uso

A continuación, se presentan casos de uso que muestran cómo se puede utilizar el IAM Identity Center para satisfacer diferentes necesidades empresariales.

Temas

Habilite el acceso mediante inicio de sesión único a sus aplicaciones de AWS (función de administrador de aplicaciones)

Este caso de uso proporciona orientación si es un administrador de aplicaciones que administra AWS aplicaciones gestionadas como Amazon SageMaker o AWS IoT SiteWise, y debe proporcionar acceso de inicio de sesión único a sus usuarios.

Antes de comenzar, tenga en cuenta lo siguiente:

- ¿Desea crear un entorno de prueba o producción en una organización independiente en AWS Organizations?
- ¿El IAM Identity Center ya está activado en su organización? ¿Tiene permisos para habilitar el IAM Identity Center en la cuenta de administración de AWS Organizations?

Consulte las siguientes instrucciones para determinar los próximos pasos en función de las necesidades de su empresa.

Configurar mi aplicación de AWS en una Cuenta de AWS independiente

Si debe proporcionar un acceso de inicio de sesión único a una aplicación de AWS y sabe que su departamento de TI aún no utiliza el IAM Identity Center, es posible que necesite crear una Cuenta de AWS independiente para empezar. De forma predeterminada, al crear su propia Cuenta de AWS, dispondrá de los permisos necesarios para crear y gestionar su propia organización de AWS. Para activar el IAM Identity Center, debe disponer de permisos de Usuario raíz de la cuenta de AWS.

El IAM Identity Center y AWS Organizations se pueden activar automáticamente durante la configuración de algunas aplicaciones de AWS (por ejemplo, Amazon Managed Grafana). Si su aplicación de AWS no ofrece la opción de habilitar estos servicios, debe configurar AWS Organizations y el IAM Identity Center antes de poder proporcionar acceso de inicio de sesión único a su aplicación.

El IAM Identity Center no está configurado en mi organización

Dependiendo del administrador de aplicaciones, es posible que no pueda habilitar el IAM Identity Center, en función de sus permisos. El IAM Identity Center requiere permisos específicos en la cuenta de administración de AWS Organizations. En este caso, póngase en contacto con el administrador correspondiente para habilitar IAM Identity Center en la cuenta de administración de Organizations.

Si dispone de permisos suficientes para activar el IAM Identity Center, hágalo primero y, a continuación, continúe con la configuración de la aplicación. Para obtener más información, consulte Introducción a las tareas habituales en IAM Identity Center.

El IAM Identity Center está configurado actualmente en mi organización

En este caso, puede seguir desplegando la aplicación de AWS sin realizar ninguna otra acción.

> **Note**
>
> Si su organización habilitó IAM Identity Center en la cuenta de administración antes del 25 de noviembre de 2019, también debe habilitar las aplicaciones administradas de AWS en la cuenta de administración y, opcionalmente, en las cuentas de los miembros. Si las habilita únicamente en la cuenta de administración, podrá habilitarlas en las cuentas de los miembros más adelante. Para habilitar estas aplicaciones, seleccione Habilitar el acceso en la página Configuración de la consola de IAM Identity Center, en la sección de aplicaciones administradas de AWS. Para obtener más información, consulte Configuración de IAM Identity Center para compartir información de las identidades .

Habilite el acceso de inicio de sesión único a las instancias de Amazon EC2 para Windows

Puede habilitar el acceso de inicio de sesión único a sus instancias Windows de Amazon EC2 si es un administrador de aplicaciones que gestiona los usuarios en el directorio del IAM Identity Center (la fuente de identidad predeterminada para el IAM Identity Center) o si es un proveedor de identidades (IdP) externo compatible, y debe proporcionar acceso al IAM Identity Center a sus escritorios Windows de Amazon EC2 desde la consola de Fleet Manager de AWS.

Con esta configuración, puede acceder de forma segura a sus instancias Windows de Amazon EC2 con las credenciales corporativas existentes. No necesita compartir las credenciales de administrador, acceder a las credenciales varias veces ni configurar el software cliente de acceso remoto. Puede conceder y revocar de forma centralizada el acceso a sus instancias Windows de Amazon EC2 a escala y en múltiples Cuentas de AWS. Por ejemplo, si elimina a un empleado de su fuente de identidad integrada en el IAM Identity Center, perderá automáticamente el acceso a todos los recursos de AWS, incluidas las instancias Windows de Amazon EC2.

Para obtener más información, consulte Cómo habilitar un inicio de sesión único seguro y fluido en las instancias Windows de Amazon EC2 con el IAM Identity Center.

Para ver una demostración de cómo configurar el IAM Identity Center para habilitar esta capacidad, consulte Habilitar el inicio de sesión único en Amazon EC2 Windows con el IAM Identity Center.

Usuarios, grupos y aprovisionamiento

Tenga en cuenta lo siguiente cuando trabaje con usuarios y grupos en IAM Identity Center.

Exclusividad del nombre de usuario y de la dirección de correo electrónico

Los usuarios de IAM Identity Center deben poder identificarse de forma única. IAM Identity Center implementa un nombre de usuario que es el identificador principal de sus usuarios. Aunque la mayoría de las personas definen el nombre de usuario como la dirección de correo electrónico de un usuario, IAM Identity Center y el estándar SAML 2.0 no lo requieren. Sin embargo, muchas aplicaciones basadas en SAML 2.0 utilizan una dirección de correo electrónico como identificador único de los usuarios. Estas aplicaciones obtienen esta información de las aserciones que envía un proveedor de identidades de SAML 2.0 durante la autenticación. Estas aplicaciones dependen de la exclusividad de las direcciones de correo electrónico de cada usuario. Por este motivo, IAM Identity Center le permite especificar algo distinto de una dirección de correo electrónico para el inicio de sesión de los usuarios. IAM Identity Center exige que todos los nombres de usuario y direcciones de correo electrónico de sus usuarios no sean nulos y que sean únicos.

Grupos

Los grupos son una combinación lógica de usuarios que usted define. Puede crear grupos y agregar usuarios a los grupos. IAM Identity Center no admite la adición de un grupo a otro grupo (grupos anidados). Los grupos son útiles a la hora de asignar el acceso a Cuentas de AWS y a las aplicaciones. En lugar de asignarlo a cada usuario de manera individual, concede permisos a un grupo. Más adelante, al agregar o eliminar usuarios de un grupo, el usuario obtiene o pierde de forma dinámica el acceso a las cuentas y aplicaciones que haya asignado al grupo.

Aprovisionamiento de usuarios y grupos

El aprovisionamiento es el proceso de poner la información de usuarios y grupos a disposición de IAM Identity Center y de las aplicaciones administradas de AWS o las aplicaciones administradas por el cliente. Puede crear usuarios y grupos directamente en IAM Identity Center o trabajar con los usuarios y grupos que tenga en Active Directory o en un proveedor de identidades externo. Antes de poder utilizar IAM Identity Center para asignar permisos de acceso a usuarios y grupos en una Cuenta de AWS, IAM Identity Center debe saber primero quiénes son los usuarios y grupos. Del mismo modo, las aplicaciones administradas de AWS y las aplicaciones administradas por el cliente pueden funcionar con los usuarios y grupos que IAM Identity Center conoce.

El aprovisionamiento en IAM Identity Center varía en función de la fuente de identidades que utilice. Para obtener más información, consulte Administre su fuente de identidad.

Administre su fuente de identidad

Su origen de identidad en IAM Identity Center define dónde se administran sus usuarios y grupos. Tras configurar su origen de identidad, puede buscar los usuarios o grupos para concederles acceso mediante inicio de sesión único a las Cuentas de AWS, las aplicaciones o ambas.

Solo puede tener una fuente de identidad por organización en AWS Organizations. Puede elegir una de las siguientes opciones como origen de identidad:

- Directorio de Identity Center: cuando se activa IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como fuente de identidad predeterminada. Aquí es donde usted crea sus usuarios y grupos, y donde asigna el nivel de acceso de estos a sus Cuentas de AWS y aplicaciones.
- Active Directory: elija esta opción si quiere seguir administrando a los usuarios de su directorio de AWS Managed Microsoft AD mediante el uso de AWS Directory Service o de su directorio autoadministrado en Active Directory (AD).
- Proveedor de identidad externo: elija esta opción si desea administrar a los usuarios en un proveedor de identidades externo (IdP), como Okta o Microsoft Entra ID.

> **Note**
>
> IAM Identity Center no admite Simple AD basado en SAMBA4 como fuente de identidad.

Temas

Consideraciones para cambiar la fuente de identidad

Aunque puede cambiar su fuente de identidad en cualquier momento, le recomendamos que considere cómo este cambio podría afectar a su implementación actual.

Si ya administra usuarios y grupos en un origen de identidad, cambiar a un origen de identidad diferente podría eliminar todas las asignaciones de usuarios y grupos que configuró en IAM Identity Center. Si esto ocurre, todos los usuarios, incluido el usuario administrativo del Centro de identidades de IAM, perderán el acceso de inicio de sesión único a sus Cuentas de AWS aplicaciones.

No cambie la fuente de identidad de IAM Identity Center sin revisar las siguientes consideraciones antes de proceder. Si desea continuar con el cambio de la fuente de identidad, consulte Cambiar su fuente de identidad para obtener más información.

Cambiar de IAM Identity Center a Active Directory

Si ya administra usuarios y grupos en Active Directory, le recomendamos que considere la posibilidad de conectar su directorio al habilitar IAM Identity Center y elegir su fuente de identidad. Esto debe hacerse antes de crear usuarios y grupos en el directorio predeterminado de Identity Center y de realizar cualquier asignación.

Si ya administra usuarios y grupos en el directorio predeterminado de Identity Center, tenga en cuenta lo siguiente:

- Asignaciones, usuarios y grupos eliminados: al cambiar la fuente de identidad a Active Directory, se eliminan los usuarios y grupos del directorio de Identity Center. Este cambio también elimina las asignaciones. En este caso, después de cambiar a Active Directory, debe sincronizar los usuarios y grupos de Active Directory con el directorio de Identity Center y, a continuación, volver a aplicar sus asignaciones.

  Si decide no usar Active Directory, debe crear los usuarios y grupos en el directorio de Identity Center y, a continuación, realizar las asignaciones.
- Las asignaciones no se eliminan cuando se eliminan las identidades: cuando se eliminan las identidades del directorio de Identity Center, las asignaciones correspondientes también se eliminan en IAM Identity Center. Sin embargo, cuando se eliminan las identidades (ya sea en Active Directory o en las identidades sincronizadas) en Active Directory, las asignaciones correspondientes no se eliminan.
- No hay sincronización saliente para las API: si utiliza Active Directory como fuente de identidad, le recomendamos que utilice las API de creación, actualización y eliminación con precaución.

IAM Identity Center no admite la sincronización saliente, por lo que su fuente de identidad no se actualiza automáticamente con los cambios que realiza en los usuarios o grupos que utilizan estas API.

- La URL del portal de acceso cambiará: al cambiar la fuente de identidad entre el Centro de Identidad de IAM y Active Directory, también se cambiará la URL del portal de acceso. AWS

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte Conexión un directorio Microsoft AD.

Cómo cambiar de IAM Identity Center a un IdP externo

Si cambia la fuente de identidad de IAM Identity Center a un proveedor de identidades (IdP) externo, tenga en cuenta lo siguiente:

- Las asignaciones y las membresías funcionan con las aserciones correctas: las asignaciones de usuario, las asignaciones grupales y las pertenencias a grupos seguirán funcionando mientras el nuevo IdP envíe las aserciones correctas (por ejemplo, los NameID de SAML). Estas afirmaciones deben coincidir con los nombres de usuario y los grupos del Centro de identidad de IAM.
- Sin sincronización saliente: el Centro de identidad de IAM no admite la sincronización saliente, por lo que su IdP externo no se actualizará automáticamente con los cambios en los usuarios y grupos que realice en el Centro de identidad de IAM.
- Aprovisionamiento de SCIM: si utiliza el aprovisionamiento de SCIM, los cambios en los usuarios y grupos de su proveedor de identidad solo se reflejan en el Centro de identidades de IAM después de que su proveedor de identidad los envíe al Centro de identidades de IAM. Consulte Consideraciones para utilizar el aprovisionamiento automático.
- Reversión: puede volver a utilizar el IAM Identity Center desde su fuente de identidad en cualquier momento. Consulte Cambiar de un IdP externo a IAM Identity Center.

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte Conexión a un proveedor de identidades externo.

Cambiar de un IdP externo a IAM Identity Center

Si cambia la fuente de identidad de un proveedor de identidades (IdP) externo a IAM Identity Center, tenga en cuenta lo siguiente:

- IAM Identity Center conserva todas sus asignaciones.

- Forzar el restablecimiento de la contraseña: los usuarios que tenían contraseñas en IAM Identity Center pueden seguir iniciando sesión con sus contraseñas anteriores. Para los usuarios que estaban en el IdP externo y no en IAM Identity Center, el administrador debe forzar el restablecimiento de la contraseña.

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte Administración de identidades en IAM Identity Center.

Cambiar de un IdP externo a otro IdP externo

Si ya utiliza un IdP externo como fuente de identidad para IAM Identity Center y cambia a un IdP externo diferente, tenga en cuenta lo siguiente:

- Las asignaciones y las membresías funcionan con las confirmaciones correctas: IAM Identity Center conserva todas sus tareas. Las asignaciones de usuarios, las asignaciones grupales y las membrecías a grupos seguirán funcionando mientras el nuevo IdP envíe las confirmaciones correctas (por ejemplo, los nameID de SAML).

  Estas confirmaciones deben coincidir con los nombres de usuario de IAM Identity Center cuando los usuarios se autentiquen a través del nuevo IdP externo.
- Aprovisionamiento de SCIM: si utiliza SCIM para el aprovisionamiento en IAM Identity Center, le recomendamos que revise la información específica del IdP en esta guía y la documentación proporcionada por el IdP para asegurarse de que el nuevo proveedor haga coincidir correctamente los usuarios y los grupos cuando SCIM esté habilitado.

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte Conexión a un proveedor de identidades externo.

Cambiar de Active Directory a un IdP externo

Si cambia la fuente de identidad de un IdP externo a Active Directory o de Active Directory a un IdP externo, tenga en cuenta lo siguiente:

- Se eliminan los usuarios, los grupos y las asignaciones: todos los usuarios, grupos y asignaciones se eliminan de IAM Identity Center. Ninguna información de usuario o grupo se ve afectada ni en el IdP externo ni en Active Directory.

- Aprovisionamiento de usuarios: si cambia a un IdP externo, debe configurar IAM Identity Center para aprovisionar a los usuarios. Como alternativa, debe aprovisionar manualmente los usuarios y grupos para el IdP externo antes de poder configurar las asignaciones.
- Creación de asignaciones y grupos: si cambia a Active Directory, debe crear asignaciones con los usuarios y grupos que se encuentran en el directorio de Active Directory.

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte Conexión un directorio Microsoft AD.

Cambiar su fuente de identidad

El siguiente procedimiento describe cómo cambiar de un directorio que proporciona el IAM Identity Center (el directorio predeterminado del Identity Center) a Active Directory o a un proveedor de identidad externo, o viceversa. Antes de continuar, revise la información incluida en Consideraciones para cambiar la fuente de identidad. En función de su implementación actual, este cambio podría eliminar cualquier asignación de usuarios y grupos que haya configurado en el IAM Identity Center. Si esto ocurre, todos los usuarios, incluido el usuario administrativo de IAM Identity Center, perderán el acceso con inicio de sesión único a sus Cuentas de AWS y aplicaciones.

Para cambiar la fuente de identidad:

1. Abra la Consola del IAM Identity Center.
2. Elija Settings.
3. En la página de Configuración, seleccione la pestaña Origen de la identidad. Elija Acciones y, a continuación, elija Cambiar fuente de identidad.
4. En Elegir fuente de identidad, seleccione la fuente a la que desee cambiar y, a continuación, seleccione Siguiente.

   Si va a cambiar a Active Directory, elija el directorio disponible en el menú de la página siguiente.

> **Important**
>
> Al cambiar la fuente de identidad a o desde Active Directory, se eliminan los usuarios y grupos del directorio del Identity Center. Este cambio también elimina cualquier asignación que haya configurado en el IAM Identity Center.

Si va a cambiar a un proveedor de identidad externo, recomendamos que siga los pasos descritos en Cómo conectarse a un proveedor de identidades externo.

5. Cuando haya leído el aviso legal y esté listo para continuar, introduzca Aceptar.
6. Elija Cambiar fuente de identidad. Si va a cambiar su fuente de identidad a Active Directory, vaya al siguiente paso.
7. Si cambia la fuente de identidad a Active Directory, accederá a la página de Configuración. Utilice la página de cCnfiguración para realizar cualquiera de las siguientes operaciones:

   - Seleccione Iniciar la configuración guiada. Para obtener información sobre cómo completar el proceso de configuración guiada, consulte Configuración guiada.
   - En la sección Fuente de identidad, elija Acciones y, a continuación, elija Administrar la sincronización para configurar el Alcance de la sincronización, la lista de usuarios y grupos que se van a sincronizar.

Administre el inicio de sesión y el uso de atributos para todos los tipos de fuentes de identidad

El centro de identidad de IAM ofrece el siguiente conjunto de funciones que permiten a los administradores controlar el uso del portal de AWS acceso, establecer la duración de las sesiones para los usuarios del portal de AWS acceso y sus aplicaciones, y utilizar atributos para el control de acceso. Estas características funcionan con un directorio de Identity Center o con un proveedor de identidad externo como su fuente de identidad.

> **Note**
>
> No se admite la administración de sesiones si utiliza Active Directory como fuente de identidad para IAM Identity Center.

Temas

- Gestione la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center
- Configure la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center

- Elimine las sesiones del portal de AWS acceso y las aplicaciones AWS integradas
- Atributos de usuario y grupo compatibles

Gestione la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center

El administrador del IAM Identity Center puede configurar la duración de la sesión tanto para las aplicaciones integradas con el IAM Identity Center como para las. Portal de acceso a AWS La configuración de duración de las sesiones determina la frecuencia con la que los usuarios deben volver a autenticarse. El administrador del centro de identidad de IAM puede finalizar una sesión activa en el portal de AWS acceso y, al hacerlo, también finalizar las sesiones de las aplicaciones integradas.

Para obtener más información, consulte Configure la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center. Para obtener más información sobre cómo gestionar y finalizar las sesiones de los usuarios, consulteElimine las sesiones del portal de AWS acceso y las aplicaciones AWS integradas.

> **Note**
>
> La AWS modificación de la duración de la sesión del portal de AWS acceso y la finalización de las sesiones del portal de acceso no afectan a la duración de la sesión de AWS Management Console que defina en sus conjuntos de permisos.

Configure la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center

La duración de la sesión de autenticación en las aplicaciones integradas en el IAM Identity Center Portal de acceso a AWS y en las aplicaciones integradas es el tiempo máximo que un usuario puede iniciar sesión sin volver a autenticarse. La duración predeterminada de la sesión es de 8 horas. El administrador del centro de identidad de IAM puede especificar una duración diferente, desde un mínimo de 15 minutos hasta un máximo de 90 días. Para obtener más información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulteAutenticación.

En los siguientes temas se proporciona información sobre la configuración de la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center.

Temas

Requisitos y consideraciones previos

Los siguientes son los requisitos previos y las consideraciones para configurar la duración de la sesión para el portal de AWS acceso y las aplicaciones integradas del IAM Identity Center.

Proveedores de identidades externos

El Centro de Identidad de IAM utiliza los `SessionNotOnOrAfter` atributos de las aserciones de SAML para ayudar a determinar durante cuánto tiempo puede ser válida la sesión.

- Si no `SessionNotOnOrAfter` se incluye en una afirmación de SAML, la duración de una sesión del portal de AWS acceso no se ve afectada por la duración de la sesión de IdP externa. Por ejemplo, si la duración de su sesión de IdP es de 24 horas y ha establecido una duración de sesión de 18 horas en el Centro de identidad de IAM, sus usuarios deberán volver a autenticarse en el AWS portal de acceso después de 18 horas.
- Si `SessionNotOnOrAfter` se incluye en una afirmación de SAML, el valor de duración de la sesión se establece en la duración de la sesión del portal de AWS acceso y la duración de la sesión de IDP de SAML, que sea menor. Si establece una duración de sesión de 72 horas en el Centro de identidades de IAM y su IdP tiene una duración de sesión de 18 horas, sus usuarios tendrán acceso a los AWS recursos durante las 18 horas definidas en su IdP.
- Si la duración de la sesión de su IdP es superior a la establecida en el IAM Identity Center, sus usuarios podrán iniciar una nueva sesión en el IAM Identity Center sin tener que volver a introducir sus credenciales, en función de la sesión de inicio de sesión aún válida con su IdP.

> **Note**
>
> No se admite la administración de sesiones si utiliza Active Directory como fuente de identidad para IAM Identity Center.

AWS CLI y sesiones de SDK

Si utiliza los AWS Command Line Interface kits de desarrollo de AWS software (SDK) u otras herramientas de AWS desarrollo para acceder a los AWS servicios mediante programación, debe cumplir los siguientes requisitos previos para establecer la duración de la sesión para el portal de AWS acceso y las aplicaciones integradas del IAM Identity Center.

- Debe configurar la duración de la sesión del portal de AWS acceso en la consola del IAM Identity Center.
- Debe definir un perfil para la configuración de inicio de sesión único en su archivo de configuración compartido de AWS . Este perfil se utiliza para conectarse al portal de AWS acceso. Le recomendamos que utilice la configuración del proveedor de tokens de SSO. Con esta configuración, el AWS SDK o la herramienta pueden recuperar automáticamente los tokens de autenticación actualizados. Para obtener más información, consulte Configuración del proveedor de tokens de SSO en la Guía de referencia de los SDK y las herramientas de AWS .
- Los usuarios deben ejecutar una versión del SDK AWS CLI o una versión que sea compatible con la administración de sesiones.

Versiones mínimas de la AWS CLI que admiten la administración de sesiones

Las siguientes son las versiones mínimas de las AWS CLI que admiten la administración de sesiones.

- AWS CLI V2 2.9 o posterior
- AWS CLI V1 1.27.10 o posterior

Para obtener información sobre cómo instalar o actualizar la AWS CLI versión más reciente, consulte Instalación o actualización de la última versión de. AWS CLI

Si sus usuarios están ejecutando el conjunto de permisos AWS CLI, si actualiza el conjunto de permisos justo antes de que caduque la sesión del Centro de Identidad de IAM y la duración de la sesión se establece en 20 horas, mientras que la duración del conjunto de permisos se establece en 12 horas, la AWS CLI sesión se prolongará durante un máximo de 20 horas más 12 horas para un total de 32 horas. Para obtener más información sobre la CLI de IAM Identity Center, consulte Referencia de comandos de la AWS CLI.

Versiones mínimas de los SDK que admiten la administración de sesiones de IAM Identity Center

A continuación se muestran las versiones mínimas de los SDK que admiten la administración de sesiones de IAM Identity Center.

SDK	Versión mínima
Python	1.26.10
PHP	3,245.0
Ruby	aws-sdk-core 3.167,0
Java V2	AWS SDK para Java v2 (2.18.13)
Go V2	SDK completo: release-2022-11-11 y módulos Go específicos: credentials/v1.13.0, config/v1 .18.0
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

Cómo configurar la duración de sesiones

Utilice el siguiente procedimiento para configurar la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas de IAM Identity Center.

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de Configuración, seleccione la pestaña Autenticación.
4. En Autenticación, junto a Configuración de sesión, elija Configurar. Aparecerá el cuadro de diálogo Configurar los ajustes de la sesión.

5. En el cuadro de diálogo Establecer la configuración, elija la duración máxima de la sesión en minutos, horas y días para sus usuarios a través de la flecha desplegable. Elija la duración de la sesión y, a continuación, seleccione Guardar. Vuelva a la página Configuración.

Elimine las sesiones del portal de AWS acceso y las aplicaciones AWS integradas

Utilice el siguiente procedimiento para ver y eliminar las sesiones activas de un usuario del Centro de identidades de IAM.

Para eliminar una sesión activa del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center

1. Abra la consola de IAM Identity Center.
2. Seleccione Usuarios.
3. En la página Usuarios, elija el nombre de usuario cuyas sesiones desee administrar. Esto lo dirigirá a una página con la información del usuario.
4. En la página del usuario, elija la pestaña Sesiones activas. El número entre paréntesis junto a Sesiones activas indica el número de sesiones activas actuales de este usuario.
5. Seleccione las casillas de verificación situadas junto a las identidades que desea eliminar y elija Eliminar sesión. Aparecerá un cuadro de diálogo que confirma que está eliminando las sesiones activas de este usuario. Lea la información en el cuadro de diálogo y, si desea continuar, elija Eliminar sesión.
6. Volverá a la página del usuario. Aparecerá una barra de flash verde para indicar que las sesiones seleccionadas se eliminaron correctamente.

Para obtener más información sobre el comportamiento de las sesiones de autenticación revocadas, consulteSesiones de autenticación.

Atributos de usuario y grupo compatibles

Los atributos son fragmentos de información que le ayudan a definir e identificar a usuarios individuales o a agrupar objetos, como `name`, `email` o `members`. IAM Identity Center admite los atributos más utilizados, independientemente de si se introducen de forma manual durante la creación del usuario o si se aprovisionan de forma automática mediante un motor de sincronización, como el definido en la especificación del sistema de administración de identidades entre dominios (SCIM). Para obtener más información, consulte https://tools.ietf.org/html/rfc7642. Para obtener más

información sobre el aprovisionamiento manual y automático, consulte Aprovisionamiento cuando los usuarios provienen de un IdP externo.

Dado que IAM Identity Center admite el SCIM para los casos de uso del aprovisionamiento automático, el directorio de Identity Center admite todos los mismos atributos de usuario y grupo que figuran en la especificación del SCIM, con algunas excepciones. En las siguientes secciones, se describen los atributos que IAM Identity Center no admite.

Objetos del usuario

El almacén de identidades de IAM Identity Center admite todos los atributos del esquema de usuario de SCIM (https://tools.ietf.org/html/rfc7643#section-8.3), excepto los siguientes:

- `password`
- `ims`
- `photos`
- `entitlements`
- `x509Certificates`

Se admiten todos los subatributos de los usuarios, excepto los siguientes:

- Subatributo `'display'` de cualquier atributo con valores múltiples (por ejemplo, `emails` ophoneNumbers)
- Subatributo `'version'` del atributo `'meta'`

Agrupar objetos

Se admiten todos los atributos del esquema de grupo SCIM (https://tools.ietf.org/html/rfc7643#section-8.4).

Se admiten todos los subatributos de los grupos, excepto los siguientes:

- Subatributo `'display'` de cualquier atributo con valores múltiples (por ejemplo, miembros).

Administración de identidades en IAM Identity Center

IAM Identity Center ofrece las siguientes funciones para sus usuarios y grupos:

- Cree sus usuarios y grupos.
- Añada sus usuarios como miembros a los grupos.
- Asigne a los grupos el nivel de acceso deseado a Cuentas de AWS sus aplicaciones.

Para gestionar los usuarios y los grupos en el almacén del Centro de Identidad de IAM, AWS es compatible con las operaciones de la API que se indican en las acciones del Centro de Identidad.

Aprovisionamiento cuando los usuarios están en IAM Identity Center

Al crear usuarios y grupos directamente en IAM Identity Center, el aprovisionamiento es automático. Estas identidades están disponibles de inmediato para su uso al realizar asignaciones y para que las utilicen las aplicaciones. Para obtener más información, consulte Aprovisionamiento de usuarios y grupos.

Cambio de su fuente de identidad

Si prefiere administrar los usuarios en AWS Managed Microsoft AD, puede dejar de usar el directorio del Centro de identidad en cualquier momento y, en su lugar, conectar el Centro de identidad de IAM al directorio de Microsoft AD mediante AWS Directory Service. Para obtener información, consulte las consideraciones para Cambiar de IAM Identity Center a Active Directory.

Si prefiere administrar los usuarios en un proveedor de identidades (IdP) externo, puede conectar IAM Identity Center a su IdP y habilitar el aprovisionamiento automático. Para obtener información, consulte las consideraciones para Cómo cambiar de IAM Identity Center a un IdP externo.

Temas

- Agregar usuarios
- Cómo agregar grupos
- Agregar usuarios a grupos
- Eliminación de grupos de IAM Identity Center
- Eliminación de usuarios del Centro de identidades de IAM
- Inhabilitar el acceso de usuarios de IAM Identity Center
- Edición de propiedades del usuario
- Restablecimiento de la contraseña de usuario de IAM Identity Center para un usuario final
- Envío de un correo electrónico OTP para los usuarios creados desde la API
- Requisitos de contraseñas para administrar identidades en IAM Identity Center

Agregar usuarios

Los usuarios y grupos que cree en su directorio de Identity Center solo estarán disponibles en IAM Identity Center. Siga el procedimiento a continuación para añadir usuarios al directorio de su Identity Center mediante la consola de IAM Identity Center. Como alternativa, puede llamar a la operación de la AWS API CreateUserpara añadir usuarios.

Para añadir un usuario

1. Abra la consola de IAM Identity Center.
2. Seleccione Usuarios.
3. Elija Agregar usuario, y proporcione la siguiente información necesaria:

    a. Nombre de usuario: este nombre de usuario es obligatorio para iniciar sesión en el portal de AWS acceso y no se puede cambiar más adelante. Debe tener entre 1 y 100 caracteres de longitud.

    b. Contraseña: puede enviar un correo electrónico con las instrucciones de configuración de la contraseña (esta es la opción predeterminada) o generar una contraseña de un solo uso. Si va a crear un usuario administrativo y envía un correo electrónico, asegúrese de especificar una dirección de correo electrónico a la que pueda acceder.

        i. Envíe un correo electrónico a este usuario con las instrucciones de configuración de la contraseña. — Esta opción envía automáticamente al usuario una dirección de correo electrónico de Amazon Web Services, con el asunto Invitation to join AWS IAM Identity Center (sucesora de AWS Single Sign-On). El correo electrónico invita al usuario, en nombre de su empresa, a acceder al portal de acceso al Centro AWS de Identidad de IAM.

> **Note**
>
> En algunas regiones, IAM Identity Center envía correos electrónicos a los usuarios que utilizan Amazon Simple Email Service desde otra Región de AWS. Para obtener información sobre cómo se envían los correos electrónicos, consulte Llamadas entre regiones.
> Todos los correos electrónicos enviados por el servicio de IAM Identity Center procederán de una de estas direcciones: `no-reply@signin.aws.com` o `no-reply@login.awsapps.com`. Le recomendamos que configure su sistema de correo electrónico para que acepte los mensajes con estas direcciones

de correo electrónico como remitente y no los trate como correo basura o no deseado.

ii. Generación de una contraseña de un solo uso que pueda compartir con este usuario. — Esta opción le proporciona la URL del portal de AWS acceso y los detalles de la contraseña que puede enviar manualmente al usuario desde su dirección de correo electrónico.

c. Correo electrónico: la dirección de correo electrónico debe ser única.

d. Confirmación de la dirección de correo electrónico

e. Nombre: debe introducir un nombre aquí para que funcione el aprovisionamiento automático. Para obtener más información, consulte Aprovisionamiento estático.

f. Apellido: debe introducir un nombre aquí para que funcione el aprovisionamiento automático.

g. Display name (Nombre de visualización)

> **Note**
>
> (Opcional) Si corresponde, puede especificar valores para atributos adicionales, como el ID inmutable de Microsoft 365 del usuario, para ayudar a proporcionarle acceso de inicio de sesión único a determinadas aplicaciones empresariales.

4. Elija Siguiente.
5. Si corresponde, seleccione uno o más grupos a los que desee añadir al usuario y elija Siguiente.
6. Revise la información que especificó para el paso 1: especificar los detalles del usuario y el paso 2: agregar el usuario a los grupos (opcional). Elija Editar en uno de los pasos para realizar cualquier cambio. Tras confirmar que se ha especificado la información correcta para ambos pasos, elija Añadir usuario.

Cómo agregar grupos

Siga el procedimiento que se detalla para añadir grupos al directorio Identity Center mediante la consola de IAM Identity Center. Como alternativa, puede llamar a la operación de la AWS API CreateGrouppara añadir grupos.

Para añadir un grupo

1. Abrir la consola de IAM Identity Center.
2. Elija Grupos.
3. Elija Crear grupo.
4. Escriba un nombre de grupo y, opcionalmente, una descripción. La descripción debe proporcionar detalles sobre qué permisos se han asignado o se asignará al grupo. En Añadir usuarios al grupo: opcional, busque los usuarios que desea añadir como miembros. A continuación, seleccione la casilla de verificación situada junto a cada uno de ellos.
5. Elija Crear grupo.

Tras añadir este grupo al directorio de Identity Center, puede asignar el acceso de inicio de sesión único a este grupo. Para obtener más información, consulte Asigne el acceso de los usuarios a Cuentas de AWS.

Agregar usuarios a grupos

Siga el procedimiento que se indica para añadir usuarios como miembros de un grupo que ha creado anteriormente en su directorio de IAM Identity Center con la consola IAM Identity Center. Como alternativa, puedes llamar a la operación de la AWS API CreateGroupMembershippara añadir un usuario como miembro de un grupo.

Cómo añadir un usuario como miembro de un grupo

1. Abra la consola de IAM Identity Center.
2. Elija Grupos.
3. Elija el nombre de grupo que desea actualizar.
4. En la página de detalles del grupo, en Usuarios de este grupo, elija Añadir usuarios al grupo.
5. En la página Añadir usuarios al grupo, en Otros usuarios, localice los usuarios que desea añadir como miembros. A continuación, marque la casilla de verificación situada junto a cada uno de ellos.
6. Elija Agregar usuarios.

Eliminación de grupos de IAM Identity Center

Al eliminar un grupo del directorio de IAM Identity Center, se elimina el acceso a las Cuentas de AWS y a las aplicaciones para todos los usuarios que son miembros de este grupo. Una vez que se elimina un grupo, no se puede deshacer la acción. Utilice el siguiente procedimiento para eliminar un grupo al directorio Identity Center mediante la consola de IAM Identity Center.

Cómo eliminar un grupo de IAM Identity Center

> **Important**
>
> Las instrucciones de esta página se aplican a AWS IAM Identity Center. No se aplican a AWS Identity and Access Management (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo eliminar grupos en IAM, consulte Eliminar un grupo de usuarios de IAM en la Guía del usuario de AWS Identity and Access Management .

1. Abra la consola de IAM Identity Center.
2. Elija Grupos.
3. Hay 2 formas de eliminar un grupo:
   - En la página Grupos, puede seleccionar varios grupos para su eliminación. Elija el nombre de grupo que desee eliminar y seleccione Eliminar grupo.
   - Elija el nombre de grupo que desea eliminar. En la página de detalles del grupo, elija Eliminar grupo.
4. Es posible que se le pida que confirme su intención de eliminar el grupo.
   - Si elimina varios grupos a la vez, confírmelo escribiendo “**`Delete`**“ en el cuadro de diálogo Eliminar grupo.
   - Si elimina un solo grupo que contiene usuarios, confirme su intención escribiendo el nombre del grupo que desea eliminar en el cuadro de diálogo Eliminar grupo.
5. Elija Delete group (Eliminar grupo). Si ha seleccionado varios grupos para eliminarlos, elija Eliminar # grupos.

Eliminación de usuarios del Centro de identidades de IAM

Al eliminar un usuario del directorio de IAM Identity Center, se elimina el acceso a las Cuentas de AWS y a las aplicaciones. Una vez que se elimina un usuario, no se puede deshacer la acción. Siga el procedimiento que se detalla para eliminar un usuario al directorio Identity Center mediante la consola de IAM Identity Center.

> **Note**
>
> Si deshabilita el acceso de un usuario o lo elimina en el Centro de identidad de IAM, dicho usuario no podrá iniciar sesión inmediatamente en el portal de AWS acceso y no podrá crear nuevas sesiones de inicio de sesión. Para obtener más información, consulte Sesiones de autenticación.

Cómo eliminar un usuario de IAM Identity Center

> **Important**
>
> Las instrucciones de esta página se aplican a AWS IAM Identity Center. No se aplican a AWS Identity and Access Management (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo eliminar usuarios en IAM, consulte Eliminar un usuario de IAM en la Guía del usuario de AWS Identity and Access Management .

1. Abra la consola de IAM Identity Center.
2. Seleccione Usuarios.
3. Hay 2 formas de eliminar un usuario:
   - En la página Usuarios, puede seleccionar varios usuarios para su eliminación. Seleccione el nombre de usuario que desee eliminar y seleccione Eliminar usuarios.
   - Elija el nombre de usuario que desea eliminar. En la página de detalles del usuario, vaya a la pestaña Eliminar usuario.
4. Si elimina varios usuarios a la vez, confirme su intención escribiendo **`Delete`** en el cuadro de diálogo Eliminar usuario.

5. Seleccione Eliminar usuario(s). Si ha seleccionado varios usuarios para eliminarlos, elija Eliminar # usuarios.

Inhabilitar el acceso de usuarios de IAM Identity Center

Cuando deshabilita un acceso de usuario en su directorio IAM Identity Center, no puede editar sus detalles de usuario, restablecer su contraseña, añadir el usuario a un grupo ni ver los grupos a los que pertenece. Siga el procedimiento que se detalla a continuación para deshabilitar el acceso de los usuarios al directorio de Identity Center mediante la consola de IAM Identity Center.

> **Note**
>
> Si deshabilita el acceso de un usuario o lo elimina en el Centro de identidades de IAM, dicho usuario no podrá iniciar sesión inmediatamente en el portal de AWS acceso y no podrá crear nuevas sesiones de inicio de sesión. Para obtener más información, consulte Sesiones de autenticación.

Cómo inhabilitar el acceso de usuarios de IAM Identity Center

1. Abra la consola de IAM Identity Center.

   > **Important**
   >
   > Las instrucciones de esta página se aplican a AWS IAM Identity Center. No se aplican a AWS Identity and Access Management (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo deshabilitar en IAM, consulte Administrar usuarios de IAM en la Guía del usuario de AWS Identity and Access Management .

2. Seleccione Usuarios.
3. Seleccione el nombre de usuario del usuario cuyo acceso desee deshabilitar.
4. Debajo del nombre de usuario cuyo acceso desea deshabilitar, en la sección Información general, seleccione Desactivar el acceso de los usuarios.
5. En el cuadro de diálogo Desactivar el acceso de usuarios, seleccione Desactivar el acceso de usuarios.

Edición de propiedades del usuario

Siga el procedimiento a continuación para deshabilitar el acceso de los usuarios al directorio de Identity Center mediante la consola de IAM Identity Center. Como alternativa, puedes llamar a la operación de la AWS API UpdateUserpara actualizar las propiedades del usuario.

Cómo editar las propiedades de los usuarios de IAM Identity Center

1. Abra la consola de IAM Identity Center.
2. Seleccione Usuarios.
3. Elija el usuario que desee editar.
4. En la página Perfil, al lado de Detalles del perfil seleccione Editar.
5. En la página Editar detalles del perfil, actualice las propiedades que corresponda. A continuación, elija Save changes (Guardar cambios).

> **Note**
>
> (Opcional) Puede modificar atributos adicionales como el número de empleado y la ID inmutable de Office 365 para ayudar a asignar la identidad del usuario en IAM Identity Center a determinadas aplicaciones empresariales que los usuarios necesiten utilizar.

> **Note**
>
> El atributo Correo electrónico es un campo editable y el valor que proporcione debe ser único.

Restablecimiento de la contraseña de usuario de IAM Identity Center para un usuario final

Este procedimiento es para los administradores que necesitan restablecer la contraseña de un usuario del directorio de IAM Identity Center. Utilizará la consola de IAM Identity Center para restablecer las contraseñas.

Consideraciones sobre los proveedores de identidad y los tipos de usuario

- Microsoft Active Directory o un proveedor externo: si va a conectar IAM Identity Center a Microsoft Active Directory o a un proveedor externo, las contraseñas de usuario se deben restablecer desde Active Directory o desde el proveedor externo. Esto significa que las contraseñas de esos usuarios no se pueden restablecer desde la consola de IAM Identity Center.
- Usuarios del directorio de IAM Identity Center: si es usuario de IAM Identity Center, puede restablecer su propia contraseña de IAM Identity Center. Para ello, consulte Restablecimiento de la contraseña de usuario en IAM Identity Center.

Cómo restablecer la contraseña de un usuario final de IAM Identity Center

> **Important**
>
> Las instrucciones de esta página se aplican a AWS IAM Identity Center. No se aplican a AWS Identity and Access Management (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo cambiar contraseñas para usuarios de IAM, consulte Administración de contraseñas para usuarios de IAM en la Guía del usuario de AWS Identity and Access Management .

1. Abra la consola de IAM Identity Center.
2. Seleccione Usuarios.
3. Elija el nombre del usuario cuya contraseña desea restablecer.
4. En la página de detalles del usuario, vaya a la pestaña Restablecer contraseña.
5. En el cuadro de diálogo Restablecer contraseña, seleccione una de las siguientes opciones y después elija Restablecer contraseña:

    a. Enviar un correo electrónico al usuario con instrucciones para restablecer la contraseña: esta opción envía automáticamente al usuario una dirección de correo electrónico de Amazon Web Services que le explica cómo restablecer su contraseña.

    > **Warning**
    >
    > Como práctica recomendada de seguridad, compruebe que la dirección de correo electrónico de este usuario sea correcta antes de seleccionar esta opción. Si este

correo electrónico de restablecimiento de contraseña se enviara a una dirección de correo electrónico incorrecta o mal configurada, un destinatario malintencionado podría usarlo para obtener acceso no autorizado a su AWS entorno.

b. Generar una contraseña de un solo uso y compartirla con el usuario: esta opción le proporcionará los detalles de la contraseña que puede enviar manualmente al usuario desde su dirección de correo electrónico.

Envío de un correo electrónico OTP para los usuarios creados desde la API

Al crear usuarios con la operación de CreateUserAPI, estos no tienen contraseñas. Para cambiarlo, elija enviar a los usuarios una contraseña de un solo uso (OTP) por correo electrónico cuando se creen con la API. Los usuarios reciben la OTP por correo electrónico cuando intentan iniciar sesión por primera vez. Cuando un usuario inicia sesión tras recibir el correo con la OTP, debe establecer una nueva contraseña. Si no habilita esta configuración, debe generar y compartir la OTP con los usuarios que cree mediante la API CreateUser.

Cómo enviar correos electrónicos (OTP) a los usuarios creados con la API CreateUser

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación estándar, seleccione Configurar.
5. Aparecerá un cuadro de diálogo. Marque la casilla situada junto a Enviar OTP mediante correo electrónico. A continuación, elija Guardar. El estado pasa de Deshabilitado a Habilitado.

Requisitos de contraseñas para administrar identidades en IAM Identity Center

Note

Estos requisitos se aplican únicamente a los usuarios creados en el directorio de Identity Center. Si ha configurado una fuente de identidad distinta del Centro de Identidad de IAM para la autenticación, como Active Directoryun proveedor de identidad externo, las políticas de contraseñas de sus usuarios se definen y aplican en esos sistemas, no en el Centro de Identidad de IAM. Si su fuente de identidad es AWS Managed Microsoft AD, consulte

Administrar las políticas de contraseñas AWS Managed Microsoft AD para obtener más información.

Al utilizar IAM Identity Center como fuente de identidad, los usuarios deben cumplir los siguientes requisitos de contraseña para establecer o cambiar su contraseña:

- Las contraseñas distinguen entre mayúsculas y minúsculas.
- Las contraseñas deben tener una longitud de entre 8 y 64 caracteres.
- También deben contener al menos un carácter de cada una de las siguientes cuatro categorías:
  - Letras minúsculas (a-z)
  - Letras mayúsculas (A-Z)
  - Números (0-9)
  - Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)
- Las tres últimas contraseñas no se pueden volver a utilizar.
- No se pueden usar contraseñas que se conozcan públicamente a través de un conjunto de datos que haya obtenido cualquier tercero mediante una filtración de datos.

Conexión un directorio Microsoft AD

Con AWS IAM Identity Center, puede conectar un directorio autoadministrado en Active Directory (AD) o un directorio AWS Managed Microsoft AD mediante. AWS Directory ServiceEste directorio de Microsoft AD define el grupo de identidades que los administradores pueden extraer al utilizar la consola de IAM Identity Center para asignar el acceso de inicio de sesión único. Tras conectar el directorio corporativo al Centro de identidades de IAM, puede conceder a sus usuarios o grupos de AD acceso a las aplicaciones o a Cuentas de AWSambas opciones.

AWS Directory Service le ayuda a configurar y ejecutar un AWS Managed Microsoft AD directorio independiente alojado en la AWS nube. También puede usarlo AWS Directory Service para conectar sus AWS recursos con un AD autogestionado existente. Para configurarlo AWS Directory Service para que funcione con su AD autogestionado, primero debe configurar relaciones de confianza para extender la autenticación a la nube.

El centro de identidad de IAM utiliza la conexión proporcionada por AWS Directory Service para realizar la autenticación de transferencia a la instancia de AD de origen. Si la utilizas AWS Managed Microsoft AD como fuente de identidad, el Centro de Identidad de IAM puede funcionar con usuarios

de AWS Managed Microsoft AD cualquier dominio conectado a través de un fideicomiso de AD. Si desea ubicar a sus usuarios en 4 o más dominios, los usuarios deben usar la sintaxis de `DOMAIN \user` como nombre de usuario al iniciar sesión en IAM Identity Center.

> **Notas**
>
> - Como paso previo, asegúrese de que su AD Connector o directorio en AWS Managed Microsoft AD in AWS Directory Service reside en su cuenta AWS Organizations de administración. Para obtener más información, consulte Confirme sus fuentes de identidad en el Centro de identidades de IAM.
> - IAM Identity Center no admite Simple AD basado en SAMBA 4 como directorio conectado.

Consideraciones sobre el uso de Active Directory

Si quiere utilizar Active Directory como origen de identidad, la configuración debe cumplir los siguientes requisitos previos:

- Si lo está utilizando AWS Managed Microsoft AD, debe habilitar el Centro de identidad de IAM en el mismo Región de AWS lugar donde está configurado su AWS Managed Microsoft AD directorio. IAM Identity Center almacena los datos de asignación en la misma región que el directorio. Para administrar IAM Identity Center, es posible que deba cambiarse a la región en la que está configurado IAM Identity Center. Además, tenga en cuenta que el portal de AWS acceso utiliza la misma URL de acceso que su directorio.
- Utilice un Active Directory que resida en la cuenta de administración:

  Debe tener un AD Connector o AWS Managed Microsoft AD directorio existente configurado y debe residir en AWS Directory Servicesu cuenta AWS Organizations de administración. Solo puede conectar un directorio AD Connector o un directorio AWS Managed Microsoft AD a la vez. Si necesita admitir varios dominios o bosques, utilice AWS Managed Microsoft AD. Para obtener más información, consulte:

  - Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM
  - Conexión de un directorio autoadministrado de Active Directory a IAM Identity Center
- Utilice un Active Directory que resida en la cuenta de administrador delegada:

  Si planea habilitar la administración delegada del IAM Identity Center y usar Active Directory como fuente de identidad del IAM Identity Center, puede usar un AD Connector existente o un

AWS Managed Microsoft AD directorio configurado en AWS Directory que resida en la cuenta de administrador delegado.

Si decide cambiar la fuente de identidad de IAM Identity Center de cualquier otra fuente a Active Directory o cambiarla de Active Directory a cualquier otra fuente, el directorio debe residir (ser propiedad de) la cuenta de miembro administrador delegado de IAM Identity Center si existe; de lo contrario, debe estar en la cuenta de administración.

Conexión de Active Directory y especificación de un usuario

Si ya utiliza Active Directory, los siguientes temas lo ayudarán a prepararse para conectar su directorio a IAM Identity Center.

Puede conectar un AWS Managed Microsoft AD directorio o un directorio autogestionado en Active Directory con IAM Identity Center. Si planea conectar un AWS Managed Microsoft AD directorio o un directorio autoadministrado en Active Directory, asegúrese de que la configuración de Active Directory cumpla los requisitos previos de. Confirme sus fuentes de identidad en el Centro de identidades de IAM

> **Note**
>
> Como práctica recomendada de seguridad, le recomendamos que habilite la autenticación multifactor. Si planea conectar un AWS Managed Microsoft AD directorio o un directorio autogestionado en Active Directory y no va a utilizar RADIUS MFA AWS Directory Servicecon, active la MFA en IAM Identity Center.

AWS Managed Microsoft AD

1. Revise la guía en Conexión un directorio Microsoft AD.
2. Siga los pasos de Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM.
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en IAM Identity Center. Para obtener más información, consulte Sincronice un usuario administrativo en el IAM Identity Center.

Directorio autogestionado en Active Directory

1. Revise la guía en Conexión un directorio Microsoft AD.
2. Siga los pasos de Conexión de un directorio autoadministrado de Active Directory a IAM Identity Center.
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en IAM Identity Center. Para obtener más información, consulte Sincronice un usuario administrativo en el IAM Identity Center.

IdP externo

1. Revise la guía en Conexión a un proveedor de identidades externo.
2. Siga los pasos de Cómo conectarse a un proveedor de identidades externo.
3. Configure su IdP para aprovisionar usuarios al IAM Identity Center.

> **Note**
>
> Antes de configurar el aprovisionamiento automático y basado en grupos de todas las identidades de sus empleados desde su IdP al IAM Identity Center, le recomendamos que sincronice el único usuario al que quiere conceder permisos administrativos en IAM Identity Center.

Sincronice un usuario administrativo en el IAM Identity Center

Tras conectar el directorio al IAM Identity Center, puede especificar el usuario al que quiere conceder permisos administrativos y, a continuación, sincronizar ese usuario del directorio con el IAM Identity Center.

1. Abra la Consola del IAM Identity Center.
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de Administrar sincronización, elija la pestaña Usuarios y, continuación, seleccione Añadir usuarios y grupos.
5. En la pestaña Usuarios, en Usuario, introduzca el nombre de usuario exacto y seleccione Añadir.
6. En Usuarios y grupos añadidos, haga lo siguiente:

   a. Confirme que se ha especificado el usuario a quien desea conceder permisos administrativos.
   b. Seleccione la casilla de verificación que hay junto al nombre del archivo.
   c. Elija Enviar
7. En la página Administrar sincronización, el usuario que especificó aparece en la lista de Ámbito de usuarios sincronizados.
8. En el panel de navegación, seleccione Usuarios.
9. En la página Usuarios, es posible que el usuario que especificó tarde algún tiempo en aparecer en la lista. Seleccione el icono de actualización para actualizar la lista de usuarios.

En este momento, el usuario no tiene acceso a la cuenta de administración. Para configurar el acceso administrativo a esta cuenta, debe crear un conjunto de permisos administrativos y asignar el usuario a ese conjunto de permisos. Para obtener más información, consulte Crea un conjunto de permisos..

Aprovisionamiento cuando los usuarios provienen de Active Directory

El Centro de identidad de IAM utiliza la conexión proporcionada por el AWS Directory Service para sincronizar la información de usuarios, grupos y miembros del directorio de origen de Active Directory con el almacén de identidades del Centro de identidades de IAM. La información de la contraseña no se sincroniza con IAM Identity Center, ya que la autenticación de los usuarios se realiza directamente desde el directorio de origen de Active Directory. Las aplicaciones utilizan estos datos de identidad para facilitar los escenarios de búsqueda, autorización y colaboración dentro de la aplicación sin devolver la actividad de LDAP al directorio de origen de Active Directory.

Para obtener más información sobre aprovisionamiento, consulte Aprovisionamiento de usuarios y grupos.

Temas

- Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM
- Conexión de un directorio autoadministrado de Active Directory a IAM Identity Center
- Asignaciones de atributos para el directorio AWS Managed Microsoft AD
- Aprovisionamiento de usuarios y grupos desde Active Directory

Conectar un directorio AWS Managed Microsoft AD al centro de identidad de IAM

Utilice el siguiente procedimiento para conectar un directorio gestionado por AWS Directory Service el AWS Managed Microsoft AD Centro de Identidad de IAM.

Para conectarse AWS Managed Microsoft AD al Centro de Identidad de IAM

1. Abra la consola de IAM Identity Center

> **Note**
>
> Antes de continuar con el paso siguiente, compruebe que la consola de IAM Identity Center utiliza alguna de las regiones donde se encuentra su directorio de AWS Managed Microsoft AD .

2. Elija Configuración.
3. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, Cambiar fuente de identidad.
4. En Elegir origen de identidad, seleccione Active Directory y, a continuación, seleccione Siguiente.
5. En Conectar Active Directory, elija un directorio AWS Managed Microsoft AD de la lista y, a continuación, Siguiente.
6. En Confirmar el cambio, revise la información; cuando esté todo listo, escriba ACEPTAR y, a continuación, elija Cambiar fuente de identidad.

> **Important**
>
> Para especificar un usuario de Active Directory como usuario administrativo en IAM Identity Center, primero debe sincronizar el usuario al que desea conceder permisos administrativos desde Active Directory con IAM Identity Center. Para ello, siga los pasos que se indican en Sincronice un usuario administrativo en el IAM Identity Center.

Conexión de un directorio autoadministrado de Active Directory a IAM Identity Center

Los usuarios del directorio autogestionado de Active Directory (AD) también pueden tener acceso mediante un inicio de sesión único Cuentas de AWS y a las aplicaciones del portal de acceso. AWS

Para configurar el acceso de inicio de sesión único para estos usuarios, puede realizar una de las siguientes acciones:

- Cree una relación de confianza bidireccional: cuando se crean relaciones de confianza bidireccionales entre un directorio autogestionado de AD AWS Managed Microsoft AD y un directorio autogestionado de AD, los usuarios del directorio autogestionado de AD pueden iniciar sesión con sus credenciales corporativas en diversos servicios y aplicaciones empresariales. AWS Las relaciones de confianza unidireccionales no funcionan con IAM Identity Center.

  AWS IAM Identity Center requiere una confianza bidireccional para tener permisos para leer la información de usuarios y grupos de tu dominio a fin de sincronizar los metadatos de usuarios y grupos. IAM Identity Center utiliza estos metadatos al asignar el acceso a conjuntos de permisos o aplicaciones. Las aplicaciones también utilizan los metadatos de usuarios y grupos para colaborar como, por ejemplo, cuando se comparte un panel con otro usuario o grupo. La confianza AWS Directory Service de Microsoft Active Directory en su dominio permite que IAM Identity Center confíe en su dominio para la autenticación. La confianza en la dirección opuesta otorga AWS permisos para leer los metadatos de los usuarios y grupos.

  Para obtener más información acerca de la configuración de una relación de confianza bidireccional, consulte Cuándo crear una relación de confianza en la Guía de administración deAWS Directory Service .

- Crear un conector AD: Un conector AD es una puerta de enlace de directorio que puede redirigir solicitudes del directorio al Active Directory autoadministrado sin almacenar en caché la información que hay en la nube. Para obtener más información, consulte Conectarse a un directorio en la Guía de administración deAWS Directory Service .

> **Note**
>
> Si va a conectar IAM Identity Center a un directorio de un conector AD, cualquier restablecimiento de contraseñas de usuario en el futuro deberá realizarse desde AD. Esto significa que los usuarios no podrán restablecer sus contraseñas desde el portal de AWS acceso.
> Si utiliza un conector AD para conectar el servicio de dominio de Active Directory al IAM Identity Center, IAM Identity Center solo tiene acceso a los usuarios y grupos del dominio único al que se conecta el conector AD. Si necesita admitir varios dominios o bosques, utilice AWS Directory Service para Microsoft Active Directory.

> **Note**
>
> IAM Identity Center no funciona con los directorios Simple AD basados en SAMBA 4.

Asignaciones de atributos para el directorio AWS Managed Microsoft AD

Las asignaciones de atributos se utilizan para mapear los tipos de atributos que existen en el Centro de Identidad de IAM con atributos similares en un directorio. AWS Managed Microsoft AD IAM Identity Center recupera los atributos de usuario del directorio de Microsoft AD y los asigna a los atributos de usuario de IAM Identity Center. Estas asignaciones de atributos de usuario de IAM Identity Center también se utilizan para generar aserciones de SAML 2.0 para las aplicaciones. Cada aplicación determina la lista de atributos de SAML 2.0 que necesita para un inicio de sesión único correcto.

IAM Identity Center rellena previamente un conjunto de atributos en la pestaña Asignaciones de atributos de la página de configuración de la aplicación. IAM Identity Center utiliza estos atributos de usuario para rellenar las aserciones de SAML (como atributos de SAML) que se envían a la aplicación. A su vez, estos atributos de usuario se obtienen del directorio de Microsoft AD. Para obtener más información, consulte Asignación de atributos de su aplicación con atributos de IAM Identity Center.

IAM Identity Center también administra un conjunto de atributos en la sección Mapeos de atributos de la página de configuración del directorio. Para obtener más información, consulte Asigne los atributos del Centro de identidades de IAM a los atributos de su directorio AWS Managed Microsoft AD.

Atributos de directorio admitidos

En la siguiente tabla se enumeran todos los atributos de AWS Managed Microsoft AD directorio que se admiten y que se pueden asignar a los atributos de usuario en el Centro de identidades de IAM.

Atributos admitidos en el directorio de Microsoft AD
`${dir:email}`
`${dir:displayname}`

Atributos admitidos en el directorio de Microsoft AD
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`
`${dir:lastname}`
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

Puede especificar cualquier combinación de atributos del directorio de Microsoft AD compatibles para asignarlos a un único atributo de IAM Identity Center. Por ejemplo, puede elegir el atributo `subject` en la columna Atributo de usuario en IAM Identity Center. A continuación, asígnelo a `${dir:displayname}` o `${dir:lastname}${dir:firstname }`, a uno de los atributos admitidos o a una combinación arbitraria de atributos admitidos. Para obtener una lista de las asignaciones predeterminadas de los atributos de usuario en IAM Identity Center, consulte Asignaciones predeterminadas.

Warning

Algunos atributos de IAM Identity Center no se pueden modificar porque son inmutables y se asignan de forma predeterminada a atributos de directorio específicos de Microsoft AD. Por ejemplo, el «nombre de usuario» es un atributo obligatorio en el Centro de identidades de IAM. Si asigna «nombre de usuario» a un atributo del directorio de AD con un valor vacío, el Centro de Identidad de IAM considerará el `windowsUpn` valor como el valor predeterminado de «nombre de usuario». Si desea cambiar la asignación de atributos de «nombre de usuario» de la asignación actual, confirme que los flujos del Centro de Identidad de IAM que

dependen del «nombre de usuario» sigan funcionando según lo previsto antes de realizar el cambio.

Si utiliza las acciones de la ListGroupsAPI ListUserso los comandos list-usersy list-groups AWS CLI para asignar a los usuarios y grupos acceso a Cuentas de AWS y a las aplicaciones, debe especificar el valor de `AttributeValue` como FQDN. Este valor debe tener el siguiente formato: usuario@ejemplo.com. En el siguiente ejemplo, `AttributeValue` se configura como `janedoe@example.com`.

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

Atributos de IAM Identity Center compatibles

En la siguiente tabla se enumeran todos los atributos del Centro de Identidad de IAM que se admiten y que se pueden asignar a los atributos de usuario de su directorio. AWS Managed Microsoft AD Posteriormente, cuando configure las asignaciones de los atributos de la aplicación podrá usar estos mismos atributos de IAM Identity Center para asignarlos con los atributos reales utilizados por dicha aplicación.

Atributos compatibles en IAM Identity Center
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

Atributos de proveedores de identidad externos compatibles

En la siguiente tabla se enumeran todos los atributos del proveedor de identidades (IdP) externo que se admiten y que se pueden asignar a los atributos que se pueden utilizar al configurar Atributos para controlar el acceso en IAM Identity Center. Al usar aserciones de SAML, puede usar cualquier atributo que admita su IdP.

Atributos compatibles en su IdP
`${path:userName}`
`${path:name.familyName}`
`${path:name.givenName}`
`${path:displayName}`
`${path:nickName}`
`${path:emails[primary eq true].value}`
`${path:addresses[type eq "work"].streetAddress}`
`${path:addresses[type eq "work"].locality}`
`${path:addresses[type eq "work"].region}`
`${path:addresses[type eq "work"].postalCode}`
`${path:addresses[type eq "work"].country}`
`${path:addresses[type eq "work"].formatted}`
`${path:phoneNumbers[type eq "work"].value}`
`${path:userType}`
`${path:title}`
`${path:locale}`

Atributos compatibles en su IdP
`${path:timezone}`
`${path:enterprise.employeeNumber}`
`${path:enterprise.costCenter}`
`${path:enterprise.organization}`
`${path:enterprise.division}`
`${path:enterprise.department}`
`${path:enterprise.manager.value}`

Asignaciones predeterminadas

En la siguiente tabla se enumeran las asignaciones predeterminadas de los atributos de usuario del Centro de Identidad de IAM a los atributos de usuario de su directorio. AWS Managed Microsoft AD IAM Identity Center solo admite la lista de atributos de la columna Atributo de usuario en IAM Identity Center.

> **Note**
>
> Si no tiene ninguna asignación para sus usuarios y grupos en IAM Identity Center cuando habilite la sincronización de AD configurable, se utilizan las asignaciones predeterminadas de la siguiente tabla. Para obtener información acerca de cómo personalizar estas asignaciones, consulte Configuración de las asignaciones de atributos para su sincronización.

Atributo de usuario en IAM Identity Center	Se asigna a este atributo en el directorio de Microsoft AD
`AD_GUID`	`${dir:guid}`
`email` *	`${dir:windowsUpn}`
`familyName`	`${dir:lastname}`

Atributo de usuario en IAM Identity Center	Se asigna a este atributo en el directorio de Microsoft AD
`givenName`	`${dir:firstname}`
`middleName`	`${dir:initials}`
`name`	`${dir:displayname}`
`preferredUsername`	`${dir:displayname}`
`subject`	`${dir:windowsUpn}`

* El atributo de correo electrónico de IAM Identity Center debe ser único en el directorio. De lo contrario, el proceso de inicio de sesión en JIT podría fallar.

Puede cambiar las asignaciones predeterminadas o agregar más atributos a la aserción de SAML 2.0 en función de sus requisitos. Por ejemplo, supongamos que su aplicación requiere el correo electrónico del usuario en el atributo `User.Email` de SAML 2.0. Además, suponga que las direcciones de correo electrónico se almacenan en el atributo de `windowsUpn` del directorio de Microsoft AD. Para lograr llevar a cabo esta asignación, es necesario que realice cambios en los siguientes dos lugares en la consola de IAM Identity Center:

1. En la página Directory (Directorio), en la sección Attribute mappings (Asignaciones de atributos), debería asignar el atributo de usuario **`email`** al atributo **`${dir:windowsUpn}`** (en la columna Maps to this attribute in your directory [Se asigna a este atributo en su directorio]).
2. En la página Aplicaciones, elija la aplicación de la tabla. Elija la pestaña Asignación de atributos. A continuación, asigne el atributo de `User.Email` al atributo **`${user:email}`** (en la columna Asignar a este valor de cadena o atributo de usuario en IAM Identity Center).

Tenga en cuenta que debe proporcionar cada atributo de directorio siguiendo el formato ${dir:**`AttributeName`**}. Por ejemplo, el atributo `firstname` en su directorio de Microsoft AD pasará a ser `${dir:firstname}`. Es importante que cada atributo de directorio tenga asignado un valor real. Los atributos que no tengan un valor detrás de `${dir:` causarán problemas de inicio de sesión del usuario.

Asigne los atributos del Centro de identidades de IAM a los atributos de su directorio AWS Managed Microsoft AD

Puede utilizar el siguiente procedimiento para especificar cómo deben asignarse sus atributos de usuario de IAM Identity Center con los atributos correspondientes de su directorio de Microsoft AD.

Cómo asignar atributos de IAM Identity Center a atributos de su directorio

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Atributos para el control de acceso y, a continuación, elija Administrar atributos.
4. En la página Gestionar asignaciones de atributos para el control de acceso, busque el atributo en IAM Identity Center que desea asignar y, a continuación, escriba un valor en el cuadro de texto. Por ejemplo, es posible que desee asignar el atributo de usuario **`email`** de IAM Identity Center al atributo del directorio de Microsoft AD **`${dir:windowsUpn}`**.
5. Elija Guardar cambios.

Aprovisionamiento de usuarios y grupos desde Active Directory

IAM Identity Center ofrece las dos formas siguientes de aprovisionar usuarios y grupos desde Active Directory.

- Sincronización de Active Directory (AD) configurable con IAM Identity Center (recomendada): con este método de sincronización, puede hacer lo siguiente.
  - Controle los límites de los datos definiendo explícitamente los usuarios y grupos de Microsoft Active Directory que se sincronizan automáticamente en IAM Identity Center. Puede añadir usuarios y grupos o eliminar usuarios y grupos para cambiar el alcance de la sincronización en cualquier momento.
  - Asigne a los usuarios y grupos sincronizados acceso mediante inicio de sesión único a Cuentas de AWS o acceso a las aplicaciones. Las aplicaciones pueden ser aplicaciones AWS administradas o aplicaciones administradas por el cliente.
  - Controle el proceso de sincronización pausando y reanudando la sincronización según sea necesario. Esto le ayuda a regular la carga de los sistemas de producción.
- Sincronización con IAM Identity Center AD: con este método de sincronización, se utiliza IAM Identity Center para asignar a los usuarios y grupos de Active Directory el acceso a las

cuentas y a las aplicaciones de AWS . Todas las identidades con asignaciones se sincronizan automáticamente en IAM Identity Center.

IAM Identity Center y sincronización de AD configurable

La sincronización con Active Directory (AD) configurable de IAM Identity Center le permite configurar de forma explícita las identidades de Microsoft Active Directory que se sincronizan automáticamente en IAM Identity Center y controlar el proceso de sincronización.

En los temas siguientes, se proporciona información que le permitirá configurar y administrar la sincronización configurable de AD.

Temas

Requisitos y consideraciones previos

Antes de utilizar la sincronización de AD configurable, tenga en cuenta los siguientes requisitos y consideraciones:

- Especificación de usuarios y grupos de Active Directory para la sincronización

  Antes de poder utilizar el Centro de identidades de IAM para asignar a nuevos usuarios y grupos el acceso a Cuentas de AWS las aplicaciones AWS gestionadas o gestionadas por los clientes, debe especificar los usuarios y grupos de Active Directory que desee sincronizar y, a continuación, sincronizarlos con el Centro de identidades de IAM.

  - Sincronización de AD: cuando realiza asignaciones para nuevos usuarios y grupos mediante la consola de IAM Identity Center o acciones de la API de asignación relacionadas, IAM Identity Center busca directamente en el controlador de dominio los usuarios o grupos especificados, completa la asignación y, a continuación, sincroniza periódicamente los metadatos del usuario o grupo en IAM Identity Center.
  - Sincronización de AD configurable: IAM Identity Center no busca usuarios y grupos directamente en el controlador de dominio. En su lugar, primero debe especificar la lista de usuarios y grupos que desea sincronizar. Puede configurar esta lista, también conocida como ámbito de sincronización, de una de las siguientes maneras, en función de si tiene usuarios y grupos que

ya están sincronizados en IAM Identity Center o si tiene nuevos usuarios y grupos que vaya a sincronizar por primera vez mediante la sincronización configurable de AD.

- Usuarios y grupos existentes: si tiene usuarios y grupos que ya están sincronizados en IAM Identity Center, el ámbito de sincronización de la sincronización configurable de AD se rellena previamente con una lista de esos usuarios y grupos. Para asignar nuevos usuarios o grupos, debe añadirlos específicamente al ámbito de sincronización. Para obtener más información, consulte Añadir usuarios y grupos a su ámbito de sincronización.
- Nuevos usuarios y grupos: si quiere asignar a nuevos usuarios y grupos el acceso a las aplicaciones y Cuentas de AWS , debe especificar qué usuarios y grupos quiere añadir al ámbito de sincronización en la sincronización configurable de AD antes de poder utilizar IAM Identity Center para realizar la asignación. Para obtener más información, consulte Añadir usuarios y grupos a su ámbito de sincronización.

- Asignaciones a grupos anidados en Active Directory

  Los grupos que son miembros de otros grupos se denominan grupos anidados (o grupos secundarios). Al realizar asignaciones a un grupo de Active Directory que contiene grupos anidados, la forma en que se aplican las asignaciones depende de si utiliza la sincronización de AD o la sincronización de AD configurable.

  - Sincronización con AD: al realizar asignaciones a un grupo de Active Directory que contiene grupos anidados, solo los miembros directos del grupo pueden acceder a la cuenta. Por ejemplo, si asigna el acceso al grupo A y el grupo B es miembro del grupo A, solo los miembros directos del grupo A pueden acceder a la cuenta. Ningún miembro del grupo B hereda el acceso.
  - Sincronización de AD configurable: el uso de la sincronización de AD configurable para realizar asignaciones a un grupo de Active Directory que contiene grupos anidados puede aumentar el número de usuarios que tienen acceso a las aplicaciones Cuentas de AWS o a ellas. En este caso, la asignación se aplica a todos los usuarios, incluidos los de grupos anidados. Por ejemplo, si asigna el acceso al grupo A y el grupo B es miembro del grupo A, los miembros del grupo B también consiguen el acceso.
- Actualización de los flujos de trabajo automatizados

  Si tiene flujos de trabajo automatizados que utilizan las acciones de la API del almacén de identidades de IAM Identity Center y las acciones de la API de asignación de IAM Identity Center para asignar a los nuevos usuarios y grupos el acceso a las cuentas y a las aplicaciones y sincronizarlos en IAM Identity Center, debe ajustar esos flujos de trabajo antes del 15 de

abril de 2022 para que funcionen según lo previsto con la sincronización AD configurable. La sincronización de AD configurable cambia el orden en que se realizan la asignación y el aprovisionamiento de usuarios y grupos, así como la forma en que se realizan las consultas.

- Sincronización de AD: el proceso de las asignaciones se produce primero. Usted asigna a los usuarios y grupos el acceso a Cuentas de AWS y a las aplicaciones. Una vez asignado el acceso a los usuarios y grupos, se aprovisionan automáticamente (se sincronizan con IAM Identity Center). Si tiene un flujo de trabajo automatizado, esto significa que, al añadir un nuevo usuario a Active Directory, el flujo de trabajo automatizado puede consultar el usuario en Active Directory mediante la acción de la API de `ListUser` del almacén de identidades y, a continuación, asignar al usuario el acceso mediante las acciones de la API de asignación de IAM Identity Center. Como el usuario tiene una asignación, ese usuario se aprovisiona automáticamente en IAM Identity Center.
- Sincronización AD configurable: el aprovisionamiento se produce primero y no se realiza automáticamente. En su lugar, primero debe añadir usuarios y grupos de forma explícita al almacén de identidades, agregándolos a su ámbito de sincronización. Para obtener información sobre los pasos recomendados para automatizar la configuración de sincronización para una sincronización AD configurable, consulte Automatizar la configuración de sincronización para una sincronización AD configurable.

Cómo funciona la sincronización de AD configurable

IAM Identity Center actualiza los datos de identidad basados en anuncios en el almacén de identidades mediante el siguiente proceso.

Creación

Tras conectar el directorio autogestionado de Active Directory o el directorio gestionado por él AWS Directory Service al Centro de identidades de IAM, puede configurar de forma explícita los usuarios y grupos de Active Directory que desee sincronizar en el almacén de identidades del Centro de identidades de IAM. AWS Managed Microsoft AD Las identidades que elija se sincronizarán aproximadamente cada 3 horas en el almacén de identidades de IAM Identity Center. Según el tamaño del directorio, el proceso de sincronización puede tardar más.

Los grupos que son miembros de otros grupos (denominados grupos anidados o grupos secundarios) también se escriben en el almacén de identidades. Al realizar asignaciones a un grupo de Active Directory que contiene grupos anidados, la forma en que se aplican las asignaciones depende de si se utiliza la sincronización de AD o la sincronización de AD configurable. Para obtener más información, consulte Making assignments to nested groups in Active Directory.

Solo puede asignar el acceso a nuevos usuarios o grupos después de que estén sincronizados en el almacén de identidades de IAM Identity Center.

Actualización

Los datos de identidad del almacén de identidades de IAM Identity Center se mantienen actualizados al leer periódicamente los datos del directorio de origen de Active Directory. De forma predeterminada, IAM Identity Center sincroniza los datos de su Active Directory cada hora en un ciclo de sincronización. Los datos pueden tardar entre 30 minutos y 2 horas en sincronizarse con el Centro de identidades de IAM, según el tamaño de su Active Directory.

Los objetos de usuario y grupo que se encuentran en el ámbito de la sincronización y sus pertenencias se crean o actualizan en IAM Identity Center para asignarlos a los objetos correspondientes del directorio de origen de Active Directory. En el caso de los atributos de usuario, solo el subconjunto de atributos que aparece en la sección Atributos para controlar el acceso de la consola de IAM Identity Center se actualiza en IAM Identity Center. Las actualizaciones de atributos que realices en Active Directory pueden tardar un ciclo de sincronización en reflejarse en el Centro de identidades de IAM.

También puede actualizar el subconjunto de usuarios y grupos que sincroniza en el almacén de identidades de IAM Identity Center. Puede optar por añadir nuevos usuarios o grupos a este subconjunto o eliminarlos. Todas las identidades que añada se sincronizarán en la próxima sincronización programada. Las identidades que elimine del subconjunto dejarán de actualizarse en el almacén de identidades de IAM Identity Center. Los usuarios que no estén sincronizados durante más de 28 días quedarán inhabilitados en el almacén de identidades de IAM Identity Center. Los objetos de usuario correspondientes se deshabilitarán automáticamente en el almacén de identidades de IAM Identity Center durante el siguiente ciclo de sincronización, a menos que formen parte de otro grupo que siga formando parte del ámbito de sincronización.

Eliminación

Los usuarios y grupos se eliminan del almacén de identidades de IAM Identity Center cuando los objetos de usuario o grupo correspondientes se eliminan del directorio de origen de Active Directory. Como alternativa, puede eliminar de forma explícita los objetos de usuario del almacén de identidades de IAM Identity Center mediante la consola de IAM Identity Center. Si utiliza la consola de IAM Identity Center, también debe eliminar los usuarios del ámbito de sincronización para garantizar que no se vuelvan a sincronizar con IAM Identity Center durante el siguiente ciclo de sincronización.

También puede pausar y reiniciar la sincronización en cualquier momento. Si pausa la sincronización durante más de 28 días, se deshabilitarán todos los usuarios.

Configuración y administración del alcance de la sincronización

Puede configurar el ámbito de sincronización de cualquiera de las siguientes formas:

- Configuración guiada: si va a sincronizar sus usuarios y grupos de Active Directory con IAM Identity Center por primera vez, siga los pasos que se indican en Configuración guiada para configurar el ámbito de sincronización. Tras completar la configuración guiada, puede modificar el ámbito de sincronización en cualquier momento siguiendo los demás procedimientos de esta sección.
- Si ya tiene usuarios y grupos sincronizados en IAM Identity Center o si no desea seguir la configuración guiada, elija Administrar la sincronización. Omita el procedimiento de configuración guiada y siga los demás procedimientos de esta sección según sea necesario para configurar y gestionar el ámbito de la sincronización.

Procedimientos

- Configuración guiada
- Añadir usuarios y grupos a su ámbito de sincronización
- Eliminación de usuarios y grupos de su ámbito de sincronización
- Pausa y reanudación de la sincronización
- Configuración de las asignaciones de atributos para su sincronización
- Automatizar la configuración de sincronización para una sincronización AD configurable

Configuración guiada

1. Abra la consola de IAM Identity Center.

   > **Note**
   >
   > Asegúrese de que la consola del IAM Identity Center utilice una de las Regiones de AWS ubicaciones de su AWS Managed Microsoft AD directorio antes de continuar con el siguiente paso.

2. Elija Configuración.

3. En la parte superior de la página, en el mensaje de notificación, seleccione Iniciar configuración guiada.
4. En el paso 1 (opcional): configurar las asignaciones de atributos, revise las asignaciones de atributos de usuario y grupo predeterminadas. Si no es necesario realizar cambios, seleccione Siguiente. Si es necesario realizar cambios, realice los cambios y, a continuación, seleccione Guardar cambios.
5. En el paso 2 (opcional): configurar el alcance de la sincronización, seleccione la pestaña Usuarios. A continuación, introduzca el nombre de usuario exacto del usuario que quiere añadir a su ámbito de sincronización y seleccione Añadir. Seleccione la pestaña Grupos. A continuación, introduzca el nombre de grupo exacto del grupo que quiere añadir a su ámbito de sincronización y seleccione Añadir. A continuación, elija Siguiente. Si quiere añadir usuarios y grupos a su ámbito de sincronización más adelante, no realice ningún cambio y seleccione Siguiente.
6. En el paso 3: revisar y guardar la configuración, confirme las asignaciones de atributos en el paso 1: asignaciones de atributos y sus usuarios y grupos en el paso 2: ámbito de sincronización. Seleccione Guardar configuración. Esto le llevará a la página Administrar sincronización.

Añadir usuarios y grupos a su ámbito de sincronización

Para agregar usuarios

1. Abra la consola de IAM Identity Center.
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de Administrar sincronización, elija la pestaña Usuarios y, continuación, seleccione Añadir usuarios y grupos.
5. En la pestaña Usuarios, en Usuario, introduzca el nombre de usuario exacto y seleccione Añadir.
6. En Usuarios y grupos agregados, revise el usuario que desea agregar.
7. Elija Enviar.
8. En el panel de navegación, seleccione Usuarios.
9. En la página Usuarios, es posible que el usuario que especificó tarde algún tiempo en aparecer en la lista. Seleccione el icono de actualización para actualizar la lista de usuarios.

Cómo añadir grupos:

1. Abra la consola de IAM Identity Center.
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de administrar la sincronización, elija la pestaña Grupos y, continuación, seleccione Añadir usuarios y grupos.
5. Seleccione la pestaña Groups (Grupos). En Grupo, introduzca el nombre exacto del grupo y seleccione Añadir.
6. En Usuarios y grupos añadidos, revise el grupo que desea agregar.
7. Elija Enviar.
8. En el panel de navegación, elija Grupos.
9. En la página Grupos, es posible que el grupo que especificó tarde algún tiempo en aparecer en la lista. Seleccione el icono de actualización para actualizar la lista de grupos.

Eliminación de usuarios y grupos de su ámbito de sincronización

Para obtener más información sobre lo que ocurre cuando elimina usuarios y grupos del ámbito de sincronización, consulte Cómo funciona la sincronización de AD configurable.

Cómo eliminar usuarios:

1. Abra la consola de IAM Identity Center.
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. Elija la pestaña Users.
5. En Usuarios en el ámbito de sincronización, seleccione la casilla de verificación situada junto al usuario que desea eliminar. Para eliminar todos los usuarios, seleccione la casilla de verificación situada junto al nombre de usuario.
6. Elija Eliminar.

Cómo eliminar grupos:

1. Abra la consola de IAM Identity Center.
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. Seleccione la pestaña Groups (Grupos).
5. En Grupos en el ámbito de sincronización, seleccione la casilla de verificación situada junto al usuario que desea eliminar. Para eliminar todos los grupos, seleccione la casilla de verificación situada junto al nombre del grupo.
6. Elija Eliminar.

Pausa y reanudación de la sincronización

Al pausar la sincronización, se pausan todos los ciclos de sincronización futuros e impide que los cambios que realice en los usuarios y grupos de Active Directory se reflejen en IAM Identity Center. Tras reanudar la sincronización, el ciclo de sincronización recoge los cambios de la siguiente sincronización programada.

Cómo pausar la sincronización:

1. Abra la consola de IAM Identity Center.
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En Administrar la sincronización, seleccione Pausar la sincronización.

Cómo reanudar la sincronización:

1. Abra la consola de IAM Identity Center.
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En Administrar la sincronización, seleccione Reanudar la sincronización.

> **Note**
>
> Si aparece Pausar la sincronización en lugar de Reanudar la sincronización, significa que la sincronización de Active Directory con IAM Identity Center ya se ha reanudado.

Configuración de las asignaciones de atributos para su sincronización

Cómo obtener más información acerca de los atributos disponibles, consulte Asignaciones de atributos para el directorio AWS Managed Microsoft AD.

Cómo configurar las asignaciones de atributos de IAM Identity Center a su directorio:

1. Abra la consola de IAM Identity Center.
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En Administrar sincronización, seleccione Ver asignaciones de atributos.
5. En Atributos de usuario de Active Directory, configure los atributos del almacén de identidades de IAM Identity Center y los atributos de usuario de Active Directory. Por ejemplo, puede que desee asignar el atributo `email` del almacén de identidades de IAM Identity Center al atributo `${objectguid}` del directorio de usuarios de Active Directory.

   > **Note**
   >
   > En Atributos de grupo, no se pueden cambiar los atributos del almacén de identidades de IAM Identity Center ni los atributos de grupo de Active Directory.

6. Elija Guardar cambios. Esto le llevará a la página de Administrar sincronización.

Automatizar la configuración de sincronización para una sincronización AD configurable

Para garantizar que su flujo de trabajo automatizado funcione según lo esperado con la sincronización de AD configurable, le recomendamos que realice los siguientes pasos para automatizar la configuración de la sincronización.

Cómo automatizar la configuración de sincronización para una sincronización AD configurable:

1. En Active Directory, cree un Grupo de sincronización principal que contenga todos los usuarios y grupos que desee sincronizar en IAM Identity Center. Por ejemplo, puede asignar el nombre IdentityCenterAllUsersAndGroupsIAM al grupo.
2. En IAM Identity Center, añada el grupo de sincronización principal a su lista de sincronización configurable. IAM Identity Center sincronizará todos los usuarios, grupos, subgrupos y miembros de todos los grupos incluidos en el grupo de sincronización principal.
3. Use las acciones de la API de administración de usuarios y grupos de Active Directory proporcionadas por Microsoft para añadir o eliminar usuarios y grupos del grupo de sincronización principal.

Sincronización con IAM Identity Center AD

Con IAM Identity Center AD sync, puede utilizar el IAM Identity Center para asignar a los usuarios y grupos de Active Directory el acceso a las aplicaciones AWS gestionadas o gestionadas por el cliente Cuentas de AWS y a ellas. Todas las identidades con asignaciones se sincronizan automáticamente en IAM Identity Center.

Cómo funciona la sincronización de la API de IAM Identity Center

IAM Identity Center actualiza los datos de identidad basados en anuncios en el almacén de identidades mediante el siguiente proceso.

Creación

Al asignar usuarios o grupos o aplicaciones mediante la AWS consola Cuentas de AWS o las llamadas a la API de asignación, la información sobre los usuarios, los grupos y los miembros se sincroniza periódicamente en el almacén de identidades del IAM Identity Center. Los usuarios o grupos que se añaden a las asignaciones del Centro de Identidad de IAM suelen aparecer en el almacén de AWS identidades en un plazo de dos horas. En función de la cantidad de datos que se sincronicen, este proceso puede tardar más. Solo se sincronizan los usuarios y grupos a los que se les ha asignado acceso directamente o que son miembros de un grupo al que se le ha asignado acceso.

Los grupos que son miembros de otros grupos (llamados “grupos anidados”) también se escriben en el almacén de identidades. Al realizar asignaciones a un grupo de Active Directory que contiene grupos anidados, la forma en que se aplican las asignaciones depende de si utiliza la sincronización AD o la sincronización AD configurable.

- Sincronización con AD: al realizar asignaciones a un grupo de Active Directory que contiene grupos anidados, solo los miembros directos del grupo pueden acceder a la cuenta. Por ejemplo, si asigna el acceso al grupo A y el grupo B es miembro del grupo A, solo los miembros directos del grupo A pueden acceder a la cuenta. Ningún miembro del grupo B hereda el acceso.
- Sincronización de AD configurable: el uso de la sincronización de AD configurable para realizar asignaciones a un grupo de Active Directory que contiene grupos anidados puede aumentar el número de usuarios que tienen acceso a las aplicaciones Cuentas de AWS o a ellas. En este caso, la asignación se aplica a todos los usuarios, incluidos los de grupos anidados. Por ejemplo, si asigna el acceso al grupo A y el grupo B es miembro del grupo A, los miembros del grupo B también consiguen el acceso.

Si un usuario accede al Centro de identidades de IAM antes de sincronizar su objeto de usuario por primera vez, el objeto de almacén de identidades de ese usuario se crea bajo demanda mediante el aprovisionamiento just-in-time (JIT). Los usuarios creados mediante el aprovisionamiento de JIT no se sincronizan a menos que tengan derechos de IAM Identity Center asignados directamente o basados en grupos. La pertenencia a grupos para los usuarios aprovisionados por JIT no está disponible hasta después de la sincronización.

Para obtener instrucciones sobre cómo asignar el acceso a los usuarios, consulte. Cuentas de AWSAcceso mediante inicio de sesión único a Cuentas de AWS

Actualización

Los datos de identidad del almacén de identidades de IAM Identity Center se mantienen actualizados al leer periódicamente los datos del directorio de origen de Active Directory. Los datos de identidad que se modifican en Active Directory suelen aparecer en el almacén de AWS identidades en un plazo de cuatro horas. En función de la cantidad de datos que se sincronicen, este proceso puede tardar más.

Los objetos de usuario y grupo y sus pertenencias se crean o actualizan en IAM Identity Center para asignarlos a los objetos correspondientes del directorio de origen de Active Directory. En el caso de los atributos de usuario, solo el subconjunto de atributos que aparece en la sección Gestionar atributos para controlar el acceso de la consola de IAM Identity Center se actualiza en IAM Identity Center. Además, los atributos de usuario se actualizan con cada evento de autenticación de usuario.

Eliminación

Los usuarios y grupos se eliminan del almacén de identidades de IAM Identity Center cuando los objetos de usuario o grupo correspondientes se eliminan del directorio de origen de Active Directory.

Conexión a un proveedor de identidades externo

Si utiliza un directorio autoadministrado en Active Directory o un directorio AWS Managed Microsoft AD, consulteConexión un directorio Microsoft AD. Para otros proveedores de identidad externos (IdPs), puede utilizarlos AWS IAM Identity Center para autenticar identidades IdPs mediante el estándar del lenguaje de marcado de aserciones de seguridad (SAML) 2.0. Esto permite a los usuarios iniciar sesión en el portal de AWS acceso con sus credenciales corporativas. A continuación, pueden navegar hasta las cuentas, funciones y aplicaciones asignadas alojadas en un servidor externo IdPs.

Por ejemplo, puede conectar un IdP externo, como Okta o Microsoft Entra ID, a IAM Identity Center. A continuación, sus usuarios pueden iniciar sesión en el portal de AWS acceso con sus Microsoft Entra ID credenciales Okta o credenciales existentes. Para controlar lo que pueden hacer sus usuarios una vez que han iniciado sesión, puede asignarles permisos de acceso de forma centralizada en todas las cuentas y aplicaciones de su AWS organización. Además, los desarrolladores pueden simplemente iniciar sesión en AWS Command Line Interface (AWS CLI) con sus credenciales actuales y beneficiarse de la generación y rotación automáticas de credenciales a corto plazo.

El protocolo SAML no proporciona una forma de consultar al IdP para obtener información sobre los usuarios y los grupos. Por lo tanto, debe hacer que IAM Identity Center conozca a esos usuarios y grupos aprovisionándolos en IAM Identity Center.

Aprovisionamiento cuando los usuarios provienen de un IdP externo

Al utilizar un IdP externo, debe aprovisionar todos los usuarios y grupos aplicables en el Centro de Identidad de IAM antes de poder realizar cualquier asignación o aplicación. Cuentas de AWS Para ello, puede configurar el Aprovisionamiento estático para sus usuarios y grupos o bien utilizar el Aprovisionamiento manual. Independientemente de cómo aprovisione a los usuarios, IAM Identity Center redirige la AWS Management Console interfaz de línea de comandos y la autenticación de la aplicación a su IdP externo. A continuación, IAM Identity Center concede el acceso a esos recursos en función de las políticas que cree en IAM Identity Center. Para obtener más información sobre la capacidad aprovisionada, consulte Aprovisionamiento de usuarios y grupos.

Cómo conectarse a un proveedor de identidades externo

Hay step-by-step tutoriales disponibles para los compatibles: IdPs

- CyberArk

- Google Workspace
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping Identity

Existen diferentes requisitos previos, consideraciones y procedimientos de aprovisionamiento para los distintos dispositivos externos compatibles. IdPs En el siguiente procedimiento se proporciona una descripción general del procedimiento que se utiliza con todos los proveedores de identidades externos.

Cómo conectarse a un proveedor de identidades externo

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, Cambiar fuente de identidad.
4. En Elegir la fuente de identidad, seleccione Proveedor de identidades externo y, a continuación, Siguiente.
5. En Configurar un proveedor de identidad externo, haga lo siguiente:

    a. En Metadatos del proveedor de servicios, seleccione Descargar archivo de metadatos para descargar el archivo de metadatos y guardarlo en el sistema. El proveedor de identidades externo necesita el archivo de metadatos SAML de IAM Identity Center.

    b. En Metadatos del proveedor de identidad, elija Elegir archivo y busque el archivo de metadatos que descargó de su proveedor de identidades externo. A continuación, cargue el archivo. Este archivo de metadatos contiene el certificado x509 público necesario que se utiliza para confiar en los mensajes que se envían desde el IdP.

    c. Elija Siguiente.

> **Important**
>
> Al cambiar la fuente a o desde Active Directory, se eliminan todas las asignaciones de usuarios y grupos existentes. Debe volver a aplicar las asignaciones manualmente una vez que haya cambiado correctamente la fuente.

6. Cuando haya leído el aviso legal, introduzca ACCEPT para continuar.
7. Elija Cambiar fuente de identidad. Un mensaje de estado le informa de que ha cambiado correctamente el origen de identidad.

Temas

Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos

IAM Identity Center implementa los siguientes protocolos basados en estándares para la federación de identidades:

- SAML 2.0 para la autenticación de usuarios
- SCIM para el aprovisionamiento

Se espera que cualquier proveedor de identidades (IdP) que implemente estos protocolos estándar interactúe correctamente con IAM Identity Center, teniendo en cuenta las siguientes consideraciones especiales:

- SAML
  - IAM Identity Center requiere un formato de identificador de nombre SAML para la dirección de correo electrónico (es decir, `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`).
  - El valor del campo “nameID” en las aserciones debe ser una cadena de caracteres compatible con la norma RFC 2822 (https://tools.ietf.org/html/rfc2822) (“`name@domain.com`”) que cumpla con las especificaciones addr-spec (https://tools.ietf.org/html/rfc2822#section-3.4.1).

  - El archivo de metadatos no puede tener más de 75 000 caracteres.
  - Los metadatos deben contener un ID de entidad, un certificado X509 y formar parte de la URL de inicio de SingleSignOnService sesión.
  - No se admite el cifrado SSE-KMS.

- SCIM
  - La implementación del SCIM del IAM Identity Center se basa en los RFC 7642 (https://tools.ietf.org/html/rfc7642), 7643 (https://tools.ietf.org/html/rfc7643) y 7644 (https://tools.ietf.org/html/rfc7644) del SCIM, y en los requisitos de interoperabilidad establecidos en el borrador de marzo de 2020 del Perfil SCIM básico 1.0 (https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4). FastFed Las diferencias entre estos documentos y la implementación actual en IAM Identity Center se describen en la sección Operaciones de API compatibles de la Guía para desarrolladores de implementación del SCIM de IAM Identity Center.

IdPs no se admiten aquellos que no se ajusten a los estándares y consideraciones mencionados anteriormente. Póngase en contacto con su IdP si cualquier pregunta o necesita más información sobre la conformidad de sus productos con estas normas y consideraciones.

Si tiene problemas para conectar su IdP al IAM Identity Center, compruebe lo siguiente:

- AWS CloudTrail se registra filtrando por el nombre del evento ExternalIdP DirectoryLogin
- Registros específicos de IdP o registros de depuración
- Resolución de problemas de IAM Identity Center

> **Note**
>
> Algunos IdPs, como los delTutoriales de introducción, ofrecen una experiencia de configuración simplificada para el IAM Identity Center en forma de «aplicación» o «conector» creado específicamente para el IAM Identity Center. Si su IdP ofrece esta opción, le recomendamos que la utilice, teniendo cuidado al elegir el elemento creado específicamente para IAM Identity Center. Otros elementos denominados «AWS», «AWS federación» o nombres genéricos similares de ««AWS pueden utilizar otros enfoques de federación o puntos finales, y es posible que no funcionen como se esperaba con el IAM Identity Center.

Perfil SCIM e implementación de SAML 2.0

Tanto SCIM como SAML son consideraciones importantes a la hora de configurar IAM Identity Center.

Implementación de SAML 2.0

IAM Identity Center admite la federación de identidades con lenguaje de marcado para confirmaciones de seguridad SAML 2.0. Esto permite al IAM Identity Center autenticar las identidades de proveedores de identidad externos (). IdPs SAML 2.0 es un estándar abierto que se utiliza para intercambiar aserciones de SAML de forma segura. SAML 2.0 transfiere información sobre un usuario entre una autoridad de SAML (denominada proveedor de identidades o IdP) y un consumidor de SAML (denominado proveedor de servicios o SP). El servicio de IAM Identity Center utiliza esta información para proporcionar un inicio de sesión único federado. El inicio de sesión único permite a los usuarios acceder a las aplicaciones Cuentas de AWS y configurarlas en función de sus credenciales de proveedor de identidad existentes.

El Centro de identidad de IAM añade las capacidades de IdP de SAML a su almacén del Centro de identidades de IAM o a un proveedor AWS Managed Microsoft AD de identidad externo. A continuación, los usuarios pueden iniciar sesión de forma única en los servicios compatibles con SAML, incluidas las aplicaciones AWS Management Console y las de terceros, como, y. Microsoft 365 Concur Salesforce

El protocolo SAML no proporciona una forma de consultar al IdP para obtener información sobre los usuarios y los grupos. Por lo tanto, debe hacer que IAM Identity Center conozca a esos usuarios y grupos aprovisionándolos en IAM Identity Center.

Perfil SCIM

IAM Identity Center es compatible con el estándar Sistema de la administración de identidades entre dominios (SCIM) v2.0. El SCIM mantiene las identidades de su IAM Identity Center sincronizadas con las identidades de su IdP. Esto incluye cualquier aprovisionamiento, actualización y desaprovisionamiento de usuarios entre su IdP y IAM Identity Center.

Para obtener más información acerca de cómo implementar una capa personalizada, consulte Aprovisionamiento estático. Para obtener más información sobre la implementación del SCIM de IAM Identity Center, consulte la Guía para desarrolladores de implementación de IAM Identity Center SCIM.

Temas

- Aprovisionamiento estático
- Aprovisionamiento manual
- Administración de certificados SAML 2.0

Aprovisionamiento estático

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de usuarios y grupos de su proveedor de identidades (IdP) a IAM Identity Center mediante el protocolo Sistema de administración de identidades entre dominios (SCIM) v2.0. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario del proveedor de identidades (IdP) con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y su IdP. Esta conexión se configura en el IdP mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center.

Temas

- Consideraciones para utilizar el aprovisionamiento automático
- Cómo monitorizar la caducidad del token de acceso
- Cómo habilitar el aprovisionamiento automático
- Cómo habilitar el aprovisionamiento automático
- Cómo generar un nuevo token de acceso
- Cómo eliminar un token de acceso
- Cómo eliminar un token de acceso

Consideraciones para utilizar el aprovisionamiento automático

Antes de comenzar a implementar el SCIM, le recomendamos revisar primero las siguientes consideraciones importantes sobre su funcionamiento con IAM Identity Center. Para obtener información adicional sobre el aprovisionamiento, consulte la sección Tutoriales de introducción correspondiente a su IdP.

- Si va a aprovisionar una dirección de correo electrónico principal, el valor de este atributo debe ser único para cada usuario. En algunos casos IdPs, es posible que la dirección de correo electrónico principal no sea una dirección de correo electrónico real. Por ejemplo, puede ser un nombre principal universal (UPN) que solo se parece a un correo electrónico. Es IdPs posible que tengan una dirección de correo electrónico secundaria o «otra» que contenga la dirección de correo

electrónico real del usuario. Debe configurar SCIM en su IdP para asignar la dirección de correo electrónico única no nula al atributo de dirección de correo electrónico principal de IAM Identity Center. Además, debe asignar el identificador de inicio de sesión único no nulo del usuario al atributo de nombre de usuario de IAM Identity Center. Compruebe si su IdP tiene un valor único que sea tanto el identificador de inicio de sesión como el nombre de correo electrónico del usuario. Si es así, puede asignar ese campo de IdP al correo electrónico principal de IAM Identity Center y al nombre de usuario de IAM Identity Center.

- Para que la sincronización de SCIM funcione, cada usuario debe tener un nombre, apellidos, nombre de usuario y nombre para mostrar especificados. Si falta alguno de estos valores en un usuario, este no se aprovisionará.
- Si necesita utilizar aplicaciones de terceros, primero tendrá que asignar el atributo de asunto de SAML saliente al atributo de nombre de usuario. Si la aplicación de terceros necesita una dirección de correo electrónico enrutable, debe proporcionar el atributo de correo electrónico a su IdP.
- El proveedor de identidades controla los intervalos de aprovisionamiento y actualización de SCIM. Los cambios en los usuarios y grupos de su proveedor de identidades solo se reflejan en IAM Identity Center después de que su proveedor de identidades los envíe a IAM Identity Center. Consulte con su proveedor de identidades para obtener más información sobre la frecuencia de las actualizaciones de usuarios y grupos.
- Actualmente, SCIM no proporciona atributos con varios valores (como varios correos electrónicos o números de teléfono para un usuario determinado). Los intentos de sincronizar atributos con varios valores en IAM Identity Center con SCIM fallarán. Para evitar errores, asegúrese de que solo se pase un valor único para cada atributo. Si tiene usuarios con atributos de varios valores, elimine o modifique las asignaciones de atributos duplicadas en SCIM en su IdP para la conexión con IAM Identity Center.
- Compruebe que el mapeo SCIM de `externalId` en su IdP corresponde a un valor que sea único, que esté siempre presente y que tenga menos probabilidades de cambiar para sus usuarios. Por ejemplo, su IdP puede proporcionar un `objectId` garantizado u otro tipo de identificador que no se vea afectado por los cambios en los atributos del usuario, como el nombre y el correo electrónico. Si es así, puede asignar ese valor al campo `externalId` de SCIM. Esto garantiza que tus usuarios no pierdan sus AWS derechos, asignaciones o permisos si necesitas cambiarles el nombre o el correo electrónico.
- Usuarios que aún no se han asignado a una aplicación o que no se Cuenta de AWS pueden aprovisionar en el Centro de identidades de IAM. Para sincronizar usuarios y grupos, asegúrese de que estén asignados a la aplicación u otra configuración que represente la conexión de su IdP a IAM Identity Center.

- El comportamiento de desaprovisionamiento de los usuarios lo gestiona el proveedor de identidades y puede variar según su implementación. Consulta con tu proveedor de identidad para obtener más información sobre el desaprovisionamiento de usuarios.

Para obtener más información sobre la implementación de SCIM de IAM Identity Center, consulte la guía para desarrolladores de implementación de IAM Identity Center SCIM.

Cómo monitorizar la caducidad del token de acceso

Los tokens de acceso SCIM se generan con una validez de un año. Cuando tu token de acceso SCIM caduque en 90 días o menos, te AWS envía recordatorios a la consola del IAM Identity Center y a través del AWS Health panel de control para ayudarte a cambiar el token. Al rotar el token de acceso de SCIM antes de que caduque, asegura de forma continua el aprovisionamiento automático de la información de usuarios y grupos. Si el token de acceso SCIM caduca, se interrumpe la sincronización de la información de usuarios y grupos de su proveedor de identidades con IAM Identity Center, por lo que el aprovisionamiento automático ya no puede realizar actualizaciones ni crear y eliminar información. La interrupción del aprovisionamiento automático puede aumentar los riesgos de seguridad y afectar al acceso a sus servicios.

Los recordatorios de la consola de Identity Center persisten hasta que rote el token de acceso SCIM y elimine los tokens de acceso no utilizados o vencidos. Los eventos del AWS Health panel de control se renuevan semanalmente entre 90 y 60 días, dos veces por semana entre 60 y 30 días, tres veces por semana entre 30 y 15 días y todos los días desde 15 días hasta que caduquen los tokens de acceso del SCIM.

Cómo habilitar el aprovisionamiento automático

Siga el siguiente procedimiento para habilitar el aprovisionamiento automático de usuarios y grupos desde su IdP a IAM Identity Center mediante el protocolo SCIM.

> **Note**
>
> Antes de comenzar con este procedimiento, le recomendamos que revise primero las consideraciones de aprovisionamiento aplicables a su IdP. Para obtener más información, consulte la Tutoriales de introducción para su IdP.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie todos los valores de las opciones siguientes. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
    a. Punto de conexión de SCIM
    b. Token de acceso
5. Elija Close.

Después de completar este procedimiento, debe configurar el aprovisionamiento automático en su IdP. Para obtener más información, consulte la Tutoriales de introducción para su IdP.

Cómo habilitar el aprovisionamiento automático

Siga el siguiente procedimiento para desactivar el aprovisionamiento automático en la consola de IAM Identity Center.

> **Important**
>
> Debe eliminar el token de acceso antes de iniciar este procedimiento. Para obtener más información, consulte Cómo eliminar un token de acceso.

Siga el siguiente procedimiento para desactivar el aprovisionamiento automático en la consola de IAM Identity Center.

1. En la consola de IAM Identity Center, elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar el aprovisionamiento.

3. En la página de aprovisionamiento automático, seleccione Deshabilitar.
4. En el cuadro de diálogo Desactivar el aprovisionamiento automático, revise la información, escriba DISABLE y, a continuación, elija Deshabilitar el aprovisionamiento automático.

Cómo generar un nuevo token de acceso

Siga el siguiente procedimiento para generar un nuevo token de acceso en la consola de IAM Identity Center.

> **Note**
>
> Este procedimiento requiere que haya habilitado previamente el aprovisionamiento automático. Para obtener más información, consulte Cómo habilitar el aprovisionamiento automático.

Cómo generar un nuevo token de acceso

1. En la consola de IAM Identity Center, elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página de aprovisionamiento automático, en Tokens de acceso, seleccione Generar token.
4. En el cuadro de diálogo Generar un nuevo token de acceso, copie el nuevo token de acceso y guárdelo en un lugar seguro.
5. Elija Close.

Cómo eliminar un token de acceso

Siga el procedimiento que se detalla a continuación para eliminar un token de acceso actual de la consola de IAM Identity Center.

Cómo eliminar una clave de acceso

1. En la consola de IAM Identity Center, elija Configuración en el panel izquierdo de navegación del servicio.

2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página de aprovisionamiento automático, en Tokens de acceso, seleccione el token de acceso que desee eliminar y, a continuación, Eliminar.
4. En el cuadro de diálogo Eliminar el token de acceso, revise la información, escriba ELIMINAR y, a continuación, elija Eliminar el token de acceso.

Cómo eliminar un token de acceso

Un directorio de IAM Identity Center admite hasta 2 tokens de acceso a la vez. Para generar un token de acceso adicional antes de cualquier rotación, elimine los tokens de acceso caducados o no utilizados.

Si su token de acceso SCIM está a punto de caducar, puede seguir el procedimiento que se describe a continuación para rotar un token de acceso existente en la consola de IAM Identity Center.

Cómo eliminar un token de acceso

1. En la consola de IAM Identity Center, elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página de aprovisionamiento automático, en Tokens de acceso, anote el ID del token que desee rotar.
4. Siga los pasos que encontrará en Cómo generar un nuevo token de acceso para crear un nuevo token. Si ya ha creado el número máximo de tokens de acceso a SCIM, primero tendrá que eliminar uno de los tokens actuales.
5. Vaya al sitio web de su proveedor de identidades y configure el nuevo token de acceso para el aprovisionamiento de SCIM y, a continuación, pruebe la conectividad con IAM Identity Center con el nuevo token de acceso de SCIM. Una vez que haya confirmado que el aprovisionamiento funciona correctamente con el nuevo token, continúe con el siguiente paso de este procedimiento.
6. Siga los pasos que se indican en Cómo eliminar un token de acceso para eliminar el token de acceso que anotó anteriormente. También puede usar la fecha de creación del token como una pista sobre qué token eliminar.

Aprovisionamiento manual

Algunos IdPs no son compatibles con el Sistema de Gestión de Identidad entre Dominios (SCIM) o tienen una implementación de SCIM incompatible. En esos casos, puede aprovisionar usuarios manualmente a través de la consola de IAM Identity Center. Cuando añada usuarios a IAM Identity Center, asegúrese de configurar el nombre de usuario para que sea idéntico al nombre de usuario que tiene en su IdP. Como mínimo, debe tener una dirección de correo electrónico y un nombre de usuario únicos. Para obtener más información, consulte Exclusividad del nombre de usuario y de la dirección de correo electrónico.

También debe gestionar todos los grupos manualmente en IAM Identity Center. Para ello, debe crear los grupos y añadirlos mediante la consola de IAM Identity Center. No es necesario que estos grupos coincidan con los que existen en su IdP. Para obtener más información, consulte Grupos.

Administración de certificados SAML 2.0

IAM Identity Center utiliza certificados para establecer una relación de confianza de SAML entre IAM Identity Center y su proveedor de identidades (IdP) externo. Al añadir un IdP externo a IAM Identity Center, también debe obtener al menos un certificado SAML 2.0 X.509 público del IdP externo. Por lo general, ese certificado se instala automáticamente durante el intercambio de metadatos SAML del IdP durante la creación de relaciones de confianza.

Como administrador de IAM Identity Center, en ocasiones tendrá que sustituir los certificados de IdP antiguos por otros más nuevos. Por ejemplo, debe sustituir un certificado cuando se aproxime la fecha de vencimiento del certificado. El proceso de sustituir un certificado antiguo por uno más nuevo se denomina rotación de certificados.

Temas

- Rotar un certificado SAML 2.0
- Indicadores de estado de caducidad de certificados

Rotar un certificado SAML 2.0

Es posible que tenga que importar certificados periódicamente para rotar los certificados no válidos o vencidos emitidos por su proveedor de identidades. Esto ayuda a evitar la interrupción de la autenticación o el tiempo de inactividad. Todos los certificados importados se activan automáticamente. Los certificados solo se deben eliminar después de asegurarse de que ya no se utilizan con el proveedor de identidades asociado.

También debe tener en cuenta que es IdPs posible que algunos no admitan varios certificados. En este caso, el hecho de rotar los certificados con ellos IdPs podría suponer una interrupción temporal del servicio para los usuarios. El servicio se restablece cuando la confianza con ese IdP se ha restablecido correctamente. Si es posible, planifique esta operación cuidadosamente durante las horas de menor actividad.

> **Note**
>
> Como práctica recomendada de seguridad, ante cualquier indicio de que un certificado SAML existente está en peligro o se está usando de forma incorrecta, debe retirarlo inmediatamente y cambiarlo.

La rotación de un certificado de IAM Identity Center es un proceso de varios pasos que incluye lo siguiente:

- Obtención de un nuevo certificado del IdP
- Importación del nuevo certificado a IAM Identity Center
- Activación del nuevo certificado en el IdP
- Eliminación del certificado anterior

Siga todos los procedimientos que se detallan a continuación para completar el proceso de rotación del certificado y, al mismo tiempo, evitar cualquier tiempo de inactividad de la autenticación.

Paso 1: obtención de un nuevo certificado del IdP

Vaya al sitio web del IdP y descargue su certificado SAML 2.0. Asegúrese de que el archivo del certificado se descargue en formato codificado PEM. La mayoría de los proveedores le permiten crear varios certificados SAML 2.0 en el IdP. Es probable que se marquen como deshabilitados o inactivos.

Paso 2: importación del nuevo certificado a IAM Identity Center

Siga el procedimiento que se detalla a continuación para importar el nuevo certificado mediante la consola de IAM Identity Center.

1. En la consola de IAM Identity Center, elija Configuración.

2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página Administrar certificados SAML 2.0, seleccione Importar certificado.
4. En el cuadro de diálogo Importar certificado SAML 2.0, seleccione Elegir archivo, navegue hasta el archivo de certificado, selecciónelo y, a continuación, elija Importar certificado.

En este punto, IAM Identity Center confiará en todos los mensajes SAML entrantes firmados desde los 2 certificados que haya importado.

Paso 3: activación del nuevo certificado en el IdP

Regrese al sitio web del IdP y marque el nuevo certificado que creó anteriormente como principal o activo. En este punto, todos los mensajes SAML firmados por el IdP deberían usar el nuevo certificado.

Paso 4: eliminación del certificado anterior

Siga el procedimiento que se detalla para completar el proceso de rotación de certificados para su IdP. Siempre debe haber al menos un certificado válido en la lista y no se puede eliminar.

> **Note**
>
> Asegúrese de que su proveedor de identidades ya no firme las respuestas de SAML con este certificado antes de eliminarlo.

1. En la página Administrar certificados SAML 2.0, seleccione el certificado que desea eliminar. Elija Eliminar.
2. En el cuadro de diálogo Eliminar el certificado SAML 2.0, escriba **`DELETE`** para confirmarlo y, a continuación, elija Eliminar.
3. Regrese al sitio web del IdP y lleve a cabo los pasos necesarios para eliminar el certificado inactivo anterior.

Indicadores de estado de caducidad de certificados

En la página Administrar certificados de SAML 2.0, es posible que vea iconos indicadores de estado de colores. Estos iconos aparecen en la columna Caduca el situada junto a cada certificado de la

lista. A continuación, se describen los criterios que IAM Identity Center utiliza para determinar qué icono se muestra en cada certificado.

- Rojo: indica que un certificado está caducado actualmente.
- Amarillo: indica que un certificado caducará en 90 días o menos.
- Verde: indica que un certificado es válido actualmente y seguirá siendo válido durante al menos 90 días más.

Cómo comprobar el estado de la renovación de un certificado:

1. En la consola de IAM Identity Center, elija Configuración.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página Administrar la autenticación de SAML 2.0, en Administrar certificados de SAML 2.0, consulte el estado de los certificados de la lista tal y como se indica en la columna Caduca el.

Uso del portal de AWS acceso

El portal de AWS acceso les proporciona a los usuarios finales un acceso de inicio de sesión único a todas sus aplicaciones en la nube Cuentas de AWS y a las más utilizadas, como Office 365, Concur, Salesforce y muchas más. Puede lanzar rápidamente varias aplicaciones. Solo tiene que elegir el icono de la Cuenta de AWS o de la aplicación en el portal. La presencia de íconos de aplicaciones en su portal de AWS acceso significa que un administrador de su empresa le ha concedido acceso a esas aplicaciones o aplicaciones. Cuentas de AWS También significa que puede acceder a todas estas cuentas o aplicaciones desde el portal de AWS acceso sin tener que solicitar más datos de inicio de sesión.

Póngase en contacto con su administrador o con el servicio de asistencia para solicitar acceso adicional en las siguientes situaciones:

- No ves ninguna aplicación Cuenta de AWS o aplicación a la que necesites acceder.
- El acceso que tienes a una cuenta o aplicación determinada no es el que esperabas.

Temas

- Aceptación de la invitación para unirse a IAM Identity Center

- Iniciar sesión en el portal de AWS acceso
- Restablecimiento de la contraseña de usuario en IAM Identity Center
- Obtener las credenciales de usuario del IAM Identity Center para el AWS CLI o los SDK AWS
- Crear enlaces de acceso directo a AWS Management Console destinos
- Registro de un dispositivo para MFA
- Personalización de la URL del portal de AWS acceso

Aceptación de la invitación para unirse a IAM Identity Center

Si es la primera vez que inicia sesión en el portal de AWS acceso, consulte su correo electrónico para obtener instrucciones sobre cómo activar sus credenciales de usuario.

Para activar las credenciales de usuario

1. Según el correo electrónico que haya recibido de su empresa, elija uno de los siguientes métodos para activar sus credenciales de usuario y poder empezar a utilizar el portal de AWS acceso.

   a. Si ha recibido un correo electrónico con el asunto Invitación a unirse al AWS IAM Identity Center (sucesor del AWS Single Sign-On), ábralo y seleccione Aceptar invitación. En la página de Registro de usuarios nuevos, introduzca y confirme una contraseña y, a continuación, seleccione Establecer nueva contraseña. Deberá utilizar esa contraseña cada vez que inicie sesión en el portal.

   b. Si fue el equipo de asistencia de TI o el administrador de TI de la empresa el que le envió el correo electrónico, siga las instrucciones proporcionadas para activar sus credenciales de usuario.

2. Tras activar sus credenciales de usuario proporcionando una nueva contraseña, el portal de AWS acceso iniciará sesión automáticamente. Si esto no ocurre, puede iniciar sesión manualmente en el portal de usuarios AWS usando las instrucciones que se indican en el siguiente paso.

Iniciar sesión en el portal de AWS acceso

En este momento, un administrador debería haberle proporcionado una URL de inicio de sesión específica en el portal de AWS acceso. En cuanto la tenga, podrá continuar con los pasos que se

describen a continuación para iniciar sesión en el portal. Para obtener más información, consulte Iniciar sesión en el portal de AWS acceso.

> **Note**
>
> Después de iniciar sesión, la duración predeterminada de la sesión del portal de AWS acceso es de 8 horas. Tenga en cuenta que un administrador puede cambiar la duración de esta sesión.

Dispositivos de confianza

Después de seleccionar la opción Este es un dispositivo de confianza en la página de inicio de sesión, IAM Identity Center considerará que todos los inicios de sesión futuros desde ese dispositivo están autorizados. Esto significa que IAM Identity Center no ofrecerá la opción de introducir un código MFA mientras utilice ese dispositivo de confianza. Sin embargo, hay algunas excepciones, como iniciar sesión desde un navegador nuevo o cuando el dispositivo recibe una dirección IP desconocida.

Consejos para iniciar sesión en el portal de AWS acceso

Estos son algunos consejos que le ayudarán a administrar su experiencia con el portal de AWS acceso.

- De vez en cuando, puede que tenga que cerrar sesión y volver a iniciarla en el portal de AWS acceso. Esto puede ser necesario para poder acceder a las nuevas aplicaciones que el administrador le haya asignado recientemente. Sin embargo, no será necesario, ya que todas las nuevas aplicaciones se actualizan cada hora.
- Al iniciar sesión en el portal de AWS acceso, puede abrir cualquiera de las aplicaciones que aparecen en el portal seleccionando el icono de la aplicación. Cuando haya terminado de usar la aplicación, puede cerrarla o cerrar sesión en el portal de AWS acceso. Al cerrar la aplicación solo finaliza la sesión de la aplicación en cuestión. Todas las demás aplicaciones que haya abierto desde el portal de AWS acceso permanecerán abiertas y en ejecución.
- Antes de iniciar sesión con otro usuario, primero debe cerrar la sesión del portal de usuario AWS . El cierre de sesión del portal elimina por completo sus credenciales de la sesión del navegador.
- Una vez que inicie sesión en el portal de AWS acceso, podrá cambiar a un rol. Esto anula temporalmente los permisos de usuario originales y, en su lugar, le otorga los permisos asignados al rol. Para obtener más información, consulte Cambiar a un rol (consola).

Cerrar sesión en el portal de AWS acceso

Al cerrar sesión del portal, se eliminan por completo sus credenciales de la sesión del navegador. Para obtener más información, consulte Cerrar sesión en el portal de AWS acceso en la AWS Sign-Inguía.

Para cerrar sesión en el portal de AWS acceso

- En el portal de AWS acceso, seleccione Cerrar sesión en la barra de navegación.

> **Note**
>
> Antes de iniciar sesión con otro usuario, primero debe cerrar la sesión del portal de usuario AWS .

Restablecimiento de la contraseña de usuario en IAM Identity Center

El portal de AWS acceso proporciona a los usuarios del Centro de Identidad de IAM un acceso de inicio de sesión único a todas sus AWS cuentas asignadas y aplicaciones en la nube a través de un portal web. El portal de AWS acceso es diferente del AWS Management Console, que es un conjunto de consolas de servicio para gestionar los recursos. AWS

Utilice este procedimiento para restablecer la contraseña de usuario del IAM Identity Center para el portal de AWS acceso. Más información sobre los tipos de usuario en la Guía del usuario de AWS Sign-In .

Consideraciones

La función de restablecimiento de la contraseña para el portal de AWS acceso solo está disponible para los usuarios de las instancias del Centro de Identidad que utilizan el directorio de Identity Center o AWS Managed Microsoft ADcomo fuente de identidad. Si el usuario está conectado a un proveedor de identidad externo o a AD Connector, el restablecimiento de la contraseña del usuario debe realizarse desde el proveedor de identidad externo o estar conectadoActive Directory.

- Si su fuente de identidad es un directorio del Centro de identidades de IAM, consulte. Requisitos de contraseñas para administrar identidades en IAM Identity Center
- Si su fuente de identidad es una AWS Managed Microsoft AD, consulte Requisitos de contraseña al restablecer una contraseña en. AWS Managed Microsoft AD

Para restablecer la contraseña del portal de AWS acceso

1. Abra un navegador web y vaya a la página de inicio de sesión de su portal de AWS acceso.

   Si no tiene la URL del portal de AWS acceso, compruebe su correo electrónico. Deberías haber recibido por correo electrónico una invitación para unirte al Centro de Identidad de AWS IAM que incluya una URL de inicio de sesión específica en el AWS portal de acceso. Como alternativa, es posible que su administrador le haya proporcionado directamente una contraseña de un solo uso y la URL del portal de AWS acceso. Si no encuentra esta información, pida al administrador que se la envíe.

   Para obtener más información sobre cómo iniciar sesión en el portal de AWS acceso, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.
2. Escriba su nombre y, a continuación, elija Siguiente.
3. En Contraseña, seleccione He olvidado la contraseña.

   Proporcione su nombre de usuario y escriba los caracteres de la imagen para confirmar que no es un robot. A continuación, elija Next. Es posible que tenga que deshabilitar el software bloqueador de anuncios si no puede introducir caracteres.
4. Aparecerá un mensaje para confirmar que se envió un correo electrónico para restablecer la contraseña. Elija Continuar.
5. Recibirá un correo electrónico de `no-reply@signin.aws` con el asunto Se solicita el restablecimiento de la contraseña. En el correo electrónico, seleccione Restablecer contraseña.
6. En la página Restablecer la contraseña, compruebe su nombre de usuario, especifique una nueva contraseña para el portal de AWS acceso y, a continuación, seleccione Establecer nueva contraseña.
7. Recibirá un correo electrónico de `no-reply@signin.aws` con el asunto Se solicita el restablecimiento de la contraseña.

> **Note**
>
> Un administrador puede restablecer su contraseña enviándole un correo electrónico con instrucciones para restablecerla o generando una contraseña de un solo uso y compartiéndola con usted. Si es un administrador, consulte Restablecimiento de la contraseña de usuario de IAM Identity Center para un usuario final.

Obtener las credenciales de usuario del IAM Identity Center para el AWS CLI o los SDK AWS

Puede acceder a AWS los servicios mediante programación mediante los kits de desarrollo de software (SDK) AWS Command Line Interface o los kits de desarrollo de AWS software (SDK) con credenciales de usuario del IAM Identity Center. En este tema se describe cómo obtener credenciales temporales para un usuario en IAM Identity Center.

El portal de AWS acceso proporciona a los usuarios del Centro de Identidad de IAM un acceso único a sus aplicaciones y a las de la nube. Cuentas de AWS Tras iniciar sesión en el portal de AWS acceso como usuario del IAM Identity Center, podrá obtener credenciales temporales. A continuación, puede utilizar las credenciales, también denominadas credenciales de usuario del Centro de Identidad de IAM, en los AWS CLI AWS SDK para acceder a los recursos de un. Cuenta de AWS

Si utiliza el AWS CLI para acceder a los AWS servicios mediante programación, puede utilizar los procedimientos de este tema para iniciar el acceso al. AWS CLI Para obtener información sobre el AWS CLI, consulte la Guía del AWS Command Line Interface usuario.

Si utiliza los AWS SDK para acceder a los AWS servicios mediante programación, si sigue los procedimientos de este tema, también se establece directamente la autenticación de los SDK. AWS Para obtener información sobre los AWS SDK, consulte la Guía de referencia de los AWS SDK y las herramientas.

> **Note**
>
> Los usuarios de IAM Identity Center son diferentes a los usuarios de IAM. Los usuarios de IAM reciben credenciales a largo plazo para acceder a los recursos. AWS Los usuarios de IAM Identity Center reciben credenciales temporales. Le recomendamos que utilice credenciales temporales como práctica recomendada de seguridad para acceder a sus cuentas, Cuentas de AWS ya que estas credenciales se generan cada vez que inicia sesión.

Requisitos previos

Para obtener credenciales temporales para su usuario de IAM Identity Center, necesitará lo siguiente:

- Un usuario de IAM Identity Center: iniciará sesión en el portal de acceso AWS como este usuario. Usted o su administrador pueden crearlo. Para obtener información sobre cómo activar IAM Identity Center y crear un usuario de IAM Identity Center, consulte Introducción a las tareas habituales en IAM Identity Center.
- Acceso de usuario a un Cuenta de AWS: para conceder permiso a un usuario del Centro de Identidad de IAM para recuperar sus credenciales temporales, usted o un administrador deben asignar al usuario del Centro de Identidad de IAM un conjunto de permisos. Los conjuntos de permisos se guardan en IAM Identity Center y definen el nivel de acceso que tienen los usuarios y grupos de una Cuenta de AWS. Si su administrador creó el usuario de IAM Identity Center por usted, pídale que añada este acceso. Para obtener más información, consulte Asigne el acceso de los usuarios a Cuentas de AWS.
- AWS CLI instalado: para utilizar las credenciales temporales, debe instalar el. AWS CLI Para obtener instrucciones de instalación, consulte Instalar o actualizar la última versión de la AWS CLI en la Guía del usuario de AWS CLI .

Consideraciones

Antes de completar los pasos para obtener credenciales temporales para el usuario de IAM Identity Center, tenga en cuenta los siguientes aspectos:

- IAM Identity Center crea roles de IAM: cuando se asigna a un usuario de IAM Identity Center un conjunto de permisos, IAM Identity Center crea un rol de IAM correspondiente a partir del conjunto de permisos. Las funciones de IAM creadas mediante conjuntos de permisos se diferencian de las funciones de IAM creadas AWS Identity and Access Management en los siguientes aspectos:
  - IAM Identity Center posee y protege los roles creados por los conjuntos de permisos. Solo IAM Identity Center puede modificar estos roles.
  - Solo los usuarios de IAM Identity Center pueden asumir los roles que corresponden a sus conjuntos de permisos asignados. No puede asignar el acceso a los conjuntos de permisos a los usuarios de IAM, a los usuarios federados de IAM ni a las cuentas de servicio.
  - No puede modificar una política de confianza de roles en estos roles para permitir el acceso a entidades principales fuera de IAM Identity Center.

  Para obtener información sobre cómo obtener credenciales temporales para un rol que cree en IAM, consulte Uso de credenciales de seguridad temporales con la AWS CLI en la Guía del usuario de AWS Identity and Access Management .

- Puede configurar la duración de la sesión para los conjuntos de permisos: tras iniciar sesión en el portal de AWS acceso, el conjunto de permisos al que está asignado su usuario del Centro de Identidad de IAM aparece como función disponible. IAM Identity Center crea una sesión independiente para este rol. Esta sesión puede durar de una a 12 horas según la duración de la sesión configurada para el conjunto de permisos. De forma predeterminada, la sesión durará 1 hora. Para obtener más información, consulte Definir la duración de la sesión.

Obtención y actualización de credenciales temporales

Puede obtener y actualizar credenciales temporales de su usuario de IAM Identity Center de forma automática o manual.

Temas

- Actualización automática de credenciales (recomendada)
- Actualización manual de credenciales

Actualización automática de credenciales (recomendada)

La actualización automática de credenciales utiliza el estándar de autorización de código de dispositivo Open ID Connect (OIDC)). Con este método, se inicia el acceso directamente mediante el comando `aws configure sso` en la AWS CLI. Puede utilizar este comando para acceder automáticamente a cualquier rol que esté asociado a cualquier conjunto de permisos que tenga asignado a cualquiera Cuenta de AWS de ellos.

Para acceder al rol creado para su usuario del Centro de Identidad de IAM, ejecute el `aws configure sso` comando y, a continuación, autorícelo AWS CLI desde una ventana del navegador. Mientras tenga una sesión activa en el portal de AWS acceso, AWS CLI recuperará automáticamente las credenciales temporales y las actualizará automáticamente.

Para obtener más información, consulte Configurar el perfil con el `aws configure sso wizard` en la Guía del usuario AWS Command Line Interface .

Cómo obtener credenciales temporales que se actualicen automáticamente:

1. Inicie sesión en el portal de AWS acceso mediante la URL de inicio de sesión específica proporcionada por su administrador. Si creó el usuario del Centro de identidad de IAM, AWS envíe una invitación por correo electrónico que incluya su URL de inicio de sesión. Para obtener

más información, consulte Iniciar sesión en el portal de AWS acceso en la Guía del usuario de AWS inicio de sesión.

2. En la pestaña Cuentas, localice la página Cuenta de AWS de la que desea recuperar las credenciales. Al seleccionar la cuenta, aparecerán el nombre y el ID de la cuenta y la dirección de correo electrónico asociados a la cuenta.

> **Note**
>
> Si no ve ninguna Cuentas de AWS en la lista, es probable que aún no se le haya asignado un conjunto de permisos dicha cuenta o cuentas. En este caso, póngase en contacto con su administrador y pídale que añada este acceso. Para obtener más información, consulte Asigne el acceso de los usuarios a Cuentas de AWS.

3. Debajo del nombre de la cuenta, los permisos al que está asignado el usuario de IAM Identity Center aparecen como un rol disponible. Por ejemplo, si a su usuario del Centro de Identidad de IAM se le asigna el conjunto de PowerUserAccesspermisos de la cuenta, el rol aparecerá en el portal de AWS acceso como PowerUserAccess.
4. Según la opción que elija junto al nombre del rol, elija Teclas de acceso o elija Acceso mediante línea de comandos o mediante programación.
5. En el cuadro de diálogo Obtener credenciales, elija macOS y Linux, Windows o PowerShell, según el sistema operativo en el que haya instalado AWS CLI.
6. En Credenciales de IAM Identity Center de AWS (recomendadas), se muestran sus credenciales de `SSO Start URL` y `SSO Region`. Estos valores son necesarios para configurar un perfil habilitado para IAM Identity Center y `sso-session` para la AWS CLI Para completar esta configuración, siga las instrucciones de Configurar el perfil con el `aws configure sso wizard` en la Guía del usuario de AWS Command Line Interface .

Siga utilizándolas AWS CLI según sea necesario Cuenta de AWS hasta que las credenciales hayan caducado.

Actualización manual de credenciales

Puede usar el método de actualización manual de credenciales para obtener credenciales temporales para un rol que esté asociado a un conjunto de permisos específico en un rol específico Cuenta de AWS. Para ello, debe copiar y pegar los comandos necesarios para las credenciales temporales. Con este método, debe actualizar las credenciales temporales manualmente.

Puedes ejecutar AWS CLI comandos hasta que caduquen tus credenciales temporales.

Cómo obtener credenciales que se actualizan manualmente

1. Inicie sesión en el portal de AWS acceso mediante la URL de inicio de sesión específica proporcionada por su administrador. Si creó el usuario del Centro de identidad de IAM, AWS envíe una invitación por correo electrónico que incluya su URL de inicio de sesión. Para obtener más información, consulte Iniciar sesión en el portal de AWS acceso en la Guía del usuario de AWS inicio de sesión.
2. En la pestaña Cuentas, busque la Cuenta de AWS de la que desea recuperar las credenciales de acceso y amplíela para que muestre el nombre del rol de IAM (por ejemplo, Administrador). Según la opción que elija junto al nombre del rol de IAM, elija Teclas de acceso o elija Acceso mediante línea de comandos o mediante programación.

   > **Note**
   >
   > Si no ve ninguna Cuentas de AWS en la lista, es probable que aún no se le haya asignado un conjunto de permisos dicha cuenta o cuentas. En este caso, póngase en contacto con su administrador y pídale que añada este acceso. Para obtener más información, consulte Asigne el acceso de los usuarios a Cuentas de AWS.

3. En el cuadro de diálogo Obtener credenciales, elija macOS y Linux, Windows o PowerShell, según el sistema operativo en el que haya instalado AWS CLI.
4. Elija una de las siguientes opciones:

   - Opción 1: Establecer variables de AWS entorno

     Elija esta opción para anular toda la configuración de credenciales, incluida la configuración de los `credentials` archivos y `config` archivos. Para obtener más información, consulte Variables de entorno para configurar la AWS CLI en la Guía del usuario de AWS CLI .

     Para utilizar esta opción, copie los comandos en el portapapeles, péguelos en la ventana del AWS CLI terminal y, a continuación, pulse Entrar para configurar las variables de entorno necesarias.

   - Opción 2: añada un perfil al archivo de AWS credenciales

     Elija esta opción para ejecutar comandos con diferentes conjuntos de credenciales.

Para usar esta opción, copie los comandos en el portapapeles y, a continuación, péguelos en el AWS `credentials` archivo compartido para configurar un nuevo perfil con nombre. Para obtener más información, consulte Archivos de configuración y credenciales compartidos en la Guía de referencia de SDK y herramientas de AWS . Para usar esta credencial, especifique la `--profile` opción en el comando. AWS CLI Esto afecta a todos los símbolos del sistema que utilicen el mismo archivo de credenciales.

- Opción 3: utilice valores individuales en su AWS cliente de servicio

  Elija esta opción para acceder a AWS los recursos de un cliente AWS de servicio. Para obtener más información, consulte Herramientas sobre las que basarse AWS.

  Para usar esta opción, copie los valores en el portapapeles, péguelos en el código y asígnelos a las variables adecuadas para su SDK. Para obtener más información, consulte la documentación específica de su específico SDK API.

Crear enlaces de acceso directo a AWS Management Console destinos

Los enlaces de acceso directo creados en el portal de AWS acceso llevan a los usuarios del Centro de Identidad de IAM a un destino específico en el AWS Management Console, con un conjunto de permisos específico y en un lugar específico. Cuenta de AWS

Los enlaces de acceso directo le ahorran tiempo a usted y a sus colaboradores. En lugar de navegar hasta la URL de destino deseada en AWS Management Console (por ejemplo, una página de instancia de bucket de Amazon S3) a través de varias páginas, incluido el portal de AWS acceso, puede utilizar un enlace de acceso directo para llegar al mismo destino automáticamente.

Opciones de destino del enlace de acceso directo

Los enlaces de acceso directo tienen tres opciones de destino, que se enumeran aquí por prioridad:

- (Opcional) Cualquier URL de destino AWS Management Console especificada en el enlace de acceso directo. Por ejemplo, la página de instancias de bucket de Amazon S3.
- (Opcional) URL de estado de retransmisión configurada por el administrador para el conjunto de permisos en cuestión. Para obtener más información sobre cómo configurar el estado de retransmisión, consulte. Configura el estado de retransmisión
- AWS Management Console hogar. El destino predeterminado si no especificas ninguno.

> **Note**
>
> La navegación automática a un destino solo se realiza correctamente si se ha autenticado en el Centro de Identidad de IAM y se ha asignado el conjunto de permisos necesario para la AWS cuenta y la URL de destino.

El portal de AWS acceso incluye un botón Crear acceso directo que le ayuda a crear un enlace de acceso directo que se pueda compartir. Si tiene pensado especificar una URL de destino (la primera opción de la lista anterior), puede copiar la URL en un portapapeles para compartirla.

Cree un enlace de acceso directo en el portal de AWS acceso

1. Con la sesión iniciada en el portal de AWS acceso, seleccione la pestaña Cuentas y, a continuación, pulse el botón Crear acceso directo.
2. En el cuadro de diálogo:

   a. Elija una Cuenta de AWS utilizando el ID de cuenta o el nombre de la cuenta. A medida que escribes, un menú desplegable muestra los ID de cuenta y los nombres correspondientes a los que puedes acceder. Solo puede elegir una cuenta a la que tenga acceso.

   b. Si lo desea, elija un rol de IAM de la lista desplegable. Estos son los conjuntos de permisos que se le han asignado para la cuenta seleccionada. Si omite la elección del rol, se les pide a los usuarios que seleccionen uno que se les haya asignado para la cuenta elegida al utilizar el enlace de acceso directo.

   > **Note**
   >
   > No puedes conceder nuevos accesos con los enlaces de acceso directo. Los enlaces de acceso directo solo funcionan con los conjuntos de permisos ya asignados al usuario. Si el usuario no tiene asignados los conjuntos de permisos necesarios para la cuenta y la URL de destino, se le deniega el acceso.

   c. Si lo desea, introduzca la URL de destino del portal de AWS acceso. Si omite introducir una URL, el destino se determina automáticamente al utilizar el enlace de acceso directo, en función de las opciones de destino del enlace de acceso directo mencionadas anteriormente.

d. El enlace de acceso directo se genera en la parte inferior del cuadro de diálogo, en función de lo que introduzca. Pulse el botón Copiar URL. Ahora puedes crear un marcador con el enlace de acceso directo copiado o compartirlo con tus colaboradores que tengan acceso a la misma cuenta con el mismo conjunto de permisos o con otro conjunto de permisos suficiente.

Construir enlaces de AWS Management Console acceso directo seguros con codificación de URL

Todos los valores de los parámetros de la URL, incluidos el ID de cuenta, el nombre del conjunto de permisos y la URL de destino, deben estar codificados en URL.

Los enlaces de acceso directo amplían la URL del portal de AWS acceso con la siguiente ruta:

```
/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

La URL completa de la AWS partición clásica sigue este patrón:

```
https://[your_subdomain].awsapps.com/start/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

Este es un ejemplo de enlace abreviado que permite a un usuario acceder a una cuenta `123456789012` con el conjunto de `S3FullAccess` permisos y acceder a la página principal de la consola S3:

- `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

Registro de un dispositivo para MFA

Utilice el siguiente procedimiento en el portal de AWS acceso para registrar su nuevo dispositivo para la autenticación multifactor (MFA).

> **Note**
>
> Le recomendamos que primero descargue la aplicación de autenticación adecuada en su dispositivo antes de iniciar los pasos de este procedimiento. Para obtener una lista de las aplicaciones probadas que puede utilizar con dispositivos de MFA, consulte Aplicaciones de autenticación virtual.

Cómo registrar el dispositivo para su uso con MFA

1. Inicie sesión en su portal de AWS acceso. Para obtener más información, consulte Iniciar sesión en el portal de AWS acceso.
2. Cerca de la parte superior derecha de la página, seleccione dispositivos MFA.
3. En la página Dispositivos de autenticación multifactor (MFA), seleccione Registrar dispositivo.

   > **Note**
   >
   > Si la opción Registrar dispositivo MFA aparece atenuada, póngase en contacto con el administrador para que le ayude a registrar el dispositivo.

4. En la página Registrar dispositivo MFA, seleccione uno de los siguientes tipos de dispositivos MFA y siga las instrucciones:

   - Aplicación de autenticación
     1. En la página Configurar la aplicación de autenticación, IAM Identity Center muestra la información de configuración del nuevo dispositivo de MFA, incluido un gráfico de código QR. El gráfico es una representación de la clave secreta que se puede introducir manualmente en los dispositivos que no admiten códigos QR.
     2. Con el dispositivo de MFA físico, haga lo siguiente:
        a. Abra una aplicación de autenticación MFA compatible. Para obtener una lista de las aplicaciones probadas que puede utilizar con dispositivos de MFA, consulte Aplicaciones de autenticación virtual. Si la aplicación de MFA admite varias cuentas (varios dispositivos de MFA), elija la opción para crear una nueva cuenta (un nuevo dispositivo de MFA).
        b. Determine si la aplicación de MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones de la página Configurar la aplicación de autenticación.

i. Elija Mostrar código QR y, a continuación, utilice la aplicación para escanear el código QR. Por ejemplo, puede elegir el icono de la cámara o una opción similar a Escanear código. A continuación, use la cámara del dispositivo para escanear el código.

ii. Seleccione Mostrar clave secreta y, a continuación, introduzca esa clave secreta en su aplicación de MFA.

> **Important**
>
> Cuando configure un dispositivo MFA para que funcione con IAM Identity Center, recomendamos que guarde una copia del código QR o la clave secreta en un lugar seguro. Esto puede ayudarle si pierde el teléfono o tiene que volver a instalar la aplicación de autenticación MFA. Si ocurre alguna de estas cosas, puede volver a configurar rápidamente la aplicación para que utilice la misma configuración de MFA.

3. En la página Configurar la aplicación de Authenticator, en Código de autenticación, escriba la contraseña de uso único que aparece actualmente en el dispositivo MFA físico.

> **Important**
>
> Envíe su solicitud inmediatamente después de generar el código. Si genera el código y después espera demasiado tiempo a enviar la solicitud, el dispositivo MFA se asociará correctamente a su usuario, pero no estará sincronizado. Esto ocurre porque las contraseñas temporales de un solo uso (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo.

4. Elija Asignar MFA. El dispositivo MFA ahora puede empezar a generar contraseñas de un solo uso y ya está listo para su uso. AWS

- Llave de seguridad o autenticador integrado

1. En la página Registrar la clave de seguridad de su usuario, siga las instrucciones que le dé su navegador o plataforma.

> **Note**
>
> La experiencia varía según el navegador o la plataforma. Una vez que el dispositivo se haya registrado correctamente, podrá asociar un nombre descriptivo al dispositivo recién inscrito. Si desea cambiarlo, seleccione Cambiar nombre, escriba el nuevo nombre y, a continuación, seleccione Guardar.

Personalización de la URL del portal de AWS acceso

De forma predeterminada, puede acceder al portal de AWS acceso mediante una URL que siga este formato:d-*xxxxxxxxxx*.awsapps.com/start. Puede personalizar el complemento del modo siguiente: *your_subdomain*.awsapps.com/start.

> **Important**
>
> Si cambias la URL del portal de AWS acceso, no podrás editarla más adelante.

Cómo personalizar la URL

1. Abre la AWS IAM Identity Center consola en https://console.aws.amazon.com/singlesignon/.
2. En la consola del IAM Identity Center, seleccione Dashboard en el panel de navegación y busque la sección de resumen de la configuración.
3. Pulse el botón Personalizar situado debajo de la URL del portal de AWS acceso.

   > **Note**
   >
   > Si el botón Personalizar no aparece, significa que el portal de AWS acceso ya se ha personalizado. La personalización de la URL del portal de AWS acceso es una operación que se realiza una sola vez y no se puede revertir.

4. Introduce el nombre de subdominio que desees y selecciona Guardar.

Ahora puede iniciar sesión en la AWS consola a través de su portal de AWS acceso con su URL personalizada.

Autenticación multifactor para usuarios de Identity Center

La autenticación multifactor (MFA) proporciona una forma sencilla y segura de añadir una capa adicional de protección además del mecanismo de autenticación predeterminado del nombre de usuario y la contraseña.

Cuando los administradores habilitan la MFA, los usuarios deben iniciar sesión en el portal de acceso de AWS teniendo en cuenta dos factores:

- Su nombre de usuario y contraseña. Este es el primer factor y es un elemento que los usuarios saben.
- Ya sea un código, una clave de seguridad o datos biométricos. Este es el segundo factor y es un elemento que los usuarios tienen (posesión) o son (biométrico). El segundo factor puede ser un código de autenticación generado desde su dispositivo móvil, una clave de seguridad conectada a su ordenador o el escaneo biométrico del usuario.

En conjunto, estos múltiples factores proporcionan una mayor seguridad al impedir el acceso no autorizado a sus recursos de AWS, a menos que se haya completado correctamente una impugnación de MFA válida.

Cada usuario puede registrar hasta dos aplicaciones de autenticación virtual, que son aplicaciones de autenticación de contraseñas de un solo uso instaladas en su dispositivo móvil o tableta, y seis autenticadores FIDO, que incluyen autenticadores y claves de seguridad integrados, para un total de ocho dispositivos MFA. Encontrará más información en Tipos de MFA disponibles para el IAM Identity Center.

> **Important**
>
> Como práctica recomendada de seguridad, le recomendamos que habilite la autenticación multifactor.

Temas

Tipos de MFA disponibles para el IAM Identity Center

La autenticación multifactor (MFA) es un mecanismo simple y eficaz para mejorar la seguridad de los usuarios. El primer factor del usuario, su contraseña, es un secreto que debe memorizar, también conocido como factor de conocimiento. Otros factores pueden ser factores de posesión (algo que posea, como una clave de seguridad) o factores inherentes (algo que sea suyo y solo suyo, como un escaneo biométrico). Se recomienda encarecidamente que configure una MFA para agregar una capa adicional para la seguridad de su cuenta.

La MFA de IAM Identity Center admite los siguientes tipos de dispositivos: Se admiten todos los tipos de MFA tanto para el acceso a la consola desde un navegador como para el uso de la versión 2 de AWS CLI con el IAM Identity Center.

- Autenticadores FIDO2, incluidos los autenticadores y las claves de seguridad integrados
- Aplicaciones de autenticación virtual
- Su propia implementación de MFA en RADIUS conectada a través de AWS Managed Microsoft AD

Un usuario puede tener hasta ocho dispositivos MFA, que incluyen hasta dos aplicaciones de autenticación virtual y seis autenticadores FIDO, registrados en una cuenta. También puede configurar los ajustes de habilitación de MFA para que requieran MFA cada vez que los usuarios inicien sesión o para habilitar dispositivos de confianza que no requieren MFA en cada inicio de sesión. Para obtener más información acerca de cómo configurar los tipos de MFA para sus usuarios, consulte Elegir tipos de MFA y Configurar la aplicación de dispositivos MFA.

Autenticadores FIDO2

FIDO2 es un estándar que incluye CTAP2 y WebAuthn y se basa en criptografía de clave pública. Las credenciales FIDO son eficaces ante intentos de suplantación de identidad porque son exclusivas del sitio web en el que se crearon, por ejemplo AWS.

AWS admite los dos factores de forma más comunes para los autenticadores FIDO: los autenticadores integrados y las claves de seguridad. Consulte la sección que aparece a continuación para obtener más información sobre los tipos más comunes de autenticadores FIDO.

Temas

- Autentificadores integrados
- Claves de seguridad

- Administradores de contraseñas, proveedores de claves de acceso y otros autenticadores FIDO

Autentificadores integrados

Algunos ordenador y teléfonos móviles actuales tienen autenticadores integrados, como el TouchID del MacBook o una cámara compatible con Windows Hello. Si su dispositivo tiene un autenticador integrado compatible con FIDO, puede usar su huella digital, su rostro o el PIN del dispositivo como segundo factor.

Claves de seguridad

Las llaves de seguridad son autenticadores de hardware externos compatibles con FIDO que puede comprar y conectar a su dispositivo a través de USB, BLE o NFC. Cuando se le pida la MFA, solo tiene que realizar un gesto con el sensor de la tecla. Algunos ejemplos de claves de seguridad incluyen las claves YubiKeys y Feitian, y las claves de seguridad más comunes crean credenciales FIDO vinculadas al dispositivo. Para obtener una lista de todas las llaves de seguridad certificadas por FIDO, consulte los Productos certificados por FIDO.

Administradores de contraseñas, proveedores de claves de acceso y otros autenticadores FIDO

Existen varios proveedores externos que admiten la autenticación FIDO en las aplicaciones móviles, como características disponibles en administradores de contraseñas, tarjetas inteligentes con modo FIDO y otros formatos. Estos dispositivos compatibles con FIDO pueden funcionar con IAM Identity Center, pero le recomendamos que pruebe usted mismo un autenticador FIDO antes de activar esta opción como MFA.

> **Note**
>
> Algunos autenticadores FIDO pueden crear credenciales FIDO reconocibles, conocidas como claves de acceso. Las claves de acceso pueden estar vinculadas al dispositivo que las crea o pueden sincronizarse y guardarse copias de seguridad en una nube. Por ejemplo, se puede registrar una clave de acceso con el Apple Touch ID en un MacBook compatible y, a continuación, iniciar sesión en un sitio desde un portátil Windows con Google Chrome con la clave de acceso en iCloud siguiendo las instrucciones que aparecen en pantalla al iniciar sesión. Para obtener más información sobre qué dispositivos admiten claves de acceso sincronizables y la interoperabilidad actual de claves entre sistemas operativos y navegadores, consulte Asistencia para dispositivos en passkeys.dev, un recurso proporcionado por la Alianza FIDO y el Consorcio World Wide Web (W3C).

Aplicaciones de autenticación virtual

Las aplicaciones de autenticación son autenticadores de terceros basados en contraseñas de un solo uso (OTP). Puede utilizar una aplicación de autenticación instalada en su dispositivo móvil o tableta como dispositivo MFA autorizado. La aplicación de autenticación de terceros debe cumplir con RFC 6238, que es un algoritmo de contraseña temporal de un solo uso (TOTP) basado en estándares y capaz de generar códigos de autenticación de seis dígitos.

Cuando se le pida la MFA, el usuario debe introducir un código válido de su aplicación de autenticación en el cuadro de entrada que aparece. Cada dispositivo MFA asignado a un usuario debe ser único. Se pueden registrar dos aplicaciones de autenticación para un usuario determinado.

Aplicaciones de autenticación probada

Cualquier aplicación compatible con TOTP funcionará con la MFA de IAM Identity Center. La siguiente tabla muestra las aplicaciones de autenticación de terceros conocidas que puede elegir.

Sistema operativo	Aplicación de autenticación probada
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

MFA en RADIUS

El Remote Authentication Dial-In User Service (RADIUS) es un protocolo cliente-servidor estándar en el sector que proporciona autenticación, autorización y gestión de cuentas para que los usuarios puedan conectarse a servicios de red. AWS Directory Service incluye un cliente RADIUS que se conecta al servidor RADIUS sobre el que se ha implementado su solución de MFA. Para obtener más información, consulte Activar autenticación multifactor de AWS Managed Microsoft AD.

Puede utilizar MFA en RADIUS o MFA en el IAM Identity Center para los inicios de sesión de los usuarios en el portal de usuarios, pero no en ambos. La MFA en IAM Identity Center es una alternativa a la MFA en RADIUS en los casos en que desee una autenticación de AWS nativa de dos factores para acceder al portal.

Al habilitar la MFA en el IAM Identity Center, los usuarios necesitan un dispositivo de MFA para iniciar sesión en el portal de acceso de AWS. Si ya había utilizado MFA en RADIUS, la activación de la MFA en IAM Identity Center anula de manera efectiva la MFA en RADIUS para los usuarios que inician sesión en el portal de acceso de AWS. Sin embargo, la MFA en RADIUS sigue siendo un desafío para los usuarios cuando inician sesión en todas las demás aplicaciones que funcionan con AWS Directory Service, como Amazon WorkDocs.

Si la MFA está Deshabilitado en la consola del IAM Identity Center y ha configurado la MFA en RADIUS con AWS Directory Service, la MFA en RADIUS rige el inicio de sesión en el portal de acceso de AWS. Esto significa que el IAM Identity Center recurre a la configuración de MFA en RADIUS si la MFA está deshabilitada.

Configurar MFA

En los temas siguientes se proporcionan instrucciones para configurar los dispositivos MFA en el IAM Identity Center.

Temas

Consideraciones antes de habilitar la MFA en el IAM Identity Center

Antes de activar la MFA, tenga en cuenta lo siguiente:

- Se recomienda a los usuarios que registren varios autenticadores de respaldo para todos los tipos de MFA habilitados. Esta práctica puede evitar la pérdida de acceso en caso de que un dispositivo MFA se rompa o se pierda.
- No elija la opción Exigirles que proporcionen una contraseña de un solo uso enviada por correo electrónico si los usuarios deben iniciar sesión en el portal de acceso de AWS para acceder a su correo electrónico. Por ejemplo, sus usuarios podrían utilizar Microsoft 365 en el portal de acceso de AWS para leer su correo electrónico. En este caso, los usuarios no podrán recuperar el código de verificación ni podrán iniciar sesión en el portal de acceso de AWS. Para obtener más información, consulte Configurar la aplicación de dispositivos MFA.

- Si ya utiliza la MFA en RADIUS que configuró con AWS Directory Service, no necesita habilitar la MFA en IAM Identity Center. La MFA del IAM Identity Center es una alternativa a la MFA en RADIUS para los usuarios de Microsoft Active Directory del IAM Identity Center. Para obtener más información, consulte MFA en RADIUS.
- Puede utilizar las capacidades de MFA en el IAM Identity Center cuando su fuente de identidad esté configurada con el almacén de identidades del IAM Identity Center, AWS Managed Microsoft AD o AD Connector. Actualmente, los Proveedores de identidad externos no admiten la MFA en el IAM Identity Center.

Activar la MFA en el IAM Identity Center

Puede habilitar el acceso seguro al portal de acceso de AWS, a las aplicaciones integradas del IAM Identity Center y a AWS CLI al habilitar la autenticación multifactor (MFA).

Temas

- Solicitar MFA a los usuarios
- Desactivación de la MFA para el directorio del IAM Identity Center

Solicitar MFA a los usuarios

Siga los siguientes pasos para habilitar la MFA en la consola del IAM Identity Center. Antes de comenzar, le recomendamos que comprenda los Tipos de MFA disponibles para el IAM Identity Center.

> **Note**
>
> Si utiliza un IdP externo, la sección de Autenticación multifactor no estará disponible. Su IdP externo gestiona la configuración de MFA en lugar del IAM Identity Center.

Para habilitar la MFA

1. Abra la Consola del IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de Configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.

5. En la página Configurar la autenticación multifactor, en Solicitar MFA a los usuarios, elija uno de los siguientes modos de autenticación en función del nivel de seguridad que necesite su empresa:

   - Solo cuando su contexto de inicio de sesión cambie (en función del contexto)

     En este modo (el predeterminado), el IAM Identity Center ofrece a los usuarios la opción de confiar en su dispositivo durante el inicio de sesión. Cuando un usuario indica que quiere confiar en un dispositivo, el IAM Identity Center solicita al usuario la MFA una vez y analiza el contexto de inicio de sesión (como el dispositivo, el navegador y la ubicación) para los siguientes inicios de sesión del usuario. Para los inicios de sesión posteriores, el IAM Identity Center determina si el usuario inicia sesión con un contexto en el que anteriormente se confiaba. Si el contexto de inicio de sesión del usuario cambia, el IAM Identity Center solicita al usuario la MFA además de sus credenciales de dirección de correo electrónico y contraseña.

     Este modo facilita su uso a los usuarios que inician sesión con frecuencia desde su lugar de trabajo, por lo que no necesitan completar la MFA cada vez que inician sesión. Solo se les solicita la MFA si cambia su contexto de inicio de sesión.

   - Cada vez que inician sesión (siempre activo)

     En este modo, el IAM Identity Center requiere que se pregunte a los usuarios con un dispositivo MFA registrado cada vez que inicien sesión. Debe utilizar este modo si tiene políticas organizativas o de conformidad que exigen que los usuarios completen la MFA cada vez que inicien sesión en el portal de acceso de AWS. Por ejemplo, PCI DSS recomienda encarecidamente la MFA durante cada inicio de sesión para acceder a las aplicaciones que admiten transacciones de pago de alto riesgo.

   - Nunca (desactivado)

     Mientras estén en este modo, todos los usuarios iniciarán sesión únicamente con su nombre de usuario y contraseña estándar. Al elegir esta opción, se deshabilita la MFA del IAM Identity Center.

     > **Note**
     >
     > Si ya utiliza la MFA en RADIUS con AWS Directory Service y desea seguir utilizándolo como el tipo de MFA predeterminado, puede dejar el modo de autenticación desactivado para omitir las capacidades de MFA en el IAM Identity Center. Al cambiar

del modo Desactivado al modo En función del contexto o Siempre activo, se anulará la configuración de MFA en RADIUS existente. Para obtener más información, consulte MFA en RADIUS.

6. Elija Save changes.

Temas relacionados

- Elegir tipos de MFA
- Configurar la aplicación de dispositivos MFA
- Permita a los usuarios registrar sus propios dispositivos MFA

Desactivación de la MFA para el directorio del IAM Identity Center

Al deshabilitar la autenticación multifactor (MFA) en el directorio del IAM Identity Center, los usuarios pueden iniciar sesión únicamente con su nombre de usuario y contraseña estándar. Si bien la MFA está deshabilitada en el directorio de usuarios de Identity Center, no puede administrar los dispositivos MFA en sus datos de usuario y los usuarios del directorio de Identity Center no pueden administrar los dispositivos MFA desde el portal de acceso de AWS.

Para desactivar la MFA para el directorio del IAM Identity Center:

> **Important**
>
> Las instrucciones figuran en esta sección aplican a AWS IAM Identity Center. No se aplican a AWS Identity and Access Management (IAM). Los usuarios, grupos y credenciales de usuario del IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo desactivar la MFA para los usuarios de IAM, consulte Desactivación de dispositivos de MFA en la Guía del usuario de AWS Identity and Access Management.

1. Abra la Consola del IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de Configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.

5. En la página Configurar la autenticación multifactor, en la sección Solicitar MFA a los usuarios, pulse el botón de opción Nunca (deshabilitado).
6. Elija Save changes (Guardar cambios).

Elegir tipos de MFA

Utilice el siguiente procedimiento para elegir los tipos de dispositivos con los que los usuarios pueden autenticarse cuando se les solicite la MFA en el portal de acceso de AWS.

Para configurar los tipos de MFA para sus usuarios:

1. Abra la Consola del IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de Configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.
5. En la página Configurar la autenticación multifactor, en Los usuarios pueden autenticarse con estos tipos de MFA, elija uno de los siguientes tipos de MFA en función de las necesidades de su empresa. Para obtener más información, consulte Tipos de MFA disponibles para el IAM Identity Center.
   - Los autenticadores FIDO2, incluidos los autenticadores y las claves de seguridad integrados
   - Aplicaciones de autenticación virtual
6. Elija Save changes (Guardar cambios).

Configurar la aplicación de dispositivos MFA

Utilice el siguiente procedimiento para determinar si los usuarios deben tener un dispositivo MFA registrado al iniciar sesión en el portal de acceso de AWS.

Para configurar la aplicación de dispositivos de MFA para sus usuarios:

1. Abra la Consola del IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de Configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.

5. En la página Configurar la autenticación multifactor, en Si un usuario aún no tiene un dispositivo MFA registrado, elija una de las siguientes opciones en función de las necesidades de su empresa:

   - Exija que registren un dispositivo MFA al iniciar sesión

     Esta es la configuración predeterminada al configurar MFA por primera vez para el IAM Identity Center. Utilice esta opción cuando desee solicitar a los usuarios que aún no tengan un dispositivo MFA registrado que autoinscriban un dispositivo durante el inicio de sesión tras una autenticación con contraseña correcta. Esto le permite proteger los entornos de AWS de su organización con MFA sin tener que inscribir y distribuir individualmente los dispositivos de autenticación a sus usuarios. Durante la inscripción automática, sus usuarios pueden registrar cualquier dispositivo de los Tipos de MFA disponibles para el IAM Identity Center disponibles que haya activado anteriormente. Tras completar el registro, los usuarios tienen la opción de asignar un nombre descriptivo a su dispositivo MFA recién inscrito, tras lo cual el IAM Identity Center redirige al usuario a su destino original. Si el dispositivo del usuario se pierde o se lo roban, solo tiene que eliminarlo de su cuenta y el IAM Identity Center le pedirá que registre automáticamente un dispositivo nuevo la próxima vez que inicie sesión.

   - Solicite que proporcionen una contraseña de un solo uso enviada por correo electrónico para iniciar sesión

     Use esta opción si desea que los códigos de verificación se envíen a los usuarios por correo electrónico. Como el correo electrónico no está enlazado a un dispositivo específico, esta opción no cumple con los requisitos de autenticación multifactor estándar del sector. Sin embargo, mejora la seguridad en comparación con tener solo una contraseña. La verificación por correo electrónico solo se solicitará si el usuario no ha registrado un dispositivo MFA. Si se ha habilitado el método de autenticación Dependiente del contexto, el usuario tendrá la oportunidad de marcar el dispositivo en el que recibe el correo electrónico como de confianza. Posteriormente, no se les pedirá que verifiquen un código de correo electrónico en futuros inicios de sesión desde esa combinación de dispositivo, navegador y dirección IP.

     > **Note**
     >
     > Si utiliza Active Directory como fuente de identidad habilitada para el IAM Identity Center, la dirección de correo electrónico siempre se basará en el atributo de Active Directory de `email`. Las asignaciones personalizadas de atributos de Active Directory no anularán este comportamiento.

- Bloquear su inicio de sesión

  Utilice la opción Bloquear su inicio de sesión cuando desee obligar a todos los usuarios a utilizar MFA antes de que puedan iniciar sesión en AWS.

  > **Important**
  >
  > Si el método de autenticación está configurado como En función del contexto, el usuario puede seleccionar la casilla Este es un dispositivo de confianza en la página de inicio de sesión. En ese caso, no se le solicitará la MFA a ese usuario aunque tenga habilitada la configuración Bloquear su inicio de sesión. Si desea que se les pregunte a estos usuarios, cambie el método de autenticación a Siempre activo.

- Permitirles iniciar sesión

  Utilice esta opción para indicar que los dispositivos MFA no son necesarios para que los usuarios inicien sesión en el portal de acceso de AWS. A los usuarios que hayan decidido registrar dispositivos MFA se les seguirá solicitando la MFA.

6. Elija Save changes (Guardar cambios).

Permita a los usuarios registrar sus propios dispositivos MFA

Utilice el siguiente procedimiento para permitir que los usuarios registren automáticamente sus propios dispositivos MFA.

Para permitir a los usuarios registrar sus propios dispositivos MFA:

1. Abra la Consola del IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de Configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.
5. En la página Configurar la autenticación multifactor, en Quién puede administrar los dispositivos MFA, elija Los usuarios pueden agregar y administrar sus propios dispositivos MFA.
6. Elija Save changes (Guardar cambios).

> **Note**
>
> Tras configurar el registro automático de los usuarios, es posible que desee enviarles un enlace al procedimiento de Registro de un dispositivo para MFA. En este tema se proporcionan instrucciones sobre cómo configurar sus propios dispositivos de MFA.

Administrar dispositivos MFA en el IAM Identity Center

En los temas siguientes se proporcionan instrucciones para administrar los dispositivos MFA en el IAM Identity Center.

Temas

- Registrar un dispositivo MFA
- Administrar el dispositivo MFA de un usuario

Registrar un dispositivo MFA

Utilice el siguiente procedimiento para configurar un nuevo dispositivo MFA al que pueda acceder un usuario específico en la consola del IAM Identity Center. Debe tener acceso físico al dispositivo de MFA del usuario para poder registrarlo. Por ejemplo, si configura la MFA para un usuario que use un dispositivo de MFA que se ejecute en un smartphone, necesitará acceso físico al teléfono inteligente para completar el proceso de registro. También puede permitir a los usuarios configurar y administrar sus propios dispositivos MFA. Para obtener más información, consulte Permita a los usuarios registrar sus propios dispositivos MFA.

Para registrar un dispositivo MFA:

1. Abra la Consola del IAM Identity Center.
2. En el panel de navegación izquierdo, elija Users (Usuarios). Elija un usuario de la lista. No seleccione la casilla de verificación situada junto al usuario para este paso.
3. En la página de detalles del usuario, vaya a la pestaña Dispositivos MFA y, a continuación, elija Registrar dispositivo MFA.
4. En la página Registrar dispositivo MFA, seleccione uno de los siguientes tipos de dispositivos MFA y siga las instrucciones:

    - Aplicación de autenticación

1. En la página Configurar la aplicación de autenticación, el IAM Identity Center muestra la información de configuración del nuevo dispositivo de MFA, incluido un gráfico de código QR. El gráfico es una representación de la clave secreta que se puede introducir manualmente en dispositivos que no admiten códigos QR.
2. Con el dispositivo MFA físico, haga lo siguiente:
   a. Abra una aplicación de autenticación MFA compatible. Para obtener una lista de las aplicaciones probadas que puede utilizar con dispositivos de MFA, consulte Aplicaciones de autenticación virtual. Si la aplicación de MFA admite varias cuentas (varios dispositivos de MFA), elija la opción para crear una nueva cuenta (un nuevo dispositivo MFA).
   b. Determine si la aplicación MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones de la página Configurar la aplicación de autenticación:
      i. Elija Mostrar código QR y, a continuación, utilice la aplicación para escanear el código QR. Por ejemplo, puede elegir el icono de la cámara o una opción similar a Escanear código. A continuación, use la cámara del dispositivo para escanear el código.
      ii. Seleccione Mostrar clave secreta y, a continuación, introduzca esa clave secreta en su aplicación de MFA.

      > **Important**
      >
      > Cuando configure un dispositivo MFA para que funcione con el IAM Identity Center, recomendamos que guarde una copia del código QR o la clave secreta en un lugar seguro. Esto puede ayudar si el usuario asignado pierde el teléfono o tiene que volver a instalar la aplicación de autenticación MFA. Si ocurre alguna de estas cosas, puede volver a configurar rápidamente la aplicación para que utilice la misma configuración de MFA. Así evita tener que crear un nuevo dispositivo MFA en el IAM Identity Center para el usuario.
3. En la página Configurar la aplicación de autenticación, en Código de autenticación, escriba la contraseña de uso único que aparece actualmente en el dispositivo MFA físico.

   > **Important**
   >
   > Envíe su solicitud inmediatamente después de generar el código. Si genera el código y después espera demasiado tiempo a enviar la solicitud, el dispositivo MFA

está correctamente asociado al usuario. Sin embargo, el dispositivo MFA no está sincronizado. Esto ocurre porque las contraseñas de un solo uso basadas en el tiempo (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo.

4. Elija Assign MFA (Asignar MFA). El dispositivo MFA ahora puede empezar a generar contraseñas de un solo uso y ya está listo para usarse con AWS.

- Clave de seguridad

1. En la página Registrar la clave de seguridad de su usuario, siga las instrucciones que le dé su navegador o plataforma.

> **Note**
>
> La experiencia aquí varía en función de los distintos sistemas operativos y navegadores, así que sigue las instrucciones que se muestran en su navegador o plataforma. Una vez que el dispositivo de su usuario se haya registrado correctamente, tendrá la opción de asociar un nombre descriptivo para mostrar al dispositivo recién inscrito del usuario. Si desea cambiarlo, seleccione Cambiar nombre, escriba el nuevo nombre y, a continuación, seleccione Guardar. Si ha activado la opción que permite a los usuarios gestionar sus propios dispositivos, el usuario verá este nombre descriptivo en el portal de acceso de AWS.

Administrar el dispositivo MFA de un usuario

Utilice los siguientes procedimientos cuando necesite cambiar el nombre o eliminar el dispositivo MFA de un usuario.

Para cambiar el nombre de un dispositivo MFA:

1. Abra la Consola del IAM Identity Center.
2. En el panel de navegación izquierdo, elija Users (Usuarios). Elija el usuario en la lista. No seleccione la casilla de verificación situada junto al usuario para este paso.
3. En la página de detalles del usuario, vaya a la pestaña Dispositivos MFA y, a continuación, elija Cambiar nombre.

4. Cuando se le solicite, introduzca el nuevo nombre y, a continuación, seleccione Cambiar nombre.

Para eliminar un dispositivo MFA

1. Abra la Consola del IAM Identity Center.
2. En el panel de navegación izquierdo, elija Users (Usuarios). Elija el usuario en la lista.
3. En la página de detalles del usuario, vaya a la pestaña Dispositivos MFA y, a continuación, elija Eliminar.
4. Elija Eliminar y luego, Eliminar para confirmar la acción.

Gestione el acceso a Cuentas de AWS

AWS IAM Identity Center está integrado con AWS Organizations, lo que le permite administrar de forma centralizada los permisos de varias cuentas Cuentas de AWS sin tener que configurar cada una de sus cuentas manualmente. Puede definir permisos y asignarlos a los usuarios de la fuerza laboral para controlar su acceso a determinados permisos Cuentas de AWS.

Cuenta de AWS tipos

Existen dos tipos de Cuentas de AWS entradas AWS Organizations:

- Cuenta de administración: la Cuenta de AWS que se utiliza para crear la organización.
- Cuentas de miembros: el resto Cuentas de AWS que pertenecen a una organización.

Para obtener más información sobre Cuenta de AWS los tipos, consulte AWS Organizations Terminología y conceptos en la Guía del AWS Organizations usuario.

También puede optar por registrar una cuenta de miembro como administrador delegado de IAM Identity Center. Los usuarios de esta cuenta pueden realizar la mayoría de las tareas administrativas de IAM Identity Center. Para obtener más información, consulte Administración delegada.

La siguiente tabla indica si los usuarios de la cuenta pueden realizar la tarea administrativa de IAM Identity Center para cada tipo de tarea y cuenta.

Tareas administrativas de IAM Identity Center	Cuenta miembro	Cuenta de administrador delegado	Cuenta de administración
Lectura de usuarios o grupos (leer el grupo en sí y sus miembros)	 Sí	 Sí	 Sí

Tareas administrativas de IAM Identity Center	Cuenta miembro	Cuenta de administrador delegado	Cuenta de administración
Cómo agregar, editar o eliminar usuarios o grupos	No	Sí	Sí
Cómo habilitar o deshabilitar el acceso de usuarios	No	Sí	Sí
Cómo habilitar, deshabilitar o administrar los atributos entrantes	No	Sí	Sí
Cambio o administración de las fuentes de identidad	No	Sí	Sí
Creación, edición o eliminación de aplicaciones	No	Sí	Sí
Configurarción de MFA	No	Sí	Sí

Tareas administrativas de IAM Identity Center	Cuenta miembro	Cuenta de administrador delegado	Cuenta de administración
Administración de conjuntos de permisos no aprovisionados en la cuenta de administración	No	Sí	Sí
Administración de conjuntos de permisos aprovisionados en la cuenta de administración	No	No	Sí
Activar IAM Identity Center	No	No	Sí
Eliminación de la configuración de IAM Identity Center	No	No	Sí
Cómo habilitar o deshabilitar el acceso de los usuarios en la cuenta de administración	No	No	Sí
Registro o cancelación de una cuenta miembro como administrador delegado	No	No	Sí

Asignación Cuenta de AWS de acceso

Puede usar los conjuntos de permisos para simplificar la forma en que asigna el acceso a los usuarios, grupos y Cuentas de AWS de su organización. Los conjuntos de permisos se guardan en IAM Identity Center y definen el nivel de acceso que tienen los usuarios y grupos en una cuenta Cuenta de AWS. Puede crear un único conjunto de permisos y asignarlo a varios Cuentas de AWS de su organización. También puede asignar varios conjuntos de permisos al mismo usuario.

Para obtener más información sobre los conjuntos de permisos, consulte Creación, administración y eliminación de conjuntos de permisos.

> **Note**
>
> También puede asignar a sus usuarios acceso de inicio de sesión único a las aplicaciones. Para obtener más información, consulte Administración del acceso a las aplicaciones.

La experiencia del usuario final

El portal de AWS acceso proporciona a los usuarios del IAM Identity Center un acceso de inicio de sesión único a todas sus aplicaciones Cuentas de AWS y aplicaciones asignadas a través de un portal web. El portal de AWS acceso es diferente del AWS Management Console, que es un conjunto de consolas de servicio para administrar los recursos. AWS

Al crear un conjunto de permisos, el nombre que especifique para el conjunto de permisos aparece en el portal de AWS acceso como un rol disponible. Los usuarios inician sesión en el portal de AWS acceso, eligen un rol y Cuenta de AWS, a continuación, eligen el rol. Tras elegir el rol, pueden acceder a los AWS servicios mediante el uso de las credenciales temporales AWS Management Console o recuperar las credenciales temporales para acceder a AWS los servicios mediante programación.

Para abrir AWS Management Console o recuperar las credenciales temporales y acceder a ellas AWS mediante programación, los usuarios siguen estos pasos:

1. Los usuarios abren una ventana del navegador y utilizan la URL de inicio de sesión que usted proporciona para ir al AWS portal de acceso.
2. Con sus credenciales de directorio, inician sesión en el portal de AWS acceso.

3. Tras la autenticación, en la página del portal de AWS acceso, eligen la pestaña Cuentas para ver la lista Cuentas de AWS a la que tienen acceso.
4. A continuación, los usuarios eligen lo Cuenta de AWS que quieren usar.
5. Debajo del nombre del Cuenta de AWS, todos los conjuntos de permisos a los que estén asignados los usuarios aparecen como roles disponibles. Por ejemplo, si asignó un usuario `john_stiles` al conjunto de `PowerUser` permisos, el rol se mostrará en el portal de AWS acceso como`PowerUser/john_stiles`. Los usuarios que tienen asignados varios conjuntos de permisos eligen el rol de que quieren utilizar. Los usuarios pueden elegir su rol para acceder al AWS Management Console.
6. Además del rol, los usuarios del portal de AWS acceso pueden recuperar credenciales temporales para el acceso mediante línea de comandos o mediante programación seleccionando las teclas de acceso.

Para step-by-step obtener información que puede proporcionar a los usuarios de su plantilla, consulte Uso del portal de AWS acceso yObtener las credenciales de usuario del IAM Identity Center para el AWS CLI o los SDK AWS.

Aplicación y limitación del acceso

Al habilitar IAM Identity Center, este crea un rol vinculado a un servicio. También puede usar políticas de control de servicios (SCP).

Delegación y aplicación del acceso

Un rol vinculado a un servicio es un tipo de rol de IAM que está vinculado directamente a un servicio. AWS Tras activar el Centro de identidad de IAM, el Centro de identidades de IAM puede crear un rol vinculado a un servicio en cada uno de los componentes de la organización. Cuenta de AWS Esta función proporciona permisos predefinidos que permiten al Centro de Identidad de IAM delegar y hacer cumplir qué usuarios tienen acceso de inicio de sesión único a determinados miembros de su organización. Cuentas de AWS AWS Organizations Para utilizar esta característica, debe asignar a uno o más usuarios el acceso a una cuenta. Para obtener más información, consulte Roles vinculados al servicio y Uso de roles vinculados a servicios para IAM Identity Center.

Límite de acceso al almacén de identidades desde las cuentas de los miembros

En el caso del servicio de almacén de identidades utilizado por IAM Identity Center, los usuarios que tienen acceso a una cuenta de miembro pueden utilizar acciones de la API que requieren permisos de lectura. Las cuentas de los miembros tienen acceso a las acciones de lectura en los espacios de nombres sso-directory e identitystore. Para obtener más información, consulte Acciones, recursos y claves de condición del AWS IAM Identity Center directorio y Acciones, recursos y claves de condición de AWS Identity Store en la Referencia de autorización de servicios.

Para evitar que los usuarios de las cuentas de los miembros utilicen las operaciones de la API en el almacén de identidades, puede asociar una política de control de servicio (SCP). Un SCP es un tipo de política de organización que puede utilizar para administrar permisos en su organización. El siguiente ejemplo de SCP impide que los usuarios de las cuentas de los miembros accedan a cualquier operación de la API del almacén de identidades.

```
{
    "Sid": "ExplicitlyBlockIdentityStoreAccess",
    "Effect": "Deny",
    "Action": "identitystore:*", "sso-directory:*"],
    "Resource": "*"
}
```

> **Note**
>
> Limitar el acceso de las cuentas de los miembros puede afectar a la funcionalidad de las aplicaciones habilitadas para IAM Identity Center.

Para obtener más información, consulte Políticas de control de servicios (SCP) en la Guía del usuario de AWS Organizations .

Administración delegada

La administración delegada proporciona una forma cómoda para que los usuarios asignados a una cuenta miembro registrada realicen la mayoría de las tareas administrativas de IAM Identity Center. Al activar el Centro de Identidad de IAM, su instancia del Centro de Identidad de IAM se

crea en la cuenta de gestión de forma AWS Organizations predeterminada. Se diseñó originalmente de esta manera para que IAM Identity Center pudiera aprovisionar, desaprovisionar y actualizar las características en todas las cuentas de los miembros de su organización. Aunque su instancia del IAM Identity Center debe residir siempre en la cuenta de administración, puede delegar la administración del Centro de Identidad de IAM a una cuenta de miembro en AWS Organizations, lo que amplía la capacidad de administrar el Centro de Identidad de IAM desde fuera de la cuenta de administración.

Habilitar la administración delegada proporciona los siguientes beneficios:

- Minimiza la cantidad de personas que necesitan acceder a la cuenta de administración para ayudar a mitigar los problemas de seguridad
- Permite a determinados administradores asignar usuarios y grupos a las aplicaciones y a las cuentas de los miembros de su organización

Para obtener más información sobre cómo funciona el Centro de Identidad de IAM, consulte. AWS OrganizationsGestione el acceso a Cuentas de AWS Para obtener información adicional y revisar un ejemplo de escenario empresarial que muestre cómo configurar la administración delegada, consulte Getting started with IAM Identity Center delegated administration en el blog de seguridad de AWS .

Temas

Prácticas recomendadas

Estas son algunas prácticas recomendadas antes de configurar la administración delegada.

- Otorgue el mínimo privilegio a la cuenta de administración: dado que la cuenta de administración es una cuenta con muchos privilegios y para cumplir con el principio de privilegios mínimos, le recomendamos encarecidamente que restrinja el acceso a la cuenta de administración al menor número posible de personas. La característica de administrador delegado tiene por objeto minimizar el número de personas que necesitan acceder a la cuenta de administración.

- Cree conjuntos de permisos para usarlos únicamente en la cuenta de administración: esto facilita la administración de conjuntos de permisos diseñados específicamente para los usuarios que acceden a su cuenta de administración y ayuda a diferenciarlos de los conjuntos de permisos administrados por su cuenta de administrador delegado.
- Tenga en cuenta su ubicación de Active Directory: si piensa utilizar Active Directory como fuente de identidad de IAM Identity Center, localice el directorio en la cuenta del miembro en la que haya activado la característica de administrador delegado de IAM Identity Center. Si decide cambiar la fuente de identidad de IAM Identity Center de cualquier otra fuente a Active Directory, o cambiarla de Active Directory a cualquier otra fuente, el directorio debe residir en (ser propiedad de) la cuenta de miembro administrador delegado de IAM Identity Center, si existe alguna; de lo contrario, debe estar en la cuenta de administración.
- Cree asignaciones de usuarios únicamente en la cuenta de administración: el administrador delegado no puede modificar los conjuntos de permisos aprovisionados en la cuenta de administración. Sin embargo, los administradores delegados pueden añadir, editar y eliminar grupos y asignaciones de grupo.

Requisitos previos

Antes de poder registrar una cuenta como administrador delegado, primero debe configurar el siguiente entorno implementado:

- AWS Organizations debe estar habilitado y configurado con al menos una cuenta de miembro además de su cuenta de administración predeterminada.
- Si su fuente de identidad está configurada en Active Directory, la característica IAM Identity Center y sincronización de AD configurable debe estar habilitada.

Registro de una cuenta miembro

Para configurar una administración delegada, primero debe registrar una cuenta miembro en su organización como administrador delegado. Los usuarios de la cuenta de ese miembro que tengan permisos suficientes tendrán acceso administrativo a IAM Identity Center. Una vez que la cuenta miembro se registra correctamente para la administración delegada, se denomina una cuenta de administrador delegado. Para obtener más información sobre las tareas que puede realizar la cuenta de administrador delegado, consulte Cuenta de AWS tipos.

IAM Identity Center solo permite registrar una cuenta miembro como administrador delegado a la vez. Solo puede registrar una cuenta de miembro si ha iniciado sesión con las credenciales de la cuenta de administración.

Utilice el siguiente procedimiento para conceder acceso administrativo al Centro de identidad de IAM registrando una cuenta de miembro específica en su AWS organización como administrador delegado.

> **Important**
>
> Esta operación delega el acceso administrativo de IAM Identity Center a los usuarios administradores de esta cuenta miembro. Todos los usuarios que dispongan de permisos suficientes para acceder a esta cuenta de administrador delegado pueden realizar todas las tareas administrativas de IAM Identity Center desde la cuenta, excepto:
>
> - Habilitación de IAM Identity Center
> - Eliminación de las configuraciones de IAM Identity Center
> - Administración de conjuntos de permisos aprovisionados en la cuenta de administración
> - Registro o cancelación del registro de otras cuentas de miembros como administradores delegados
> - Habilitación o deshabilitación del acceso de usuarios en la cuenta de administración
>
> El administrador delegado puede editar la pertenencia al grupo.

Registro de una cuenta miembro

1. Inicie sesión AWS Management Console con las credenciales de su cuenta de administración. AWS Organizations Se requieren las credenciales de la cuenta de administración para ejecutar la RegisterDelegatedAdministratorAPI.
2. Seleccione la región en la que está activado IAM Identity Center y, a continuación, abra la consola de IAM Identity Center.
3. Elija Configuración y, a continuación, seleccione la pestaña Administración.
4. En la sección Administrador delegado, elija Registro de cuenta.
5. En la página Registrar un administrador delegado, selecciona el Cuenta de AWS que deseas registrar y, a continuación, selecciona Registrar cuenta.

Anulación del registro de una cuenta miembro

Solo puede cancelar el registro de una cuenta de miembro si ha iniciado sesión con las credenciales de la cuenta de administración.

Utilice el siguiente procedimiento para eliminar el acceso administrativo al Centro de identidad de IAM anulando el registro de una cuenta de miembro de su AWS organización que anteriormente había sido designada como administrador delegado.

> **Important**
>
> Al anular el registro de una cuenta, se elimina de forma efectiva la posibilidad de que todos los usuarios administradores administren IAM Identity Center desde esa cuenta. Como resultado, ya no pueden administrar las identidades de IAM Identity Center, la gestión del acceso, la autenticación o el acceso a las aplicaciones desde esta cuenta. Esta operación no afectará a ningún permiso o asignación configurados en el Centro de Identidad de IAM y, por lo tanto, no afectará a los usuarios finales, ya que seguirán teniendo acceso a sus aplicaciones y Cuentas de AWS desde el portal de acceso. AWS

Anulación del registro de una cuenta miembro

1. Inicie sesión AWS Management Console con las credenciales de su cuenta de administración. AWS Organizations Se requieren las credenciales de la cuenta de administración para ejecutar la DeregisterDelegatedAdministratorAPI.
2. Seleccione la región en la que está activado IAM Identity Center y, a continuación, abra la consola de IAM Identity Center.
3. Elija Configuración y, a continuación, seleccione la pestaña Administración.
4. En la sección Administrador delegado, elija Anular el registro de cuenta.
5. En el cuadro de diálogo Anular el registro de cuenta, revise las implicaciones de seguridad y, a continuación, escriba el nombre de la cuenta miembro para confirmar que lo entiende.
6. Elija Anular el registro de la cuenta.

Consulte qué cuenta miembro se ha registrado como administrador delegado

Utilice el siguiente procedimiento para averiguar qué cuenta de miembro de su cuenta se AWS Organizations ha configurado como administrador delegado del Centro de Identidad de IAM.

Cómo ver su cuenta de miembro registrado

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la sección Detalles, busque el nombre de la cuenta registrada en Administrador delegado. También puede encontrar esta información seleccionando la pestaña Administración y consultándola en la sección Administrador delegado.

Acceso elevado temporal

Todo acceso a la suya Cuenta de AWS implica algún nivel de privilegio. Las operaciones delicadas, como cambiar la configuración de un recurso de alto valor, por ejemplo, un entorno de producción, requieren un tratamiento especial debido al alcance y al impacto potencial. El acceso elevado temporal (también conocido como just-in-time acceso) es una forma de solicitar, aprobar y realizar un seguimiento del uso de un permiso para realizar una tarea específica durante un tiempo específico. El acceso elevado temporal complementa otras formas de control de acceso, como los conjuntos de permisos y la autenticación multifactorial.

AWS IAM Identity Center proporciona las siguientes opciones para la administración temporal del acceso elevado en diferentes entornos empresariales y técnicos:

- Soluciones gestionadas y compatibles por el proveedor: AWS ha validado las integraciones del IAM Identity Center con las ofertas de algunos socios y ha evaluado sus capacidades en relación con un conjunto común de requisitos de los clientes. Elija la solución que mejor se adapte a su situación y siga las instrucciones del proveedor para habilitar esta funcionalidad con IAM Identity Center.
- Autogestionado y autosuficiente: esta opción proporciona un punto de partida si está interesado en ampliar temporalmente el acceso a AWS solo una capacidad que pueda implementar, personalizar y mantener por sí mismo. Para obtener más información, consulte Temporary elevated access management (TEAM).

Socios AWS de seguridad validados para un acceso elevado temporal

AWS Los socios de seguridad utilizan diferentes enfoques para abordar un conjunto común de requisitos de acceso elevado temporal. Le recomendamos que revise detenidamente las soluciones de cada socio para poder elegir la que mejor se adapte a sus necesidades y preferencias, incluidas las de su empresa, la arquitectura de su entorno de nube y su presupuesto.

> **Note**
>
> Para la recuperación ante desastres, le recomendamos que configure el acceso de emergencia AWS Management Console antes de que se produzca una interrupción.

AWS Identity ha validado las capacidades y la integración con el IAM Identity Center de las siguientes just-in-time ofertas de AWS Security Partners:

- CyberArk Secure Cloud Access— Como parte de elloCyberArk Identity Security Platform, esta oferta proporciona un acceso elevado bajo demanda AWS y entornos multinube. Las aprobaciones se gestionan mediante la integración con el ITSM o con las herramientas. ChatOps Todas las sesiones se pueden grabar para su auditoría y cumplimiento.
- Tenable (previously Ermetic)— La Tenable plataforma incluye el aprovisionamiento de un acceso just-in-time privilegiado para las operaciones administrativas en AWS entornos multinube. Los registros de sesión de todos los entornos de nube, incluidos los registros de acceso de AWS CloudTrail , están disponibles en una única interfaz para su análisis y auditoría. La capacidad se integra con herramientas empresariales y para desarrolladores, como Slack y Microsoft Teams.
- OktaSolicitudes de acceso: parte del gobierno de la Okta identidad, le permite configurar un flujo de trabajo de solicitudes de just-in-time acceso utilizando Okta como proveedor de identidad externo (IdP) de IAM Identity Center y sus conjuntos de permisos de IAM Identity Center.

Esta lista se actualizará a medida que se AWS validen las capacidades de otras soluciones de socios y la integración de estas soluciones con el IAM Identity Center.

> **Note**
>
> Si utiliza políticas basadas en recursos, Amazon Elastic Kubernetes Service (Amazon EKS AWS Key Management Service) o (Hacer referencia a conjuntos de permisos en las políticas

de recursos, Amazon EKS y AWS KMS)AWS KMS, consulte antes de elegir la solución. just-in-time

Se evaluaron las capacidades de acceso elevado temporal para su validación por parte de los socios AWS

AWS Identity ha comprobado que las capacidades de acceso elevado temporal que ofrecen y las solicitudes de Okta acceso responden a los siguientes requisitos comunes de los clientes: CyberArk Secure Cloud AccessTenable

- Los usuarios pueden solicitar el acceso a un conjunto de permisos durante un período de tiempo especificado por el usuario, especificando la AWS cuenta, el conjunto de permisos, el período de tiempo y el motivo.
- Los usuarios pueden recibir el estado de aprobación de su solicitud.
- Los usuarios no pueden invocar una sesión con un alcance determinado, a menos que haya una solicitud aprobada con el mismo alcance e invoquen la sesión durante el período de tiempo aprobado.
- Hay una forma de especificar quién puede aprobar las solicitudes.
- Los aprobadores no pueden aprobar sus propias solicitudes.
- Los aprobadores tienen una lista de solicitudes pendientes, aprobadas y rechazadas y pueden exportarla para los auditores.
- Los aprobadores pueden aprobar y rechazar las solicitudes pendientes.
- Los aprobadores pueden añadir una nota en la que expliquen su decisión.
- Los aprobadores pueden revocar una solicitud aprobada, lo que impide el uso futuro del acceso elevado.

> **Note**
>
> Si un usuario inicia sesión con acceso restringido cuando se revoca una solicitud aprobada, su sesión permanece activa hasta una hora después de que se revoque la aprobación. Para obtener más información acerca de las sesiones de autenticación, consulte Autenticación.

- Las acciones y aprobaciones de los usuarios están disponibles para su auditoría.

Acceso mediante inicio de sesión único a Cuentas de AWS

Puede asignar permisos a los usuarios de su directorio conectado a la cuenta de administración o a las cuentas de los miembros de su organización en AWS Organizations función de las funciones laborales más comunes. También puede utilizar permisos personalizados para satisfacer sus requisitos de seguridad específicos. Por ejemplo, puede conceder a los administradores de bases de datos permisos amplios a Amazon RDS en las cuentas de desarrollo pero limitar sus permisos en las cuentas de producción. IAM Identity Center configura todos los permisos de usuario necesarios en sus cuentas de Cuentas de AWS de forma automática.

> **Note**
>
> Puede que tengas que conceder permisos a los usuarios o grupos para operar en la cuenta AWS Organizations de administración. Como se trata de una cuenta con muchos privilegios, las restricciones de seguridad adicionales requieren que tengas la FullAccess política de IAM o permisos equivalentes antes de poder configurarla. Estas restricciones de seguridad adicionales no son obligatorias para ninguna de las cuentas de los miembros de su AWS organización.

Asigne el acceso de los usuarios a Cuentas de AWS

Utilice el siguiente procedimiento para asignar el acceso de inicio de sesión único a usuarios y grupos del directorio conectado y para utilizar conjuntos de permisos para determinar su nivel de acceso.

Para comprobar el acceso existente de usuarios y grupos, consulteVea las asignaciones de usuarios y grupos.

> **Note**
>
> Para simplificar la administración de los permisos de acceso, se recomienda asignar el acceso directamente a grupos en lugar de a usuarios individuales. Con los grupos puede conceder o denegar permisos para grupos de usuarios en lugar de asignar esos permisos a cada individuo. Si un usuario se va a otra organización, basta con cambiarlo a un grupo diferente y automáticamente recibirá los permisos necesarios para la nueva organización.

Para asignar el acceso de usuario o grupo a Cuentas de AWS

1. Abra la consola de IAM Identity Center

   > **Note**
   >
   > Antes de continuar con el paso siguiente, compruebe que la consola de IAM Identity Center utiliza alguna de las regiones donde se encuentra su directorio AWS Managed Microsoft AD .

2. En el panel de navegación, en Permisos para varias cuentas, elijaCuentas de AWS.
3. En la página Cuentas de AWS, aparece una lista de su organización en forma de árbol. Seleccione la casilla de verificación situada junto a una o varias Cuentas de AWS a las que desea asignar el acceso de inicio de sesión único.

   > **Note**
   >
   > Puede seleccionar hasta 10 Cuentas de AWS a la vez por conjunto de permisos al asignar el acceso de inicio de sesión único a los usuarios y grupos. Para asignar más de 10 Cuentas de AWS al mismo conjunto de usuarios y grupos, repita este procedimiento según sea necesario para las cuentas adicionales. Cuando se le solicite, seleccione los mismos usuarios, grupos y conjunto de permisos.

4. Seleccione Asignar usuarios o grupos.
5. Para el Paso 1: seleccionar usuarios y grupos, en la página Asignar usuarios y grupos a "***AWS nombre-de-cuenta***", haga lo siguiente:

   1. En la pestaña Usuarios, seleccione uno o más usuarios a los que desee conceder el acceso de inicio de sesión único.

      Para filtrar los resultados, escriba el nombre del usuario que desea en el cuadro de búsqueda.

   2. En la pestaña Grupos, seleccione uno o más grupos a los que desee conceder el acceso de inicio de sesión único.

      Para filtrar los resultados, escriba el nombre del grupo que desea en el cuadro de búsqueda.

   3. Para mostrar los usuarios y grupos que ha seleccionado, elija el triángulo lateral situado junto a Usuarios y grupos seleccionados.

4. Tras confirmar que se haya seleccionado los usuarios y grupos correctos, seleccione Siguiente.

6. Para el paso 2: seleccionar conjuntos de permisos, en la página Asignar conjuntos de permisos a “***AWS-account-name***”, haga lo siguiente:

   1. Seleccione uno o varios conjuntos de permisos. Si es necesario, puede crear y seleccionar nuevos conjuntos de permisos.
      - Para seleccionar uno o más conjuntos de permisos existentes, en Conjuntos de permisos, seleccione los conjuntos de permisos que desee aplicar a los usuarios y grupos que seleccionó en el paso anterior.
      - Para crear uno o más conjuntos de permisos nuevos, elija Crear conjunto de permisos y siga los pasos que se indican en Crea un conjunto de permisos.. Tras crear los conjuntos de permisos que desea aplicar, en la consola de IAM Identity Center, vuelva a las Cuentas de AWS y siga las instrucciones hasta llegar al paso 2: seleccionar conjuntos de permisos. Cuando llegue a este paso, seleccione los nuevos conjuntos de permisos que ha creado y continúe con el siguiente paso de este procedimiento.
   2. Tras confirmar que se haya seleccionado los conjuntos de permisos correctos, seleccione Siguiente.

7. Para el Paso 3: Revisar y enviar, en la página Revisar y enviar las tareas a "***AWS-nombre-de-cuenta***", haga lo siguiente:

   1. Revise los usuarios, grupos y los conjuntos de permisos seleccionados.
   2. Tras confirmar que se haya seleccionado los usuarios, grupos y los conjuntos de permisos correctos, seleccione Enviar.

> **Important**
>
> El proceso de asignación de usuarios y grupos puede tardar unos minutos en completarse. Es importante que deje esta página abierta hasta que se complete el proceso correctamente.

> **Note**
>
> Puede que tenga que conceder permisos a los usuarios o grupos para operar en la cuenta AWS Organizations de administración. Como se trata de una cuenta con

muchos privilegios, las restricciones de seguridad adicionales requieren que tengas la FullAccess política de IAM o permisos equivalentes antes de poder configurarla. Estas restricciones de seguridad adicionales no son obligatorias para ninguna de las cuentas de los miembros de su AWS organización.

Elimine el acceso de usuarios y grupos

Utilice este procedimiento para eliminar el acceso de inicio de sesión único a uno o varios usuarios y grupos del directorio conectado. Cuenta de AWS

Para eliminar el acceso de usuarios y grupos a un Cuenta de AWS

1. Abra la consola de IAM Identity Center.
2. En el panel de navegación, en Permisos para varias cuentas, elijaCuentas de AWS.
3. En la página Cuentas de AWS, aparece una lista de su organización en forma de árbol. Seleccione el nombre Cuenta de AWS que contiene los usuarios y grupos a los que desea eliminar el acceso de inicio de sesión único.
4. En la página de información general de Cuenta de AWS, en Usuarios y grupos asignados, seleccione el nombre de uno o más usuarios o grupos y elija Eliminar el acceso.
5. En el cuadro de diálogo Eliminar el acceso, confirme que los nombres de los usuarios o grupos son correctos y elija Eliminar el acceso.

Revoca las sesiones de roles de IAM activas creadas por conjuntos de permisos

El siguiente es un procedimiento general para revocar una sesión de conjunto de permisos activa para un usuario del IAM Identity Center. El procedimiento parte del supuesto de que se desea eliminar todos los accesos de un usuario cuyas credenciales estén comprometidas o de un usuario fraudulento que se encuentre en el sistema. El requisito previo es haber seguido las instrucciones que figuran en el presente documentoPrepárese para revocar una sesión de rol de IAM activa creada por un conjunto de permisos. Suponemos que la política de denegación total está presente en una política de control de servicios (SCP).

> **Note**
>
> AWS recomienda desarrollar la automatización para gestionar todos los pasos, excepto las operaciones que solo se realizan en la consola.

1. Obtenga el seudónimo de la persona cuyo acceso debe revocar. Puedes usar las API del almacén de identidades para buscar al usuario por su nombre de usuario.
2. Actualice la política de denegación para añadir el ID de usuario del paso 1 de su política de control de servicios (SCP). Tras completar este paso, el usuario objetivo pierde el acceso y no puede realizar ninguna acción con ninguna de las funciones a las que afecte la política.
3. Elimine todas las asignaciones de conjuntos de permisos para el usuario. Si el acceso se asigna mediante la pertenencia a un grupo, elimine al usuario de todos los grupos y de todas las asignaciones directas de conjuntos de permisos. Este paso impide que el usuario asuma funciones de IAM adicionales. Si un usuario tiene una sesión activa en el portal de AWS acceso y usted lo desactiva, podrá seguir asumiendo nuevas funciones hasta que se le quite el acceso.
4. Si usa un proveedor de identidad (IdP) o Microsoft Active Directory como fuente de identidad, deshabilite al usuario en la fuente de identidad. La desactivación del usuario impide la creación de sesiones adicionales en el portal de AWS acceso. Utilice su IdP o la documentación de la API de Microsoft Active Directory para obtener información sobre cómo automatizar este paso. Si utiliza el directorio del Centro de identidades de IAM como fuente de identidad, no desactive todavía el acceso de los usuarios. Inhabilitará el acceso de los usuarios en el paso 6.
5. En la consola del IAM Identity Center, busque al usuario y elimine su sesión activa.

   a. Seleccione Usuarios.

   b. Elija el usuario cuya sesión activa desee eliminar.

   c. En la página de detalles del usuario, selecciona la pestaña Sesiones activas.

   d. Seleccione las casillas de verificación situadas junto a las sesiones que desee eliminar y elija Eliminar sesión.

   Esto garantiza que la sesión del usuario en el portal de AWS acceso se detenga en aproximadamente 60 minutos. Más información sobre la duración de la sesión.
6. En la consola del IAM Identity Center, deshabilite el acceso de los usuarios.

   a. Seleccione Usuarios.

b. Elija el usuario cuyo acceso desee deshabilitar.

c. En la página de detalles del usuario, expanda Información general y pulse el botón Desactivar el acceso del usuario para evitar que el usuario vuelva a iniciar sesión.

7. Deje en vigor la política de denegación durante al menos 12 horas. De lo contrario, el usuario con una sesión de rol de IAM activa habrá restablecido las acciones con el rol de IAM. Si esperas 12 horas, las sesiones activas caducan y el usuario no podrá volver a acceder a la función de IAM.

> **Important**
>
> Si deshabilita el acceso de un usuario antes de detener la sesión de usuario (completó el paso 6 sin completar el paso 5), ya no podrá detener la sesión del usuario a través de la consola del IAM Identity Center. Si inhabilita el acceso del usuario sin darse cuenta antes de detenerla, puede volver a habilitar al usuario, detener su sesión y, a continuación, volver a deshabilitar su acceso.

Ahora puede cambiar las credenciales del usuario si su contraseña se ha visto comprometida y restaurar sus asignaciones.

Delegue quién puede asignar el acceso de inicio de sesión único a los usuarios y grupos de la cuenta de administración

La concesión de acceso de inicio de sesión único a la cuenta de administración utilizando la consola de IAM Identity Center es una acción que requiere privilegios. De forma predeterminada, solo un usuario Usuario raíz de la cuenta de AWS o un usuario que tenga asociadas las políticas IAMFullAccess AWS administradas AWSSSOMasterAccountAdministratory las políticas administradas puede asignar el acceso de inicio de sesión único a la cuenta de administración. Las IAMFullAccesspolíticas AWSSSOMasterAccountAdministratory gestionan el acceso mediante inicio de sesión único a la cuenta de administración de una organización. AWS Organizations

Siga los pasos que se describen a continuación para delegar permisos para administrar el acceso de inicio de sesión único a los usuarios y grupos en su directorio.

Para otorgar permisos para administrar el acceso de inicio de sesión único a los usuarios y grupos del directorio

1. Inicie sesión en la consola de IAM Identity Center como usuario raíz de la cuenta de administración o con otro usuario que tenga permisos de administrador en la cuenta de administración.
2. Siga los pasos que se indican en Crea un conjunto de permisos. para crear un conjunto de permisos y, a continuación, haga lo siguiente:

    1. En la página Crear un conjunto de permisos nuevo, active la casilla Crear un conjunto de permisos personalizado y, a continuación, elija Siguiente: Detalles.
    2. En la página Crear un nuevo conjunto de permisos, especifique un nombre para el conjunto de permisos personalizado y, si lo desea, una descripción. Si es necesario, modifique la duración de la sesión y especifique una URL de estado de retransmisión.

        > **Note**
        >
        > Para la URL del estado de retransmisión, debe especificar una URL que esté en la AWS Management Console. Por ejemplo:
        > **`https://console.aws.amazon.com/ec2/`**
        > Para obtener más información, consulte Configura el estado de retransmisión.

    3. En ¿Qué políticas desea incluir en su conjunto de permisos?, active la casilla Adjuntar políticas administradas de AWS .
    4. En la lista de políticas de IAM, selecciona las políticas gestionadas AWSSSOMasterAccountAdministratory IAMFullAccess AWS las políticas gestionadas. Estas políticas conceden permisos a todos los usuarios a los que se les asigne acceso a este conjunto de permisos en el futuro.
    5. Elija Siguiente: etiquetas.
    6. En Añadir etiquetas (opcional), especifique los valores de clave y valor (opcional) y, a continuación, seleccione Siguiente: revisar. Para obtener más información acerca de las etiquetas, consulte Etiquetado de recursos de AWS IAM Identity Center.
    7. Revise las selecciones y, a continuación, elija Crear.
3. Siga los pasos que se indican en Asigne el acceso de los usuarios a Cuentas de AWS para asignar los usuarios y grupos adecuados al conjunto de permisos que acaba de crear.

4. Comunique lo siguiente a los usuarios asignados: cuando inicien sesión en el portal de AWS acceso y elijan la pestaña Cuentas, deberán elegir el nombre de función adecuado para autenticarse con los permisos que usted acaba de delegar.

Conjuntos de permisos

Un conjunto de permisos es una plantilla que usted crea y mantiene, y que define un conjunto de una o más políticas de IAM. Los conjuntos de permisos simplifican la asignación del Cuenta de AWS acceso a los usuarios y grupos de su organización. Por ejemplo, puede crear un conjunto de permisos de administrador de base de datos que incluya políticas para administrar los servicios de AWS RDS, DynamoDB y Aurora, y usar ese conjunto de permisos único para conceder acceso a una lista de objetivos Cuentas de AWS de su organización a los administradores de AWS bases de datos.

El Centro de identidad de IAM asigna el acceso a un usuario o grupo de uno o más con conjuntos de permisos. Cuentas de AWS Cuando asigna un conjunto de permisos, IAM Identity Center crea los roles de IAM controlados por IAM Identity Center correspondientes en cada cuenta y adjunta a esos roles las políticas especificadas en el conjunto de permisos. El Centro de identidad de IAM administra la función y permite que los usuarios autorizados que haya definido asuman la función mediante el portal de usuarios de IAM Identity Center o la CLI AWS . A medida que modifica el conjunto de permisos, IAM Identity Center garantiza que las políticas y los roles de IAM correspondientes se actualicen en consecuencia.

Puede agregar políticas administradas por AWS, políticas administradas por los clientes, políticas insertadas y políticas administradas por AWS para las funciones de trabajo a sus conjuntos de permisos. También puede asignar una política administrada por AWS o una política administrada por el cliente como límite de permisos.

Para crear un conjunto de permisos, consulte Creación, administración y eliminación de conjuntos de permisos.

Temas

- Permisos predefinidos
- Permisos personalizados
- Creación, administración y eliminación de conjuntos de permisos
- Configure las propiedades del conjunto de permisos

Permisos predefinidos

Puede crear un conjunto de permisos predefinido con políticas AWS gestionadas.

Cuando crea un conjunto de permisos con permisos predefinidos, elige una política de una lista de políticas AWS administradas. Dentro de las políticas disponibles, puede elegir entre políticas de permisos comunes y políticas de funciones de trabajo.

Políticas de permisos comunes

Elija de una lista de políticas AWS administradas que le permitan acceder a los recursos en su totalidad Cuenta de AWS. Puede agregar una de las siguientes políticas:

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

Políticas de funciones de trabajo

Elija de una lista de políticas AWS administradas que le permitan acceder a sus recursos Cuenta de AWS que puedan ser relevantes para un puesto en su organización. Puede agregar una de las siguientes políticas:

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

Para obtener una descripción detallada de las políticas de permisos y las políticas de funciones de trabajo comunes disponibles, consulte políticas administradas de AWS para las funciones de trabajo en la Guía del usuario de AWS Identity and Access Management .

Para obtener instrucciones acerca de cómo crear un conjunto de permisos, consulte Creación, administración y eliminación de conjuntos de permisos.

Permisos personalizados

Puedes crear un conjunto de permisos con permisos personalizados y combinar cualquiera de las políticas AWS administradas y administradas por los clientes que tengas en AWS Identity and Access Management (IAM) con políticas integradas. También puedes incluir el límite de permisos, estableciendo el máximo de permisos posibles que otras políticas pueden conceder a los usuarios de tu conjunto de permisos.

Para obtener instrucciones acerca de cómo crear un conjunto de permisos, consulte Creación, administración y eliminación de conjuntos de permisos.

Tipos de políticas que puede adjuntar a su conjunto de permisos

Temas

- Políticas insertadas
- AWS políticas gestionadas
- Políticas administradas por el cliente
- Límites de permisos

Políticas insertadas

Puede adjuntar una política insertada a un conjunto de permisos. Una política insertada es un bloque de texto con el formato de una política de IAM que se añade directamente al conjunto de permisos. Al crear un conjunto de permisos nuevo, puede pegar una política o generar una nueva con la herramienta de creación de políticas de la consola de IAM Identity Center. También puede crear políticas de IAM con el generador de políticas de AWS.

Al implementar un conjunto de permisos con una política en línea, el Centro de Identidad de IAM crea una política de IAM en la que Cuentas de AWS se asigna el conjunto de permisos. IAM Identity Center crea la política al asignar el conjunto de permisos definido en la cuenta. A continuación, la política se adjunta a la función de IAM Cuenta de AWS que asuma su usuario.

Cuando crea una política en línea y asigna su conjunto de permisos, el Centro de Identidad de IAM configura las políticas propias por usted. Cuentas de AWS Al crear su conjunto de permisosPolíticas administradas por el cliente, debe crear las políticas usted Cuentas de AWS mismo antes de asignar el conjunto de permisos.

AWS políticas gestionadas

Puede adjuntar políticas AWS administradas a su conjunto de permisos. AWS las políticas gestionadas son políticas de IAM que AWS mantiene. Por el contrario, Políticas administradas por el cliente son las políticas de IAM de su cuenta las que usted crea y mantiene. AWS las políticas gestionadas abordan los casos de uso más comunes con privilegios mínimos en su Cuenta de AWS. Puede asignar una política AWS gestionada como permisos para la función que crea IAM Identity Center o como límite de permisos.

AWS mantiene políticas AWS gestionadas para las funciones laborales que asignan permisos de acceso a sus recursos específicos para cada trabajo. AWS Puede agregar una política de función de trabajo si decide utilizar permisos predefinidos con su conjunto de permisos. Al elegir permisos personalizados, puede agregar más de una política de función de trabajo.

Cuenta de AWS También contiene una gran cantidad de políticas de IAM AWS gestionadas para aplicaciones específicas Servicios de AWS y combinaciones de ellas. Servicios de AWS Al crear un conjunto de permisos con permisos personalizados, puede elegir entre muchas políticas AWS gestionadas adicionales para asignarlas a su conjunto de permisos.

AWS rellena cada una de ellas Cuenta de AWS con políticas AWS administradas. Para implementar un conjunto de permisos con políticas AWS administradas, no necesita crear primero una política en su Cuentas de AWS. Al crear su conjunto de permisosPolíticas administradas por el cliente, debe crear las políticas usted Cuentas de AWS mismo antes de asignar el conjunto de permisos.

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

Políticas administradas por el cliente

Puede adjuntar políticas administradas por el cliente a su conjunto de permisos. Las políticas administradas por el cliente son políticas de IAM de su cuenta que usted crea y mantiene. Por el contrario, AWS políticas gestionadas son las políticas de IAM de su cuenta las que se AWS mantienen. Puede asignar una política administrada por el cliente como permisos para el rol que crea IAM Identity Center o como límite de permisos.

Al crear un conjunto de permisos con una política gestionada por el cliente, debe crear una política de IAM con el mismo nombre y la misma ruta en cada uno de los Cuenta de AWS lugares en los que IAM Identity Center asigne el conjunto de permisos. Si va a especificar una ruta personalizada, asegúrese de especificar la misma ruta en cada una de Cuenta de AWS. Para obtener más información, consulte Nombres fáciles de recordar y rutas en la Guía del usuario de IAM. IAM Identity

Center adjunta la política de IAM al rol de IAM que crea en su Cuenta de AWS. Como práctica recomendada, aplique los mismos permisos a la política en cada cuenta a la que asigne el conjunto de permisos. Para obtener más información, consulte Utilice las políticas de IAM en los conjuntos de permisos.

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

Límites de permisos

Puede adjuntar un límite de permisos a su conjunto de permisos. Un límite de permisos es una política de IAM AWS gestionada o gestionada por el cliente que establece los permisos máximos que una política basada en la identidad puede conceder a un responsable de IAM. Cuando aplica un límite de permisos, su Políticas insertadas, Políticas administradas por el cliente y AWS políticas gestionadas no pueden conceder ningún permiso que exceda los permisos que concede su límite de permisos. Un límite de permisos no concede ningún permiso, sino que hace que IAM ignore todos los permisos que exceden límite.

Al crear un conjunto de permisos con una política administrada por el cliente como límite de permisos, debe crear una política de IAM con el mismo nombre en cada Cuenta de AWS donde IAM Identity Center asigne el conjunto de permisos. IAM Identity Center adjunta la política de IAM como límite de permisos al rol de IAM que usted crea en su Cuenta de AWS .

Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

Creación, administración y eliminación de conjuntos de permisos

Los conjuntos de permisos definen el nivel de acceso que tienen los usuarios y grupos en una Cuenta de AWS. Los conjuntos de permisos se almacenan en IAM Identity Center y se pueden aprovisionar a una o varias Cuentas de AWS. Puedes asignar más de un conjunto de permisos a un usuario. Para obtener más información acerca de los conjuntos de permisos y cómo se usan en IAM Identity Center, consulte Conjuntos de permisos.

Tenga en cuenta las siguientes consideraciones al crear conjuntos de permisos:

- Comience con un conjunto de permisos predefinido

  Con un conjunto de permisos predefinido, que utiliza permisos predefinidos, puede elegir una única política AWS gestionada de una lista de políticas disponibles. Cada política otorga un nivel

específico de acceso a AWS los servicios y recursos o permisos para una función laboral común. Para obtener información sobre cada una de estas políticas, consulte Políticas administradas de AWS para funciones de trabajo. Una vez recopilados los datos de uso, puede refinar el conjunto de permisos para que sea más restrictivo.

- Limite la duración de las sesiones de administración a periodos de trabajo razonables

  Cuando los usuarios se federan Cuenta de AWS y utilizan la consola de AWS gestión o la interfaz de línea de AWS comandos (AWS CLI), IAM Identity Center utiliza la configuración de duración de la sesión del conjunto de permisos para controlar la duración de la sesión. Cuando la sesión del usuario alcance la duración de la sesión, se cerrará la sesión de la consola y se le pedirá que vuelva a iniciar sesión. Como práctica recomendada de seguridad, es aconsejable que no defina una duración de la sesión mayor de la que necesita para realizar el rol. De forma predeterminada, el valor de Duración de la sesión es de una hora. Puede especificar un valor máximo de 12 horas. Para obtener más información, consulte Definir la duración de la sesión.
- Limite la duración de las sesiones en el portal de usuarios de la plantilla

  Los usuarios de la plantilla utilizan las sesiones del portal para elegir los roles y acceder a las aplicaciones. De forma predeterminada, el valor de Duración máxima de la sesión, que determina el tiempo que un usuario de la fuerza laboral puede iniciar sesión en el portal de AWS acceso antes de volver a autenticarse, es de ocho horas. Puede especificar un valor máximo de 90 días. Para obtener más información, consulte Configure la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas del IAM Identity Center.
- Utilice el rol que proporcione permisos con privilegios mínimos

  Cada conjunto de permisos que cree y asigne a su usuario aparece como un rol disponible en el portal de AWS acceso. Cuando inicie sesión en el portal en calidad de ese usuario, elija el rol que corresponda al conjunto de permisos más restrictivo que pueda usar para realizar tareas en la cuenta, en lugar de `AdministratorAccess`. Pruebe sus conjuntos de permisos para comprobar que proporcionan el acceso necesario antes de enviar la invitación al usuario.

> **Note**
>
> También puede utilizar AWS CloudFormation para crear y asignar conjuntos de permisos y asignar usuarios a esos conjuntos de permisos.

Temas

- Crea un conjunto de permisos.
- Delegue la administración del conjunto de permisos
- Utilice las políticas de IAM en los conjuntos de permisos
- Borrado de conjuntos de permisos

Crea un conjunto de permisos.

Utilice este procedimiento para crear un conjunto de permisos predefinido que utilice una única política administrada o un conjunto de permisos personalizado de AWS que utilice hasta 10 políticas de AWS administradas o administradas por el cliente y una política integrada. Puede solicitar un ajuste en el número máximo de 10 políticas en la consola Service Quotas para IAM.

Puede crear un conjunto de permisos en la consola de IAM Identity Center.

Para crear un conjunto de permisos

1. Abra la consola de IAM Identity Center
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija Crear conjunto de permisos.
4. En la página Seleccione el tipo de conjunto de permisos, en Tipo de conjunto de permisos, seleccione un tipo.
5. Elija una o más políticas que desee usar para el conjunto de permisos, en característica del tipo de conjunto de permisos:

   - Conjunto de permisos predefinido
     1. En Política para un conjunto de permisos predefinido, seleccione una de las políticas de funciones de IAM Job o Políticas de permisos comunes de la lista y, a continuación, seleccione Siguiente. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas características de trabajo administradas por AWS en la Guía del usuario de AWS Identity and Access Management IAM.
     2. Vaya al paso 6 para completar la página de detalles sobre cómo especificar el conjunto de permisos.
   - Conjunto de permisos personalizado
     1. Elija Siguiente.
     2. En la página Especificar las políticas y los límites de los permisos, elija los tipos de políticas de IAM que desee aplicar a su nuevo conjunto de permisos. De forma predeterminada,

puede añadir cualquier combinación de hasta 10 políticas administradas de AWS y políticas administradas por el cliente a su conjunto de permisos. Esta cuota la establece IAM. Para aprovechar esta cuota, solicite un aumento de la cuota de IAM en las políticas administradas asociadas a un rol de IAM en la consola de Service Quotas para cada Cuenta de AWS en la que desee asignar el conjunto de permisos.

- Amplíe las políticas AWS gestionadas para añadir políticas de IAM que creen AWS y mantengan. Para obtener más información, consulte AWS políticas gestionadas.
  a. Busque y elija las políticas administradas de AWS que desee aplicar a sus usuarios en el conjunto de permisos.
  b. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página de detalles sobre cómo especificar el conjunto de permisos.
- Amplíe las políticas administradas por el cliente para añadir políticas de IAM que usted cree y mantiene. Para obtener más información, consulte Políticas administradas por el cliente.
  a. Elija Adjuntar políticas e introduzca el nombre de la política que desee añadir a su conjunto de permisos. En cada cuenta a la que desee asignar el conjunto de permisos, cree una política con el nombre que ingresó. Como práctica recomendada, asigne los mismos permisos a la política en cada cuenta.
  b. Seleccione Adjuntar más para añadir otra política.
  c. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página de detalles de especificar el conjunto de permisos.
- Amplíe la política en línea para añadir un texto de política personalizado con formato JSON. Las políticas integradas no se corresponden con los recursos de IAM existentes. Para crear una política en línea, introduce un lenguaje de política personalizado en el formulario proporcionado. IAM Identity Center añade la política a los recursos de IAM que crea en las cuentas de sus miembros. Para obtener más información, consulte Políticas insertadas.
  a. Añada las acciones y los recursos que desee en el editor interactivo a su política en línea. Se pueden agregar declaraciones adicionales con Agregar nueva declaración.

b. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página de detalles de especificar el conjunto de permisos.

- Amplíe el límite de permisos para añadir una AWS política de IAM gestionada o gestionada por el cliente como máximo de permisos que pueden asignar las demás políticas del conjunto de permisos. Para obtener más información, consulte Límites de permisos.

  a. Elija Utilizar un límite de permisos para controlar los permisos máximos.

  b. Elija una política administrada por AWS para establecer una política de IAM que AWS cree y mantenga como sus límites de permisos. Elija políticas administradas por el cliente para establecer una política de IAM que usted cree y mantenga como sus límites de permisos.

  c. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página de detalles sobre cómo especificar el conjunto de permisos.

6. En la página Especificar detalles de conjunto de permisos, haga lo siguiente:

   1. En Nombre del conjunto de permisos, escriba un nombre para identificar este conjunto de permisos en IAM Identity Center. El nombre que especifique para este conjunto de permisos aparece en el portal de AWS acceso como un rol disponible. Los usuarios inician sesión en el portal de AWS acceso, eligen un rol y Cuenta de AWS, a continuación, eligen el rol.
   2. (Opcional) También puede introducir una descripción. La descripción solo aparece en la consola del IAM Identity Center, no en el portal de AWS acceso.
   3. (Opcional) Especifique el valor de la duración de la sesión. Este valor determina el tiempo que un usuario puede iniciar sesión antes de que la consola cierre su sesión. Para obtener más información, consulte Definir la duración de la sesión.
   4. (Opcional) Especifique el valor del estado de retransmisión. Este valor se utiliza en el proceso de federación para redirigir a los usuarios dentro de la cuenta. Para obtener más información, consulte Configura el estado de retransmisión.

      > **Note**
      >
      > La URL del estado de retransmisión debe estar dentro de la AWS Management Console. Por ejemplo:

```
https://console.aws.amazon.com/ec2/
```

5. Expanda Etiquetas (opcional), elija Añadir etiqueta, y especifique los valores de Clave y valor (opcional).

   Para obtener más información acerca de las etiquetas, consulte Etiquetado de recursos de AWS IAM Identity Center.

6. Elija Siguiente.

7. En la página Revisar y crear, revise las selecciones que ha realizado y, a continuación, elija Crear.

8. De forma predeterminada, al crear un conjunto de permisos, el conjunto de permisos no se aprovisiona (se usa en ninguno Cuentas de AWS). Para aprovisionar un conjunto de permisos en una Cuenta de AWS, debe asignar el acceso al Centro de Identidad de IAM a los usuarios y grupos de la cuenta y, a continuación, aplicar el conjunto de permisos a esos usuarios y grupos. Para obtener más información, consulte Acceso mediante inicio de sesión único a Cuentas de AWS.

Delegue la administración del conjunto de permisos

IAM Identity Center le permite delegar la administración de los conjuntos de permisos y las asignaciones en las cuentas mediante la creación de políticas de IAM que hacen referencia a los nombres de recursos de Amazon (ARN) de los recursos de IAM Identity Center. Por ejemplo, puede crear políticas que permitan a distintos administradores administrar las asignaciones en cuentas específicas para conjuntos de permisos con etiquetas específicas.

Puede utilizar uno de los siguientes métodos para crear este tipo de políticas.

- (Recomendado) Cree conjuntos de permisos en IAM Identity Center, cada uno con una política diferente, y asigne los conjuntos de permisos a distintos usuarios o grupos. Esto le permite administrar permisos administrativos de los usuarios que inician sesión en el origen de identidad de IAM Identity Center que haya elegido.
- Cree políticas personalizadas en IAM y, a continuación, adjúntelas a los roles de IAM que asuman sus administradores. Para obtener información sobre las características, consulte Roles de IAM para obtener los permisos administrativos que se les han asignado en IAM Identity Center.

> **Important**
>
> Los ARN de recursos de IAM Identity Center distinguen entre mayúsculas y minúsculas

A continuación, se muestra el caso adecuado para hacer referencia al conjunto de permisos y los tipos de recursos de la cuenta de IAM Identity Center.

Tipos de recursos	ARN	Claves de contexto
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
Cuenta	`arn:${Partition}:sso:::account/${AccountId}`	No aplicable

Utilice las políticas de IAM en los conjuntos de permisos

En Crea un conjunto de permisos., aprendió a añadir políticas, incluidas las políticas administradas por el cliente y los límites de permisos, a un conjunto de permisos. Al añadir políticas y permisos administrados por el cliente a un conjunto de permisos, IAM Identity Center no crea ninguna política en Cuentas de AWS. En su lugar, debe crear esas políticas por adelantado en cada cuenta a la que desee asignar su conjunto de permisos y hacerlas coincidir con las especificaciones de nombre y ruta de su conjunto de permisos. Al asignar un conjunto de permisos a un Cuenta de AWS miembro de su organización, el Centro de Identidad de IAM crea un rol AWS Identity and Access Management (IAM) y asocia sus políticas de IAM a ese rol.

> **Note**
>
> Antes de asignar el conjunto de permisos a las políticas de IAM, debe preparar su cuenta de miembro. El nombre de una política de IAM de su cuenta de miembro debe coincidir con el nombre de la política de su cuenta de administración, distinguiendo mayúsculas de minúsculas. IAM Identity Center no puede asignar el conjunto de permisos si la política no existe en su cuenta de miembro.

Los permisos que otorga la política no tienen por qué coincidir exactamente entre las cuentas.

Cómo asignar una política de IAM a un conjunto de permisos

1. Cree una política de IAM en cada uno de los lugares a los Cuentas de AWS que desee asignar el conjunto de permisos.
2. Asignar permisos a la política de IAM. Puede asignar diferentes permisos en diferentes cuentas. Para disfrutar de una experiencia coherente, configure y mantenga permisos idénticos en cada política. Puedes usar recursos de automatización, por ejemplo, AWS CloudFormation StackSets para crear copias de una política de IAM con el mismo nombre y permisos en cada cuenta de miembro. Para obtener más información al respecto CloudFormation StackSets, consulte Cómo trabajar con ella AWS CloudFormation StackSets en la guía del AWS CloudFormation usuario.
3. Cree un conjunto de permisos en su cuenta de administración y añada su política de IAM a las políticas administradas por el cliente o al límite de permisos. Para obtener más información sobre cómo crear un conjunto de permisos, consulte Crea un conjunto de permisos..
4. Añada cualquier política integrada, política administrada por AWS o política de IAM adicional que haya preparado.
5. Cree y asigne su conjunto de permisos.

Borrado de conjuntos de permisos

Si desea revocar una sesión de conjunto de permisos activa, consulteRevoca las sesiones de roles de IAM activas creadas por conjuntos de permisos.

Antes de poder eliminar un conjunto de permisos de IAM Identity Center, debe eliminarlo de todas las Cuentas de AWS que utilizan el conjunto de permisos. Para comprobar el acceso existente de usuarios y grupos, consulteVea las asignaciones de usuarios y grupos.

Para eliminar un conjunto de permisos de un Cuenta de AWS

1. Abra la consola de IAM Identity Center
2. En Permisos para varias cuentas, elija Cuentas de AWS.
3. En la página Cuentas de AWS, aparece una lista de su organización en forma de árbol. Seleccione el nombre Cuenta de AWS del que desea eliminar el conjunto de permisos.

4. En la página de descripción general del Cuenta de AWS, seleccione la pestaña Conjuntos de permisos.
5. Seleccione la casilla de verificación junto a los permisos que desee eliminar y, a continuación, elija Eliminar.
6. En el cuadro de diálogo Eliminar conjunto de permisos, confirme que se ha seleccionado el conjunto de permisos correcto, escriba **`Delete`** para confirmar la eliminación y, a continuación, seleccione Eliminar acceso.

Utilice el siguiente procedimiento para eliminar uno o más conjuntos de permisos, de modo que ningún miembro de la organización pueda utilizarlos. Cuenta de AWS

> **Note**
>
> Todos los usuarios y grupos a los que se haya asignado este conjunto de permisos, independientemente de quién lo utilice, ya no podrán iniciar sesión. Cuenta de AWS Para comprobar el acceso existente de usuarios y grupos, consulteVea las asignaciones de usuarios y grupos.

Para eliminar un conjunto de permisos de un Cuenta de AWS

1. Abra la consola de IAM Identity Center
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Seleccione el conjunto de permisos que desea eliminar y, a continuación, elija Eliminar.
4. En el cuadro de diálogo Eliminar conjunto de permisos, escriba el nombre del conjunto de permisos para confirmar la eliminación y, a continuación, seleccione Eliminar. El nombre distingue entre mayúsculas y minúsculas.

Configure las propiedades del conjunto de permisos

En IAM Identity Center, puede personalizar la experiencia del usuario configurando las siguientes propiedades del conjunto de permisos.

Temas

- Definir la duración de la sesión

- Configura el estado de retransmisión
- Usa una política de denegación para revocar los permisos de usuario activos

Definir la duración de la sesión

Para cada conjunto de permisos, puede especificar una duración de la sesión para controlar el tiempo durante el cual un usuario puede iniciar sesión en una cuenta de Cuenta de AWS. Cuando transcurra la duración especificada, AWS cierra la sesión del usuario.

Al crear un nuevo conjunto de permisos, la duración de la sesión se establece de forma predeterminada en una hora (en segundos). La duración mínima de la sesión es de una hora y se puede establecer en un máximo de 12 horas. IAM Identity Center crea automáticamente características de IAM en cada cuenta asignada para cada conjunto de permisos y las configura con una duración máxima de sesión de 12 horas.

Cuando los usuarios se federan en su Cuenta de AWS consola o cuando se utiliza el AWS Command Line Interface (AWS CLI), el Centro de Identidad de IAM utiliza la configuración de duración de la sesión del conjunto de permisos para controlar la duración de la sesión. De forma predeterminada, los roles de IAM generados por IAM Identity Center para los conjuntos de permisos solo los pueden asumir los usuarios de IAM Identity Center, lo que garantiza que se cumpla la duración de sesión especificada en el conjunto de permisos de IAM Identity Center.

> **Important**
>
> Como práctica recomendada de seguridad, es aconsejable que no defina una duración de la sesión mayor de la que necesita para realizar el rol.

Una vez que se ha creado un conjunto de permisos, puede actualizarlo para aplicar una nueva duración de la sesión. Utilice el siguiente procedimiento para modificar la duración de la sesión para un conjunto de permisos.

Para definir la duración de la sesión

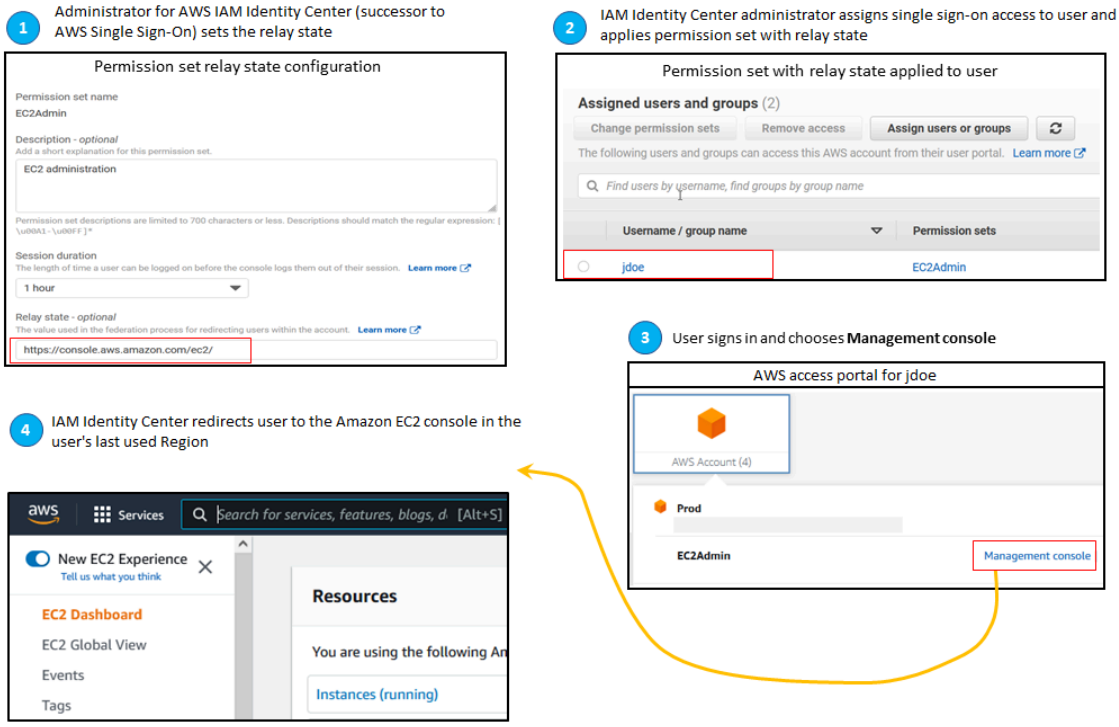
1. Abra la consola de IAM Identity Center
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija el nombre del conjunto de permisos para el que desea cambiar la duración de la sesión.

4. En la página de detalles del conjunto de permisos, a la derecha del encabezado de la sección Configuración general, elija Editar.
5. En la página Editar la configuración general del conjunto de permisos, elija un nuevo valor para la duración de la sesión.
6. Si el conjunto de permisos está aprovisionado en alguno Cuentas de AWS, los nombres de las cuentas aparecen en Para volver Cuentas de AWS a aprovisionarse automáticamente. Una vez actualizado el valor de duración de la sesión del conjunto de permisos, se vuelve a aprovisionar a todas las personas Cuentas de AWS que utilizan el conjunto de permisos. Esto significa que el nuevo valor de esta configuración se aplica a todos los Cuentas de AWS que usen el conjunto de permisos.
7. Elija Guardar cambios.
8. En la parte superior de la página de Cuentas de AWS, aparece una notificación.

    - Si el conjunto de permisos está aprovisionado en una o varias Cuentas de AWS, la notificación confirma que las Cuentas de AWS se han reaprovisionado correctamente y que el conjunto de permisos actualizado se ha aplicado a las cuentas.
    - Si el conjunto de permisos no está aprovisionado en una Cuenta de AWS, la notificación confirma que se actualizó la configuración del conjunto de permisos.

Configura el estado de retransmisión

De forma predeterminada, cuando un usuario inicia sesión en el portal de AWS acceso, elige una cuenta y, a continuación, elige el rol que AWS crea a partir del conjunto de permisos asignado, el Centro de Identidad de IAM redirige el navegador del usuario al. AWS Management Console Puede cambiar este comportamiento si configura el estado de retransmisión en la URL de una consola diferente. La configuración del estado de la retransmisión permite proporcionar al usuario un acceso rápido a la consola más adecuada para su rol. Por ejemplo, puede establecer el estado de retransmisión en la URL de la consola de Amazon EC2 (**`https://console.aws.amazon.com/ec2/`**) para redirigir al usuario a esa consola cuando elija el rol de administrador de Amazon EC2. Durante el redireccionamiento a la URL predeterminada o a la URL del estado de retransmisión, el Centro de Identidad de IAM dirige el navegador del usuario al punto final de la consola, en el último lugar Región de AWS utilizado por el usuario. Por ejemplo, si un usuario finalizó la última sesión de su consola en la región de Europa (Estocolmo) (eu-north-1), se redirige al usuario a la consola Amazon EC2 de esa región.



Para configurar IAM Identity Center para que redirija al usuario a una consola en una Región de AWS específica, incluya la especificación de la región como parte de la URL. Por ejemplo, para redirigir al usuario a la consola de Amazon EC2 en la región Este de EE. UU. (Ohio) (us-east-2), especifique la URL de la consola de Amazon EC2 en esa región (**`https://us-east-2.console.aws.amazon.com/ec2/`**). Si ha habilitado IAM Identity Center en la región Oeste de EE. UU. (Oregón) (us-west-2) y desea dirigir al usuario a esa región, especifique **`https://us-west-2.console.aws.amazon.com`**.

Utilice el siguiente procedimiento para configurar la URL del estado de retransmisión de un conjunto de permisos.

Cómo configurar el estado de la retransmisión

1. Abra la consola de IAM Identity Center
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija el nombre del conjunto de permisos para el que desea configurar la nueva URL de estado de retransmisión.
4. En la página de detalles del conjunto de permisos, a la derecha del encabezado de la sección Configuración general, elija Editar.

5. En la página Editar la configuración general del conjunto de permisos, en Estado de retransmisión, escriba la URL de la consola para cualquiera de los AWS servicios. Por ejemplo:

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > La URL del estado de retransmisión debe estar dentro de la AWS Management Console.

6. Si el conjunto de permisos está aprovisionado en alguno Cuentas de AWS, los nombres de las cuentas aparecen en Cuentas de AWS Para volver a aprovisionarse automáticamente. Una vez actualizada la URL del estado de retransmisión del conjunto de permisos, se vuelve a aprovisionar a todas las personas Cuentas de AWS que utilizan el conjunto de permisos. Esto significa que el nuevo valor de esta configuración se aplica a todos los Cuentas de AWS que usen el conjunto de permisos.
7. Elija Guardar cambios.
8. En la parte superior de la página de organización de AWS , aparece una notificación.

   - Si el conjunto de permisos está aprovisionado en una o varias Cuentas de AWS, la notificación confirma que las Cuentas de AWS se han reaprovisionado correctamente y que el conjunto de permisos actualizado se ha aplicado a las cuentas.
   - Si el conjunto de permisos no está aprovisionado en una Cuenta de AWS, la notificación confirma que se actualizó la configuración del conjunto de permisos.

> **Note**
>
> Puedes automatizar este proceso mediante la AWS API, un AWS SDK o el AWS Command Line Interface(AWS CLI). Para obtener más información, consulte:
>
> - Las acciones `CreatePermissionSet` o `UpdatePermissionSet` de la referencia de la API de IAM Identity Center
> - Los comandos `create-permission-set` o `update-permission-set` de la sección sso-admin de la Referencia de comandos de AWS CLI .

Usa una política de denegación para revocar los permisos de usuario activos

Es posible que tenga que revocar el acceso de un usuario del Centro de Identidad de IAM Cuentas de AWS mientras el usuario esté utilizando activamente un conjunto de permisos. Puedes quitarle la posibilidad de usar sus sesiones de rol de IAM activas implementando una política de denegación para un usuario no especificado con antelación y, cuando sea necesario, puedes actualizar la política de denegación para especificar el usuario cuyo acceso deseas bloquear. En este tema se explica cómo crear una política de denegación y las consideraciones sobre cómo implementarla.

Prepárese para revocar una sesión de rol de IAM activa creada por un conjunto de permisos

Puede impedir que el usuario tome medidas con una función de IAM que esté utilizando activamente aplicando una política de denegación de acceso total a un usuario específico mediante el uso de una política de control de servicios. También puede impedir que un usuario utilice cualquier conjunto de permisos hasta que cambie su contraseña, lo que evita que un usuario malintencionado o haga un uso indebido de credenciales robadas. Si necesita denegar el acceso de forma generalizada e impedir que un usuario vuelva a entrar en un conjunto de permisos o acceda a otros conjuntos de permisos, también puede eliminar todos los accesos de los usuarios, detener la sesión activa del portal de AWS acceso e inhabilitar el inicio de sesión del usuario. Consulte Revoca las sesiones de roles de IAM activas creadas por conjuntos de permisos para obtener información sobre cómo usar la política de denegación junto con acciones adicionales para una revocación de acceso más amplia.

Política de denegación

Puede utilizar una política de denegación con una condición que coincida con la del usuario en el almacén `UserID` de identidades del Centro de Identidad de IAM para evitar que una función de IAM que el usuario esté utilizando activamente lleve a cabo nuevas acciones. El uso de esta política evita que otros usuarios puedan estar utilizando el mismo conjunto de permisos al implementar la política de denegación. Esta política utiliza el seudónimo *`Add user ID here`*, `"identitystore:userId"` que debes actualizar con el seudónimo al que deseas revocar el acceso.

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

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
                }
            }
        }
    ]
}
```

Aunque puedes usar otra clave de condición, por ejemplo“`aws:userId`”, “`identitystore:userId`” es cierto que se trata de un valor único a nivel mundial que está asociado a una persona. El uso de esta condición puede verse afectado por la forma “`aws:userId`” en que se sincronizan los atributos del usuario con respecto a la fuente de identidades y puede cambiar si el nombre de usuario o la dirección de correo electrónico del usuario cambian.

En la consola del IAM Identity Center, puede buscar el nombre de un usuario. Para `identitystore:userId` ello, vaya a Usuarios, busque el usuario por su nombre, amplíe la sección de información general y copie el seudónimo. También es práctico detener la sesión del portal de AWS acceso de un usuario e inhabilitar su acceso de inicio de sesión en la misma sección mientras busca el seudónimo. Para automatizar el proceso de creación de una política de denegación, obtenga el seudónimo del usuario consultando las API del almacén de identidades.

Implementación de la política de denegación

Puede utilizar un seudónimo que no sea válido, por ejemplo*`Add user ID here`*, para implementar la política de denegación por anticipado mediante una política de control de servicios (SCP) que adjunte a Cuentas de AWS los usuarios a la que puedan tener acceso. Este es el enfoque recomendado por su facilidad y rapidez de impacto. Cuando revoques el acceso de un usuario con la política de denegación, editarás la política para reemplazar el seudónimo por el seudónimo de la persona cuyo acceso deseas revocar. Esto impide que el usuario realice ninguna acción con los permisos establecidos en todas las cuentas que asocie al SCP. Bloquea las acciones del usuario incluso si utiliza su sesión activa en el portal de AWS acceso para navegar a diferentes cuentas y asumir funciones diferentes. Con el acceso del usuario totalmente bloqueado por el SCP, puede deshabilitar su capacidad de iniciar sesión, revocar sus asignaciones y detener su sesión en el portal de AWS acceso si es necesario.

Como alternativa al uso de los SCP, también puede incluir la política de denegación en la política integrada de conjuntos de permisos y en las políticas gestionadas por los clientes que utilizan los conjuntos de permisos a los que el usuario puede acceder.

Si debe revocar el acceso a más de una persona, puede utilizar una lista de valores en el bloque de condiciones, como:

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> Independientemente del método o los métodos que utilices, debes tomar cualquier otra medida correctiva y mantener el seudónimo del usuario en la política durante al menos 12 horas. Transcurrido ese tiempo, todas las funciones que el usuario haya asumido caducarán y, a continuación, podrá eliminar su seudónimo de la política de denegación.

Hacer referencia a conjuntos de permisos en las políticas de recursos, Amazon EKS y AWS KMS

Al asignar un conjunto de permisos a una AWS cuenta, el Centro de Identidad de IAM crea un rol con un nombre que comienza por. `AWSReservedSSO_`

El nombre completo y el nombre de recurso de Amazon (ARN) del rol utilizan el siguiente formato:

Nombre	ARN
`AWSReservedSSO_` *permission-set-name_unique-suffix*	`arn:aws:iam::` *aws-account-ID*`:role/aws-reserved/sso.amazonaws.com/` *aws-region* `/AWSReservedSSO_` *permission-set-name_unique-suffix*

Por ejemplo, si crea un conjunto de permisos que concede acceso a la AWS cuenta a los administradores de bases de datos, se crea el rol correspondiente con el siguiente nombre y ARN:

Nombre	ARN
`AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`

Si elimina todas las asignaciones a este conjunto de permisos de la AWS cuenta, también se eliminará el rol correspondiente que creó IAM Identity Center. Si más adelante realiza una nueva asignación al mismo conjunto de permisos, IAM Identity Center crea un nuevo rol para el conjunto de permisos. El nombre y el ARN del nuevo rol incluyen un sufijo diferente y único. En este ejemplo, el sufijo único es abcdef0123456789.

Nombre	ARN
`AWSReservedSSO_DatabaseAdministrator_` **`abcdef0123456789`**	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_` **`abcdef0123456789`**

El cambio de sufijo en el nuevo nombre y ARN del rol provocará que cualquier política que haga referencia al nombre y al ARN originales lo out-of-date sea, lo que interrumpirá el acceso de las personas que usen el conjunto de permisos correspondiente. Por ejemplo, un cambio en el ARN del rol interrumpirá el acceso de los usuarios del conjunto de permisos si se hace referencia al ARN original en las siguientes configuraciones:

- En el fichero `aws-auth ConfigMap` para Amazon Elastic Kubernetes Service (Amazon EKS)
- En una política basada en recursos para una clave (). AWS Key Management Service AWS KMS Esta política también se denomina política de claves.

Si bien puede actualizar las políticas basadas en recursos de la mayoría de AWS los servicios para que hagan referencia a un nuevo ARN para un rol que corresponda a un conjunto de permisos, debe tener un rol de respaldo que cree en IAM para Amazon EKS si AWS KMS el ARN cambia. En el caso de Amazon EKS, el rol de IAM de respaldo debe existir en `aws-auth ConfigMap`. Para AWS KMS, debe existir en sus políticas de claves. Si no tiene un rol de IAM de respaldo en ninguno de los 2 casos, debe ponerse en contacto con AWS Support.

Recomendaciones para evitar interrupciones en el acceso

Para evitar interrupciones en el acceso debido a cambios en el ARN de un rol que corresponde a un conjunto de permisos, le recomendamos que haga lo siguiente.

- Mantenga al menos una asignación de conjunto de permisos.

  Mantenga esta asignación en las AWS cuentas que contienen las funciones a las que hace referencia en Amazon EKS, en las políticas clave o en AWS KMS las políticas basadas en recursos para otras. `aws-auth ConfigMap` Servicios de AWS

  Por ejemplo, si crea un conjunto de `EKSAccess` permisos y hace referencia al ARN de rol correspondiente desde la AWS cuenta`111122223333`, asigna permanentemente un grupo administrativo al conjunto de permisos de esa cuenta. Como la asignación es permanente, IAM Identity Center no eliminará el rol correspondiente, lo que elimina el riesgo de cambiar el nombre. El grupo administrativo siempre tendrá acceso sin correr el riesgo de que se incrementen los privilegios.
- Para Amazon EKS y AWS KMS: incluya un rol creado en IAM.

  Si hace referencia a los ARN de los roles para los conjuntos de permisos de una `aws-auth ConfigMap` para un clúster de Amazon EKS o en las políticas clave para las claves de AWS KMS , le recomendamos que también incluya al menos un rol que cree en IAM. El rol debe permitirle acceder al clúster de Amazon EKS o administrar la política AWS KMS clave. El conjunto de permisos debe poder asumir este rol. De esta forma, si el ARN del rol de un conjunto de permisos cambia, puede actualizar la referencia al ARN en la `aws-auth ConfigMap` política clave o. AWS KMS En la siguiente sección, se proporciona un ejemplo de cómo se puede crear una política de confianza para un rol creado en IAM. El rol solo lo puede asumir un conjunto de permisos de `AdministratorAccess`.

Ejemplo de políticas de confianza personalizadas

A continuación se muestra un ejemplo de una política de confianza personalizada que proporciona un conjunto de `AdministratorAccess` permisos con acceso a un rol creado en IAM. Entre los elementos clave de esta base, se incluyen los siguientes:

- El elemento principal de esta política de confianza especifica el principal de una AWS cuenta. En esta política, los directores de la AWS cuenta `111122223333` con `sts:AssumeRole` permisos pueden asumir la función que se creó en IAM.
- El `Condition element` de esta política de confianza especifica requisitos adicionales para las entidades principales que pueden asumir el rol creado en IAM. En esta política, el conjunto de permisos con el siguiente rol ARN puede asumir el rol.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> El elemento `Condition` incluye el operador de condiciones `ArnLike` y utiliza un comodín al final del ARN del rol de permisos, en lugar de un sufijo único. Esto significa que la política permite que el conjunto de permisos asuma el rol creado en IAM incluso si el ARN del rol del conjunto de permisos cambia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
```

```
    }
  ]
}
```

La inclusión de un rol que cree en IAM en dicha política le proporcionará acceso de emergencia a sus clústeres de Amazon EKS u otros AWS recursos si un conjunto de permisos o todas las asignaciones al conjunto de permisos se eliminan y se vuelven a crear accidentalmente. AWS KMS keys

Control de acceso basado en atributos

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. Puede utilizar el Centro de Identidad de IAM para gestionar el acceso a sus AWS recursos a través de varios Cuentas de AWS atributos de usuario que procedan de cualquier fuente de identidad del Centro de Identidad de IAM. En AWS, estos atributos se denominan etiquetas. El uso de los atributos de usuario como etiquetas le AWS ayuda a simplificar el proceso de creación de permisos detallados AWS y garantiza que sus empleados solo tengan acceso a AWS los recursos con las etiquetas correspondientes.

Por ejemplo, puede asignar a los desarrolladores Bob y Sally, que pertenecen a 2 equipos diferentes, el mismo conjunto de permisos en IAM Identity Center y, a continuación, seleccionar el atributo del nombre del equipo para controlar el acceso. Cuando Bob y Sally inician sesión en su Cuentas de AWS, el Centro de Identidad de IAM envía el atributo del nombre del equipo en la AWS sesión para que Bob y Sally solo puedan acceder a los recursos AWS del proyecto si el atributo del nombre del equipo coincide con la etiqueta del nombre del equipo del recurso del proyecto. Si Bob se pasa al equipo de Sally en el futuro, puede modificar su acceso simplemente actualizando el atributo de nombre de su equipo en el directorio corporativo. La próxima vez que Bob inicie sesión, tendrá acceso automáticamente a los recursos del proyecto de su nuevo equipo sin necesidad de actualizar los permisos de AWS.

Este enfoque también ayuda a reducir el número de permisos distintos que hay que crear y gestionar en IAM Identity Center, ya que los usuarios asociados a los mismos conjuntos de permisos ahora pueden tener permisos únicos en característica de sus atributos. Puede utilizar estos atributos de usuario en los conjuntos de permisos y las políticas basadas en recursos del Centro de Identidad de IAM para implementar el ABAC en los recursos y simplificar la gestión de permisos a gran escala AWS .

Ventajas

Las siguientes son ventajas adicionales del uso de ABAC en IAM Identity Center.

- ABAC requiere menos conjuntos de permisos: dado que no tiene que crear diferentes políticas para diferentes roles de trabajo, debe crear menos conjuntos de permisos. Esto reduce la complejidad de la administración de permisos.
- Con ABAC, los equipos pueden cambiar y crecer rápidamente: los permisos para los nuevos recursos se conceden automáticamente en característica de los atributos cuando los recursos se etiquetan adecuadamente al crearlos.
- Utilice los atributos de los empleados de su directorio corporativo con ABAC: puede utilizar los atributos de los empleados existentes de cualquier fuente de identidad configurada en IAM Identity Center para tomar decisiones de control de acceso en AWS.
- AWS CloudTrail Controle quién accede a los recursos: los administradores de seguridad pueden determinar fácilmente la identidad de una sesión al revisar los atributos del usuario para realizar un seguimiento de la actividad de los usuarios. AWS

Para obtener información acerca de cómo configurar ABAC mediante la consola de IAM Identity Center, consulte Atributos para controlar el acceso. Para obtener información sobre cómo habilitar y configurar ABAC mediante las API del IAM Identity Center, consulte la Guía de referencia de CreateInstanceAccessControlAttributeConfigurationlas API del IAM Identity Center.

Temas

- Lista de comprobación: configurar ABAC mediante el IAM Identity Center AWS
- Atributos para controlar el acceso

Lista de comprobación: configurar ABAC mediante el IAM Identity Center AWS

Esta lista de comprobación incluye las tareas de configuración necesarias para preparar los recursos de AWS y configurar IAM Identity Center para el acceso a ABAC. Completar las tareas en esta lista de verificación en orden. Cuando un enlace de referencia lo lleve a un tema, vuelva a ese tema para poder continuar con el resto de las tareas de esta lista de verificación.

Paso	Tarea	Referencia
1	Revise cómo añadir etiquetas a todos sus recursos. AWS Para implementar ABAC en IAM Identity Center, primero tendrá que añadir etiquetas a todos los recursos de AWS en los que desee implementar ABAC.	• Etiquetar recursos AWS
2	Revise cómo configurar su origen de identidad en IAM Identity Center con las identidades y los atributos de usuario asociados en su almacén de identidades. El Centro de Identidad de IAM le permite utilizar los atributos de usuario de cualquier fuente de identidad del Centro de Identidad de IAM compatible para ABAC in. AWS	• Administre su fuente de identidad
3	En función de los siguientes criterios, determine qué atributos desea utilizar para tomar decisiones de control de acceso AWS y envíelos al IAM Identity Center.	• Introducción
	• Si utiliza un proveedor de identidades (IdP) externo, decida si desea utilizar los atributos transferidos desde el IdP o seleccionar los atributos de IAM Identity Center.	• Elección de los atributos al utilizar un proveedor de identidades externo como fuente de identidad
	• Si elige que su IdP envíe atributos, configure su IdP para que transmita los atributos en las aserciones de SAML. Consulte las `Optional` secciones del tutorial correspondientes a su IdP específico.	• Tutoriales de introducción
	• Si utiliza un IdP como fuente de identidad y elige seleccionar atributos en IAM Identity Center, averigüe cómo configurar el SCIM para que los valores de los atributos procedan de su IdP. Si no puede utilizar SCIM con su IdP, añada los usuarios y sus atributos mediante la página de usuario de la consola de IAM Identity Center.	• Aprovisionamiento estático • Atributos de proveedor es de identidad externos compatibles

Paso	Tarea	Referencia
	• Si utiliza Active Directory o IAM Identity Center como fuente de identidad, o si utiliza un IdP y elige seleccionar atributos en IAM Identity Center, revise los atributos disponibles que puede configurar. A continuación, vaya inmediatamente al paso 4 para empezar a configurar los atributos de ABAC mediante la consola de IAM Identity Center.	• Elección de los atributos al utilizar IAM Identity Center como fuente de identidad • Elección de los atributos al utilizar AWS Managed Microsoft AD como origen de identidad • Asignaciones predeterminadas
4	Seleccione los atributos que desee utilizar para ABAC en la página Atributos para el control de acceso de la consola de IAM Identity Center. En esta página, puede seleccionar los atributos para el control de acceso desde el origen de identidad que configuró en el paso 2. Una vez que sus identidades y sus atributos estén en el Centro de identidades de IAM, debe crear pares clave-valor (mapeos) que se le transferirán Cuentas de AWS para que los utilice en las decisiones de control de acceso.	• Habilitación y configuración de atributos para el control de acceso
5	Cree políticas de permisos personalizadas dentro de su conjunto de permisos y utilice los atributos de control de acceso para crear reglas ABAC, de modo que los usuarios solo puedan acceder a los recursos con etiquetas coincidentes. Los atributos de usuario que configuró en el paso 4 se utilizan como etiquetas en AWS para tomar decisiones sobre el control de acceso. Puede hacer referencia a los atributos de control de acceso en la política de permisos mediante la condición `aws:PrincipalTag/key` .	• Crear políticas de permisos para ABAC en IAM Identity Center

Paso	Tarea	Referencia
6	En sus archivos Cuentas de AWS, asigne los usuarios a los conjuntos de permisos que creó en el paso 5. De este modo, se garantiza que, cuando se federen en sus cuentas y accedan a AWS los recursos, solo obtengan acceso en función de las etiquetas coincidentes.	• Asigne el acceso de los usuarios a Cuentas de AWS

Tras completar estos pasos, los usuarios que se federen en un único inicio Cuenta de AWS de sesión tendrán acceso a sus AWS recursos en función de los atributos coincidentes.

Atributos para controlar el acceso

Atributos para el control de acceso es el nombre de la página de la consola de IAM Identity Center en la que se seleccionan los atributos de usuario que se quieren utilizar en las políticas para controlar el acceso a los recursos. Puedes asignar usuarios a las cargas de trabajo en AWS función de los atributos existentes en la fuente de identidad de los usuarios.

Por ejemplo, suponga que desea asignar acceso a los buckets de S3 en característica de los nombres de los departamentos. En la página Atributos para el control de acceso, seleccione el atributo de usuario Departamento para su uso con el control de acceso basado en atributos (ABAC). En el conjunto de permisos de IAM Identity Center, escriba una política que conceda acceso a los usuarios solo cuando el atributo Departmento coincida con la etiqueta de departamento que asignó a sus buckets de S3. IAM Identity Center transfiere el atributo de departamento del usuario a la cuenta a la que se accede. A continuación, el atributo se utiliza para determinar el acceso en característica de la política. Para obtener más información acerca de PITR, consulte Control de acceso basado en atributos.

Introducción

La forma de empezar a configurar los atributos para el control de acceso depende del origen de identidad que utilice. Independientemente del origen de identidad que elija, una vez seleccionados los atributos, tendrá que crear o editar las políticas de conjuntos de permisos. Estas políticas deben permitir que las identidades de los usuarios accedan a los recursos de AWS .

Elección de los atributos al utilizar IAM Identity Center como fuente de identidad

Al configurar IAM Identity Center como fuente de identidad, primero se añaden los usuarios y se configuran sus atributos. A continuación, vaya a la página Atributos para el control de acceso y

seleccione los atributos que desee utilizar en las políticas. Por último, navegue hasta la página Cuentas de AWS para crear o editar conjuntos de permisos para usar los atributos de ABAC.

Elección de los atributos al utilizar AWS Managed Microsoft AD como origen de identidad

Al configurar el Centro de identidades de IAM AWS Managed Microsoft AD como fuente de identidad, primero se asigna un conjunto de atributos de Active Directory a los atributos de usuario del Centro de identidades de IAM. A continuación, vaya a la página de atributos para el control de acceso. A continuación, elija los atributos que desee utilizar en la configuración de ABAC en característica del conjunto existente de atributos de SSO mapeados desde Active Directory. Por último, cree reglas de ABAC utilizando los atributos de control de acceso de los conjuntos de permisos para permitir que las identidades de los usuarios accedan a los recursos de AWS . Para obtener una lista de las asignaciones predeterminadas de los atributos de usuario del Centro de identidades de IAM a los atributos de usuario de su directorio, consulte. AWS Managed Microsoft AD Asignaciones predeterminadas

Elección de los atributos al utilizar un proveedor de identidades externo como fuente de identidad

Al configurar IAM Identity Center con un proveedor de identidades (IdP) externo como origen de identidad, hay 2 formas de utilizar los atributos de ABAC.

- Puede configurar su IdP para que envíe los atributos mediante aserciones de SAML. En este caso, IAM Identity Center transfiere el nombre y el valor del atributo desde el IdP para la evaluación de la política.

  > **Note**
  >
  > Los atributos de las aserciones de SAML no estarán visibles en la página Atributos para el control de acceso. Deberá conocer estos atributos con antelación y añadirlos a las reglas de control de acceso al crear políticas. Si decide confiar en los atributos externos IdPs , estos atributos siempre se transferirán cuando los usuarios se federen en ellos. Cuentas de AWS En situaciones en las que los mismos atributos llegan a IAM Identity Center a través de SAML y SCIM, el valor de los atributos de SAML prevalece en las decisiones de control de acceso.

- Puede configurar los atributos que utilizará en la página Atributos para el control de acceso de la consola de IAM Identity Center. Los valores de atributos que elija aquí sustituyen a los valores de cualquier atributo coincidente que provenga de un IdP a través de una afirmación. Dependiendo de si utiliza o no SCIM, tenga en cuenta lo siguiente:

- Si utiliza SCIM, el IdP sincroniza automáticamente los valores de los atributos en IAM Identity Center. Es posible que los atributos adicionales necesarios para el control de acceso no estén presentes en la lista de atributos del SCIM. En ese caso, considere la posibilidad de colaborar con el administrador de TI de su IdP para enviar dichos atributos a IAM Identity Center mediante aserciones de SAML con el prefijo requerido `https://aws.amazon.com/SAML/Attributes/AccessControl:`. Para obtener información sobre cómo configurar los atributos de usuario para el control de acceso en su IdP para enviarlos mediante aserciones de SAML, consulte la para Tutoriales de introducción su IdP.
- Si no utiliza SCIM, debe añadir los usuarios manualmente y establecer sus atributos como si utilizara IAM Identity Center como origen de identidad. A continuación, vaya a la página Atributos para el control de acceso y seleccione los atributos que desee utilizar en las políticas.

Para obtener una lista completa de los atributos de usuario compatibles entre los atributos de usuario del Centro de Identidad de IAM y los atributos de usuario del externo, consulte. IdPs Atributos de proveedores de identidad externos compatibles

Para comenzar a utilizar ABAC en IAM Identity Center, consulte los temas siguientes.

Temas

- Habilitación y configuración de atributos para el control de acceso
- Crear políticas de permisos para ABAC en IAM Identity Center

Habilitación y configuración de atributos para el control de acceso

Para utilizar ABAC en todos los casos, primero debe activar ABAC mediante la consola de IAM Identity Center o la API de IAM Identity Center. Si decide utilizar IAM Identity Center para seleccionar los atributos, utilice la página Atributos para el control de acceso de la consola de IAM Identity Center o la API de IAM Identity Center. Si utiliza un proveedor de identidades (IdP) externo como origen de identidades y elige enviar atributos a través de las aserciones de SAML, debe configurar su IdP para que pase los atributos. Si una aserción SAML pasa cualquiera de estos atributos, IAM Identity Center reemplazará el valor del atributo por el valor del almacén de identidades de IAM Identity Center. Solo los atributos configurados en IAM Identity Center se enviarán para tomar decisiones de control de acceso cuando los usuarios se federen en sus cuentas.

> **Note**
>
> No puede ver los atributos configurados y enviados por un IdP externo desde la página Atributos para el control de acceso de la consola de IAM Identity Center. Si transfiere atributos de control de acceso en las aserciones de SAML desde su IdP externo, esos atributos se envían directamente a la Cuenta de AWS cuando los usuarios se federan. Los atributos no estarán disponibles en IAM Identity Center para su mapeo.

Activar atributos para el control de acceso

Utilice el siguiente procedimiento para activar la característica de control de los atributos de acceso (ABAC) mediante la consola de IAM Identity Center.

> **Note**
>
> Si ya tiene conjuntos de permisos y planea habilitar ABAC en su instancia de IAM Identity Center, las restricciones de seguridad adicionales requieren que primero tenga la política `iam:UpdateAssumeRolePolicy`. Estas restricciones de seguridad adicionales no son obligatorias si no ha creado ningún conjunto de permisos en su cuenta.

Cómo activar atributos para el control de acceso

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, busque el cuadro de información Atributos para el control de acceso y, a continuación, elija Activar. Continúe con el siguiente procedimiento para configurarlo.

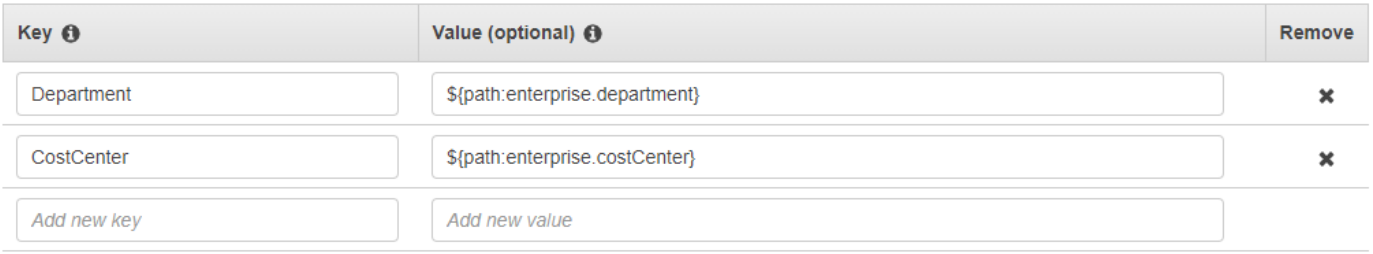
Seleccione sus atributos

Utilice el siguiente procedimiento para configurar atributos para la configuración de ABAC.

Selección de los atributos mediante la consola de IAM Identity Center

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.

3. En la página de configuración, seleccione la pestaña Atributos para el control de acceso y, a continuación, elija Administrar atributos.
4. En la página Atributos para el control de acceso, seleccione Añadir atributo e introduzca los detalles de clave y valor. Aquí es donde mapeará el atributo que proviene de su fuente de identidad a un atributo que IAM Identity Center pasa como etiqueta de sesión.



La clave representa el nombre que se le da al atributo para su uso en las políticas. Puede ser cualquier nombre arbitrario, pero debe especificar ese nombre exacto en las políticas que cree para el control de acceso. Por ejemplo, supongamos que utiliza Okta (un IdP externo) como fuente de identidad y necesita transferir los datos del centro de costos de su organización como etiquetas de sesión. En Key, debe introducir un nombre que coincida de forma similar, CostCentercomo el nombre de su clave. Es importante tener en cuenta que, sea cual sea el nombre que elija aquí, también debe tener el mismo nombre en su Clave de condición de aws:PrincipalTag (es decir, `"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"`).

> **Note**
>
> Use un atributo de un solo valor para su clave (por ejemplo, **`Manager`**). Por ejemplo, IAM Identity Center no admite atributos con varios valores para ABAC (por ejemplo, **`Manager, IT Systems`**).

El valor representa el contenido del atributo que proviene del origen de la identidad configurada. Aquí puede introducir cualquier valor de la tabla de fuentes de identidad correspondiente que aparece en Asignaciones de atributos para el directorio AWS Managed Microsoft AD. Por ejemplo, utilizando el contexto proporcionado en el ejemplo mencionado anteriormente, revisaría la lista de atributos de IdP admitidos y determinaría que la coincidencia más cercana con un atributo compatible sería **`${path:enterprise.costCenter}`** y, a continuación, lo introduciría en el campo Valor. Consulta la captura de pantalla proporcionada arriba como referencia. Tenga

en cuenta que no puede usar valores de atributos de IdP externos fuera de esta lista para ABAC a menos que utilice la opción de pasar los atributos a través de la aserción SAML.

5. Elija Guardar cambios.

Ahora que ha configurado el mapeo de sus atributos de control de acceso, debe completar el proceso de configuración de ABAC. Para ello, cree sus reglas de ABAC y agréguelas a sus conjuntos de permisos o políticas basadas en recursos. Esto es necesario para poder conceder a las identidades de los usuarios el acceso a los recursos de AWS . Para obtener más información, consulte Crear políticas de permisos para ABAC en IAM Identity Center.

Desactivar atributos para el control de acceso

Utilice el siguiente procedimiento para deshabilitar la característica ABAC y eliminar todas las asignaciones de atributos que se hayan configurado.

A fin de desactivar atributos para el control de acceso, siga estos pasos:

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Atributos para el control de acceso y, a continuación, elija Desactivar.
4. En el cuadro de diálogo Desactivar los atributos para el control de acceso, revise la información y, cuando esté listo, escriba ELIMINAR y, a continuación, elija Confirmar.

> **Important**
>
> Este paso elimina todos los atributos que se hayan configurado. Una vez eliminados, no se transferirán los atributos que se reciban de un origen de identidad ni los atributos personalizados que haya configurado previamente.

Crear políticas de permisos para ABAC en IAM Identity Center

Puede crear políticas de permisos que determinen quién puede acceder a sus recursos de AWS en característica de los valores de atributos configurados. Cuando habilita ABAC y especifica atributos, IAM Identity Center transfiere los valores de atributo del usuario autenticado a IAM para utilizarlos en la evaluación de políticas.

Clave de condición de aws:PrincipalTag

Puede utilizar los atributos de control de acceso en sus conjuntos de permisos mediante la clave de condición `aws:PrincipalTag` para crear reglas de control de acceso. Por ejemplo, en la siguiente política de confianza, puede etiquetar todos los recursos de su organización con sus respectivos centros de costos. También puede utilizar un único conjunto de permisos que conceda a los desarrolladores acceso a los recursos de sus centros de costos. Ahora, cuando los desarrolladores se federan en la cuenta mediante el inicio de sesión único y su atributo de centro de costos, solo tienen acceso a los recursos de sus respectivos centros. A medida que el equipo vaya añadiendo más desarrolladores y recursos a su proyecto, solo tendrás que etiquetar los recursos con el centro de costos correcto. Luego, pasa la información del centro de costos en la AWS sesión cuando los desarrolladores se federan Cuentas de AWS. Por tanto, a medida que la organización agrega nuevos recursos y desarrolladores al centro de costos, los desarrolladores pueden administrar los recursos alineados con sus centros sin necesidad de actualizar los permisos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"
                }
            }
        }
    ]
}
```

Para obtener más información, consulte aws:PrincipalTag y EC2: Iniciar o detener instancias en característica de las etiquetas principales y de recursos coincidentes en la Guía del usuario de IAM.

Si las políticas contienen atributos no válidos en sus condiciones, la condición de la política fallará y se denegará el acceso. Para obtener más información, consulte Error: “Se ha producido un error inesperado” cuando un usuario intenta iniciar sesión con un proveedor de identidad externo.

Proveedor de identidad de &IAM;

Al añadir un acceso de inicio de sesión único a un Cuenta de AWS, el Centro de Identidad de IAM crea un proveedor de identidades de IAM en cada uno de ellos. Cuenta de AWS Un proveedor de identidad de IAM le ayuda a proteger su Cuenta de AWS , ya que no tiene que distribuir ni integrar credenciales de seguridad a largo plazo, como por ejemplo, claves de acceso, en su aplicación.

Reparar el proveedor de identidad de IAM

Si elimina o modifica accidentalmente su proveedor de identidades, debe volver a aplicar manualmente las asignaciones de usuarios y grupos. Al volver a aplicar las asignaciones de usuarios y grupos, se vuelve a crear el proveedor de identidades. Para obtener más información, consulte:

- Gestione el acceso a Cuentas de AWS
- Administración del acceso a las aplicaciones

Roles vinculados al servicio

Roles vinculados a servicios son permisos predefinidos que permiten a IAM Identity Center delegar e implementar qué usuarios tienen acceso de inicio de sesión único a determinadas Cuentas de AWS de su organización en AWS Organizations. El servicio habilita esta funcionalidad al proporcionar un rol vinculado al servicio en cada uno de los miembros de su organización. Cuenta de AWS Luego, el servicio permite que otros AWS servicios, como IAM Identity Center, aprovechen esas funciones para realizar tareas relacionadas con el servicio. Para obtener más información, consulte AWS Organizations y los roles vinculados a servicios.

Al activar IAM Identity Center, este crea un rol vinculado al servicio en todas las cuentas de la organización en AWS Organizations. IAM Identity Center también crea el mismo rol vinculado a servicios en todas las cuentas que se añaden posteriormente a su organización. Este rol permite a IAM Identity Center acceder a los recursos de cada cuenta en su nombre. Para obtener más información, consulte Gestione el acceso a Cuentas de AWS.

Las funciones vinculadas al servicio que se crean en cada una de ellas reciben un nombre. Cuenta de AWS `AWSServiceRoleForSSO` Para obtener más información, consulte Uso de roles vinculados a servicios para IAM Identity Center.

Administración del acceso a las aplicaciones

Con él AWS IAM Identity Center, puede controlar quién puede tener acceso mediante un inicio de sesión único a sus aplicaciones. Los usuarios obtienen acceso estable a estas aplicaciones en cuanto usan las credenciales de directorio para iniciar sesión.

IAM Identity Center se comunica de forma segura con estas aplicaciones a través de una relación de confianza entre IAM Identity Center y el proveedor de servicios de la aplicación. Esta confianza se puede crear de diferentes maneras, según el tipo de aplicación.

IAM Identity Center admite dos tipos de aplicaciones: aplicaciones administradas y aplicaciones AWS administradas por el cliente. AWS las aplicaciones gestionadas se configuran directamente desde las consolas de aplicaciones correspondientes o mediante las API de las aplicaciones. Debe agregar las aplicaciones administradas por el cliente a la consola de IAM Identity Center y configurarlas con los metadatos correspondientes tanto para IAM Identity Center como para el proveedor de servicios.

Tras configurar las aplicaciones para que funcionen con IAM Identity Center, puede administrar los usuarios o grupos que acceden a las aplicaciones. De forma predeterminada, no hay ningún usuario asignado a las aplicaciones.

También puede conceder a sus empleados el AWS Management Console acceso a una instancia específica Cuenta de AWS de su organización. Para obtener más información, consulte Gestione el acceso a Cuentas de AWS.

Temas

AWS aplicaciones gestionadas

AWS las aplicaciones gestionadas se integran con el Centro de identidad de IAM y pueden utilizarlo para los servicios de autenticación y directorio.

La integración de las aplicaciones AWS gestionadas con el Centro de Identidad de IAM ofrece una forma más sencilla de asignar el acceso de los usuarios, sin necesidad de configurar una federación independiente o una sincronización de usuarios y grupos para cada aplicación. Puede conectar la fuente de identidad que desee usar para la autenticación una vez y obtendrá una vista única de las asignaciones de usuarios y grupos. Los administradores de las aplicaciones que permiten una propagación de identidades fiable pueden definir y auditar el acceso a los recursos de sus aplicaciones en función del usuario o de la pertenencia al grupo del usuario, sin necesidad de asignarlos a las funciones de IAM.

AWS las aplicaciones gestionadas proporcionan una interfaz de usuario administrativa que puede utilizar para gestionar el acceso a los recursos de la aplicación. Por ejemplo, QuickSight los administradores pueden asignar a los usuarios el acceso a los paneles en función de la pertenencia a un grupo. La mayoría de las aplicaciones AWS administradas también ofrecen una AWS Management Console experiencia que permite asignar usuarios a la aplicación. La experiencia de la consola de estas aplicaciones podría integrar ambas funciones para combinar las capacidades de asignación de usuarios con la capacidad de administrar el acceso a los recursos de la aplicación.

AWS Las aplicaciones gestionadas integradas con IAM Identity Center incluyen:

AWS aplicaciones gestionadas que se integran con IAM Identity Center

AWS aplicación gestionada	Integrada con la instancia organizativa del IAM Identity Center	Integrado con las instancias de cuentas del IAM Identity Center	Permite una propagación de identidad fiable a través del IAM Identity Center
Amazon Athena SQL	 S	 S	 Sí
Amazon CodeCatalyst	 S	 S	 No

AWS aplicación gestionada	Integrada con la instancia organizativa del IAM Identity Center	Integrado con las instancias de cuentas del IAM Identity Center	Permite una propagación de identidad fiable a través del IAM Identity Center
Cuadernos Amazon EMR	 S	 N	 No
Amazon EMR en Amazon EC2	 S	 S	 Sí
Amazon EMR Studio	 S	 S	 Sí
Amazon Kendra	 S	 N	 No
Amazon Managed Grafana	 S	 N	 No
Amazon Monitron	 S	 N	 No
Amazon Nimble Studio	 S	 N	 No
Amazon Pinpoint	 S	 N	 No

AWS aplicación gestionada	Integrada con la instancia organizativa del IAM Identity Center	Integrado con las instancias de cuentas del IAM Identity Center	Permite una propagación de identidad fiable a través del IAM Identity Center
Amazon Q Business	S	S	No
Amazon Q Developer	S	S *	No
Amazon QuickSight	S	S	Sí
Amazon Redshift	S	S	Sí
Concesiones de acceso a Amazon S3	S	S	Sí
Amazon SageMaker Studio	S	N	No
Amazon WorkSpaces Web	S	N	No

AWS aplicación gestionada	Integrada con la instancia organizativa del IAM Identity Center	Integrado con las instancias de cuentas del IAM Identity Center	Permite una propagación de identidad fiable a través del IAM Identity Center
AWS CLI	S	N	No
AWS Deadline Cloud	S	S	No
AWS IoT Events	S	N	No
AWS IoT Fleet Hub	S	N	No
AWS IoT SiteWise	S	N	No
AWS Lake Formation	S	S	Sí
AWS Supply Chain	S	N	No
AWS Systems Manager	S	N	No

AWS aplicación gestionada	Integrada con la instancia organizativa del IAM Identity Center	Integrado con las instancias de cuentas del IAM Identity Center	Permite una propagación de identidad fiable a través del IAM Identity Center
Acceso verificado de AWS	 S	 N	 No

* Se admiten las instancias de cuentas de IAM Identity Center, a menos que los usuarios necesiten acceder a Amazon Q en la AWS consola.

Temas

- Control del acceso
- Coordinación de las tareas administrativas
- Configuración de IAM Identity Center para compartir información de las identidades
- Consideraciones para compartir información de identidad en Cuentas de AWS
- Habilitar sesiones de consola con reconocimiento de identidad
- Restringir el uso de aplicaciones gestionadas AWS
- Visualización de los detalles de una aplicación administrada por AWS
- Deshabilitar una aplicación gestionada AWS

Control del acceso

El acceso a las aplicaciones AWS gestionadas se controla de dos maneras:

- Entrada inicial en la aplicación: IAM Identity Center administra esto mediante asignaciones a la aplicación. De forma predeterminada, las asignaciones son obligatorias para las aplicaciones AWS administradas.
- Acceso a los recursos de la aplicación: la aplicación administra esto mediante asignaciones de recursos independientes que controla.

Coordinación de las tareas administrativas

Si es administrador de aplicaciones, puede elegir si desea solicitar asignaciones a una aplicación. Si las asignaciones son obligatorias, cuando los usuarios inicien sesión en el portal de AWS acceso, solo los usuarios que estén asignados a la aplicación directamente o mediante una asignación grupal podrán ver el mosaico de la aplicación. Como alternativa, si las asignaciones no son obligatorias, puede permitir que todos los usuarios de IAM Identity Center entren en la aplicación. En este caso, la aplicación administra el acceso a los recursos y todos los usuarios que visitan el portal de AWS acceso pueden ver el mosaico de la aplicación.

Si es administrador del IAM Identity Center, puede utilizar la consola del IAM Identity Center para eliminar las asignaciones a las aplicaciones AWS gestionadas. Antes de eliminar las asignaciones, le recomendamos que colabore con el administrador de la aplicación. También debe colaborar con el administrador de la aplicación si tiene previsto modificar la configuración que determina si las asignaciones son obligatorias o automatizar las asignaciones de la aplicación.

Configuración de IAM Identity Center para compartir información de las identidades

IAM Identity Center proporciona un almacén de identidades que contiene los atributos de usuario y grupo, sin incluir las credenciales de inicio de sesión. Puede utilizar cualquiera de los siguientes métodos para mantener actualizados a los usuarios y grupos de su almacén de identidades de IAM Identity Center:

- Utilice el almacén de identidades de IAM Identity Center como fuente de identidades principal. Si elige este método, gestiona los usuarios, sus credenciales de inicio de sesión y los grupos desde la consola del IAM Identity Center o (). AWS Command Line Interface AWS CLI Para obtener más información, consulte Administración de identidades en IAM Identity Center.
- Configure el aprovisionamiento (sincronización) de los usuarios y grupos procedentes de cualquiera de las siguientes fuentes de identidad en el almacén de identidades de IAM Identity Center:
  - Active Directory: para más información, consulte Conexión un directorio Microsoft AD.
  - Proveedor de identidades externo: para más información, consulte Conexión a un proveedor de identidades externo.

Si elige este método de aprovisionamiento, seguirá administrando sus usuarios y grupos desde su origen de identidad y esos cambios se sincronizarán con el almacén de identidades de IAM Identity Center.

Sea cual sea la fuente de identidad que elija, el Centro de Identidad de IAM puede compartir la información del usuario y del grupo con AWS las aplicaciones gestionadas. De esta forma, puede conectar un origen de identidad a IAM Identity Center una vez y, a continuación, compartir la información de identidad con varias aplicaciones en la Nube de AWS. De este modo, se elimina la necesidad de configurar el aprovisionamiento de identidades y federaciones de forma independiente con cada aplicación. Esta característica de uso compartido también facilita el acceso de los usuarios a muchas aplicaciones en diferentes Cuentas de AWS.

Consideraciones para compartir información de identidad en Cuentas de AWS

IAM Identity Center admite los atributos más utilizados en todas las aplicaciones. Estos atributos pueden ser el nombre y apellido, el número de teléfono, la dirección de correo electrónico, la dirección y el idioma preferido. Considere detenidamente qué aplicaciones y qué cuentas pueden utilizar esta información de identificación personal.

Puede controlar el acceso a esta información de cualquiera de las siguientes maneras. Puede optar por habilitar el acceso solo en la cuenta AWS Organizations de administración o en todas las cuentas de AWS Organizations. O bien, puede utilizar políticas de control de servicio (SCP) para controlar qué aplicaciones pueden acceder a la información y a qué cuentas de AWS Organizations. Por ejemplo, si habilita el acceso únicamente a la cuenta AWS Organizations de administración, las aplicaciones de las cuentas de los miembros no tendrán acceso a la información. Sin embargo, si habilita el acceso a todas las cuentas, puede usar los SCP para impedir el acceso a todas las aplicaciones, excepto a las que desee permitir.

Habilitar sesiones de consola con reconocimiento de identidad

Una sesión de consola con reconocimiento de identidad mejora la sesión de AWS consola del usuario al proporcionar un contexto de usuario adicional para personalizar la experiencia de ese usuario. Actualmente, los usuarios de Amazon Q admiten esta capacidad en la AWS consola.

En la actualidad, puede habilitar sesiones de consola con reconocimiento de identidad sin realizar ningún cambio en los patrones de acceso existentes ni en la federación en la AWS consola. Si sus

usuarios inician sesión en la AWS consola con IAM (por ejemplo, si inician sesión como usuarios de IAM o mediante un acceso federado con IAM), pueden seguir utilizando estos métodos. Si sus usuarios inician sesión en el portal de AWS acceso, pueden seguir utilizando sus credenciales de usuario del IAM Identity Center.

Temas

Requisitos y consideraciones previos

Antes de habilitar las sesiones de consola con reconocimiento de identidad, revise los siguientes requisitos previos y consideraciones:

- Debe habilitar las sesiones de consola con reconocimiento de identidad para los usuarios que necesiten acceder a Amazon Q en la AWS consola.
- Actualmente, las sesiones de consola con reconocimiento de identidad solo se admiten para su uso con Amazon Q en la AWS consola.
- Las sesiones de consola con reconocimiento de identidad requieren una instancia organizativa del IAM Identity Center.
- La integración con Amazon Q no se admite si habilitas IAM Identity Center de forma opcional Región de AWS.
- Una vez que habilites las sesiones de consola con reconocimiento de identidad, no podrás deshabilitar esta capacidad.
- Para habilitar las sesiones de consola con reconocimiento de identidad, debes tener los siguientes permisos:
  - `sso:CreateApplication`
  - `sso:GetSharedSsoConfiguration`
  - `sso:ListApplications`
  - `sso:PutApplicationAssignmentConfiguration`
  - `sso:PutApplicationAuthenticationMethod`
  - `sso:PutApplicationGrant`
  - `sso:PutApplicationAccessScope`

  - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
  - `signin:ListTrustedIdentityPropagationApplicationForConsole`
  -

- Para permitir que sus usuarios utilicen sesiones de consola con reconocimiento de identidad, debe concederles el `sts:setContext` permiso en virtud de una política basada en la identidad. Para obtener más información, consulte Otorgar a los usuarios permisos para usar sesiones de consola con reconocimiento de identidad.

¿Cómo habilitar las sesiones identity-aware-console

Puede habilitar sesiones de consola con reconocimiento de identidad en la consola de Amazon Q o en la consola de IAM Identity Center.

Habilite las sesiones de consola con reconocimiento de identidad en la consola Amazon Q

Antes de habilitar las sesiones de consola con reconocimiento de identidad, debe tener una instancia organizativa del IAM Identity Center con una fuente de identidad conectada. Si ya ha configurado el Centro de identidades de IAM, vaya al paso 3.

1. Abra la consola de IAM Identity Center Seleccione Activar y cree una instancia organizativa del IAM Identity Center. Para obtener más información, consulte Habilitar AWS IAM Identity Center.
2. Conecte su fuente de identidad al Centro de identidades de IAM y aprovisione usuarios al Centro de identidades de IAM. Puede elegir el directorio predeterminado del Centro de Identidad de IAM como fuente de identidad o puede utilizar otro proveedor de identidad. Para obtener más información, consulte Tutoriales de introducción.
3. Cuando termine de configurar el Centro de identidades de IAM, abra la consola de Amazon Q y siga los pasos de Suscripciones de la Guía del usuario para desarrolladores de Amazon Q. Asegúrese de activar las sesiones de consola con reconocimiento de identidad.

> **Note**
>
> Si no tiene los permisos suficientes para habilitar las sesiones de consola con reconocimiento de identidad, es posible que tenga que pedirle a un administrador del IAM Identity Center que realice esta tarea por usted en la consola del IAM Identity Center. Para obtener más información, consulte el siguiente procedimiento.

Habilite las sesiones de consola con reconocimiento de identidad en la consola del IAM Identity Center

Si es administrador del IAM Identity Center, es posible que otro administrador le pida que habilite las sesiones de consola con reconocimiento de identidad en la consola del IAM Identity Center.

1. Abra la consola de IAM Identity Center
2. En el panel de navegación, seleccione Configuración.
3. En Habilitar sesiones con reconocimiento de identidad, seleccione Habilitar.
4. En el segundo mensaje, selecciona Activar.
5. Cuando termine de habilitar las sesiones de consola con reconocimiento de identidad, aparecerá un mensaje de confirmación en la parte superior de la página de configuración.
6. En la sección Detalles, el estado de las sesiones con reconocimiento de identidad es Habilitado.

Cómo funcionan las sesiones de consola con reconocimiento de identidad

Con las sesiones de consola con reconocimiento de identidad, los usuarios de Amazon Q en la AWS consola pueden iniciar sesión AWS, abrir el sitio web AWS Management Console u otro AWS sitio web, elegir el icono de Amazon Q e iniciar un chat o utilizar otras funciones compatibles. Para obtener más información, consulte la Guía del usuario de Amazon Q Developer.

El Centro de Identidad de IAM mejora la sesión de consola actual del usuario para incluir el ID de usuario activo del Centro de Identidad de IAM y el ID de sesión del Centro de Identidad de IAM.

Las sesiones de consola con reconocimiento de identidad incluyen los tres valores siguientes:

- ID de usuario del almacén de identidades (almacén de identidades: UserId): este valor se utiliza para identificar de forma exclusiva a un usuario en la fuente de identidad que está conectada al Centro de identidades de IAM.
- Directorio de almacenes de identidades ARN (almacén de identidades: IdentityStoreArn): este valor es el ARN del almacén de identidades que está conectado al Centro de identidades de IAM y en el que puede buscar los atributos. `identitystore:UserId`
- ID de sesión del IAM Identity Center: este valor indica si la sesión del usuario en el IAM Identity Center sigue siendo válida.

Los valores son los mismos, pero se obtienen de formas distintas y se añaden en distintos puntos del proceso, en función de cómo inicie sesión el usuario:

- Centro de identidad de IAM (portal de AWS acceso): en este caso, los valores de ID de usuario y ARN del almacén de identidades del usuario ya se proporcionan en la sesión activa del Centro de identidades de IAM. El Centro de Identidad de IAM mejora la sesión actual al añadir únicamente el ID de sesión.
- Otros métodos de inicio de sesión: si el usuario inicia sesión AWS como usuario de IAM, con un rol de IAM o como usuario federado con IAM, no se proporciona ninguno de estos valores. IAM Identity Center mejora la sesión actual al añadir el ID de usuario del almacén de identidades, el ARN del directorio del almacén de identidades y el ID de sesión.

Restringir el uso de aplicaciones gestionadas AWS

Al activar el IAM Identity Center por primera vez, AWS permite el uso de aplicaciones AWS gestionadas de forma automática en todas las cuentas de IAM. AWS Organizations Para restringir las aplicaciones, debe implementar los SCP. Puede utilizar las SCP para bloquear el acceso a la información de usuarios y grupos de IAM Identity Center y para impedir que se inicie la aplicación, excepto en las cuentas designadas.

Visualización de los detalles de una aplicación administrada por AWS

Tras conectar una aplicación AWS gestionada al IAM Identity Center mediante la consola o las API de la aplicación, la aplicación se registra en el IAM Identity Center. Una vez registrada una aplicación en IAM Identity Center, puede ver información detallada sobre la aplicación en la consola de IAM Identity Center.

Para ver información sobre una aplicación AWS gestionada en la consola del IAM Identity Center

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. Seleccione la pestaña Aplicaciones administradas por AWS .
4. En la lista de aplicaciones, seleccione el nombre de la aplicación de la que desea ver información detallada.
5. La información sobre la aplicación incluye si son obligatorias las asignaciones de usuarios y grupos y, si corresponde, los usuarios y grupos asignados y las aplicaciones de confianza para la propagación de identidades. Para obtener más información acerca de la propagación de identidades de confianza, consulte Propagación de identidad de confianza en aplicaciones.

Deshabilitar una aplicación gestionada AWS

Para evitar que los usuarios se autentiquen en una aplicación AWS gestionada, puede inhabilitar la aplicación en la consola del IAM Identity Center.

> **Warning**
>
> Al deshabilitar una aplicación, se eliminan todos los permisos de usuario de la aplicación, se desconecta la aplicación del IAM Identity Center y se vuelve inaccesible. Si es administrador de IAM Identity Center, le recomendamos que se ponga en contacto con el administrador de la aplicación antes de realizar esta tarea.

Para deshabilitar una aplicación gestionada AWS

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. En la página Aplicaciones, en Aplicaciones administradas por AWS , seleccione la aplicación que desee deshabilitar.
4. Con la aplicación seleccionada, seleccione Acciones y, a continuación, seleccione Deshabilitar.
5. En el cuadro de diálogo Suspender la aplicación, seleccione Suspender.
6. En la lista Aplicaciones administradas por AWS , el estado de la aplicación aparece como Inactiva.

Aplicaciones administradas por el cliente

Con el IAM Identity Center, puede crear o conectar a los usuarios de la fuerza laboral y gestionar de forma centralizada su acceso a todas sus Cuentas de AWS aplicaciones. IAM Identity Center actúa como un servicio de identidades central y proporciona diferentes formas de autenticar a los usuarios. Si ya utiliza un proveedor de identidades (IdP), IAM Identity Center puede integrarse con su IdP para que pueda aprovisionar sus usuarios y grupos en IAM Identity Center y utilizar su IdP para la autenticación.

Si usa aplicaciones administradas por el cliente que admiten SAML 2.0, puede federar su IdP a IAM Identity Center mediante SAML 2.0 y usar IAM Identity Center para administrar el acceso de los usuarios a esas aplicaciones. IAM Identity Center proporciona un catálogo de aplicaciones de uso común compatibles con SAML 2.0, como Salesforce y Microsoft 365. Este catálogo está disponible

en la consola del IAM Identity Center. También puede configurar sus propias aplicaciones de SAML 2.0.

> **Note**
>
> Si tienes aplicaciones gestionadas por el cliente que son compatibles con OAuth 2.0 y tus usuarios necesitan acceder a los AWS servicios desde estas aplicaciones, puedes utilizar la propagación de identidades fiable. Con una propagación de identidad fiable, un usuario puede iniciar sesión en una aplicación y esa aplicación puede transmitir la identidad de los usuarios en las solicitudes de acceso a los datos de los servicios. AWS Para obtener más información, consulte Uso de la propagación de identidades de confianza con aplicaciones administradas por el cliente.

Temas

SAML 2.0 y OAuth 2.0

IAM Identity Center le permite ofrecer a sus usuarios acceso mediante inicio de sesión único a las aplicaciones de SAML 2.0 u OAuth 2.0. En los siguientes temas se proporciona una descripción general de SAML 2.0 y OAuth 2.0.

Temas

SAML 2.0

SAML 2.0 es un estándar del sector utilizado para intercambiar de forma segura aserciones de SAML que transmiten información sobre un usuario entre una autoridad de SAML (denominada proveedor de identidades o IdP) y un consumidor de SAML 2.0 (denominado proveedor de servicios o SP). El Centro de Identidad de IAM utiliza esta información para proporcionar acceso federado de inicio de sesión único a los usuarios que están autorizados a utilizar las aplicaciones del portal de acceso. AWS

OAuth 2.0

OAuth 2.0 es un protocolo que permite a las aplicaciones acceder a los datos de los usuarios y compartirlos de forma segura sin compartir contraseñas. Esta capacidad proporciona a los usuarios una forma segura y estandarizada de permitir que las aplicaciones accedan a sus recursos. El acceso se ve facilitado por diferentes flujos de concesión de OAuth 2.0.

El Centro de identidades de IAM permite a las aplicaciones que se ejecutan en clientes públicos recuperar credenciales temporales de acceso Cuentas de AWS y servicios mediante programación en nombre de sus usuarios. Los clientes públicos suelen ser ordenadores de sobremesa, portátiles u otros dispositivos móviles que se utilizan para ejecutar aplicaciones de forma local. Algunos ejemplos de AWS aplicaciones que se ejecutan en clientes públicos son AWS Command Line Interface (AWS CLI) y los kits de desarrollo de AWS software (SDK). AWS Toolkit Para permitir que estas aplicaciones obtengan credenciales, el Centro de Identidad de IAM admite partes de los siguientes flujos de OAuth 2.0:

- Concesión de códigos de autorización con clave de prueba para el intercambio de códigos (PKCE) (RFC 6749 y RFC 7636)
- Concesión de autorización de dispositivos (RFC 8628)

> **Note**
>
> Estos tipos de concesión solo se pueden utilizar si Servicios de AWS admiten esta capacidad. Es posible que estos servicios no admitan este tipo de subvención en su totalidad Regiones de AWS. Consulte la documentación pertinente Servicios de AWS para conocer las diferencias regionales.

OpenID Connect (OIDC) es un protocolo de autenticación que se basa en el marco OAuth 2.0. El OIDC especifica cómo usar OAuth 2.0 para la autenticación. A través de las API del servicio OIDC del IAM Identity Center, una aplicación registra un cliente de OAuth 2.0 y utiliza uno de estos flujos para obtener un token de acceso que proporciona permisos a las API protegidas del IAM Identity Center. Una aplicación especifica los ámbitos de acceso para declarar el usuario de API al que va dirigido. Una vez que usted, como administrador del Centro de Identidad de IAM, haya configurado su fuente de identidad, los usuarios finales de la aplicación deberán completar un proceso de inicio de sesión, si aún no lo han hecho. A continuación, los usuarios finales deben dar su consentimiento para permitir que la aplicación realice llamadas a la API. Estas llamadas a la API se realizan con

los permisos de los usuarios. En respuesta, IAM Identity Center devuelve un token de acceso a la aplicación que contiene los ámbitos de acceso a los que los usuarios dieron su consentimiento.

Uso de un flujo de concesión de OAuth 2.0

Los flujos de concesión de OAuth 2.0 solo están disponibles a través de aplicaciones AWS gestionadas que admiten los flujos. Para usar un flujo de OAuth 2.0, su instancia de IAM Identity Center y cualquier aplicación AWS gestionada compatible que utilice deben implementarse en una sola. Región de AWS Consulte la documentación de cada una de ellas Servicio de AWS para determinar la disponibilidad regional de las aplicaciones AWS gestionadas y la instancia del IAM Identity Center que desea utilizar.

Para utilizar una aplicación que utilice un flujo de OAuth 2.0, el usuario final debe introducir la URL a la que se conectará la aplicación y registrarse en su instancia de IAM Identity Center. Según la aplicación, como administrador, debe proporcionar a sus usuarios la URL del portal de AWS acceso o la URL del emisor de su instancia de IAM Identity Center. Puede encontrar estos dos ajustes en la página de configuración de la consola de IAM Identity Center. Para obtener información adicional sobre la configuración de una aplicación cliente, consulte la documentación de esa aplicación.

La experiencia del usuario final a la hora de iniciar sesión en una aplicación y dar su consentimiento depende de si la aplicación utiliza Concesión de código de autorización con PKCE oConcesión de autorización del dispositivo.

Concesión de código de autorización con PKCE

Este flujo lo utilizan las aplicaciones que se ejecutan en un dispositivo que tiene un navegador.

1. Se abre una ventana del navegador.
2. Si el usuario no se ha autenticado, el navegador lo redirige para completar la autenticación del usuario.
3. Tras la autenticación, se presenta al usuario una pantalla de consentimiento que muestra la siguiente información:
   - El nombre de la aplicación
   - Los ámbitos de acceso para los que la aplicación solicita el consentimiento
4. El usuario puede cancelar el proceso de consentimiento o puede dar su consentimiento y la aplicación procederá al acceso en función de los permisos del usuario.

Concesión de autorización del dispositivo

Las aplicaciones que se ejecutan en un dispositivo con o sin navegador pueden utilizar este flujo. Cuando la aplicación inicia el flujo, presenta una URL y un código de usuario que el usuario debe verificar más adelante en el flujo. El código de usuario es necesario porque la aplicación que inicia el flujo puede estar ejecutándose en un dispositivo diferente al dispositivo en el que el usuario da su consentimiento. El código garantiza que el usuario dé su consentimiento al flujo que inició en el otro dispositivo.

1. Cuando el flujo se inicia desde un dispositivo con un navegador, se abre una ventana del navegador. Cuando el flujo se inicia desde un dispositivo sin navegador, el usuario debe abrir un navegador en un dispositivo diferente e ir a la URL que presentó la aplicación.
2. En cualquier caso, si el usuario no se ha autenticado, el navegador lo redirige para completar la autenticación del usuario.
3. Tras la autenticación, se presenta al usuario una pantalla de consentimiento que muestra la siguiente información:
   - El nombre de la aplicación
   - Los ámbitos de acceso para los que la aplicación solicita el consentimiento
   - El código de usuario que la aplicación presentó al usuario
4. El usuario puede cancelar el proceso de consentimiento o puede dar su consentimiento y la aplicación procederá al acceso en función de los permisos del usuario.

Ámbitos de acceso

Un ámbito define el acceso a un servicio para un servicio al que se puede acceder a través de un flujo de OAuth 2.0. Los ámbitos permiten al servicio, también denominado servidor de recursos, agrupar los permisos relacionados con las acciones y los recursos del servicio, y especifican las operaciones más generales que los clientes de OAuth 2.0 pueden solicitar. Cuando un cliente de OAuth 2.0 se registra en el servicio OIDC del IAM Identity Center, el cliente especifica los ámbitos para declarar las acciones que pretende realizar, para lo cual el usuario debe dar su consentimiento.

Los clientes de OAuth 2.0 utilizan `scope` los valores definidos en la sección 3.3 de OAuth 2.0 (RFC 6749) para especificar qué permisos se solicitan para un token de acceso. Los clientes pueden especificar un máximo de 25 ámbitos al solicitar un token de acceso. Cuando un usuario da su consentimiento durante la concesión de un código de autorización con el PKCE o el flujo de concesión de autorización de un dispositivo, el IAM Identity Center codifica los ámbitos en el token de acceso que devuelve.

AWS añade ámbitos al Centro de Identidad de IAM para que sean compatibles. Servicios de AWS En la siguiente tabla se enumeran los ámbitos que admite el servicio OIDC del Centro de Identidad de IAM al registrar un cliente público.

Ámbitos de acceso compatibles con el servicio OIDC de IAM Identity Center al registrar a un cliente público

Ámbito	Descripción	Servicios admitidos por
`sso:account:access`	Acceda a las cuentas administradas y a los conjuntos de permisos de IAM Identity Center.	IAM Identity Center
`codewhisperer:analysis`	Habilite el acceso al análisis de código para desarrolladores de Amazon Q.	ID de creador de AWS y el Centro de Identidad de IAM
`codewhisperer:completions`	Habilita el acceso a las sugerencias de códigos en línea de Amazon Q.	ID de creador de AWS y el Centro de Identidad de IAM
`codewhisperer:conversations`	Habilita el acceso al chat de Amazon Q.	ID de creador de AWS y el centro de identidad de IAM
`codewhisperer:taskassist`	Habilite el acceso a Amazon Q Developer Agent para el desarrollo de software.	ID de creador de AWS y el Centro de Identidad de IAM
`codewhisperer:transformations`	Habilite el acceso a Amazon Q Developer Agent para la transformación del código.	ID de creador de AWS y el Centro de Identidad de IAM
`codecatalyst:read_write`	Lee y escribe en tus CodeCatalyst recursos de Amazon, lo que te permite acceder a todos tus recursos existentes.	ID de creador de AWS y IAM Identity Center

Configuración de aplicaciones de SAML 2.0 administradas por el cliente

Si usa aplicaciones administradas por el cliente que admiten SAML 2.0, puede federar su IdP a IAM Identity Center mediante SAML 2.0 y usar IAM Identity Center para administrar el acceso de los usuarios a esas aplicaciones. Puede seleccionar una aplicación de SAML 2.0 de un catálogo de aplicaciones de uso frecuente en la consola de IAM Identity Center o puede configurar su propia aplicación de SAML 2.0.

> **Note**
>
> Si tiene aplicaciones gestionadas por clientes compatibles con OAuth 2.0 y sus usuarios necesitan acceder desde estas aplicaciones a los AWS servicios, puede utilizar la propagación de identidades fiable. Con una propagación de identidad fiable, un usuario puede iniciar sesión en una aplicación y esa aplicación puede transmitir la identidad de los usuarios en las solicitudes de acceso a los datos de los servicios. AWS Para obtener más información, consulte Uso de la propagación de identidades de confianza con aplicaciones administradas por el cliente.

Temas

- Catálogo de aplicaciones de IAM Identity Center
- Configuración de su propia aplicación de SAML 2.0

Catálogo de aplicaciones de IAM Identity Center

Puede utilizar el catálogo de aplicaciones de la consola de IAM Identity Center para agregar muchas aplicaciones de SAML 2.0 de uso común que funcionan con IAM Identity Center. Algunos ejemplos son Salesforce, Box y Microsoft 365.

La mayoría de aplicaciones proporcionan información detallada sobre cómo configurar la confianza entre IAM Identity Center y el proveedor de servicios de la aplicación. Esta información está disponible en la página de configuración de la aplicación, después de seleccionarla en el catálogo. Tras configurar la aplicación, puede asignar el acceso a los usuarios o grupos de IAM Identity Center según sea necesario.

Temas

- Configuración de una aplicación del catálogo de aplicaciones

Configuración de una aplicación del catálogo de aplicaciones

Utilice este procedimiento para configurar una relación de confianza de SAML 2.0 entre IAM Identity Center y el proveedor de servicios de la aplicación.

Antes de comenzar este procedimiento, resulta útil disponer del archivo de intercambio de metadatos del proveedor de servicios para que pueda configurar la relación de confianza de manera más eficiente. Aunque no disponga de este archivo, puede utilizar este procedimiento para configurar la confianza manualmente.

Para añadir y configurar una aplicación del catálogo de aplicaciones

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, elija Deseo seleccionar una aplicación del catálogo.
6. En Catálogo de aplicaciones, empiece a escribir el nombre de la aplicación que desea agregar en el cuadro de búsqueda.
7. Elija el nombre de la aplicación en la lista cuando aparezca en los resultados de la búsqueda y, a continuación, seleccione Siguiente.
8. En la página Configurar aplicación, los campos Nombre de visualización y Descripción se rellenan automáticamente con los detalles correspondientes de la aplicación. Puede modificar esta información.
9. En Metadatos de IAM Identity Center, haga lo siguiente:

    a. En a Archivo de metadatos del SAML de IAM Identity Center, elija Descargar para descargar los metadatos del proveedor de identidad.
    b. En el a Certificado de IAM Identity Center, elija Descargar certificado para descargar el certificado del proveedor de identidad.

> **Note**
>
> Necesitará estos archivos más tarde al configurar la aplicación desde el sitio web del proveedor de servicios. Siga las instrucciones de dicho proveedor.

10. (Opcional) En Propiedades de la aplicación, puede especificar URL de inicio de aplicación, Estado de retransmisión y Duración de la sesión. Para obtener más información, consulte Configuración de las propiedades de la aplicación en la consola de IAM Identity Center.
11. En Metadatos de la aplicación, realice una de las siguientes acciones:

    a. Si tiene un archivo de metadatos, seleccione Cargar archivo de metadatos de SAML de la aplicación. A continuación, seleccione Elegir archivo para buscar y seleccionar el archivo de metadatos.
    b. Si no tiene un archivo de metadatos, elija Escribir manualmente los valores de los metadatos y, a continuación, proporcione los valores de URL de ACS de la aplicación y Audiencia de SAML de la aplicación.
12. Seleccione Submit (Enviar). Accederá a la página de detalles de la aplicación que acaba de añadir.

Configuración de su propia aplicación de SAML 2.0

Puede configurar sus propias aplicaciones que permitan la federación de identidades mediante SAML 2.0 y agregarlas a IAM Identity Center. La mayoría de los pasos para configurar sus propias aplicaciones de SAML 2.0 son los mismos que para configurar una aplicación de SAML 2.0 desde el catálogo de aplicaciones de la consola de IAM Identity Center. Sin embargo, también debe proporcionar más asignaciones de atributos de SAML para sus aplicaciones de SAML 2.0. Estas asignaciones permiten que IAM Identity Center rellene correctamente la aserción de SAML 2.0 para su aplicación. Puede proporcionar esta asignación de atributos SAML adicionales cuando configure la aplicación por primera vez. También puede proporcionar asignaciones de atributos de SAML 2.0 en la página de detalles de la aplicación de la consola de IAM Identity Center.

Utilice el siguiente procedimiento para configurar una relación de confianza de SAML 2.0 entre IAM Identity Center y el proveedor de servicios de la aplicación de SAML 2.0. Antes de comenzar este procedimiento, asegúrese de que dispone del certificado y del archivo de intercambio de metadatos del proveedor de servicios para que pueda completar la configuración de la relación de confianza.

Para configurar su propia aplicación de SAML 2.0

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.

5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, seleccione Tengo una aplicación que quiero configurar.
6. En Tipo de aplicación, seleccione SAML 2.0.
7. Elija Siguiente.
8. En la página Configurar aplicación, en Configurar aplicación, introduzca un nombre para mostrar para la aplicación, por ejemplo **`MyApp`**. Escriba una descripción en Descripción.
9. En Metadatos de IAM Identity Center, haga lo siguiente:

   a. En a Archivo de metadatos del SAML de IAM Identity Center, elija Descargar para descargar los metadatos del proveedor de identidad.

   b. Junto a Certificado de IAM Identity Center, seleccione Descargar para descargar el certificado del proveedor de identidades.

   > **Note**
   >
   > Necesitará estos archivos más tarde al configurar la aplicación personalizada desde el sitio web del proveedor de servicios.

10. (Opcional) En Propiedades de la aplicación, también puede especificar los valores de URL de inicio de aplicación, Estado de retransmisión y Duración de la sesión. Para obtener más información, consulte Configuración de las propiedades de la aplicación en la consola de IAM Identity Center.
11. En Metadatos de la aplicación, elija Escribir manualmente los valores de los metadatos. A continuación, proporcione valores para la URL de ACS de la aplicación y la audiencia de SAML de la aplicación.
12. Seleccione Submit (Enviar). Accederá a la página de detalles de la aplicación que acaba de añadir.

Propagación de identidad de confianza en aplicaciones

La propagación de identidad fiable permite a los AWS servicios hacer lo siguiente:

- Autoriza el acceso a AWS los recursos en función del contexto de identidad del usuario.
- Comparta de forma segura el contexto de identidad del usuario con otros AWS servicios.

Estas capacidades permiten definir, conceder y registrar más fácilmente el acceso de los usuarios.

Con una propagación de identidad fiable, un usuario puede iniciar sesión en una aplicación y esa aplicación puede transmitir el contexto de identidad de los usuarios en las solicitudes de acceso a los datos de los AWS servicios. Como el acceso se administra en función de la identidad del usuario, los usuarios no necesitan utilizar las credenciales de usuario local de la base de datos ni asumir un rol de IAM para acceder a los datos.

Temas

Descripción general de la propagación de identidades de confianza

Con una propagación de identidad confiable, el acceso de los usuarios a AWS los recursos se puede definir, conceder y registrar más fácilmente. La propagación de identidades de confianza se basa en el marco de autorización de OAuth 2.0, que permite a las aplicaciones acceder a los datos de los usuarios y compartirlos de forma segura sin compartir contraseñas. OAuth 2.0 proporciona un acceso delegado seguro a los recursos de la aplicación. El acceso es delegado porque el administrador de los recursos aprueba o delega la aplicación en la que el usuario inicia sesión para acceder a la otra aplicación.

Para evitar compartir las contraseñas de los usuarios, la propagación de identidades de confianza utiliza tokens. Los tokens proporcionan una forma estándar para que una aplicación de confianza indique quién es el usuario y qué solicitudes están permitidas entre dos aplicaciones. AWS las aplicaciones gestionadas que se integran con una propagación de identidad fiable obtienen los tokens directamente del Centro de Identidad de IAM. IAM Identity Center también ofrece una opción para que las aplicaciones intercambien tokens de identidad y tokens de acceso que provienen de un servidor de autorización de OAuth 2.0 externo. Esto permite que una aplicación se autentique y obtenga los tokens fuera de él AWS, los intercambie por un token del IAM Identity Center y utilice el nuevo token para realizar solicitudes a los servicios. AWS Para obtener más información, consulte Uso de aplicaciones con un emisor de tokens de confianza.

El proceso de OAuth 2.0 comienza cuando un usuario inicia sesión en una aplicación. La aplicación en la que inicia sesión el usuario inicia una solicitud para acceder a los recursos de la otra aplicación.

La aplicación iniciadora (solicitante) puede acceder a la aplicación receptora en nombre del usuario solicitando un token al servidor de autorización. El servidor de autorización devuelve el token y la aplicación iniciadora pasa ese token a la aplicación receptora, junto con una solicitud de acceso.

Casos de uso fiables para la propagación de identidades

Como administrador del centro de identidad de IAM, es posible que se le pida que ayude a configurar la propagación de identidad confiable entre las siguientes aplicaciones de inicio que admiten esta capacidad y los servicios conectados AWS . En las siguientes secciones se proporciona más información sobre los casos de uso específicos que admiten las aplicaciones que pueden iniciar la propagación de identidades de forma fiable.

Temas

Amazon EMR

Puede utilizar Amazon EMR como aplicación de inicio para los siguientes casos de uso de propagación de identidad de confianza.

Descripción	Otros servicios utilizados AWS	Más información
Ejecute análisis interactivos con Apache Spark en clústeres de Amazon EMR o Amazon EC2 a través de Amazon EMR Studio. Aplique un control de acceso basado en las identidades de los empleados y los atributos asociados a Catalog Through AWS Glue . AWS Lake Formation	Amazon EMR en Amazon EC2 autorizado a través de AWS Lake Formation Amazon S3 Access Grants, Amazon S3, AWS Service Catalog	• Integre Amazon EMR con el centro de identidad de IAM en la guía de administración de Amazon EMR. • Las concesiones de acceso de Amazon S3 y las identidades de los directorios corporativos en la guía del usuario

Descripción	Otros servicios utilizados AWS	Más información
	Note • Requiere acceso a través de Amazon EMR Studio. • Solo control de acceso a nivel de mesa. • No se admiten Apache Hive, PrestoSQL/ Trino ni EMR Serverless.	de Amazon Simple Storage Service. • Cómo conectarse AWS Lake Formation con el IAM Identity Center en la guía AWS Lake Formation para desarrolladores • Utilice sus identidades corporativas para realizar análisis con Amazon EMR e IAM Identity Center en el AWS blog sobre big data

Descripción	Otros servicios utilizados AWS	Más información
Realice análisis ad hoc con Trino en Athena a través de Amazon EMR Studio. Aplique un control de acceso basado en las identidades de los empleados y los atributos asociados a Catalog Through. AWS Glue AWS Lake Formation Proteja el acceso a una ubicación de depósito de resultados de consultas de Athena en Amazon S3 mediante Amazon S3 Access Grants.	Athena autorizada a través de AWS Lake Formation Amazon S3 Access Grants **Note** Requiere acceso a través de Amazon EMR Studio. No se admite el acceso directo desde la Amazon Athena consola.	• Integre Amazon EMR con el centro de identidad de IAM en la guía de administración de Amazon EMR. • El uso de IAM Identity Center habilitó los grupos de trabajo de Athena en la Guía del usuario de Amazon Athena. • Las concesiones de acceso de Amazon S3 y las identidades de los directorios corporativos en la guía del usuario de Amazon Simple Storage Service. • Cómo conectarse AWS Lake Formation con el IAM Identity Center en la guía para AWS Lake Formation desarrolladores. • Aporte la identidad de sus empleados a Amazon EMR Studio y Athena en el AWS blog sobre big data.

Amazon QuickSight

Puedes usar Amazon QuickSight como aplicación de inicio para los siguientes casos de uso de propagación de identidad de confianza.

Descripción	Otros AWS servicios utilizados	Más información
QuickSight Los usuarios de Amazon pueden consultar los datos de Amazon Redshift. Un administrador de Amazon Redshift concede el acceso a los datos en Amazon Redshift.	Amazon Redshift	• Conecte Redshift con IAM Identity Center para ofrecer a los usuarios una experiencia de inicio de sesión único en la Guía de administración de Amazon Redshift. • Conecte Amazon Redshift con el centro de identidades de IAM a través de Amazon QuickSight en la guía de administración de Amazon Redshift.
QuickSight Los usuarios de Amazon pueden consultar Amazon Redshift Spectrum para obtener datos estructur ados en Amazon S3, con un acceso autorizado por AWS Lake Formation un administrador.	Amazon Redshift Spectrum, datos estructurados de Amazon S3 *A través de Amazon Redshift Spectrum, autorizado a través de AWS Lake Formation	• Conecte Redshift con IAM Identity Center para ofrecer a los usuarios una experiencia de inicio de sesión único en la Guía de administración de Amazon Redshift. • Conecte Amazon Redshift con el centro de identidades de IAM a través de Amazon QuickSight en la guía de administración de Amazon Redshift. • Cómo conectarse AWS Lake Formation con el centro de identidad de IAM en la guía para desarrolladores.AWS Lake Formation • Simplifique la administración del acceso con Amazon Redshift y, AWS Lake Formation para los usuarios de un proveedor de identidad

Descripción	Otros AWS servicios utilizados	Más información
		externo, en el blog sobre AWS macrodatos.
QuickSight Los usuarios de Amazon pueden consultar los datos compartidos de Amazon Redshift para obtener datos estructurados en Amazon S3, con un acceso autorizado por un administrador. AWS Lake Formation	Datos compartidos de Amazon Redshift, datos estructurados de Amazon S3 *A través de Amazon Redshift, autorizado a través de AWS Lake Formation	• Conecte Amazon Redshift con el centro de identidades de IAM a través de Amazon QuickSight en la guía de administración de Amazon Redshift. • Cómo conectarse AWS Lake Formation con el centro de identidad de IAM en la guía para desarrolladores.AWS Lake Formation • Simplifique la administración del acceso con Amazon Redshift y, AWS Lake Formation para los usuarios de un proveedor de identidad externo, en el blog sobre AWS macrodatos.

Editor de consultas de Amazon Redshift v2

Puede utilizar el editor de consultas Amazon Redshift v2 como aplicación de inicio para los siguientes casos de uso de propagación de identidades de confianza.

Descripción	Otros servicios utilizados AWS	Más información
Los usuarios del editor de consultas de Amazon Redshift v2 pueden consultar los datos de Amazon Redshift. Un administr	Amazon Redshift	• Conecte Redshift con IAM Identity Center para ofrecer a los usuarios una experiencia de inicio de sesión único en

Descripción	Otros servicios utilizados AWS	Más información
ador de Amazon Redshift concede el acceso a los datos en Amazon Redshift.		la Guía de administración de Amazon Redshift. • Conéctese a una base de datos de Amazon Redshift en la Guía de administración de Amazon Redshift. • Intégrelo Okta con Amazon Redshift Query Editor V2 mediante el sencillo inicio AWS IAM Identity Center de sesión único en el AWS blog de big data.
Los usuarios del editor de consultas de Amazon Redshift v2 pueden consultar tablas externas de Amazon Redshift Spectrum en busca de datos estructurados en Amazon S3, con acceso autorizado por un administrador. AWS Lake Formation	Amazon Redshift Spectrum, datos estructurados de Amazon S3 *A través de Amazon Redshift Spectrum, autorizado a través de AWS Lake Formation	• Conecte Redshift con IAM Identity Center para ofrecer a los usuarios una experiencia de inicio de sesión único en la Guía de administración de Amazon Redshift. • Conéctese a una base de datos de Amazon Redshift en la Guía de administración de Amazon Redshift. • Conexión AWS Lake Formation con el centro de identidad de IAM en la AWS Lake Formation guía para desarrolladores.

Descripción	Otros servicios utilizados AWS	Más información
Los usuarios del editor de consultas de Amazon Redshift v2 pueden consultar los datos compartidos de Amazon Redshift con un acceso autorizado por un administrador. AWS Lake Formation	datos compartidos de Amazon Redshift, AWS Lake Formation	• Conéctese a una base de datos de Amazon Redshift en la Guía de administración de Amazon Redshift. • Conexión AWS Lake Formation con el centro de identidad de IAM en la AWS Lake Formation guía para desarrolladores.

Aplicaciones de inteligencia empresarial de terceros

Puede usar una aplicación de inteligencia empresarial de terceros, como Tableau, como aplicación de inicio para casos de uso específicos de propagación de identidades confiables. Las aplicaciones de inteligencia empresarial de terceros modificadas pueden transmitir al controlador de Amazon Redshift la identidad de un usuario a través de tokens de identidad o de acceso de OAuth para solicitar datos a Amazon Redshift, con un acceso autorizado por un administrador de Amazon Redshift.

Aplicaciones desarrolladas a medida

Puede utilizar sus propias aplicaciones desarrolladas a medida como aplicación de inicio para los siguientes casos de uso fiables de propagación de identidades.

Descripción	Otros servicios utilizados AWS	Más información
Cree una aplicación que autentique a los usuarios a través de un servidor de autorización de OAuth AWS IAM Identity Center y, a continuación, utilice un IAM para obtener una credencial de rol de IAM con	AWS IAM Identity Center, datos no estructurados de Amazon S3 *Autorizado a través de Amazon S3 Access Grants	• Las concesiones de acceso de Amazon S3 y las identidades de los directorios corporativos en la guía del usuario de Amazon Simple Storage Service.

Descripción	Otros servicios utilizados AWS	Más información
una identidad mejorada. Esta credencial se utiliza para solicitar acceso a datos no estructurados en Amazon S3, con acceso autorizado por un administrador de Amazon S3 Access Grants.		• Cómo desarrollar una aplicación de datos orientada al usuario con IAM Identity Center y Amazon S3 Access Grants (parte 1) y (parte 2) en el blog de AWS almacenamiento.
Cree una aplicación personalizada que interactúe con Amazon Q Business para responder a las preguntas de los usuarios en función de su propio contenido y los permisos del usuario.	Centro de identidad de IAM, Amazon Q Business	• Habilite y configure una instancia del centro de identidad de IAM en la Guía del usuario de Amazon Q Business. • Cómo utilizar las aplicaciones AWS gestionadas con IAM Identity Center: habilite Amazon Q sin migrar los flujos de federación de IAM existentes en el AWS blog de seguridad.

Configuración de la propagación de identidades de confianza

La propagación fiable de la identidad permite que las aplicaciones se autentiquen de distintas maneras para poder transmitir la identidad de un usuario a los servicios. AWS La configuración de la propagación de identidades de confianza varía en función de los tipos de aplicaciones y de la forma en que se autentican.

> **Note**
>
> Debe configurar un emisor de token de confianza si tiene aplicaciones administradas por el cliente que solicitan acceso a las aplicaciones AWS administradas, pero no utilizan AWS las API para conectarse.

Temas

- Requisitos y consideraciones previos
- Uso de la propagación de identidades confiable con aplicaciones AWS administradas
- Uso de la propagación de identidades de confianza con aplicaciones administradas por el cliente

Requisitos y consideraciones previos

Antes de configurar la propagación de identidades de confianza, revise los siguientes requisitos previos y consideraciones.

Temas

- Requisitos previos
- Consideraciones adicionales

Requisitos previos

Para utilizar la propagación de identidades de confianza, asegúrese de que el entorno cumple los siguientes requisitos previos.

- Implementación de IAM Identity Center con usuarios y grupos aprovisionados

  Para utilizar la propagación de identidades de confianza, debe habilitar IAM Identity Center y aprovisionar usuarios y grupos. Para obtener más información, consulte Introducción a las tareas habituales en IAM Identity Center.

  Instancia de organización recomendada: le recomendamos que utilice una instancia de organización de IAM Identity Center que habilite en la cuenta de administración de AWS Organizations. Si piensa utilizar una propagación de identidades fiable para permitir a los usuarios acceder a los AWS servicios y recursos relacionados de distintas partes de la misma organización, puede delegar la administración de su instancia de IAM Identity Center Cuentas de AWS en una cuenta de miembro.

  Si planea usar una instancia de cuenta única del Centro de identidad de IAM, todos los AWS servicios y recursos a los que desee que accedan los usuarios mediante la propagación de identidad confiable deben residir en la misma cuenta independiente Cuenta de AWS o en la misma cuenta de miembro de la organización en la que habilitó el Centro de identidad de IAM. Para obtener más información, consulte Instancias de cuenta de IAM Identity Center.
- Para aplicaciones AWS gestionadas, conexión al IAM Identity Center

Para utilizar una propagación de identidad fiable, las aplicaciones AWS gestionadas deben integrarse con el Centro de identidades de IAM.

Consideraciones adicionales

Tenga en cuenta las siguientes consideraciones adicionales para utilizar la propagación de identidades de confianza.

- No modifique la configuración Requerir asignaciones para las aplicaciones AWS gestionadas

  AWS las aplicaciones administradas tienen una configuración predeterminada que determina si las asignaciones son necesarias para los usuarios y los grupos. Le recomendamos que no modifique esta configuración. Incluso si ha configurado permisos detallados que permiten a los usuarios acceder a recursos específicos, la modificación de la configuración Requerir asignaciones puede provocar un comportamiento inesperado, como la interrupción del acceso de los usuarios a estos recursos.
- No se requieren permisos de varias cuentas (conjuntos de permisos)

  La propagación de identidades de confianza no requiere que configure permisos de varias cuentas (conjuntos de permisos). Puede habilitar IAM Identity Center y utilizarlo únicamente para la propagación de identidades de confianza.

Uso de la propagación de identidades confiable con aplicaciones AWS administradas

La propagación fiable de la identidad permite a una aplicación AWS gestionada solicitar el acceso a los datos de AWS los servicios en nombre de un usuario. La administración del acceso a los datos se basa en la identidad del usuario, por lo que los administradores pueden conceder el acceso en función de la pertenencia actual de los usuarios a grupos y usuarios. La identidad del usuario, las acciones realizadas en su nombre y otros eventos se registran en registros y CloudTrail eventos específicos del servicio.

La propagación de identidades de confianza se basa en el estándar OAuth 2.0. Para utilizar esta capacidad, las aplicaciones AWS gestionadas deben integrarse con el IAM Identity Center. AWS los servicios de análisis pueden proporcionar interfaces basadas en controladores que permitan a una aplicación compatible utilizar una propagación de identidad fiable. Por ejemplo, los controladores de JDBC, ODBC y Python permiten que las herramientas de consulta compatibles utilicen la

propagación de identidades de confianza sin necesidad de completar pasos de configuración adicionales.

Temas

Configure aplicaciones AWS gestionadas para una propagación de identidad fiable

AWS los servicios que admiten la propagación de identidades confiable proporcionan una interfaz de usuario administrativa y API que puede usar para configurar esta capacidad. No es necesario que configure nada en IAM Identity Center para estos servicios.

A continuación se presenta el proceso de alto nivel para configurar un AWS servicio de propagación de identidades confiable. Los pasos específicos varían según la interfaz administrativa y las API que proporciona la aplicación.

1. Uso de la consola de la aplicación o las API para conectar la aplicación a su instancia de IAM Identity Center

   Utilice la consola de la aplicación AWS gestionada o las API de la aplicación para conectar la aplicación a su instancia de IAM Identity Center. Cuando utiliza la consola de la aplicación, la interfaz de usuario administrativa incluye un widget que agiliza el proceso de configuración y conexión.
2. Uso de la consola de la aplicación o las API para configurar el acceso de los usuarios a los recursos de la aplicación

   Complete este paso para autorizar a qué recursos o datos puede acceder un usuario. El acceso se basa en la identidad del usuario o en su pertenencia a un grupo. El modelo de autorización varía en función de la aplicación.

> **Important**
>
> Debe completar este paso para permitir que los usuarios accedan a los recursos del servicio de AWS . De lo contrario, los usuarios no podrán acceder a los recursos, incluso si la aplicación solicitante está autorizada a solicitar acceso al servicio.

Flujos de solicitudes de propagación de identidad fiables para aplicaciones AWS gestionadas

Todos los flujos de propagación de identidad fiables a las aplicaciones AWS gestionadas deben comenzar con una aplicación que obtenga un token del IAM Identity Center. Este token es obligatorio porque contiene una referencia a un usuario conocido en IAM Identity Center y a las aplicaciones que están registradas en IAM Identity Center.

En las siguientes secciones se describen las formas en que una aplicación AWS gestionada puede obtener un token del Centro de Identidad de IAM para iniciar la propagación de identidades de forma fiable.

Temas

- Autenticación de IAM Identity Center basada en la web
- Solicitudes de autenticación iniciadas por el usuario y basadas en la consola

Autenticación de IAM Identity Center basada en la web

Para este flujo, la aplicación AWS gestionada proporciona una experiencia de inicio de sesión único basada en la web mediante el IAM Identity Center para la autenticación.

Cuando un usuario abre una aplicación AWS gestionada, se activa un flujo de inicio de sesión único que utiliza el IAM Identity Center. Si no hay ninguna sesión activa para el usuario en IAM Identity Center, verá una página de inicio de sesión basada en el origen de identidad que haya especificado e IAM Identity Center creará una sesión para el usuario.

El Centro de Identidad de IAM proporciona a la aplicación AWS gestionada un token que incluye la identidad del usuario y una lista de audiencias (AUD) y ámbitos relacionados para los que la aplicación está registrada. A continuación, la aplicación puede utilizar el token para realizar solicitudes a otros servicios de AWS de recepción.

Solicitudes de autenticación iniciadas por el usuario y basadas en la consola

Para este flujo, la aplicación AWS gestionada proporciona una experiencia de consola que los usuarios inician.

En este caso, la aplicación AWS gestionada se ingresa desde la consola AWS de administración después de asumir un rol. Para que la aplicación obtenga un token, el usuario debe iniciar un proceso para que la aplicación autentique al usuario. Esto inicia la autenticación mediante IAM Identity Center, que redirigirá al usuario al origen de identidad que haya configurado.

Después de que una aplicación obtenga un token

Una vez que la aplicación solicitante obtiene un token de IAM Identity Center, la aplicación lo actualiza periódicamente y se podrá utilizar durante toda la sesión del usuario. La aplicación, durante este tiempo, podría hacer lo siguiente:

- Obtener más información sobre el token para determinar quién es el usuario y qué ámbitos puede utilizar la aplicación con otras aplicaciones administradas por AWS receptoras.
- Transfiera el token en las llamadas a otras aplicaciones AWS administradas receptoras que admitan el uso de tokens.
- Obtenga sesiones de rol de IAM con identidad mejorada que pueda utilizar para realizar solicitudes a otras aplicaciones AWS gestionadas que utilicen AWS Signature Version 4.

  Una sesión de rol de IAM con identidad mejorada es una sesión de rol de IAM que contiene la identidad propagada del usuario almacenada en un token que ha creado IAM Identity Center.

Sesiones de rol de IAM con identidad mejorada

AWS Security Token Service Esto permite que una aplicación obtenga una sesión de rol de IAM con identidad mejorada. AWS las aplicaciones administradas que admiten el contexto de usuario en una sesión de rol pueden usar la información de identidad para autorizar el acceso en función del usuario que se encuentre en la sesión de rol. Este nuevo contexto permite a las aplicaciones gestionadas realizar solicitudes a las aplicaciones AWS gestionadas que admiten la propagación fiable de la identidad mediante solicitudes de la API AWS Signature versión 4.

Cuando una aplicación AWS gestionada utiliza una sesión de rol de IAM con identidad mejorada para acceder a un recurso, CloudTrail registra la identidad del usuario (ID de usuario), la sesión de inicio y la acción realizada.

Cuando una aplicación realiza una solicitud a una aplicación receptora mediante una sesión de rol de IAM con identidad mejorada, agrega contexto a la sesión para que la aplicación receptora pueda autorizar el acceso en función de la identidad del usuario, de su pertenencia a un grupo o del rol de IAM. Si la aplicación receptora o el recurso solicitado no están configurados para autorizar el acceso en función de la identidad del usuario o de su pertenencia a un grupo, las aplicaciones receptoras compatibles con la propagación de identidades de confianza devolverán un error.

Para evitar este problema, lleve a cabo alguna de las siguientes operaciones:

- Compruebe que la aplicación receptora esté conectada a IAM Identity Center.
- Utilice la consola de la aplicación receptora o las API de las aplicaciones a fin de configurar la aplicación para que autorice el acceso a los recursos en función de la identidad del usuario o de su pertenencia a un grupo. Los requisitos de configuración varían en función de la aplicación.

Para obtener más información, consulte la documentación de la aplicación administrada por AWS receptora.

Tipos de sesiones de rol de IAM con identidad mejorada

Una aplicación obtiene una sesión de rol de IAM con identidad mejorada realizando una solicitud a la AWS STS `AssumeRole` API y pasando una afirmación de contexto en el parámetro de la solicitud. `ProvidedContexts` `AssumeRole` La aserción de contexto se obtiene de la notificación `idToken` que está disponible en la respuesta a la solicitud `SSO OIDC` `CreateTokenWithIAM`.

AWS STS puede crear dos tipos diferentes de sesiones de roles de IAM con identidad mejorada, en función de la afirmación de contexto proporcionada a la solicitud: `AssumeRole`

- Sesiones en las que solo se registra la identidad del usuario. CloudTrail
- Sesiones que permiten la autorización en función de la identidad del usuario propagada y en las que se registra. CloudTrail

Para obtener una sesión de rol de IAM con identidad mejorada AWS STS que solo proporcione información de auditoría registrada en un CloudTrail registro, indique el valor de la `sts:audit_context` reclamación a la solicitud. `AssumeRole` Para obtener una sesión que también permita al AWS servicio receptor autorizar al usuario del Centro de Identidad de IAM a realizar una acción, indique el valor de la `sts:identity_context` reclamación a la solicitud. `AssumeRole` Solo puede proporcionar un contexto.

Sesiones de rol de IAM con identidad mejorada creadas mediante **`sts:audit_context`**

Cuando se realiza una solicitud a un AWS servicio mediante una sesión de rol de IAM con identidad mejorada creada con ellasts:audit_context, el centro de identidad de IAM del usuario inicia sesión en el userId elemento. CloudTrail OnBehalfOf

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

> **Note**
>
> Estas sesiones no se pueden utilizar para autorizar al usuario de Identity Center. Sin embargo, sí se pueden utilizar para autorizar el rol de IAM.

Para obtener este tipo de sesión de rol AWS STS, indique el valor del `sts:audit_context` campo de la `AssumeRole` solicitud en el parámetro de solicitud. `ProvidedContexts` Utilice `arn:aws:iam::aws:contextProvider/IdentityStore` como valor para `ProviderArn`.

Sesiones de rol de IAM con identidad mejorada creadas mediante **`sts:identity_context`**

Cuando un usuario realiza una solicitud a un AWS servicio mediante una sesión de rol de IAM con identidad mejorada creada con ellasts:identity_context, el centro userId de identidad de IAM del usuario inicia sesión CloudTrail en el onBehalfOf elemento de la misma manera que en una sesión creada con. sts:audit_context

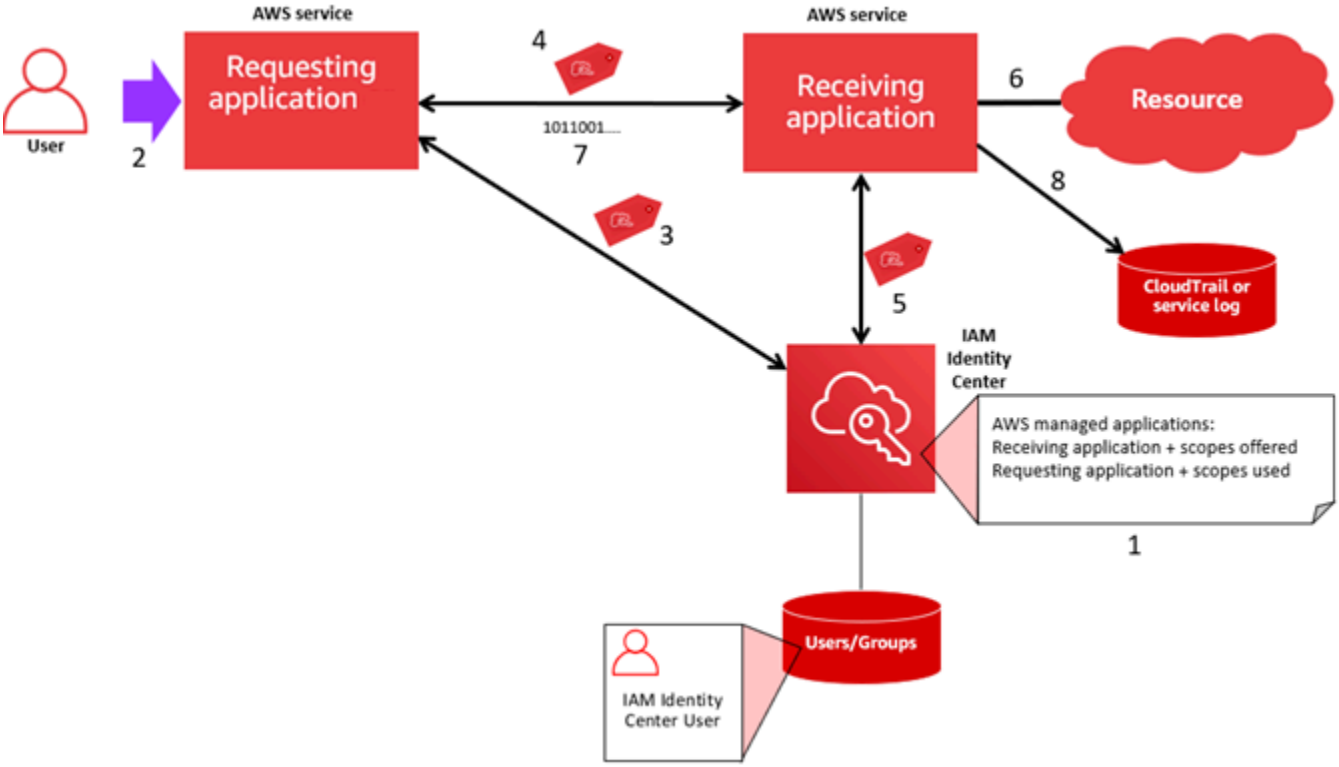
Además de registrar el registro del usuario del Centro de Identidad de IAM CloudTrail, userId las API compatibles también utilizan este tipo de sesión para autorizar acciones en función de la identidad del usuario propagada. Para ver una lista de las acciones de IAM para las API compatibles, consulta la AWSIAMIdentityCenterAllowListForIdentityContext AWS política gestionada. Esta política AWS gestionada se proporciona como política de sesión cuando se crea una sesión de rol de IAM con identidad mejorada. sts:identity_context La política impide utilizar la sesión de rol con servicios no compatibles. AWS

Para obtener este tipo de sesión de rol AWS STS, proporcione el valor del sts:identity_context campo a la AssumeRole solicitud en el parámetro de ProvidedContexts solicitud. Utilice arn:aws:iam::aws:contextProvider/IdentityStore como valor para ProviderArn.

Proceso de configuración y flujo de solicitudes para las aplicaciones AWS administradas

En esta sección se describe el proceso de configuración y el flujo de solicitud para las aplicaciones administradas por AWS que utilizan una propagación de identidades de confianza y que proporcionan una experiencia de inicio de sesión único basada en la web.

En el diagrama siguiente se proporciona una descripción general de este proceso.



En los pasos siguientes tiene más información sobre este proceso.

1. Utilice la consola de la aplicación AWS gestionada o las API de la aplicación para hacer lo siguiente:
   a. Conectar la aplicación a su instancia de IAM Identity Center.
   b. Configurar los permisos para autorizar a qué recursos de la aplicación puede acceder un usuario.
2. El flujo de solicitudes comienza cuando un usuario abre una aplicación AWS administrada que puede solicitar acceso a los recursos (una aplicación solicitante).
3. Para obtener un token que permita acceder a la aplicación AWS gestionada receptora, la aplicación AWS gestionada solicitante inicia una solicitud de inicio de sesión en el IAM Identity Center.

   Si el usuario no ha iniciado sesión, IAM Identity Center activa un flujo de autenticación del usuario en el origen de identidad que haya especificado. De este modo, se crea una nueva sesión en el portal de AWS acceso para el usuario con la duración que haya configurado en el Centro de identidades de IAM. A continuación, el IAM Identity Center genera un token asociado a la sesión y la aplicación puede funcionar durante el resto de la sesión del usuario en el portal de AWS

acceso. Si el usuario cierra sesión en su aplicación o si se elimina su sesión, la sesión finalizará automáticamente en un plazo de dos horas.

4. La aplicación AWS gestionada inicia una solicitud a la aplicación receptora y proporciona su token.
5. La aplicación receptora realiza llamadas a IAM Identity Center para obtener la identidad del usuario y los ámbitos codificados en el token. La aplicación receptora también puede realizar solicitudes para obtener los atributos del usuario o la pertenencia del usuario a grupos desde el directorio de Identity Center.
6. La aplicación receptora utiliza su configuración de autorización para determinar si el usuario está autorizado a acceder al recurso de la aplicación solicitado.
7. Si el usuario está autorizado a acceder al recurso de la aplicación solicitado, la aplicación receptora responde a la solicitud.
8. La identidad del usuario, las acciones realizadas en su nombre y otros eventos registrados en los registros de la aplicación receptora y los eventos de AWS CloudTrail . La forma específica en que se registra esta información varía en función de la aplicación.

Uso de la propagación de identidades de confianza con aplicaciones administradas por el cliente

La propagación fiable de la identidad permite a una aplicación gestionada por el cliente solicitar el acceso a los datos de AWS los servicios en nombre de un usuario. La administración del acceso a los datos se basa en la identidad del usuario, por lo que los administradores pueden conceder el acceso en función de la pertenencia actual de los usuarios a grupos y usuarios. La identidad del usuario, las acciones realizadas en su nombre y otros eventos se registran en registros y CloudTrail eventos específicos del servicio.

Con una propagación de identidad fiable, un usuario puede iniciar sesión en una aplicación gestionada por el cliente y esa aplicación puede transmitir la identidad del usuario en las solicitudes de acceso a los datos de los servicios. AWS

> **Important**
>
> Para acceder a un AWS servicio, las aplicaciones gestionadas por el cliente deben obtener un token de un emisor de token de confianza, externo al IAM Identity Center. Un emisor de tokens de confianza es un servidor de autorización de OAuth 2.0 que crea tokens firmados. Estos tokens autorizan a las aplicaciones que inician solicitudes de acceso a AWS

los servicios (aplicaciones receptoras). Para obtener más información, consulte Uso de aplicaciones con un emisor de tokens de confianza.

Temas

- Configuración de aplicaciones de OAuth 2.0 administradas por el cliente para la propagación de identidades de confianza
- Especificación de las aplicaciones de confianza

Configuración de aplicaciones de OAuth 2.0 administradas por el cliente para la propagación de identidades de confianza

Para configurar una aplicación de OAuth 2.0 administrada por el cliente para la propagación de identidades de confianza, primero debe agregarla a IAM Identity Center. Siga el procedimiento que se indica a continuación para agregar su aplicación a IAM Identity Center.

Temas

- Paso 1: selección del tipo de aplicación
- Paso 2: especificación de los detalles de la aplicación
- Paso 3: especificación de la configuración de autenticación
- Paso 4: especificación de las credenciales de la aplicación
- Paso 5: revisión y configuración

Paso 1: selección del tipo de aplicación

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, seleccione Tengo una aplicación que quiero configurar.
6. En Tipo de aplicación, seleccione OAuth 2.0.
7. Seleccione Siguiente para continuar a la página siguiente, Paso 2: especificación de los detalles de la aplicación.

Paso 2: especificación de los detalles de la aplicación

1. En la página Especificar detalles de la aplicación, en Nombre y descripción de la aplicación, ingrese un Nombre de visualización para la aplicación, como **MyApp**. Escriba una descripción en Descripción.
2. En Método de asignación de usuarios y grupos, seleccione una de las siguientes opciones:

   - Requerir asignaciones: permita que solo los usuarios y grupos de IAM Identity Center que estén asignados a esta aplicación accedan a la aplicación.

     Visibilidad del mosaico de la aplicación: solo los usuarios que estén asignados a la aplicación directamente o mediante una asignación grupal pueden ver el mosaico de la aplicación en el portal de AWS acceso, siempre que la visibilidad de la aplicación en el portal de AWS acceso esté configurada como Visible.
   - No requerir asignaciones: permita que todos los usuarios y grupos autorizados de IAM Identity Center accedan a esta aplicación.

     Visibilidad del icono de la aplicación: el icono de la aplicación está visible para todos los usuarios que inicien sesión en el portal de acceso de AWS , a menos que la opción Visibilidad de la aplicación en el portal de acceso de AWS esté configurada como No visible.
3. En Portal de acceso de AWS , ingrese la URL desde la que los usuarios pueden acceder a la aplicación y especifique si el icono de la aplicación estará visible o no en el portal de acceso de AWS . Si selecciona No visible, ni siquiera los usuarios asignados podrán ver el icono de la aplicación.
4. Expanda Etiquetas (opcional), seleccione Agregar etiqueta nueva y especifique los valores de Clave y Valor (opcional).

   Para obtener más información acerca de las etiquetas, consulte Etiquetado de recursos de AWS IAM Identity Center.
5. Seleccione Siguiente y pase a la página siguiente, Paso 3: especificación de la configuración de autenticación.

Paso 3: especificación de la configuración de autenticación

Para agregar una aplicación administrada por el cliente que sea compatible con OAuth 2.0 a IAM Identity Center, debe especificar un emisor de tokens de confianza. Un emisor de tokens de confianza es un servidor de autorización de OAuth 2.0 que crea tokens firmados. Estos

tokens autorizan a las aplicaciones que inician solicitudes (solicitudes de solicitudes) de acceso a aplicaciones AWS administradas (aplicaciones receptoras).

1. En la página Especificar configuración de autenticación, en Emisores de tokens de confianza, realice una de las siguientes acciones:

   - Para usar un emisor de tokens de confianza existente:

     Seleccione la casilla de verificación situada junto al nombre del emisor de tokens de confianza que desea usar.

   - Para agregar un nuevo emisor de tokens de confianza:

     1. Seleccione Crear emisor de tokens de confianza.
     2. Se abrirá una nueva pestaña del navegador. Siga los pasos del 5 al 8 que se indican en Cómo agregar un emisor de tokens de confianza a la consola de IAM Identity Center.
     3. Tras completar estos pasos, regrese a la ventana del navegador que está utilizando para configurar la aplicación y seleccione el emisor de tokens de confianza que acaba de agregar.
     4. En la lista de emisores de tokens de confianza, seleccione la casilla de verificación situada junto al nombre del emisor de tokens de confianza que acaba de agregar.

        Tras seleccionar un emisor de tokens de confianza, aparece la sección Configurar los emisores de tokens de confianza seleccionados.

2. En Configurar los emisores de tokens de confianza seleccionados, ingrese la notificación de audiencia. La notificación de audiencia identifica a la audiencia objetivo (destinatarios) del token que ha generado el emisor de tokens de confianza. Para obtener más información, consulte Notificación de audiencia.
3. Para evitar que sus usuarios tengan que volver a autenticarse cuando utilicen esta aplicación, seleccione Actualizar automáticamente la autenticación de usuario para la sesión activa de la aplicación. Si está seleccionada, esta opción actualiza el token de acceso de la sesión cada 60 minutos, hasta que la sesión caduque o el usuario la finalice.
4. Seleccione Siguiente y pase a la página siguiente, Paso 4: especificación de las credenciales de la aplicación.

Paso 4: especificación de las credenciales de la aplicación

Complete los pasos de este procedimiento para especificar las credenciales que la aplicación utilizará para realizar acciones de intercambio de tokens con aplicaciones de confianza. Estas credenciales se utilizan en una política basada en recursos. La política requiere que especifique una entidad principal que tenga permisos para realizar las acciones que se especifican en la política. Debe especificar una entidad principal, incluso si las aplicaciones de confianza se encuentran en la misma Cuenta de AWS.

> **Note**
>
> Cuando establezca permisos con políticas, conceda solo los permisos necesarios para llevar a cabo una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos.

Esta política requiere la acción `sso-oauth:CreateTokenWithIAM`.

1. En la página Especificar las credenciales de la aplicación, lleve a cabo una de las siguientes acciones:

   - Para especificar rápidamente uno o varios roles de IAM:

     1. Seleccione Ingresar uno o más roles de IAM.
     2. En Ingresar roles de IAM, especifique el nombre de recurso de Amazon (ARN) de un rol de IAM existente. Para especificar el ARN, utilice la siguiente sintaxis. La parte de la región del ARN está en blanco porque los recursos de IAM son globales.

        ```
        arn:aws:iam::account:role/role-name-with-path
        ```

        Para obtener más información, consulte Concesión de acceso entre cuentas con políticas de recursos y ARN de IAM en la Guía del usuario de AWS Identity and Access Management .

   - Para editar la política manualmente (obligatorio si no especificas AWS credenciales):

     1. Seleccione Editar la política de la aplicación.
     2. Para modificar la política, escriba o pegue texto en el cuadro de texto JSON.

3. Resuelva las advertencias de seguridad, errores o advertencias generales que hayan surgido durante la validación de la política. Para obtener más información, consulte Validación de políticas de IAM en la Guía del usuario de AWS Identity and Access Management .

2. Seleccione Siguiente y pase a la página siguiente, Paso 5: revisión y configuración.

Paso 5: revisión y configuración

1. En la página Revisar y configurar, revise las elecciones que ha realizado. Para realizar cambios, seleccione la sección de configuración que desee, seleccione Editar y, a continuación, realice los cambios necesarios.
2. Cuando haya terminado, seleccione Agregar aplicación.
3. La aplicación que ha agregado aparece en la lista Aplicaciones administradas por el cliente.
4. Tras configurar la aplicación gestionada por el cliente en el Centro de identidad de IAM, debe especificar uno o más AWS servicios, o aplicaciones de confianza, para la propagación de la identidad. Esto permite a los usuarios iniciar sesión en la aplicación administrada por el cliente y acceder a los datos de la aplicación de confianza.

   Para obtener más información, consulte Especificación de las aplicaciones de confianza .

Especificación de las aplicaciones de confianza

Tras configurar la aplicación gestionada por el cliente, debe especificar uno o más AWS servicios o aplicaciones de confianza para la propagación de la identidad. Especifique un AWS servicio que contenga datos a los que los usuarios de las aplicaciones gestionadas por el cliente necesiten acceder. Cuando los usuarios inicien sesión en la aplicación administrada por el cliente, esa aplicación transferirá la identidad de los usuarios a la aplicación de confianza.

Utilice el siguiente procedimiento para seleccionar un servicio y, a continuación, especifique las aplicaciones individuales que son de confianza para ese servicio.

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.

4. En la lista Aplicaciones administradas por el cliente, seleccione la aplicación de OAuth 2.0 que desea que inicie solicitudes de acceso. Esta es la aplicación en la que inician sesión los usuarios.
5. En la página de detalles, en Aplicaciones de confianza para la propagación de identidades, seleccione Especificar aplicaciones de confianza.
6. En Tipo de configuración, seleccione Aplicaciones individuales y acceso específico y, a continuación, seleccione Siguiente.
7. En la página Seleccionar servicio, seleccione el servicio de AWS que tenga aplicaciones en las que la aplicación administrada por el cliente pueda confiar para propagar identidades y, a continuación, seleccione Siguiente.

   El servicio que seleccione define las aplicaciones que son de confianza. Seleccionará las aplicaciones en el siguiente paso.
8. En la página Seleccionar aplicaciones, seleccione Aplicaciones individuales, active la casilla de verificación de cada aplicación que pueda recibir solicitudes de acceso y, a continuación, seleccione Siguiente.
9. En la página Configurar el acceso, en Método de configuración, realice una de las siguientes acciones:

   - Seleccionar el acceso por aplicación: seleccione esta opción para configurar diferentes niveles de acceso para cada aplicación. Seleccione la aplicación para la que desee configurar el nivel de acceso y, a continuación, seleccione Editar acceso. En Nivel de acceso que aplicar, cambie los niveles de acceso según sea necesario y, a continuación, seleccione Guardar cambios.
   - Aplicar el mismo nivel de acceso a todas las aplicaciones: seleccione esta opción si no tiene que configurar los niveles de acceso por aplicación.
10. Elija Siguiente.
11. En la página Revisar configuración, revise las elecciones que ha realizado. Para realizar cambios, seleccione la sección de configuración que desee, seleccione Editar acceso y, a continuación, realice los cambios necesarios.
12. Cuando haya terminado, seleccione Aplicaciones de confianza.

Uso de aplicaciones con un emisor de tokens de confianza

Los emisores de tokens confiables le permiten utilizar la propagación de identidades confiable con aplicaciones que se autentican fuera de ellas. AWS Con los emisores de tokens de confianza, puede

autorizar a estas aplicaciones para que realicen solicitudes en nombre de sus usuarios para acceder a las aplicaciones administradas por AWS .

En los siguientes temas se describe cómo funcionan los emisores de tokens de confianza y se proporcionan instrucciones de configuración.

Temas

Descripción general de los emisores de tokens de confianza

La propagación de identidades fiable proporciona un mecanismo que permite a las aplicaciones que se autentican fuera de AWS ella realizar solicitudes en nombre de sus usuarios mediante el uso de un emisor de token de confianza. Un emisor de tokens de confianza es un servidor de autorización de OAuth 2.0 que crea tokens firmados. Estos tokens autorizan a las aplicaciones que inician solicitudes (solicitudes de solicitudes) de acceso a AWS los servicios (aplicaciones receptoras). Las aplicaciones solicitantes inician las solicitudes de acceso en nombre de los usuarios que el emisor de tokens de confianza autentica. Tanto el emisor de tokens de confianza como IAM Identity Center conocen a los usuarios.

AWS los servicios que reciben solicitudes gestionan la autorización detallada de sus recursos en función de sus usuarios y la pertenencia a grupos, tal como se representa en el directorio de Identity Center. AWS los servicios no pueden usar directamente los tokens del emisor externo del token.

Para resolver este problema, IAM Identity Center proporciona una forma para que la aplicación solicitante, o un controlador de AWS que utilice la aplicación solicitante, intercambie el token que emite el emisor de tokens de confianza por un token generado por IAM Identity Center. El token que genera IAM Identity Center hace referencia al usuario correspondiente de IAM Identity Center. La aplicación solicitante, o el controlador, utiliza el nuevo token para iniciar una solicitud a la aplicación receptora. Como el nuevo token hace referencia al usuario correspondiente de IAM Identity Center, la aplicación receptora puede autorizar el acceso solicitado en función del usuario o de su grupo, tal como se representa en IAM Identity Center.

> **Important**
>
> Elegir un servidor de autorización de OAuth 2.0 para agregarlo como emisor de tokens de confianza es una decisión de seguridad que debe estudiarse detenidamente. Seleccione únicamente emisores de tokens de confianza para realizar las siguientes tareas:
>
> - Autenticar al usuario especificado en el token.
> - Autorizar el acceso de ese usuario a la aplicación receptora.
> - Generar un token que IAM Identity Center pueda intercambiar por un token creado por IAM Identity Center.

Requisitos previos y consideraciones para los emisores de tokens de confianza

Antes de configurar un emisor de tokens de confianza, revise los siguientes requisitos previos y consideraciones.

- Configuración de un emisor de tokens de confianza

  Debes configurar un servidor de autorización de OAuth 2.0 (el emisor de tokens de confianza). Aunque el emisor del token de confianza suele ser el proveedor de identidad que utilizas como fuente de identidad para el Centro de Identidad de IAM, no tiene por qué serlo. Para obtener información sobre cómo configurar el emisor de token de confianza, consulta la documentación del proveedor de identidad correspondiente.

  > **Note**
  >
  > Puede configurar hasta 10 emisores de tokens de confianza para utilizarlos con IAM Identity Center, siempre que asigne la identidad de cada usuario del emisor de tokens de confianza a un usuario correspondiente de IAM Identity Center.

- El servidor de autorización de OAuth 2.0 (el emisor de tokens de confianza) que crea el token debe tener un punto de conexión de detección de OpenID Connect (OIDC) que IAM Identity Center pueda utilizar para obtener claves públicas a fin de verificar las firmas de los tokens. Para obtener más información, consulte URL del punto final de detección del OIDC (URL del emisor).
- Tokens emitidos por el emisor de token de confianza

  Los tokens del emisor de tokens de confianza deben cumplir los siguientes requisitos:

  - El token debe estar firmado y en formato JSON Web Token (JWT) mediante el algoritmo RS256.
  - El token debe contener las siguientes afirmaciones:
    - Emisor (es): la entidad que emitió el token. Este valor debe coincidir con el valor que está configurado en el punto final de detección del OIDC (URL del emisor) en el emisor del token de confianza.
    - Asunto (sub): el usuario autenticado.
    - Público (aud): el destinatario previsto del token. Este es el AWS servicio al que se accederá después de cambiar el token por un token desde el IAM Identity Center. Para obtener más información, consulte Notificación de audiencia.
    - Tiempo de caducidad (exp): el tiempo después del cual caduca el token.
    -
  - El token puede ser un token de identidad o un token de acceso.
  - El token debe tener un atributo que pueda asignarse de forma exclusiva a un usuario de IAM Identity Center.
- Notificaciones opcionales

  IAM Identity Center admite todas las notificaciones opcionales que se definen en RFC 7523. Para obtener más información, consulte la sección 3: JWT Format and Processing Requirements de esta RFC.

  Por ejemplo, el token puede contener una notificación de JTI (ID de JWT). Esta notificación, cuando está presente, impide que los tokens que tienen el mismo JTI se reutilicen para el intercambio de tokens. Para obtener más información acerca de las notificaciones de JTI, consulte Detalles de la notificación de JTI.
- Configuración de IAM Identity Center para que funcione con un emisor de tokens de confianza

  También debe habilitar IAM Identity Center, configurar el origen de identidad de IAM Identity Center y aprovisionar a los usuarios que correspondan a los usuarios del directorio del emisor de tokens de confianza.

  Para ello, debe hacer una de las siguientes acciones:
  - Sincronice los usuarios con IAM Identity Center mediante el protocolo del sistema de administración de identidades entre dominios (SCIM) 2.0.
  - Cree los usuarios directamente en IAM Identity Center.

> **Note**
>
> Los emisores de tokens de confianza no son compatibles si utiliza Active Directory Domain Service como origen de identidad.

Detalles de la notificación de JTI

Si IAM Identity Center recibe una solicitud para intercambiar un token que IAM Identity Center ya ha intercambiado, se produce un error en la solicitud. Para detectar e impedir la reutilización de un token para los intercambios de tokens, puede incluir una notificación de JTI. IAM Identity Center protege contra la repetición de tokens en función de las notificaciones que figuran en el token.

No todos los servidores de autorización de OAuth 2.0 agregan una notificación de JTI a los tokens. Es posible que algunos servidores de autorización de OAuth 2.0 no permitan agregar un JTI como notificación personalizada. Los servidores de autorización de OAuth 2.0 que admiten el uso de una notificación de JTI pueden agregar esta notificación únicamente a los tokens de identidad, a los de acceso o a ambos. Para obtener más información, consulte la documentación del servidor de autorización de OAuth 2.0.

Para obtener información sobre cómo crear aplicaciones que intercambien tokens, consulte la documentación de la API de IAM Identity Center. Para obtener información sobre cómo configurar una aplicación administrada por el cliente para obtener e intercambiar los tokens correctos, consulte la documentación de la aplicación.

Ajustes de configuración de un emisor de tokens de confianza

En las siguientes secciones se describen los ajustes necesarios para configurar y utilizar un emisor de tokens de confianza.

Temas

- URL del punto final de detección del OIDC (URL del emisor)
- Mapeo de atributos
- Notificación de audiencia

URL del punto final de detección del OIDC (URL del emisor)

Al agregar un emisor de tokens de confianza a la consola de IAM Identity Center, debe especificar la URL del punto de conexión de detección de OIDC. Se suele hacer referencia a esta URL por su URL relativa, `/.well-known/openid-configuration`. En la consola de IAM Identity Center, esta URL se denomina URL del emisor.

> **Note**
>
> Debe pegar la URL del punto final de detección hasta y sin ella. `.well-known/openid-configuration` Si `.well-known/openid-configuration` se incluye en la URL, la configuración del emisor del token de confianza no funcionará. Como el Centro de Identidad de IAM no valida esta URL, si la URL no está formada correctamente, la configuración del emisor de token de confianza fallará sin notificación.

IAM Identity Center utiliza esta URL para obtener información adicional sobre el emisor de tokens de confianza. Por ejemplo, IAM Identity Center utiliza esta URL para obtener la información necesaria para verificar los tokens que genera el emisor de tokens de confianza. Al agregar un emisor de tokens de confianza a IAM Identity Center, debe especificar esta URL. Para encontrar la URL, consulte la documentación del proveedor del servidor de autorización de OAuth 2.0 que utiliza para generar los tokens para su aplicación o póngase en contacto directamente con el proveedor para obtener ayuda.

Mapeo de atributos

Las asignaciones de atributos permiten que IAM Identity Center vincule el usuario representado en un token emitido por un emisor de tokens de confianza con un único usuario de IAM Identity Center. Debe especificar la asignación de atributos al agregar el emisor de tokens de confianza a IAM Identity Center. Esta asignación de atributos se utiliza en una notificación del token que ha generado el emisor de tokens de confianza. El valor de la notificación se utiliza para buscar en IAM Identity Center. La búsqueda utiliza el atributo especificado para recuperar un único usuario de IAM Identity Center, que se utilizará como el usuario de AWS. La notificación que elija debe asignarse a un atributo de una lista fija de atributos disponibles en el almacén de identidades de IAM Identity Center. Puede elegir uno de los siguientes atributos del almacén de identidades de IAM Identity Center: nombre de usuario, correo electrónico e ID externo. El valor del atributo que especifique en IAM Identity Center debe ser único para cada usuario.

Notificación de audiencia

Las notificaciones de audiencia identifican a la audiencia (destinatarios) a la que se destina un token. Cuando la aplicación que solicita el acceso se autentica a través de un proveedor de identidades que no está federado en IAM Identity Center, dicho proveedor de identidades debe configurarse como un emisor de tokens de confianza. La aplicación que recibe la solicitud de acceso (la aplicación receptora) debe cambiar el token que ha generado el emisor de tokens de confianza por un token que haya generado IAM Identity Center.

Para obtener información sobre cómo obtener los valores de la notificación de audiencia para la aplicación receptora tal como están registrados en el emisor de tokens de confianza, consulte la documentación del emisor de tokens de confianza o póngase en contacto con el administrador del emisor de tokens de confianza para obtener ayuda.

Configuración de un emisor de tokens de confianza

Para habilitar la propagación de identidades de confianza en una aplicación que se autentica externamente en IAM Identity Center, uno o más administradores deben configurar un emisor de tokens de confianza. Un emisor de tokens de confianza es un servidor de autorización de OAuth 2.0 que emite tokens a las aplicaciones que inician solicitudes (aplicaciones solicitantes). Los tokens autorizan a estas aplicaciones a iniciar solicitudes en nombre de sus usuarios a una aplicación receptora (un AWS servicio).

Temas

Coordinación de los roles y responsabilidades de administración

En algunos casos, un único administrador puede realizar todas las tareas necesarias para configurar un emisor de tokens de confianza. Si varios administradores realizan estas tareas, es necesario que haya una estrecha coordinación. En la siguiente tabla se describe cómo varios administradores

pueden coordinarse para configurar un emisor de token de confianza y configurar un AWS servicio para usarlo.

> **Note**
>
> La aplicación puede ser cualquier AWS servicio que esté integrado con el Centro de Identidad de IAM y permita la propagación de identidades de forma fiable.

Para obtener más información, consulte Tareas para configurar un emisor de tokens de confianza.

Rol	Realiza estas tareas	Se coordina con
Administrador del IAM Identity Center	Agrega el IdP externo como emisor de tokens de confianza a la consola de IAM Identity Center. Ayuda a configurar la asignación de atributos correcta entre IAM Identity Center y el IdP externo. Notifica al administrador del AWS servicio cuando el emisor del token de confianza se añade a la consola del IAM Identity Center.	Administrador del IdP externo (emisor de tokens de confianza) AWS administrador del servicio
Administrador del IdP externo (emisor de tokens de confianza)	Configura el IdP externo para emitir los tokens. Ayuda a configurar la asignación de atributos correcta entre IAM Identity Center y el IdP externo. Proporciona el nombre de la audiencia (notificación de audiencia) al administrador del servicio de AWS .	Administrador del IAM Identity Center AWS administrador de servicios

Rol	Realiza estas tareas	Se coordina con
AWS administrador de servicios	Busca en la consola AWS de servicio el emisor del token de confianza. El emisor de tokens de confianza estará visible en la consola del servicio de AWS después de que el administrador de IAM Identity Center lo agregue a la consola de IAM Identity Center. Configura el AWS servicio para que utilice el emisor del token de confianza.	Administrador del IAM Identity Center Administrador del IdP externo (emisor de tokens de confianza)

Tareas para configurar un emisor de tokens de confianza

Para configurar un emisor de tokens de confianza, un administrador de IAM Identity Center, un administrador del IdP externo (emisor de tokens de confianza) y un administrador de aplicaciones deben realizar las siguientes tareas.

> **Note**
>
> La aplicación puede ser cualquier AWS servicio que esté integrado con el IAM Identity Center y permita la propagación de identidades de forma fiable.

1. Agregar el emisor de tokens de confianza a IAM Identity Center: el administrador de IAM Identity Center agrega el emisor de tokens de confianza mediante la consola de IAM Identity Center o las API. Esta configuración requiere especificar lo siguiente:
   - El nombre del emisor de tokens de confianza.
   - La URL del punto de conexión de detección de OIDC (en la consola de IAM Identity Center, esta URL se denomina URL del emisor).
   - Asignación de atributos para la búsqueda de usuarios. Esta asignación de atributos se utiliza en una notificación del token que ha generado el emisor de tokens de confianza. El valor de

la notificación se utiliza para buscar en IAM Identity Center. La búsqueda utiliza el atributo especificado para recuperar un único usuario en IAM Identity Center.

2. Conectar el AWS servicio al IAM Identity Center: el administrador del AWS servicio debe conectar la aplicación al IAM Identity Center mediante la consola de la aplicación o las API de la aplicación.

   Una vez que el emisor del token de confianza se añade a la consola del IAM Identity Center, también aparece en la consola de AWS servicio y está disponible para que el administrador del AWS servicio lo seleccione.

3. Configure el uso del intercambio de tokens: en la consola de AWS servicio, el administrador del AWS servicio configura el AWS servicio para que acepte los tokens emitidos por el emisor de token de confianza. Estos tokens se intercambian por tokens que ha generado IAM Identity Center. Para ello, es necesario especificar el nombre del emisor de los tokens de confianza del paso 1 y el valor de reclamación en AUD que corresponde al servicio. AWS

   El emisor de tokens de confianza coloca el valor de la notificación de audiencia en el token que emite para indicar que el token está destinado a que lo utilice el servicio de AWS . Para obtener este valor, póngase en contacto con el administrador del emisor de tokens de confianza.

Cómo agregar un emisor de tokens de confianza a la consola de IAM Identity Center

En una organización que tiene varios administradores, esta tarea la realiza un administrador de IAM Identity Center. Si es el administrador de IAM Identity Center, debe elegir qué IdP externo desea utilizar como emisor de tokens de confianza.

Para agregar un emisor de tokens de confianza a la consola de IAM Identity Center

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En Emisores de tokens de confianza, seleccione Crear emisor de tokens de confianza.
5. En la página Configurar un IdP externo para emitir tokens de confianza, en Detalles del emisor del token de confianza, haga lo siguiente:

   - En la URL del emisor, especifique la URL de detección de OIDC del IdP externo que emitirá los tokens para la propagación de identidades confiables. Debe especificar la URL del punto

final de detección hasta el final. `.well-known/openid-configuration` El administrador del IdP externo puede proporcionar esta URL.

> **Note**
>
> Nota: Esta URL debe coincidir con la URL de la afirmación del emisor (iss) en los tokens que se emiten para la propagación de identidades confiables.

- En Nombre del emisor de tokens de confianza, ingrese un nombre para identificar a este emisor de tokens de confianza en IAM Identity Center y en la consola de la aplicación.

6. En Asignar atributos, haga lo siguiente:
   - En Atributo de proveedor de identidad, seleccione un atributo de la lista para asignarlo a un atributo del almacén de identidades de IAM Identity Center.
   - En Atributo de IAM Identity Center, seleccione el atributo correspondiente para la asignación de atributos.
7. En Etiquetas (opcional), seleccione Agregar etiqueta nueva y especifique un valor para Clave y, si lo desea, para Valor.

   Para obtener más información acerca de las etiquetas, consulte Etiquetado de recursos de AWS IAM Identity Center.
8. Seleccione Crear emisor de tokens de confianza.
9. Cuando termine de crear el emisor de tokens de confianza, póngase en contacto con el administrador de la aplicación para que sepa el nombre del emisor de tokens de confianza y así pueda confirmar que está visible en la consola correspondiente.
10. El administrador de la aplicación debe seleccionar este emisor de tokens de confianza en la consola correspondiente para permitir que los usuarios accedan a la aplicación desde las aplicaciones que están configuradas para la propagación de identidades de confianza.

Cómo ver o editar la configuración del emisor de tokens de confianza en la consola de IAM Identity Center

Tras agregar un emisor de tokens de confianza a la consola de IAM Identity Center, podrá ver y editar la configuración correspondiente.

Si tiene previsto editar la configuración del emisor de tokens de confianza, tenga en cuenta que si lo hace, los usuarios podrían perder el acceso a cualquier aplicación que esté configurada para

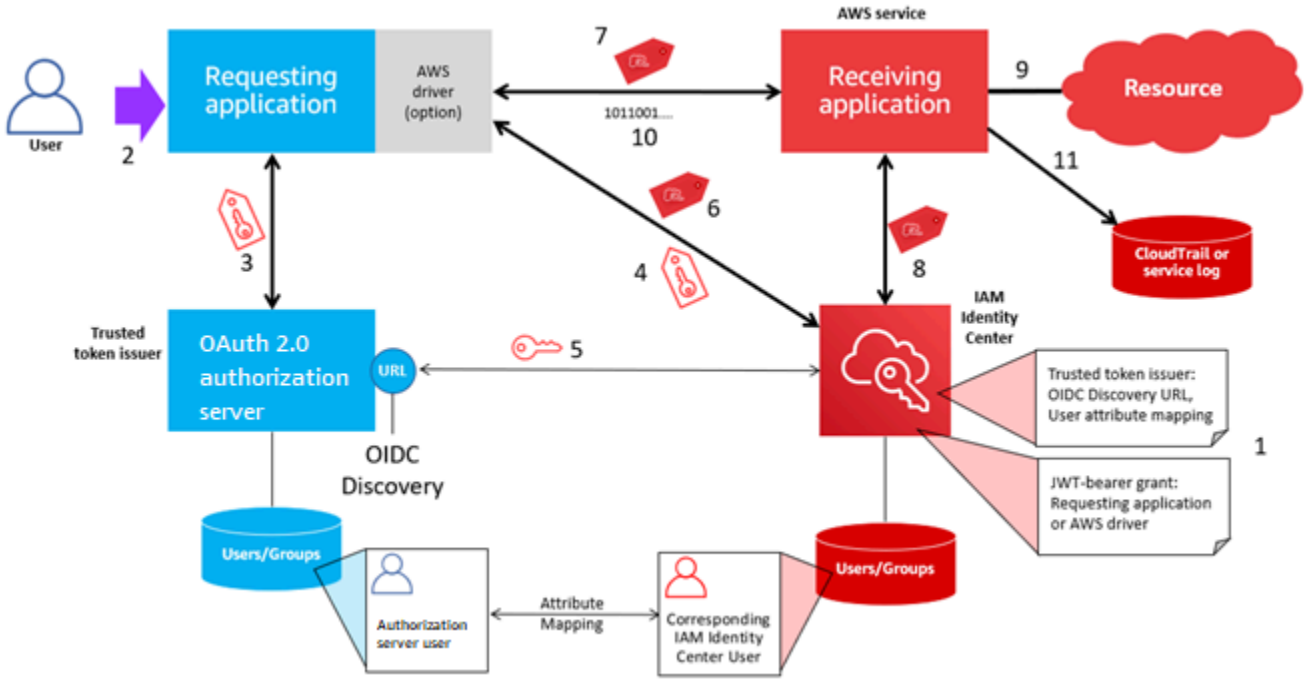
utilizar el emisor de tokens de confianza. Para evitar interrumpir el acceso de los usuarios, le recomendamos que se ponga en contacto con los administradores de cualquier aplicación que esté configurada para usar el emisor de tokens de confianza antes de editar la configuración.

Para visualizar o editar la configuración del emisor de tokens de confianza en la consola de IAM Identity Center

1. Abra la consola de IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En Emisores de tokens de confianza, seleccione el emisor de tokens de confianza que desee ver o editar.
5. Seleccione Acciones y, a continuación, Editar.
6. En la página Editar emisor de tokens de confianza, consulte o edite la configuración según sea necesario. Puede editar el nombre del emisor de tokens de confianza, las asignaciones de atributos y las etiquetas.
7. Elija Guardar cambios.
8. En el cuadro de diálogo Editar emisor de tokens de confianza, se le pedirá que confirme que desea realizar cambios. Elija Confirmar.

Proceso de configuración y flujo de solicitud para las aplicaciones que utilizan un emisor de tokens de confianza

En esta sección se describe el proceso de configuración y el flujo de solicitud para las aplicaciones que utilizan un emisor de tokens de confianza para la propagación de identidades de confianza. En el diagrama siguiente se proporciona una descripción general de este proceso.



En los pasos siguientes tiene más información sobre este proceso.

1. Configure el Centro de identidad de IAM y la aplicación AWS gestionada de recepción para utilizar un emisor de token de confianza. Para obtener más información, consulte Tareas para configurar un emisor de tokens de confianza.
2. El flujo de solicitud comienza cuando un usuario abre la aplicación solicitante.
3. La aplicación solicitante solicita un token al emisor del token de confianza para iniciar las solicitudes a la aplicación gestionada receptora AWS . Si el usuario aún no se ha autenticado, este proceso desencadena un flujo de autenticación. El token contiene la siguiente información:
   - El asunto del usuario.
   - El atributo que IAM Identity Center utiliza para buscar al usuario correspondiente en IAM Identity Center.
   - Una notificación de audiencia que contiene un valor que el emisor de tokens de confianza asocia a la aplicación administrada por AWS receptora. Si hay otras notificaciones, IAM Identity Center no las utiliza.
4. La aplicación solicitante, o el AWS controlador que utiliza, pasa el token al Centro de Identidad de IAM y solicita que se cambie por un token generado por el Centro de Identidad de IAM. Si utiliza un AWS controlador, es posible que tenga que configurarlo para este caso de uso. Para obtener más información, consulte la documentación de la aplicación AWS gestionada correspondiente.

5. IAM Identity Center utiliza el punto de conexión de detección de OIDC para obtener la clave pública que puede utilizar para verificar la autenticidad del token. A continuación, IAM Identity Center hace lo siguiente:
   - Verifica el token.
   - Busca en el directorio de Identity Center. Para ello, IAM Identity Center utiliza el atributo asignado que se especifica en el token.
   - Verifica que el usuario está autorizado para acceder a la aplicación receptora. Si la aplicación AWS gestionada está configurada para requerir asignaciones a usuarios y grupos, el usuario debe tener una asignación directa o basada en grupos a la aplicación; de lo contrario, se deniega la solicitud. Si la aplicación administrada por AWS está configurada para no requerir asignaciones de usuarios ni grupos, el procesamiento continúa.

     > **Note**
     >
     > AWS los servicios tienen una configuración predeterminada que determina si las asignaciones son necesarias para los usuarios y los grupos. Le recomendamos que no modifique la configuración Requerir asignaciones de estas aplicaciones si tiene previsto utilizarlas con la propagación de identidades de confianza. Incluso si ha configurado permisos detallados que permiten a los usuarios acceder a recursos de la aplicación específica, la modificación de la configuración Requerir asignaciones puede provocar un comportamiento inesperado, como la interrupción del acceso de los usuarios a estos recursos.

   - Comprueba que la aplicación solicitante esté configurada para utilizar ámbitos válidos para la aplicación AWS gestionada receptora.
6. Si los pasos de verificación anteriores se realizan correctamente, IAM Identity Center creará un nuevo token. El nuevo token es un token opaco (cifrado) que incluye la identidad del usuario correspondiente en el Centro de Identidad de IAM, la audiencia (AUD) de la aplicación AWS gestionada receptora y los ámbitos que la aplicación solicitante puede utilizar al realizar solicitudes a la aplicación gestionada receptora. AWS
7. La aplicación solicitante, o el controlador que utiliza, inicia una solicitud de recursos a la aplicación receptora y pasa el token que IAM Identity Center generó a la aplicación receptora.
8. La aplicación receptora realiza llamadas a IAM Identity Center para obtener la identidad del usuario y los ámbitos codificados en el token. También puede realizar solicitudes para obtener los atributos del usuario o la pertenencia del usuario a grupos desde el directorio de Identity Center.

9. La aplicación receptora utiliza su configuración de autorización para determinar si el usuario está autorizado a acceder al recurso de la aplicación solicitado.
10. Si el usuario está autorizado a acceder al recurso de la aplicación solicitado, la aplicación receptora responde a la solicitud.
11. La identidad del usuario, las acciones realizadas en su nombre y otros eventos registrados en los registros y CloudTrail eventos de la aplicación receptora. La forma específica en que se registra esta información varía en función de la aplicación.

Administrar certificados de IAM Identity Center

IAM Identity Center utiliza certificados para establecer una relación de confianza de SAML entre IAM Identity Center y el proveedor de servicios de la aplicación. Al añadir una aplicación al IAM Identity Center, se crea automáticamente un certificado de IAM Identity Center para usarlo con esa aplicación durante el proceso de configuración. De forma predeterminada, este certificado de IAM Identity Center generado automáticamente es válido durante un período de 5 años.

Como administrador de IAM Identity Center, en ocasiones tendrá que sustituir los certificados antiguos de una aplicación por otros más nuevos. Por ejemplo, puede que tenga que sustituir un certificado cuando se aproxime la fecha de vencimiento del certificado. El proceso de sustituir un certificado antiguo por uno más nuevo se denomina rotación de certificados.

Temas

Consideraciones antes de rotar un certificado

Antes de iniciar el proceso de rotación de un certificado en IAM Identity Center, tenga en cuenta lo siguiente:

- El proceso de rotación de certificaciones requiere que se restablezca la relación de confianza entre IAM Identity Center y el proveedor de servicios. Para restablecer la relación de confianza, utilice los procedimientos que se proporcionan en Rotación de un certificado de IAM Identity Center.
- La actualización del certificado con el proveedor de servicios puede provocar una interrupción temporal del servicio para los usuarios hasta que la relación de confianza se restablezca

correctamente. Si es posible, planifique esta operación cuidadosamente durante las horas de menor actividad.

Rotación de un certificado de IAM Identity Center

La rotación de un certificado de IAM Identity Center es un proceso de varios pasos que incluye lo siguiente:

- Generación de un nuevo certificado
- Adición del nuevo certificado al sitio web del proveedor de servicios
- Configuración del nuevo certificado como activo
- Eliminación del certificado inactivo

Utilice todos los procedimientos siguientes en el orden que se indica a continuación para completar el proceso de rotación de certificados para una solicitud determinada:

Paso 1: generar un nuevo certificado.

Los nuevos certificados de IAM Identity Center que genere se pueden configurar para que utilicen las siguientes propiedades:

- Período de validez: especifica el tiempo asignado (en meses) antes de que caduque un nuevo certificado de IAM Identity Center.
- Tamaño de la clave: determina el número de bits que debe utilizar una clave con su algoritmo criptográfico. Puede establecer este valor en RSA de 1024 bits o RSA de 2048 bits. Para obtener información general sobre cómo funcionan los tamaños de clave en criptografía, consulte Tamaño de clave.
- Algoritmo: especifica el algoritmo que IAM Identity Center utiliza al firmar la aserción/respuesta de SAML. Puede establecer este valor en SHA-1 o SHA-256. AWS recomienda utilizar el SHA-256 siempre que sea posible, a menos que su proveedor de servicios requiera el SHA-1. Para obtener información general sobre cómo funcionan los algoritmos de criptografía, consulte Criptografía de clave pública.

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. En la lista de aplicaciones, elija la aplicación para la que desee generar un nuevo certificado.

4. En la página de detalles de la aplicación, elija la pestaña Configuración. En Metadatos de IAM Identity Center, seleccione Administrar certificado. Si no tiene una pestaña Configuración o el ajuste de configuración no está disponible, no tiene que rotar el certificado de esta aplicación.
5. En la página de certificados de IAM Identity Center, seleccione Generar un certificado nuevo.
6. En el cuadro de diálogo Generar un nuevo certificado de IAM Identity Center, especifique los valores adecuados para el período de validez, el algoritmo y el tamaño de clave. A continuación, elija Generar.

Paso 2: actualizar el sitio web del proveedor de servicios.

Utilice el siguiente procedimiento para restablecer la relación de confianza con el proveedor de servicios de la aplicación.

> **Important**
>
> Al cargar el nuevo certificado al proveedor de servicios, es posible que los usuarios no puedan autenticarse. Para corregir esta situación, configure el nuevo certificado como activo como se describe en el paso siguiente.

1. En la consola de IAM Identity Center, elija la aplicación para la que acaba de generar un nuevo certificado.
2. En la página de detalles de la aplicación, elija la pestaña Configuración.
3. Seleccione Ver instrucciones y, a continuación, siga las instrucciones del sitio web específico del proveedor de servicios de aplicaciones para añadir el certificado recién generado.

Paso 3: configurar el nuevo certificado como activo.

Una aplicación puede tener asignados hasta dos certificados. IAM Identity Center utilizará el certificado que esté establecido como activo para firmar todas las aserciones de SAML.

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. En la lista de aplicaciones, elija su aplicación.
4. En la página de detalles de la aplicación, elija la pestaña Configuración. En los Metadatos de IAM Identity Center, seleccione Administrar certificado.

5. En la página de certificados de IAM Identity Center, seleccione el certificado que desee configurar como activo, elija Acciones y, a continuación, Establecer como activo.
6. En el cuadro de diálogo Establecer el certificado seleccionado como activo, confirme que comprende que configurar un certificado como activo puede requerir que restablezca la relación confianza y, a continuación, seleccione Activar.

Paso 4: eliminar el certificado anterior.

Use el siguiente procedimiento para completar el proceso de rotación de certificados para su aplicación. Solo puede eliminar un certificado que esté en estado inactivo.

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. En la lista de aplicaciones, elija su aplicación.
4. En la página de detalles de la aplicación, elija la pestaña Configuración. En los Metadatos de IAM Identity Center, seleccione Administrar certificado.
5. En la página de certificados de IAM Identity Center, seleccione el certificado que desee eliminar. Elija Acciones y, a continuación, elija Eliminar.
6. En el cuadro de diálogo Eliminar certificado, elija Eliminar.

Indicadores de estado de caducidad de certificados

Cuando esté en la página de Aplicaciones, en las propiedades de una aplicación, es posible que vea iconos indicadores de estado coloreados. Estos iconos aparecen en la columna Caduca el situada junto a cada certificado de la lista. A continuación, se describen los criterios que IAM Identity Center utiliza para determinar qué icono se muestra en cada certificado.

- Rojo: indica que un certificado está caducado actualmente.
- Amarillo: indica que un certificado caducará en 90 días o menos.
- Verde: indica que un certificado es válido actualmente y seguirá siendo válido durante al menos 90 días más.

Para comprobar el estado de la renovación de un certificado:

1. Abra la consola de IAM Identity Center.

2. Elija Aplicaciones.
3. En la lista de solicitudes, revise el estado de los certificados de la lista, tal y como se indica en la columna Caduca el.

Configuración de las propiedades de la aplicación en la consola de IAM Identity Center

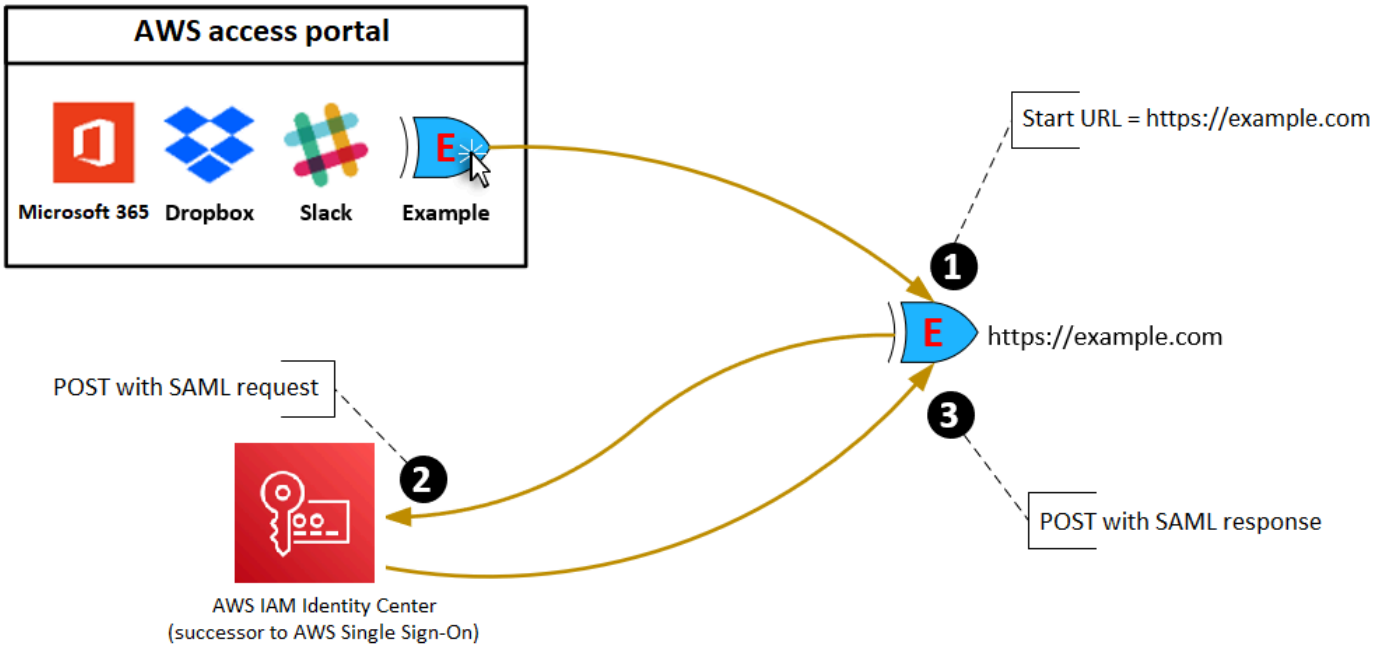
Configure la URL de inicio de la aplicación, el estado de retransmisión y la duración de la sesión en IAM Identity Center para optimizar la experiencia del usuario.

URL de inicio de la aplicación

Utilice una URL de inicio de la aplicación para iniciar el proceso de federación con la aplicación. El uso típico es para una aplicación que solo admite una conexión iniciada por el proveedor de servicio (SP).

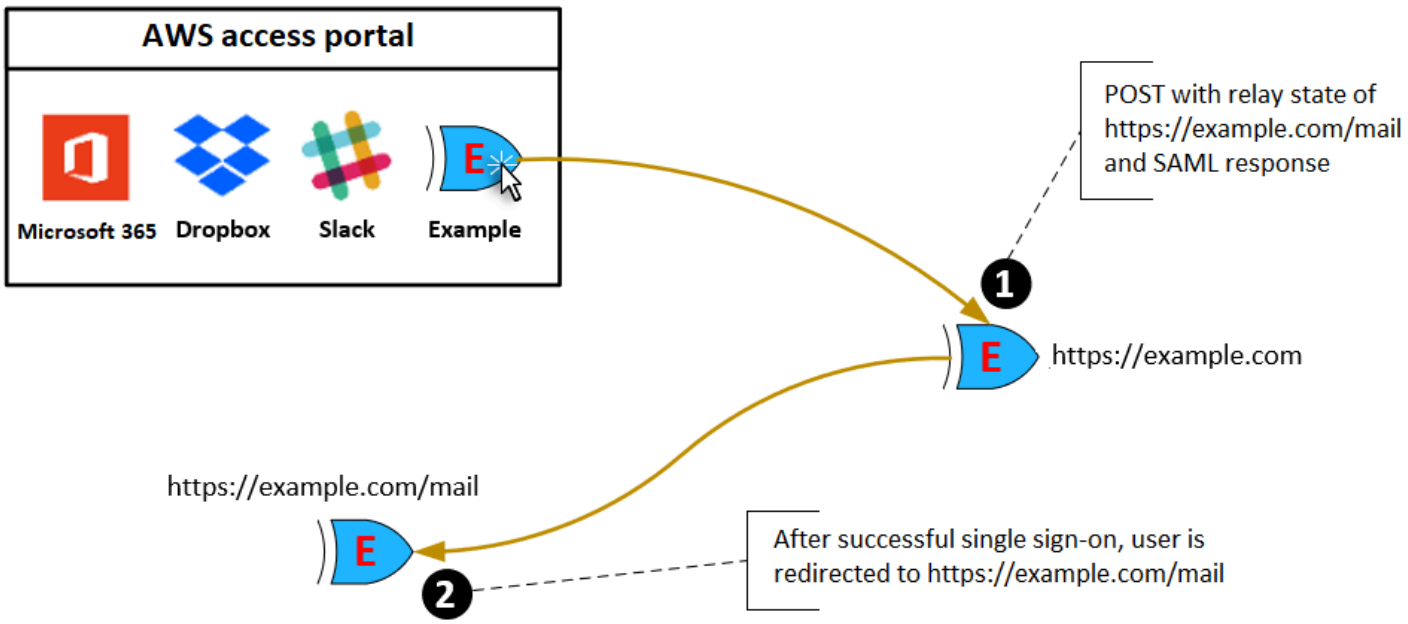
Los siguientes pasos y diagrama ilustran el flujo de trabajo de autenticación de la URL de inicio de la aplicación cuando un usuario elige una aplicación en el portal de acceso AWS :

1. El navegador del usuario redirige la solicitud de autenticación utilizando el valor de la URL de inicio de la aplicación (en este caso https://example.com).
2. La aplicación envía un `HTML POST` con `SAMLRequest` a IAM Identity Center.
3. IAM Identity Center envía después una instrucción `HTML POST` con un elemento `SAMLResponse` a la aplicación.



Estado de retransmisión

Durante el proceso de autenticación de la federación, el estado de retransmisión redirige a los usuarios dentro de la aplicación. Para SAML 2.0, este valor se pasa sin modificar a la aplicación. Una vez configuradas las propiedades de la aplicación, IAM Identity Center envía el valor de estado de retransmisión junto con una respuesta SAML a la aplicación.



Duración de la sesión

La duración de la sesión es el tiempo durante el que la sesión de un usuario de la aplicación es válida. En el caso de SAML 2.0, esta duración se utiliza para definir la fecha `SessionNotOnOrAfter` del elemento de aserción de SAML `saml2:AuthNStatement`.

Las aplicaciones pueden interpretar la duración de la sesión de las siguientes formas:

- Las aplicaciones pueden utilizarla para determinar el tiempo máximo permitido para la sesión del usuario. Las aplicaciones pueden generar una sesión de usuario con una duración más corta. Esto puede ocurrir cuando la aplicación solo admite sesiones de usuario con una duración menor que la duración de la sesión configurada.
- Las aplicaciones pueden utilizarla como la duración exacta y podrían no permitir que los administradores configuren el valor. Esto puede ocurrir cuando la aplicación solo admite una duración de la sesión específica.

Para obtener más información acerca de cómo se utiliza la duración de la sesión, consulte la documentación de su aplicación específica.

Asignar el acceso de los usuarios a las aplicaciones en la consola de IAM Identity Center

Puede asignar a los usuarios acceso mediante inicio de sesión único a las aplicaciones de SAML 2.0 del catálogo de aplicaciones o a las aplicaciones de SAML 2.0 personalizadas.

Consideraciones para las asignaciones de grupos:

- Asigne el acceso directamente a los grupos. Para simplificar la administración de los permisos de acceso, se recomienda asignar el acceso directamente a grupos en lugar de a usuarios individuales. Con los grupos puede conceder o denegar permisos para grupos de usuarios en lugar de asignar esos permisos a cada individuo. Si un usuario se muda a una organización diferente, simplemente muévalo a un grupo diferente. Así el usuario recibirá automáticamente los permisos necesarios para la nueva organización.
- No se admiten grupos anidados. Al asignar el acceso de los usuarios a las aplicaciones, IAM Identity Center no permite añadir usuarios a grupos anidados. Si añade un usuario a un grupo anidado, es posible que reciba el mensaje “No tiene ninguna aplicación” al iniciar sesión. Las asignaciones deben realizarse en función del grupo inmediato del que el usuario es miembro.

Cómo dar acceso a una aplicación a un usuario o grupo:

> **Important**
>
> En el AWS caso de las aplicaciones gestionadas, debe añadir usuarios directamente desde las consolas de aplicaciones correspondientes o mediante las API.

1. Abra la consola de IAM Identity Center

   > **Note**
   >
   > Si administra los usuarios en AWS Managed Microsoft AD, asegúrese de que la consola del IAM Identity Center utilice la AWS región en la que se encuentra su AWS Managed Microsoft AD directorio antes de dar el siguiente paso.

2. Elija Aplicaciones.
3. En la lista de aplicaciones, seleccione el nombre de la aplicación a la que quiere asignar acceso.
4. En la página de detalles de la aplicación, en la sección Usuarios asignados, elija Asignar usuarios.
5. En el cuadro de diálogo Asignar usuarios, escriba un nombre de usuario o de grupo. También puede buscar usuarios y grupos. Puede especificar varios usuarios o grupos seleccionando las cuentas aplicables tal y como aparecen en los resultados de búsqueda.
6. Elija Assign users (Asignar usuarios).

Retirada del acceso de los usuarios en la consola de IAM Identity Center

Utilice este procedimiento para eliminar el acceso de los usuarios a aplicaciones de SAML 2.0 del catálogo de aplicaciones o a aplicaciones de SAML 2.0 personalizadas.

Para eliminar el acceso de los usuarios a una aplicación

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. En la lista de aplicaciones, seleccione la aplicación cuyo acceso de usuario desea eliminar.

4. En la página de detalles de la aplicación, seleccione la pestaña Usuarios asignados, elija el usuario o grupo que desee eliminar y, a continuación, seleccione Eliminar acceso.
5. En el cuadro de diálogo Remove access (Eliminar acceso), compruebe el nombre del usuario o del grupo. A continuación, elija Remove access (Eliminar acceso).

Asignación de atributos de su aplicación con atributos de IAM Identity Center

Algunos proveedores de servicios requieren aserciones SAML personalizadas para transferir datos adicionales acerca de los inicios de sesión de los usuarios. En ese caso, puede seguir el siguiente procedimiento para especificar cómo deben asignarse los atributos de usuarios de sus aplicaciones con los atributos correspondientes en IAM Identity Center.

Cómo asignar los atributos de la aplicación con atributos de IAM Identity Center:

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. En la lista de aplicaciones, seleccione la aplicación en la que desea mapear atributos.
4. En la página de detalles de la aplicación, seleccione Acciones y, a continuación, seleccione Editar asignación de atributos.
5. Seleccione Agregar nueva asignación de atributos.
6. En el primer cuadro de texto, escriba el atributo de la aplicación.
7. En el segundo cuadro de texto, escriba el atributo de IAM Identity Center que desea asignar con el atributo de la aplicación. Por ejemplo, es posible que desee asignar el atributo de la aplicación **`Username`** al atributo del usuario **`email`** de IAM Identity Center. Para ver la lista de los atributos de usuario permitidos en IAM Identity Center, consulte la tabla que encontrará en Asignaciones de atributos para el directorio AWS Managed Microsoft AD.
8. En la tercera columna de la tabla, seleccione el formato adecuado del atributo en el menú.
9. Elija Guardar cambios.

Diseño de resiliencia y comportamiento regional

El servicio IAM Identity Center está totalmente gestionado y utiliza servicios de AWS duraderos y de alta disponibilidad, como Amazon S3 y Amazon EC2. Para garantizar la disponibilidad en caso de que se interrumpa la zona de disponibilidad, el IAM Identity Center opera en varias zonas de disponibilidad. Para obtener información sobre los objetivos del diseño de disponibilidad de IAM Identity Center, consulte Apéndice A: diseño para la disponibilidad de determinados servicios de AWS en la Guía del pilar de fiabilidad.

Habilite el IAM Identity Center en su cuenta de administración AWS Organizations. Esto es necesario para que el IAM Identity Center pueda aprovisionar, desaprovisionar y actualizar los roles de todas sus Cuentas de AWS. Al activar el IAM Identity Center, se despliega en la Región de AWS que esté seleccionada actualmente. Si desea realizar la implementación en una Región de AWS específica, cambie la selección de región antes de activar el IAM Identity Center.

> **Note**
>
> El IAM Identity Center controla el acceso a sus conjuntos de permisos y aplicaciones únicamente desde su región principal. Le recomendamos que tenga en cuenta los riesgos asociados al control de acceso cuando el IAM Identity Center opere en una sola región.

Si bien el IAM Identity Center determina el acceso desde la región en la que se habilita el servicio, las Cuentas de AWS son globales. Esto significa que, una vez que los usuarios inician sesión en el IAM Identity Center, pueden operar en cualquier región al acceder a sus Cuentas de AWS a través de IAM Identity Center. Sin embargo SageMaker, la mayoría de las aplicaciones AWS administradas, como Amazon, deben instalarse en la misma región que el Centro de identidades de IAM para que los usuarios se autentiquen y asignen el acceso a estas aplicaciones. Para obtener información sobre las restricciones regionales al utilizar una aplicación con el IAM Identity Center, consulte la documentación de la aplicación.

También puede utilizar el IAM Identity Center para autenticar y autorizar el acceso a las aplicaciones basadas en SAML a las que se puede acceder a través de una URL pública, independientemente de la plataforma o la nube en la que se haya creado la aplicación.

No recomendamos utilizar Instancias de cuenta de IAM Identity Center como medio para implementar la resiliencia, ya que se crea un segundo punto de control aislado que no está conectado a la instancia de organización.

Configure el acceso de emergencia a la AWS Management Console

El IAM Identity Center se creó a partir de una infraestructura de alta disponibilidad de AWS y utiliza una arquitectura de zonas de disponibilidad para eliminar los puntos únicos de error. Para disponer de un nivel de protección adicional en el improbable caso de que se produzca una Región de AWS interrupción o se produzca una interrupción en el centro de identidad de IAM, le recomendamos que configure una configuración que pueda utilizar para proporcionar acceso temporal al. AWS Management Console

Contenido

Información general

AWS le permite:

- Conecte su IdP de terceros a IAM Identity Center.
- Conecte su IdP de terceros a Cuentas de AWS individuales mediante la federación basada en SAML 2.0.

Si utiliza IAM Identity Center, puede utilizar estas funciones para crear la configuración de acceso de emergencia que se describe en las siguientes secciones. Esta configuración le permite utilizar IAM Identity Center como mecanismo de acceso a su Cuenta de AWS. Si IAM Identity Center

se interrumpe, los usuarios de sus operaciones de emergencia pueden iniciar sesión en la AWS Management Console mediante la federación directa con las mismas credenciales que utilizan para acceder a sus cuentas. Esta configuración funciona cuando IAM Identity Center no está disponible, pero el plano de datos de IAM y su proveedor de identidades (IdP) externo están disponibles.

> **Important**
>
> Le recomendamos que implemente esta configuración antes de que se produzca una interrupción, ya que no podrá crearla si también se interrumpe su acceso para crear los roles de IAM requeridos. Además, pruebe esta configuración periódicamente para asegurarse de que su equipo sepa qué hacer en caso de que se interrumpa IAM Identity Center.

Resumen de la configuración del acceso de emergencia

Complete las tareas siguientes para configurar el acceso de emergencia:

1. Cree una cuenta de operaciones de emergencia en su organización en AWS Organizations.
2. Conecte el IdP a la cuenta de operaciones de emergencia mediante la federación basada en SAML 2.0.
3. En la cuenta de operaciones de emergencia, cree un rol para la federación de proveedores de identidades de terceros. Además, cree un rol de operaciones de emergencia en cada una de sus cuentas de carga de trabajo, con los permisos necesarios.
4. Delegue el acceso a sus cuentas de carga de trabajo para el rol de IAM que creó en la cuenta de operaciones de emergencia. Para autorizar el acceso a su cuenta de operaciones de emergencia, cree un grupo de operaciones de emergencia en su IdP, sin miembros.
5. Permita que el grupo de operaciones de emergencia de su IdP utilice el rol de operaciones de emergencia creando una regla en su IdP que permita el acceso federado de SAML 2.0 a la AWS Management Console.

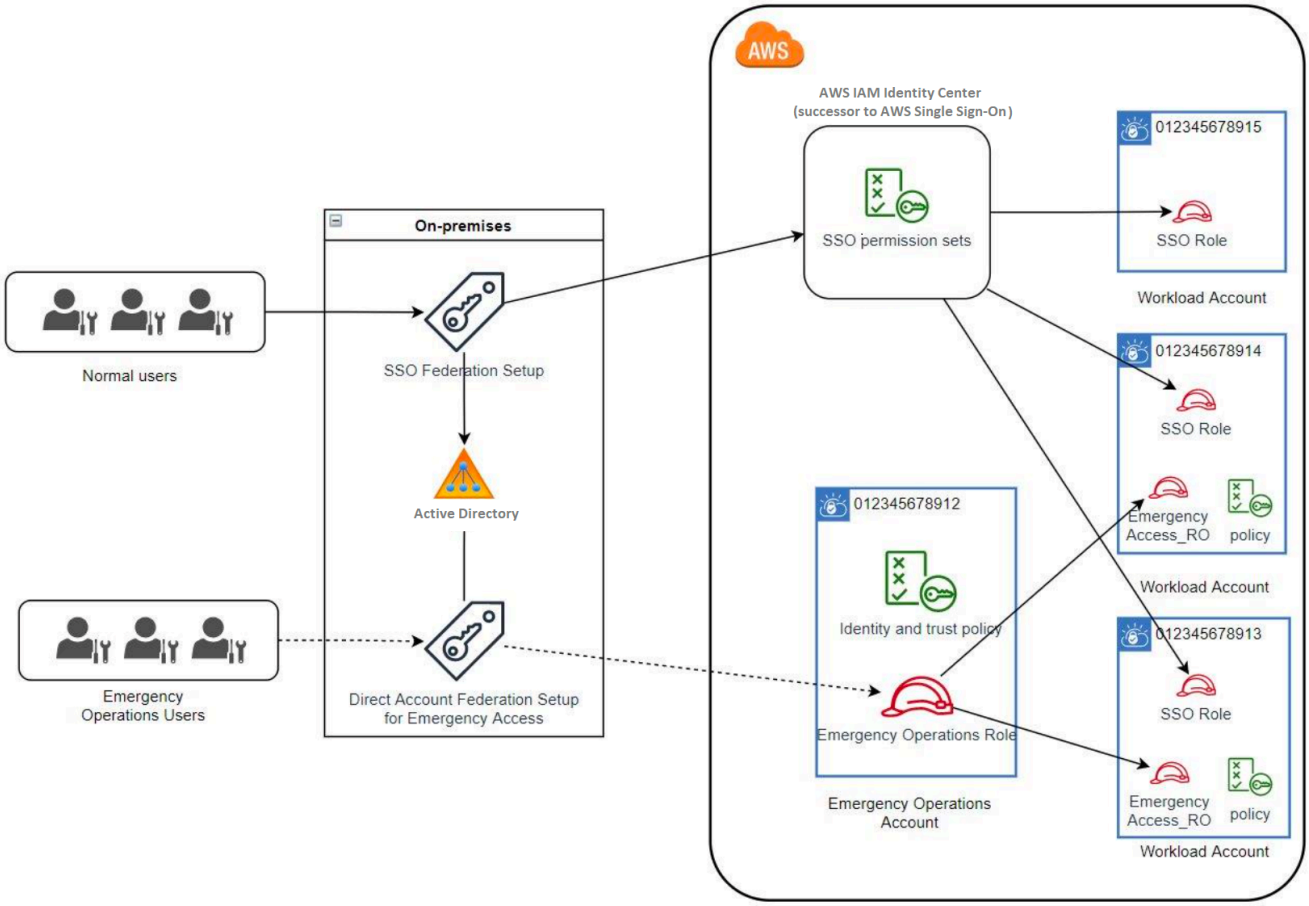
Durante las operaciones normales, nadie tiene acceso a la cuenta de operaciones de emergencia porque el grupo de operaciones de emergencia de su IdP no tiene miembros. En caso de que se produzca una interrupción en IAM Identity Center, utilice su IdP para añadir usuarios de confianza al grupo de operaciones de emergencia de su IdP. A continuación, estos usuarios pueden iniciar sesión en su IdP, acceder a la AWS Management Console y asumir el rol de operaciones de emergencia en la cuenta de operaciones de emergencia. A partir de ahí, estos usuarios pueden cambiar de rol al

rol de acceso de emergencia en sus cuentas de carga de trabajo, donde tienen que realizar tareas operativas.

Cómo diseñar sus roles de operaciones críticas

Con este diseño, se configura una única Cuenta de AWS en la que se federa a través de la IAM, de modo que los usuarios puedan asumir roles de operaciones críticas. Las funciones de operaciones críticas tienen una política de confianza que permite a los usuarios asumir el rol correspondiente en sus cuentas de carga de trabajo. Los roles de las cuentas de carga de trabajo proporcionan los permisos que los usuarios necesitan para realizar tareas esenciales.

En el diagrama siguiente se proporciona información general del diseño.



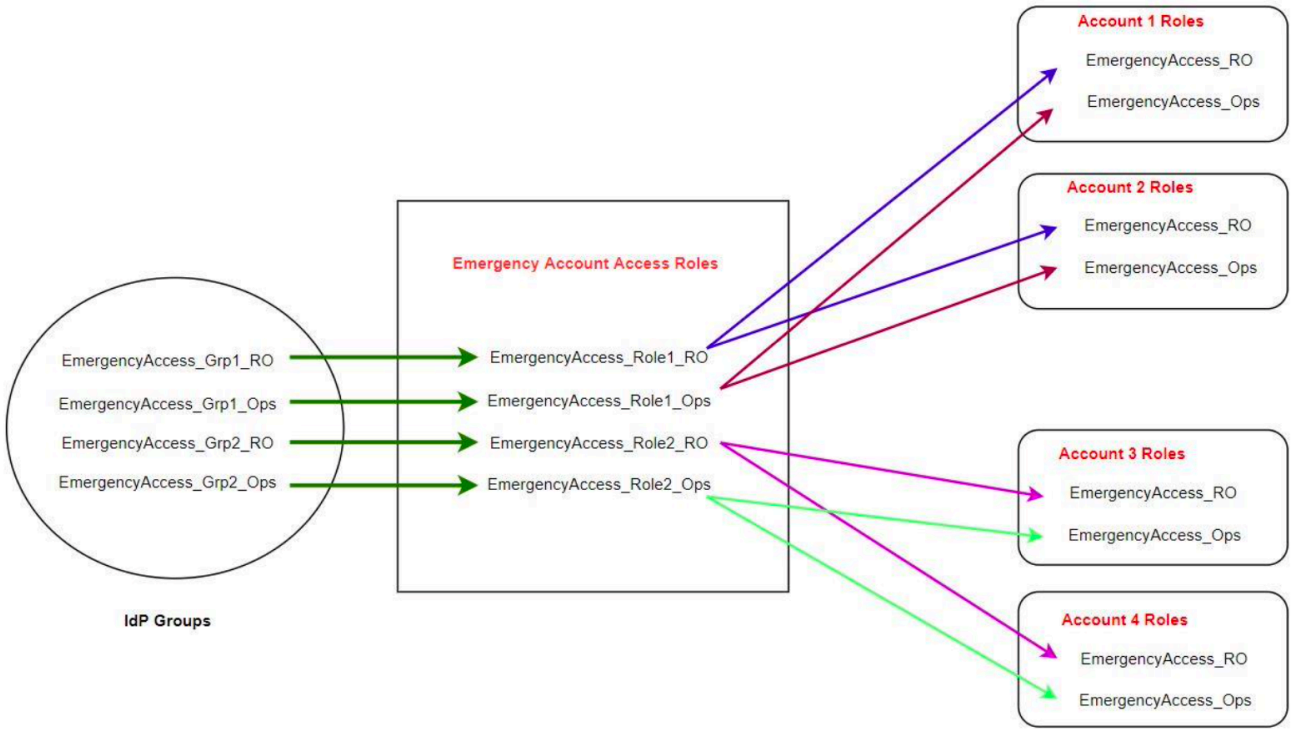
Cómo planificar su modelo de acceso

Antes de configurar el acceso de emergencia, cree un plan sobre cómo funcionará el modelo de acceso. Utilice el siguiente proceso para crear este plan:

1. Identifique las Cuentas de AWS donde el acceso de emergencia del operador es esencial durante una interrupción en el IAM Identity Center. Por ejemplo, es probable que sus cuentas de producción sean esenciales, pero es posible que sus cuentas de desarrollo y prueba no lo sean.
2. Para ese conjunto de cuentas, identifique los roles críticos específicos que necesita en sus cuentas. En todas estas cuentas, defina de manera coherente lo que pueden hacer los roles. Esto simplifica el trabajo en su cuenta de acceso de emergencia, en la que puede crear roles multicuentas. Le recomendamos que comience con dos roles distintos en estas cuentas: de solo lectura (RO) y de operaciones (Ops). Si es necesario, puede crear más roles y asignarlos a un grupo distinto de usuarios de acceso de emergencia en su configuración.
3. Identifique y cree grupos de acceso de emergencia en su IdP. Los miembros del grupo son los usuarios a los que está delegando el acceso a los roles de acceso de emergencia.
4. Defina qué roles pueden asumir estos grupos en la cuenta de acceso de emergencia. Para ello, defina reglas en su IdP que generen notificaciones que enumeren los roles a los que puede acceder el grupo. Estos grupos pueden entonces asumir sus roles de solo lectura o de operaciones en la cuenta de acceso de emergencia. A partir de esos roles, pueden asumir los roles correspondientes en sus cuentas de carga de trabajo.

Cómo diseñar una asignación de roles, cuentas y grupos de emergencia

En el siguiente diagrama, se muestra cómo asignar los grupos de acceso de emergencia a los roles de la cuenta de acceso de emergencia. El diagrama también muestra las relaciones de confianza entre roles que permiten que los roles de las cuentas de acceso de emergencia accedan a los roles correspondientes de las cuentas de carga de trabajo. Recomendamos que el diseño de su plan de emergencia utilice estas asignaciones como punto de partida.



Cómo crear la configuración de acceso de emergencia

Utilice la siguiente tabla de asignación para crear su configuración de acceso de emergencia. Esta tabla refleja un plan que incluye dos roles en las cuentas de carga de trabajo: de solo lectura (RO) y de operaciones (Ops), con las correspondientes políticas de confianza y permisos. Las políticas de confianza permiten que los roles de las cuentas de acceso de emergencia accedan a los roles de las cuentas de carga de trabajo individuales. Los roles individuales de la cuenta de carga de trabajo también tienen políticas de permisos sobre lo que el rol puede hacer en la cuenta. Las políticas de permisos pueden ser políticas administradas por AWS o políticas administradas por el cliente.

Cuenta	Roles a crear	Política de confianza	Política de permisos
Cuenta 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Cuenta 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator

Cuenta	Roles a crear	Política de confianza	Política de permisos
Cuenta 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam: :aws:policy/ ReadOnlyAccess
Cuenta 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/ SystemAdministrator
Cuenta de acceso de emergencia	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole para el recurso de rol en la cuenta

En este plan de asignación, la cuenta de acceso de emergencia contiene dos roles de solo lectura y dos roles de operaciones. Estos roles confían en su IdP para autenticar y autorizar a los grupos seleccionados a acceder a los roles pasando los nombres de los roles en aserciones. En las cuentas 1 y 2 de carga de trabajo hay los correspondientes roles de solo lectura y operaciones. Para la cuenta de carga de trabajo 1, el rol `EmergencyAccess_RO` confía en el rol `EmergencyAccess_Role1_RO` que reside en la cuenta de acceso de emergencia. En la tabla se especifican patrones de confianza similares entre los roles de solo lectura y operaciones de la cuenta de carga de trabajo y los correspondientes roles de acceso de emergencia.

Tareas de preparación de emergencias

Para preparar la configuración de acceso de emergencia, recomendamos que realice las siguientes tareas antes de que se produzca una emergencia.

1. Configure una aplicación de federación de IAM directa en su IdP. Para obtener más información, consulte Configuración única de una aplicación de federación de IAM directa en Okta.

2. Cree una conexión de IdP en la cuenta de acceso de emergencia a la que se pueda acceder durante el evento.
3. Cree roles de acceso de emergencia en las cuentas de acceso de emergencia tal y como se describe en la tabla de asignación anterior.
4. Cree roles de operaciones temporales con políticas de confianza y permisos en cada una de las cuentas de carga de trabajo.
5. Cree grupos de operaciones temporales en su IdP. Los nombres de los grupos dependerán de los nombres de los roles de operaciones temporales.
6. Pruebe la federación de IAM directa.
7. Deshabilite la aplicación de federación de IdP en su IdP para evitar su uso regular.

Proceso de conmutación por error de emergencia

Si no hay una instancia del IAM Identity Center disponible y decide que debe proporcionar acceso de emergencia a la consola de administración de AWS, le recomendamos el siguiente proceso de conmutación por error.

1. El administrador del IdP habilita la aplicación de federación de IAM directa en su IdP.
2. Los usuarios solicitan el acceso al grupo de operaciones temporal a través del mecanismo que ya tiene, como una solicitud por correo electrónico, un canal de Slack u otra forma de comunicación.
3. Los usuarios que añada a sus grupos de acceso de emergencia inician sesión en el IdP, seleccionan la cuenta de acceso de emergencia y los usuarios eligen un rol para usarlo en la cuenta de acceso de emergencia. A partir de estos roles, pueden asumir roles en las cuentas de carga de trabajo correspondientes que tienen una confianza cruzada con el rol de cuenta de emergencia.

Volver a las operaciones normales

Consulte el Panel de estado de AWS para confirmar cuándo se restablece el estado del servicio del IAM Identity Center. Para volver a las operaciones normales, siga estos pasos:

1. Cuando el icono de estado del servicio de IAM Identity Center indique que el servicio está en buen estado, inicie sesión en IAM Identity Center.
2. Si puede iniciar sesión correctamente en IAM Identity Center, comunique a los usuarios con acceso de emergencia que IAM Identity Center está disponible. Indique a estos usuarios que

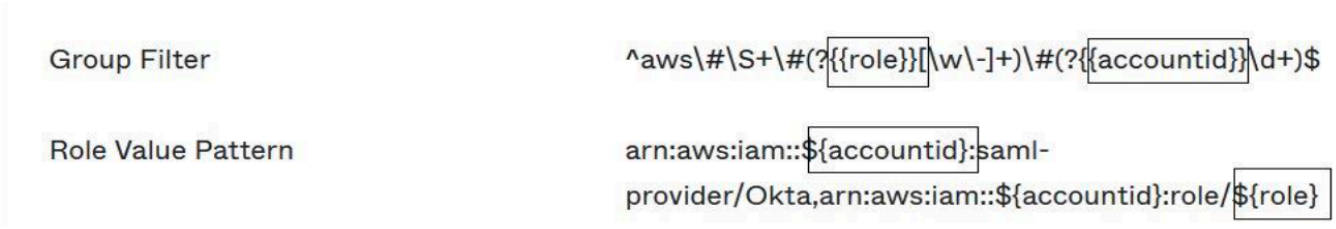
cierren sesión y usen el portal de acceso de AWS para volver a iniciar sesión en IAM Identity Center.

3. Una vez que todos los usuarios con acceso de emergencia cierren la sesión, deshabilite en el IdP la aplicación de federación de IdP. Le recomendamos que realice esta tarea después del horario de trabajo.
4. Elimine todos los usuarios del grupo de acceso de emergencia del IdP.

Su infraestructura de roles de acceso de emergencia sigue funcionando como un plan de acceso alternativo, pero ahora está deshabilitada.

Configuración única de una aplicación de federación de IAM directa en Okta

1. Inicie sesión en su cuenta de Okta como usuario con permisos administrativos.
2. En la Consola de administración de Okta, en Aplicaciones, seleccione Aplicaciones.
3. Seleccione Explorar el catálogo de aplicaciones. Busque y elija Federación de cuentas de AWS. Seleccione Agregar integración.
4. Configure la federación de IAM directa con AWS siguiendo los pasos de Cómo configurar SAML 2.0 para la federación de cuentas de AWS.
5. En la pestaña Opciones de inicio de sesión, seleccione SAML 2.0 e introduzca los ajustes de Filtro de grupo y Patrón de valores de rol. El nombre del grupo para el directorio de usuarios depende del filtro que configure.



   En la figura anterior, la variable `role` corresponde al rol de operaciones de emergencia en su cuenta de acceso de emergencia. Por ejemplo, si crea el rol `EmergencyAccess_Role1_R0` (tal como se describe en la tabla de asignación) en su Cuenta de AWS `123456789012`, y si la configuración del filtro de grupo está configurada como se muestra en la figura anterior, el nombre de su grupo debería ser `aws#EmergencyAccess_Role1_R0#123456789012`.
6. En el directorio (por ejemplo, el directorio de Active Directory), cree el grupo de acceso de emergencia y especifique un nombre para el directorio (por ejemplo,

aws#EmergencyAccess_Role1_RO#123456789012). Asigne sus usuarios a este grupo mediante el mecanismo de aprovisionamiento existente.

7. En la cuenta de acceso de emergencia, configure una política de confianza personalizada que proporcione los permisos necesarios para que se asuma el rol de acceso de emergencia durante una interrupción. A continuación, se muestra un ejemplo de una política de confianza personalizada asociada al rol EmergencyAccess_Role1_RO. Para ver un ejemplo, consulte la cuenta de emergencia en el diagrama en Cómo diseñar una asignación de roles, cuentas y grupos de emergencia.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:SetSourceIdentity",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud":"https:~/~/signin.aws.amazon.com/saml"
            }
         }
      }
   ]
}
```

8. A continuación se muestra un ejemplo de una declaración de una política de permisos asociada al rol EmergencyAccess_Role1_RO. Para ver un ejemplo, consulte la cuenta de emergencia en el diagrama en Cómo diseñar una asignación de roles, cuentas y grupos de emergencia.

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

```
         "Resource":[
            "arn:aws:iam::<account 1>:role/EmergencyAccess_RO",
            "arn:aws:iam::<account 2>:role/EmergencyAccess_RO"
         ]
      }
   ]
}
```

9. En las cuentas de carga de trabajo, configure una política de confianza personalizada. A continuación se muestra un ejemplo de declaración de una política de confianza asociada al rol `EmergencyAccess_RO`. En este ejemplo, la cuenta `123456789012` es la cuenta de acceso de emergencia. Para ver un ejemplo, consulte la cuenta de carga de trabajo en el diagrama en Cómo diseñar una asignación de roles, cuentas y grupos de emergencia.

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> La mayoría le IdPs permiten mantener desactivada la integración de una aplicación hasta que sea necesaria. Le recomendamos que mantenga la aplicación de federación de IAM directa desactivada en su IdP hasta que sea necesaria para el acceso de emergencia.

Seguridad en AWS IAM Identity Center

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

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad aplicables AWS IAM Identity Center, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza IAM Identity Center. En los siguientes temas se le mostrará cómo configurar IAM Identity Center para cumplir con sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos del IAM Identity Center.

Temas

Administración de identidades y accesos para IAM Identity Center

El acceso al Centro de Identidad de IAM requiere credenciales que AWS pueda utilizar para autenticar sus solicitudes. Esas credenciales deben tener permisos para acceder a AWS los recursos, como una aplicación AWS gestionada.

La autenticación del portal de AWS acceso está controlada por el directorio que haya conectado al IAM Identity Center. Sin embargo, la autorización de los Cuentas de AWS que están disponibles para los usuarios desde el portal de AWS acceso viene determinada por dos factores:

1. A quién se le ha asignado el acceso a ellas Cuentas de AWS en la consola del IAM Identity Center. Para obtener más información, consulte Acceso mediante inicio de sesión único a Cuentas de AWS.
2. Qué nivel de permisos se ha concedido a los usuarios en la consola de IAM Identity Center para permitirles el acceso adecuado a esas Cuentas de AWS. Para obtener más información, consulte Creación, administración y eliminación de conjuntos de permisos.

En las siguientes secciones se explica cómo, como administrador, puede controlar el acceso a la consola del IAM Identity Center o delegar el acceso administrativo a day-to-day las tareas desde la consola del IAM Identity Center.

- Autenticación
- Control de acceso

Autenticación

Aprenda a acceder AWS mediante las identidades de IAM.

Control de acceso

Aunque tenga credenciales válidas para autenticar las solicitudes, si no tiene permisos, no podrá crear recursos de IAM Identity Center ni acceder a estos. Por ejemplo, debe tener permisos para crear un directorio conectado de IAM Identity Center.

En las secciones siguientes se describe cómo administrar los permisos de IAM Identity Center. Recomendamos que lea primero la información general.

- Información general sobre la administración de permisos de acceso para los recursos de IAM Identity Center
- Ejemplos de políticas basadas en identidades para IAM Identity Center
- Uso de roles vinculados a servicios para IAM Identity Center

Información general sobre la administración de permisos de acceso para los recursos de IAM Identity Center

Cada AWS recurso es propiedad de un Cuenta de AWS, y los permisos para crear o acceder a los recursos se rigen por políticas de permisos. Para proporcionar acceso, un administrador de cuentas puede agregar permisos a las identidades de IAM (es decir, usuarios, grupos y roles). Algunos servicios (por ejemplo, AWS Lambda) también admiten añadir permisos a recursos.

> **Note**
>
> Un administrador de cuentas (o usuario administrador) es un usuario que tiene privilegios de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Temas

- Recursos y operaciones de IAM Identity Center
- Titularidad de los recursos
- Administración del acceso a los recursos
- Especificación de elementos de política: acciones, efectos, recursos y entidades principales
- Especificación de las condiciones de una política

Recursos y operaciones de IAM Identity Center

En IAM Identity Center, los recursos principales son instancias de aplicación, perfiles y conjuntos de permisos.

Titularidad de los recursos

El propietario de un recurso es Cuenta de AWS quien creó un recurso. Es decir, el propietario Cuenta de AWS del recurso es la entidad principal (la cuenta, un usuario o un rol de IAM) que autentica la solicitud que crea el recurso. Los siguientes ejemplos ilustran cómo funciona:

- Si Usuario raíz de la cuenta de AWS crea un recurso del Centro de identidad de IAM, como una instancia de aplicación o un conjunto de permisos, usted Cuenta de AWS es el propietario de ese recurso.
- Si crea un usuario en su AWS cuenta y le concede permisos para crear los recursos del IAM Identity Center, el usuario podrá crear los recursos del IAM Identity Center. Sin embargo, su AWS cuenta, a la que pertenece el usuario, es propietaria de los recursos.
- Si crea un rol de IAM en su AWS cuenta con permisos para crear recursos del Centro de Identidad de IAM, cualquier persona que pueda asumir el rol podrá crear recursos del Centro de Identidad de IAM. Su Cuenta de AWS, a la que pertenece el rol, será la propietaria de los recursos de IAM Identity Center.

Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

> **Note**
>
> En esta sección se explica el uso de IAM en el contexto de IAM Identity Center. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte What is IAM? (¿Qué es IAM?) en la Guía del usuario de IAM. Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte AWS Referencia de políticas de IAM en la Guía del usuario de IAM.

Las políticas que se asocian a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM). Las políticas que se asocian a un recurso se denominan "políticas basadas en recursos". IAM Identity Center solo admite políticas basadas en identidades (políticas de IAM).

Temas

- Políticas basadas en identidades (políticas de IAM)

- Políticas basadas en recursos

Políticas basadas en identidades (políticas de IAM)

Puede agregar permisos a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Adjunta una política de permisos a un usuario o grupo de tu cuenta Cuenta de AWS: el administrador de la cuenta puede utilizar una política de permisos asociada a un usuario concreto para conceder permisos a ese usuario para añadir un recurso del IAM Identity Center, como una nueva aplicación.
- Adjuntar una política de permisos a un rol (conceder permisos para cuentas cruzadas): puede adjuntar una política de permisos basada en identidades a un rol de IAM para conceder permisos para cuentas cruzadas.

  Para obtener más información sobre el uso de IAM para delegar permisos, consulte Access management (Administración de accesos) en la Guía del usuario de IAM.

La siguiente política de permisos concede permisos a un usuario para ejecutar todas las acciones que empiezan por `List`. Estas acciones muestran información sobre un recurso de IAM Identity Center, como una instancia de la aplicación o un conjunto de permisos. Tenga en cuenta que el carácter comodín (*) en el elemento `Resource` indica que las acciones están permitidas para todos los recursos de IAM Identity Center propiedad de la cuenta.

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

Para obtener más información acerca del uso de políticas basadas en identidades con IAM Identity Center, consulte Ejemplos de políticas basadas en identidades para IAM Identity Center. Para obtener más información acerca de los usuarios, los grupos, los roles y los permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Políticas basadas en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede asociar una política a un bucket de S3 para administrar los permisos de acceso a dicho bucket. IAM Identity Center no admite políticas basadas en recursos.

Especificación de elementos de política: acciones, efectos, recursos y entidades principales

Para cada recurso de IAM Identity Center (consulte Recursos y operaciones de IAM Identity Center), el servicio define un conjunto de operaciones de la API. Para conceder permisos para estas operaciones de la API, IAM Identity Center define un conjunto de acciones que usted puede especificar en una política. Tenga en cuenta que la realización de una operación de la API puede requerir permisos para más de una acción.

A continuación, se indican los elementos básicos de la política:

- Recurso: en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política.
- Acción: utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, el permiso `sso:DescribePermissionsPolicies` permite al usuario ejecutar la operación `DescribePermissionsPolicies` de IAM Identity Center.
- Efecto: especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). IAM Identity Center no admite políticas basadas en recursos.

Para obtener más información acerca de la sintaxis y las descripciones de las políticas del IAM, consulte Referencia de políticas de AWS IAM en la Guía del usuario de IAM.

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de acceso para especificar las condiciones que se deben cumplir para que se aplique una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte Condition en la Guía del usuario de IAM.

Para expresar condiciones, se usan claves de condición predefinidas. No hay claves de condición específicas para IAM Identity Center. Sin embargo, hay claves de AWS condición que puede utilizar según convenga. Para obtener una lista completa de AWS las claves, consulte las claves de condición globales disponibles en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para IAM Identity Center

En este tema se proporcionan ejemplos de políticas de IAM que puede crear para conceder permisos a los usuarios y roles para administrar IAM Identity Center.

> **Important**
>
> Le recomendamos que primero consulte los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a sus recursos de IAM Identity Center. Para obtener más información, consulte Información general sobre la administración de permisos de acceso para los recursos de IAM Identity Center.

En las secciones de este tema se explica lo siguiente:

- Ejemplos de políticas personalizadas
- Permisos necesarios para usar la consola de IAM Identity Center

Ejemplos de políticas personalizadas

En esta sección se proporcionan ejemplos de casos de uso habituales que requieren una política de IAM personalizada. Estas políticas de ejemplo son políticas basadas en la identidad, que no especifican el elemento de la entidad principal. Esto se debe a que, con una política basada en identidades, no se especifica la entidad principal que obtiene el permiso. En su lugar, usted adjunta la política a la entidad principal. Cuando se adjunta una política de permisos basada en la identidad a un rol de IAM, la entidad principal identificada en la política de confianza del rol obtiene los permisos.

Puede crear políticas basadas en la identidad en IAM y adjuntarlas a los usuarios, grupos o roles. También puede aplicar estas políticas a los usuarios de IAM Identity Center al crear un conjunto de permisos en IAM Identity Center.

> **Note**
>
> Utilice estos ejemplos cuando cree políticas para su entorno y asegúrese de realizar pruebas tanto en casos positivos ("acceso concedido") como negativos ("acceso denegado") antes de implementar estas políticas en su entorno de producción. Para obtener más información sobre cómo probar las políticas de IAM, consulte Probar las políticas de IAM con el simulador de política de IAM en la Guía del usuario de IAM.

Temas

Ejemplo 1: permitir que un usuario visualice IAM Identity Center

La siguiente política de permisos concede permisos de solo lectura a un usuario para que pueda visualizar todos los ajustes y la información del directorio configurados en IAM Identity Center.

> **Note**
>
> Esta política se proporciona únicamente con fines ilustrativos. En un entorno de producción, le recomendamos que utilice la política `ViewOnlyAccess` AWS gestionada del IAM Identity Center.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
```

```
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo 2: Permitir que un usuario gestione los permisos Cuentas de AWS en el Centro de identidades de IAM

La siguiente política de permisos permite a un usuario crear, administrar y desplegar conjuntos de permisos para sus Cuentas de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
```

```
                "sso:DeleteAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso:UpdatePermissionSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMListPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AccessToSSOProvisionedRoles",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        }
```

```
    ]
}
```

> **Note**
>
> Los permisos adicionales que figuran en `"Sid": "AccessToSSOProvisiondRoles"` las secciones y son necesarios únicamente para que el usuario pueda crear asignaciones en la cuenta AWS Organizations de administración. `"Sid": "IAMListPermissions"` En algunos casos, es posible que también deba agregar `iam:UpdateSAMLProvider` a estas secciones.

Ejemplo 3: permitir a un usuario administrar aplicaciones en IAM Identity Center

La siguiente política de permisos concede permisos para que los usuarios visualicen y configuren aplicaciones en IAM Identity Center, incluidas las aplicaciones SaaS preintegradas del catálogo de IAM Identity Center.

> **Note**
>
> La operación `sso:AssociateProfile` utilizada en el siguiente ejemplo de política es necesaria para administrar las asignaciones de usuarios y grupos a las aplicaciones. También permite al usuario asignar usuarios y grupos Cuentas de AWS mediante los conjuntos de permisos existentes. Si un usuario debe gestionar el Cuenta de AWS acceso desde el Centro de identidades de IAM y necesita los permisos necesarios para gestionar los conjuntos de permisos, consulteEjemplo 2: Permitir que un usuario gestione los permisos Cuentas de AWS en el Centro de identidades de IAM.

Desde octubre de 2020, muchas de estas operaciones solo están disponibles a través de la consola AWS . Este ejemplo de política incluye acciones de “lectura”, como enumerar, obtener y buscar, que, en este caso, son relevantes para que la consola funcione sin errores.

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

```
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:ImportApplicationInstanceServiceProviderMetadata",
                "sso:DeleteApplicationInstance",
                "sso:DeleteProfile",
                "sso:DisassociateProfile",
                "sso:GetApplicationTemplate",
                "sso:UpdateApplicationInstanceServiceProviderConfiguration",
                "sso:UpdateApplicationInstanceDisplayData",
                "sso:DeleteManagedApplicationInstance",
                "sso:UpdateApplicationInstanceStatus",
                "sso:GetManagedApplicationInstance",
                "sso:UpdateManagedApplicationInstanceStatus",
                "sso:CreateManagedApplicationInstance",
                "sso:UpdateApplicationInstanceSecurityConfiguration",
                "sso:UpdateApplicationInstanceResponseConfiguration",
                "sso:GetApplicationInstance",
                "sso:CreateApplicationInstanceCertificate",
                "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
                "sso:UpdateApplicationInstanceActiveCertificate",
                "sso:DeleteApplicationInstanceCertificate",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationTemplates",
                "sso:ListApplications",
                "sso:ListApplicationInstances",
                "sso:ListDirectoryAssociations",
                "sso:ListProfiles",
                "sso:ListProfileAssociations",
                "sso:ListInstances",
                "sso:GetProfile",
                "sso:GetSSOStatus",
                "sso:GetSsoConfiguration",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeUsers",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo 4: permitir a un usuario administrar usuarios y grupos en el directorio de Identity Center

La siguiente política de permisos concede permisos para permitir que un usuario pueda crear, visualizar, modificar y eliminar usuarios y grupos en IAM Identity Center.

En algunos casos, las modificaciones directas de los usuarios y grupos de IAM Identity Center están restringidas. Por ejemplo, cuando se selecciona Active Directory o un proveedor de identidades externo con el aprovisionamiento automático activado como fuente de identidad.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso-directory:ListGroupsForUser",
                "sso-directory:DisableUser",
                "sso-directory:EnableUser",
                "sso-directory:SearchGroups",
                "sso-directory:DeleteGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:DescribeDirectory",
                "sso-directory:UpdateUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "sso-directory:RemoveMemberFromGroup",
                "sso-directory:DeleteUser",
                "sso-directory:DescribeUsers",
                "sso-directory:UpdateGroup",
                "sso-directory:CreateGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

Permisos necesarios para usar la consola de IAM Identity Center

Para que un usuario pueda trabajar con la consola de IAM Identity Center sin errores, necesita permisos adicionales. Si se ha creado una política de IAM más restrictiva que los permisos

mínimos requeridos, la consola no funcionará como es debido para los usuarios con esa política. El siguiente ejemplo muestra el conjunto de permisos que podrían ser necesarios para garantizar un funcionamiento sin errores en la consola de IAM Identity Center.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribePermissionsPolicies",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetPermissionsPolicy",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
```

```
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS políticas gestionadas para el Centro de Identidad de IAM

Cómo crear políticas de IAM administradas por el cliente que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puede utilizar las políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información acerca de las políticas administradas de AWS , consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas administradas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

Las nuevas acciones que permiten enumerar y eliminar las sesiones de los usuarios están disponibles en el nuevo espacio de nombres de `identitystore-auth`. Los permisos adicionales para las acciones de este espacio de nombres se actualizarán en esta página. Al crear sus políticas de IAM personalizadas, evite utilizar `*` después de `identitystore-auth`, ya que esto se aplica a todas las acciones que existan en el espacio de nombres ahora o en el futuro.

AWS política gestionada: AWSSSOMasterAccountAdministrator

La política `AWSSSOMasterAccountAdministrator` proporciona a las entidades principales las acciones administrativas necesarias. La política está destinada a los directores que desempeñan la función de AWS IAM Identity Center administradores. Con el tiempo, la lista de acciones proporcionada se actualizará para adaptarla a la funcionalidad actual de IAM Identity Center y a las acciones que se requieren como administrador.

Puede adjuntar la política `AWSSSOMasterAccountAdministrator` a las identidades de IAM. Cuando adjuntas la `AWSSSOMasterAccountAdministrator` política a una identidad, concedes AWS IAM Identity Center permisos administrativos. Los directores que cuenten con esta política pueden acceder al Centro de Identidad de IAM desde la cuenta de AWS Organizations administración y desde todas las cuentas de los miembros. Esta entidad principal puede administrar por completo todas las operaciones de IAM Identity Center, incluida la posibilidad de crear una instancia de IAM Identity Center, los usuarios, los conjuntos de permisos y las asignaciones. El director también puede instanciar esas asignaciones en todas las cuentas de los miembros de la AWS organización y establecer conexiones entre los directorios AWS Directory Service gestionados y el IAM Identity Center. A medida que se publiquen nuevas características administrativas, el administrador de la cuenta recibirá estos permisos automáticamente.

Agrupaciones de permisos

Esta política se agrupa en instrucciones basadas en el conjunto de permisos proporcionados.

- `AWSSSOMasterAccountAdministrator`: permite a IAM Identity Center transferir el rol de servicio designado como `AWSServiceRoleforSSO` a IAM Identity Center, para que más adelante pueda asumir el rol y realizar acciones en su nombre. Esto es necesario cuando la persona o la aplicación intenta habilitar IAM Identity Center. Para obtener más información, consulte Gestione el acceso a Cuentas de AWS.
- `AWSSSOMemberAccountAdministrator`— Permite a IAM Identity Center realizar acciones de administrador de cuentas en un entorno de varias cuentas. AWS Para obtener más información, consulte AWS política gestionada: AWSSSOMemberAccountAdministrator.

- `AWSSSOManageDelegatedAdministrator`: permite a IAM Identity Center registrar y anular el registro de un administrador delegado para su organización.

Para ver los permisos de esta política, consulte la Referencia de políticas AWSSSOMasterAccountAdministratorAWS gestionadas.

Información adicional acerca de esta política

Cuando el Centro de Identidad de IAM se activa por primera vez, el servicio del Centro de Identidad de IAM crea un rol vinculado al servicio en la cuenta de AWS Organizations administración (anteriormente, cuenta maestra) para que el Centro de Identidad de IAM pueda administrar los recursos de su cuenta. Las acciones necesarias son `iam:CreateServiceLinkedRole` y `iam:PassRole`, que se muestran en los siguientes fragmentos.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
      },
      {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
         "Action":"iam:PassRole",
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
             "StringLike":{
               "iam:PassedToService":"sso.amazonaws.com"
             }
         }
      },
   ]
```

```
}
```

AWS política gestionada: AWSSSOMemberAccountAdministrator

La política `AWSSSOMemberAccountAdministrator` proporciona a las entidades principales las acciones administrativas necesarias. La política está destinada a las entidades principales que desempeñan el rol de un administrador de IAM Identity Center. Con el tiempo, la lista de acciones proporcionada se actualizará para adaptarla a la funcionalidad actual de IAM Identity Center y a las acciones que se requieren como administrador.

Puede adjuntar la política `AWSSSOMemberAccountAdministrator` a las identidades de IAM. Cuando adjuntas la `AWSSSOMemberAccountAdministrator` política a una identidad, concedes AWS IAM Identity Center permisos administrativos. Los directores que cuenten con esta política pueden acceder al Centro de Identidad de IAM desde la cuenta de AWS Organizations administración y desde todas las cuentas de los miembros. Esta entidad principal puede administrar por completo todas las operaciones de IAM Identity Center, incluida la capacidad de crear usuarios, conjuntos de permisos y asignaciones. El director también puede instanciar esas asignaciones en todas las cuentas de los miembros de la AWS organización y establecer conexiones entre los directorios AWS Directory Service gestionados y el IAM Identity Center. A medida que se publiquen nuevas características administrativas, el administrador de la cuenta recibe estos permisos automáticamente.

Para ver los permisos de esta política, consulte la Referencia de políticas AWSSSOMemberAccountAdministrator AWSgestionadas.

Información adicional acerca de esta política

Los administradores de IAM Identity Center administran a los usuarios, los grupos y las contraseñas en su almacén de directorios de Identity Center (sso-directory). El rol de administrador de la cuenta incluye permisos para las siguientes acciones:

- `"sso:*"`
- `"sso-directory:*"`

Los administradores del centro de identidad de IAM necesitan permisos limitados para realizar las siguientes AWS Directory Service acciones para realizar las tareas diarias.

- `"ds:DescribeTrusts"`

- "ds:UnauthorizeApplication"
- "ds:DescribeDirectories"
- "ds:AuthorizeApplication"
- “ds:CreateAlias”

Estos permisos permiten a los administradores de IAM Identity Center identificar los directorios existentes y administrar aplicaciones para que puedan configurarse para su uso con IAM Identity Center. Para obtener más información acerca de cada una de estas acciones, consulte Permisos de la API de AWS Directory Service : referencia acerca de las acciones, los recursos y las condiciones.

IAM Identity Center utiliza las políticas de IAM para conceder permisos a los usuarios de IAM Identity Center. Los administradores de IAM Identity Center crean conjuntos de permisos y les adjuntan políticas. El administrador de IAM Identity Center debe tener los permisos para enumerar las políticas existentes, de modo que pueda elegir qué políticas usar con el conjunto de permisos que está creando o actualizando. Para establecer permisos seguros y funcionales, el administrador de IAM Identity Center debe tener permisos para ejecutar la validación de la política de IAM Access Analyzer.

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

Los administradores del centro de identidad de IAM necesitan un acceso limitado a las siguientes AWS Organizations acciones para realizar las tareas diarias:

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"
- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"

- `"organizations:RegisterDelegatedAdministrator"`
- `"organizations:DeregisterDelegatedAdministrator"`

Estos permisos permiten a los administradores de IAM Identity Center trabajar con los recursos de la organización (cuentas) para realizar tareas administrativas básicas de IAM Identity Center, como las siguientes:

- Identificación de la cuenta de administración que pertenece a la organización
- Identificación de las cuentas de los miembros que pertenecen a la organización
- Habilitar el acceso AWS al servicio para las cuentas
- Configuración y administración de un administrador delegado

Para obtener más información acerca de cómo hacer uso de un administrador delegado con IAM Identity Center, consulte Administración delegada. Para obtener más información sobre cómo se utilizan estos permisos AWS Organizations, consulte Uso AWS Organizations con otros AWS servicios.

AWS política gestionada: AWSSSODirectoryAdministrator

Puede adjuntar la política `AWSSSODirectoryAdministrator` a las identidades de IAM.

Esta política concede permisos administrativos a los usuarios y grupos de IAM Identity Center. Las entidades principales que cuentan con esta política adjunta pueden realizar cualquier actualización a los usuarios y grupos de IAM Identity Center.

Para ver los permisos de esta política, consulte la Referencia AWSSSODirectoryAdministratorde políticas AWS gestionadas.

AWS política gestionada: AWSSSOReadOnly

Puede adjuntar la política `AWSSSOReadOnly` a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten a los usuarios ver información en IAM Identity Center. Las entidades principales que cuentan con esta política adjunta no pueden ver los usuarios y grupos de IAM Identity Center directamente. Las entidades principales que cuentan con esta política adjunta no pueden realizar ninguna actualización en IAM Identity Center. Por ejemplo, las entidades principales que cuentan con estos permisos pueden visualizar los ajustes de IAM Identity Center, pero no pueden cambiar ninguno de los valores de la configuración.

Para ver los permisos de esta política, consulte la Referencia AWSSSOReadOnlyde políticas AWS gestionadas.

AWS política gestionada: AWSSSODirectoryReadOnly

Puede adjuntar la política `AWSSSODirectoryReadOnly` a las identidades de IAM.

Esta política concede permisos de solo lectura que permiten a los usuarios ver los usuarios y grupos en IAM Identity Center. Las entidades principales que cuentan con esta política adjunta no pueden ver las asignaciones, los conjuntos de permisos, las aplicaciones ni los ajustes de IAM Identity Center. Las entidades principales que cuentan con esta política adjunta no pueden realizar ninguna actualización en IAM Identity Center. Por ejemplo, las entidades principales que cuentan con estos permisos pueden ver los usuarios de IAM Identity Center, pero no pueden cambiar ningún atributo de usuario ni asignar dispositivos de MFA.

Para ver los permisos de esta política, consulte la Referencia AWSSSODirectoryReadOnlyde políticas AWS gestionadas.

AWS política gestionada: AWSIdentitySyncFullAccess

Puede adjuntar la política `AWSIdentitySyncFullAccess` a las identidades de IAM.

Las entidades principales que cuentan con esta política adjunta tienen permisos de acceso total para crear y eliminar perfiles de sincronización, asociar o actualizar un perfil de sincronización con un destino de sincronización, crear, enumerar y eliminar filtros de sincronización, e iniciar o detener la sincronización.

Detalles del permiso

Para ver los permisos de esta política, consulte la Referencia AWSIdentitySyncFullAccessde políticas AWS gestionadas.

AWS política gestionada: AWSIdentitySyncReadOnlyAccess

Puede adjuntar la política `AWSIdentitySyncReadOnlyAccess` a las identidades de IAM.

Esta política concede permisos de solo lectura que permiten a los usuarios ver información sobre el perfil de sincronización de identidades, los filtros y la configuración de destino. Las entidades principales que cuentan con esta política adjunta no pueden actualizar la configuración de sincronización. Por ejemplo, las entidades principales que cuentan con estos permisos pueden

visualizar los ajustes de sincronización de identidades, pero no pueden cambiar ninguno de los valores del perfil o del filtro.

Para ver los permisos de esta política, consulte la Referencia AWSIdentitySyncReadOnlyAccessde políticas AWS gestionadas.

AWS política gestionada: AWSSSOServiceRolePolicy

No puede adjuntar la política `AWSSSOServiceRolePolicy` a las identidades de IAM.

Esta política está asociada a una función vinculada al servicio que permite a IAM Identity Center delegar y hacer cumplir qué usuarios tienen acceso de inicio de sesión único a una entrada específica. Cuentas de AWS AWS Organizations Al habilitar la IAM, se crea una función vinculada al servicio en todos los ámbitos de la organización. Cuentas de AWS IAM Identity Center también crea el mismo rol vinculado a servicios en todas las cuentas que se añaden posteriormente a su organización. Este rol permite a IAM Identity Center acceder a los recursos de cada cuenta en su nombre. Los roles vinculados al servicio que se crean en cada uno de ellos reciben un nombre. Cuenta de AWS `AWSServiceRoleForSSO` Para obtener más información, consulte Uso de roles vinculados a servicios para IAM Identity Center.

AWS política gestionada: AWSIAMIdentityCenterAllowListForIdentityContext

Al asumir un rol con el contexto de identidad del Centro de Identidad de IAM, AWS Security Token Service (AWS STS) asocia automáticamente la `AWSIAMIdentityCenterAllowListForIdentityContext` política al rol.

Esta política proporciona la lista de acciones que se permiten cuando se utiliza la propagación de identidades de confianza con roles que se asumen con el contexto de identidad de IAM Identity Center. Se bloquearán todas las demás acciones que se invoquen en este contexto. El contexto de identidad se transmite como `ProvidedContext`.

Para ver los permisos de esta política, consulte la Referencia de políticas AWSIAMIdentityCenterAllowListForIdentityContextAWS gestionadas.

IAM Identity Center actualiza las políticas AWS gestionadas

En la siguiente tabla se describen las actualizaciones de las políticas AWS gestionadas del Centro de Identidad de IAM desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre los cambios que se produzcan en esta página, suscríbase al canal RSS en la página de historial de documentos de IAM Identity Center.

Cambio	Descripción	Fecha
AWSIAMIdentityCenterAllowListForIdentityContext	Esta política ahora incluye las `elasticmapreduce:AddJobFlowSteps` , `elasticmapreduce:DescribeCluster` `elasticmapreduce:CancelSteps` `elasticmapreduce:DescribeStep` , y `elasticmapreduce:ListSteps` las acciones para respaldar la propagación de identidades confiables en Amazon EMR.	17 de mayo de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Esta política ahora incluye las `qapps:CreateQApp` ,,, `qapps:PredictProblemStatementFromConversation` ,`qapps:PredictQAppFromProblemStatement` ,`qapps:CopyQApp` ,`qapps:GetQApp` ,,`qapps:ListQApps` ,`qapps:UpdateQApp` ,`qapps:DeleteQApp` ,`qapps:AssociateQAppWithUser` ,,`qapps:DisassociateQAppFromUser` ,`qapps:ImportDocumentToQApp` ,`qapps:ImportDocumentToQAppS`	30 de abril de 2024

Cambio	Descripción	Fecha
	`ession` ,`qapps:Cre ateLibrar yItem` ,,`qapps:Get LibraryItem` ,`qapps:Upd ateLibraryItem` , `qapps:CreateLibrar yItemReview` `qapps:Lis tLibraryItems` `qapps:CreateSubscr iptionToken` `qapps:Sta rtQAppSession` , y `qapps:StopQAppSess ion` las acciones para respaldar las sesiones de consola con reconocimiento de identidad para las aplicacio nes AWS administradas que admiten estas sesiones.	
AWSSSOMasterAccoun tAdministrator	Esta política ahora incluye `signin:ListTrusted IdentityPropagatio nApplicationsForCo nsole` las acciones necesarias para respaldar `signin:CreateTrust edIdentityPropagat ionApplicationForC onsole` las sesiones de consola con reconocimiento de identidad para las aplicacio nes AWS administradas que admiten estas sesiones.	26 de abril de 2024

Cambio	Descripción	Fecha
AWSSSOMemberAccountAdministrator	Esta política ahora incluye `signin:ListTrustedIdentityPropagationApplicationsForConsole` las acciones necesarias para respaldar `signin:CreateTrustedIdentityPropagationApplicationForConsole` las sesiones de consola con reconocimiento de identidad para las aplicaciones AWS administradas que admiten estas sesiones.	26 de abril de 2024
AWSSSOReadOnly	Esta política ahora incluye la `signin:ListTrustedIdentityPropagationApplicationsForConsole` acción para respaldar las sesiones de consola con reconocimiento de identidad para las aplicaciones AWS administradas que admiten estas sesiones.	26 de abril de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Esta política ahora incluye la `qbusiness:PutFeedback` acción para respaldar las sesiones de consola con reconocimiento de identidad para las aplicaciones AWS administradas que admiten estas sesiones.	26 de abril de 2024

Cambio	Descripción	Fecha
AWSIAMIdentityCenterAllowListForIdentityContext	Esta política ahora incluye lasq:StartConversation ,,, q:SendMessage q:ListConversations q:GetConversation q:StartTroubleshootingAnalysis q:GetTroubleshootingResults q:StartTroubleshootingResolutionExplanation , y q:UpdateTroubleshootingCommandResult las acciones para respaldar las sesiones de consola con reconocimiento de identidad para las aplicaciones AWS administradas que admiten estas sesiones.	24 de abril de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Esta política ahora incluye la sts:SetContext acción para respaldar las sesiones de consola con reconocimiento de identidad para las aplicaciones AWS administradas que admiten estas sesiones.	19 de abril de 2024

Cambio	Descripción	Fecha
AWSIAMIdentityCenterAllowListForIdentityContext	Esta política ahora incluye lasqbusiness:Chat , qbusiness:ChatSync qbusiness:ListConversations qbusiness:ListMessages , y qbusiness:DeleteConversation las acciones para respaldar las sesiones de consola con reconocimiento de identidad para las aplicaciones AWS administradas que admiten estas sesiones.	11 de abril de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	La política ahora incluye las acciones s3:GetAccessGrantsInstanceForPrefix y s3:GetDataAccess .	26 de noviembre de 2023
AWSIAMIdentityCenterAllowListForIdentityContext	Esta política proporciona la lista de acciones que se permiten cuando se utiliza la propagación de identidades de confianza con roles que se asumen con el contexto de identidad de IAM Identity Center.	15 de noviembre de 2023
AWSSSODirectoryReadOnly	Ahora esta política incluye el nuevo espacio de nombres de identitystore-auth con nuevos permisos que permiten a los usuarios enumerar y obtener sesiones.	21 de febrero de 2023

Cambio	Descripción	Fecha
AWSSSOServiceRolePolicy	Ahora esta política permite realizar la acción `UpdateSAMLProvider` en la cuenta de administración.	20 de octubre de 2022
AWSSSOMasterAccountAdministrator	Ahora esta política incluye el nuevo espacio de nombres de `identitystore-auth` con nuevos permisos que permiten al administrador enumerar y eliminar sesiones de un usuario.	20 de octubre de 2022
AWSSSOMemberAccountAdministrator	Ahora esta política incluye el nuevo espacio de nombres de `identitystore-auth` con nuevos permisos que permiten al administrador enumerar y eliminar sesiones de un usuario.	20 de octubre de 2022
AWSSSODirectoryAdministrator	Ahora esta política incluye el nuevo espacio de nombres de `identitystore-auth` con nuevos permisos que permiten al administrador enumerar y eliminar sesiones de un usuario.	20 de octubre de 2022

Cambio	Descripción	Fecha
AWSSSOMasterAccountAdministrator	Esta política ahora incluye nuevos permisos para realizar llamadas `ListDelegatedAdministrators`. AWS Organizations Ahora esta política también incluye un subconjunto de permisos de `AWSSSOManageDelegatedAdministrator` que incluye permisos para realizar llamadas a `RegisterDelegatedAdministrator` y `DeregisterDelegatedAdministrator`.	16 de agosto de 2022
AWSSSOMemberAccountAdministrator	Esta política ahora incluye nuevos permisos para llamar `ListDelegatedAdministrators` AWS Organizations. Ahora esta política también incluye un subconjunto de permisos de `AWSSSOManageDelegatedAdministrator` que incluye permisos para realizar llamadas a `RegisterDelegatedAdministrator` y `DeregisterDelegatedAdministrator`.	16 de agosto de 2022

Cambio	Descripción	Fecha
AWSSSOReadOnly	Esta política ahora incluye nuevos permisos para llamar `ListDelegatedAdministrators` AWS Organizations.	11 de agosto de 2022
AWSSSOServiceRolePolicy	Ahora esta política incluye nuevos permisos para realizar llamadas a `DeleteRolePermissionsBoundary` en `PutRolePermisionsBoundary`.	14 de julio de 2022
AWSSSOServiceRolePolicy	Ahora esta política incluye nuevos permisos para realizar llamadas a `ListAWSServiceAccessForOrganization` and `ListDelegatedAdministrators` en AWS Organizations.	11 de mayo de 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	Agregue permisos de IAM Access Analyzer para permitir a una entidad principal utilizar las verificaciones de políticas para la validación.	28 de abril de 2022

Cambio	Descripción	Fecha
AWSSSOMasterAccountAdministrator	Ahora esta política permite todas las acciones del servicio Almacén de identidades de IAM Identity Center. Para obtener información acerca de las acciones disponibles en el servicio de almacén de identidades de IAM, consulte Referencia de la API del servicio Almacén de identidades de IAM Identity Center.	29 de marzo de 2022
AWSSSOMemberAccountAdministrator	Ahora esta política permite todas las acciones del servicio Almacén de identidades de IAM Identity Center.	29 de marzo de 2022
AWSSSODirectoryAdministrator	Ahora esta política permite todas las acciones del servicio Almacén de identidades de IAM Identity Center.	29 de marzo de 2022
AWSSSODirectoryReadOnly	Ahora esta política concede acceso a las acciones de lectura del servicio Almacén de identidades de IAM Identity Center. Este acceso es necesario para recuperar la información de los usuarios y los grupos del servicio Almacén de identidades de IAM Identity Center.	29 de marzo de 2022

Cambio	Descripción	Fecha
AWSIdentitySyncFullAccess	Esta política permite obtener acceso completo a permisos de sincronización de identidad es.	3 de marzo de 2022
AWSIdentitySyncReadOnlyAccess	Esta política concede permisos de solo lectura que permiten a una entidad principal visualizar la configuración de la sincronización de identidades.	3 de marzo de 2022
AWSSSOReadOnly	Esta política concede permisos de solo lectura que permiten a una entidad principal visualizar los ajustes de configuración de IAM Identity Center.	4 de agosto de 2021
IAM Identity Center comenzó a realizar el seguimiento de los cambios	El Centro de Identidad de IAM comenzó a realizar un seguimiento de los cambios en las políticas AWS gestionadas.	4 de agosto de 2021

Uso de roles vinculados a servicios para IAM Identity Center

AWS IAM Identity Center utiliza funciones AWS Identity and Access Management vinculadas al servicio (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a IAM Identity Center. Está predefinido por el Centro de Identidad de IAM e incluye todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre. Para obtener más información, consulte Roles vinculados al servicio.

Un rol vinculado a servicios simplifica la configuración de IAM Identity Center porque ya no tendrá que agregar manualmente los permisos necesarios. IAM Identity Center define los permisos de su rol

vinculado a servicios y, a menos que esté definido de otra manera, solo IAM Identity Center puede asumir su rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Para obtener información sobre otros servicios que son compatibles con los roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a servicios para IAM Identity Center

El Centro de identidad de IAM utiliza la función vinculada al servicio denominada AWSServiceRoleForSSOpara conceder permisos al Centro de identidad de IAM para gestionar los AWS recursos, incluidas las funciones de IAM, las políticas y el IdP de SAML en su nombre.

El rol AWSServiceRoleForSSO vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `IAM Identity Center`

La política de permisos de los roles AWSServiceRoleForSSO vinculados al servicio permite al Centro de Identidad de IAM completar lo siguiente en los roles de la ruta «/aws-reserved/sso.amazonaws.com/» y con el prefijo de nombre «_»: AWSReservedSSO

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`
- `iam:DeleteRolePermissionsBoundary`
- `iam:DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

La política de permisos de roles AWSServiceRoleForSSO vinculados al servicio permite al Centro de Identidad de IAM completar lo siguiente en los proveedores de SAML con el prefijo «_»: AWSSSO

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam:DeleteSAMLProvider`

La política de permisos de roles AWSServiceRoleForSSO vinculados al servicio permite al Centro de Identidad de IAM completar lo siguiente en todas las organizaciones:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

La política de permisos de funciones AWSServiceRoleForSSO vinculadas al servicio permite a IAM Identity Center realizar las siguientes tareas en todas las funciones de IAM (*):

- `iam:listRoles`

La política de permisos de funciones AWSServiceRoleForSSO vinculadas al servicio permite al Centro de Identidad de IAM completar lo siguiente en «arn:aws:iam: :*:role/ /sso.amazonaws.com/»: aws-service-role AWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

La política de permisos del rol permite que IAM Identity Center realice las siguientes acciones en los recursos.

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

```
            "Sid":"IAMRoleProvisioningActions",
            "Effect":"Allow",
            "Action":[
               "iam:AttachRolePolicy",
               "iam:CreateRole",
               "iam:DeleteRolePermissionsBoundary",
               "iam:PutRolePermissionsBoundary",
               "iam:PutRolePolicy",
               "iam:UpdateRole",
               "iam:UpdateRoleDescription",
               "iam:UpdateAssumeRolePolicy"
            ],
            "Resource":[
               "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
            ],
            "Condition":{
               "StringNotEquals":{
                  "aws:PrincipalOrgMasterAccountId":"${aws:PrincipalAccount}"
               }
            }
         },
         {
            "Sid":"IAMRoleReadActions",
            "Effect":"Allow",
            "Action":[
               "iam:GetRole",
               "iam:ListRoles"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"IAMRoleCleanupActions",
            "Effect":"Allow",
            "Action":[
               "iam:DeleteRole",
               "iam:DeleteRolePolicy",
               "iam:DetachRolePolicy",
               "iam:ListRolePolicies",
               "iam:ListAttachedRolePolicies"
            ],
            "Resource":[
               "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
```

```
         ]
      },
      {
         "Sid":"IAMSLRCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:DeleteRole",
            "iam:GetRole"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
         ]
      },
      {
        "Sid": "IAMSAMLProviderCreationAction",
        "Effect": "Allow",
        "Action": [
          "iam:CreateSAMLProvider"
      ],
      "Resource": [
         "arn:aws:iam::*:saml-provider/AWSSSO_*"
       ],
      "Condition": {
         "StringNotEquals": {
            "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
          }
        }
      },
      {
        "Sid": "IAMSAMLProviderUpdateAction",
        "Effect": "Allow",
        "Action": [
          "iam:UpdateSAMLProvider"
        ],
        "Resource": [
           "arn:aws:iam::*:saml-provider/AWSSSO_*"
        ]
      },
      {
         "Sid":"IAMSAMLProviderCleanupActions",
         "Effect":"Allow",
```

```
            "Action":[
               "iam:DeleteSAMLProvider",
               "iam:GetSAMLProvider"
            ],
            "Resource":[
               "arn:aws:iam::*:saml-provider/AWSSSO_*"
            ]
         },
         {
            "Effect":"Allow",
            "Action":[
               "organizations:DescribeAccount",
               "organizations:DescribeOrganization",
               "organizations:ListAccounts",
               "organizations:ListAWSServiceAccessForOrganization",
               "organizations:ListDelegatedAdministrators"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowUnauthAppForDirectory",
            "Effect":"Allow",
            "Action":[
               "ds:UnauthorizeApplication"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDescribeForDirectory",
            "Effect":"Allow",
            "Action":[
               "ds:DescribeDirectories",
               "ds:DescribeTrusts"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDescribeAndListOperationsOnIdentitySource",
```

```
         "Effect":"Allow",
         "Action":[
            "identitystore:DescribeUser",
            "identitystore:DescribeGroup",
            "identitystore:ListGroups",
            "identitystore:ListUsers"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para IAM Identity Center

No necesita crear manualmente un rol vinculado a servicios. Una vez activado, IAM Identity Center crea un rol vinculado al servicio en todas las cuentas de la organización en Organizations. AWS IAM Identity Center también crea el mismo rol vinculado a servicios en todas las cuentas que se añaden posteriormente a su organización. Este rol permite a IAM Identity Center acceder a los recursos de cada cuenta en su nombre.

Notas

- Si ha iniciado sesión en la cuenta de AWS Organizations administración, esta utilizará su función con la que ha iniciado sesión actualmente y no la función vinculada al servicio. De este modo se evita la escalada de privilegios.
- Cuando el IAM Identity Center realiza cualquier operación de IAM en la cuenta de AWS Organizations administración, todas las operaciones se realizan con las credenciales del director de IAM. Esto permite que los inicios de sesión CloudTrail proporcionen visibilidad de quién realizó todos los cambios de privilegios en la cuenta de administración.

> **Important**
>
> Si utilizaba el servicio IAM Identity Center antes del 7 de diciembre de 2017, cuando comenzó a admitir funciones vinculadas al servicio, IAM Identity Center creó la AWSServiceRoleForSSO función en su cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a un servicio y necesita crearlo de nuevo, puede seguir el mismo proceso para volver a crear el rol en su cuenta.

Edición de un rol vinculado a servicios para IAM Identity Center

El Centro de Identidad de IAM no le permite editar el rol vinculado al servicio. AWSServiceRoleForSSO Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para IAM Identity Center

No es necesario eliminar el rol manualmente. AWSServiceRoleForSSO Cuando Cuenta de AWS se elimina un rol de una AWS organización, el Centro de Identidad de IAM limpia automáticamente los recursos y elimina el rol vinculado al servicio. Cuenta de AWS

También puede utilizar la consola de IAM, la CLI de IAM o la API de IAM para eliminar manualmente el rol vinculado a servicios. Para ello, primero debe limpiar manualmente los recursos del rol vinculado al servicio para poder eliminarlo después manualmente.

> **Note**
>
> Si el servicio IAM Identity Center está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos del Centro de Identidad de IAM utilizados por el AWSServiceRoleForSSO

1. Elimine el acceso de usuarios y grupos para todos los usuarios y grupos que tengan acceso a la Cuenta de AWS.

2. Borrado de conjuntos de permisos que ha asociado con la Cuenta de AWS.

Eliminación manual del rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado al AWSServiceRoleForSSO servicio. Para más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Consola de IAM Identity Center y autorización de la API

Las API de la consola de IAM Identity Center existentes admiten la doble autorización, lo que le permite seguir utilizando las operaciones de las API existentes cuando hay API más nuevas disponibles. Si ya tiene instancias de IAM Identity Center que se hayan creado antes del 15 de noviembre de 2023 y el 15 de octubre de 2020, puede utilizar las siguientes tablas para determinar qué operaciones de la API se asignan ahora a las operaciones de la API más recientes que se publicaron después de esas fechas.

Temas

- Acciones de la API después de noviembre de 2023
- Acciones de la API después de octubre de 2020

Acciones de la API después de noviembre de 2023

Las instancias de IAM Identity Center que se crearon antes del 15 de noviembre de 2023 aceptan las acciones de la API antiguas y nuevas, siempre que no se deniegue explícitamente ninguna de ellas. Las instancias creadas después del 15 de noviembre de 2023 utilizan las acciones de la API más recientes a efectos de la autorización en la consola de IAM Identity Center.

Nombre de operación de la consola utilizado antes del 15 de noviembre de 2023	Acción de la API utilizada después del 15 de noviembre de 2023
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod

Nombre de operación de la consola utilizado antes del 15 de noviembre de 2023	Acción de la API utilizada después del 15 de noviembre de 2023
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

Acciones de la API después de octubre de 2020

Las instancias de IAM Identity Center que se crearon antes del 15 de octubre de 2020 aceptan las acciones de la API antiguas y nuevas, siempre que no se deniegue explícitamente ninguna de ellas. Las instancias creadas después del 15 de octubre de 2020 utilizan las acciones de la API más recientes a efectos de la autorización en la consola de IAM Identity Center.

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS condicionan las claves de contexto del Centro de Identidad de IAM

Cuando un director hace una solicitud AWS, AWS recopila la información de la solicitud en un contexto de solicitud, que se utiliza para evaluar y autorizar la solicitud. Puede utilizar el elemento `Condition` de una política JSON para comparar las claves de la solicitud de contexto con los valores de claves que especifique en su política. La información de la solicitud proviene de diferentes fuentes, como el principal que realiza la solicitud, el recurso, la solicitud con la que se realiza y los metadatos sobre la solicitud en sí. Las claves de condición específicas del servicio se definen para su uso con un servicio individual AWS .

El IAM Identity Center incluye un proveedor de AWS STS contexto que permite a las aplicaciones AWS gestionadas y a las aplicaciones de terceros añadir valores a las claves de condición definidas por el IAM Identity Center. Estas claves se incluyen en las funciones de IAM. Los valores clave se

establecen cuando una aplicación pasa un token a AWS STS. La aplicación obtiene el token al que pasa de una AWS STS de las siguientes maneras:

- Durante la autenticación con IAM Identity Center.
- Tras el intercambio de fichas con un emisor de fichas de confianza para propagar la identidad de forma fiable. En este caso, la aplicación obtiene un token de un emisor de token de confianza y lo cambia por un token del IAM Identity Center.

Estas claves suelen ser utilizadas por aplicaciones que se integran con la propagación de identidades de confianza. En algunos casos, cuando hay valores clave, puede utilizarlas en las políticas de IAM que cree para permitir o denegar permisos.

Por ejemplo, es posible que desee proporcionar acceso condicional a un recurso en función del valor de. `UserId` Este valor indica qué usuario del Centro de identidades de IAM utiliza el rol. El ejemplo es similar a usar`SourceId`. Sin embargo`SourceId`, a diferencia de lo que ocurre con el valor de, `UserId` representa a un usuario verificado específico del almacén de identidades. Este valor está presente en el token que la aplicación obtiene y al que, a AWS STS continuación, pasa. No es una cadena de uso general que pueda contener valores arbitrarios.

Temas

- almacén de identidades: UserId
- almacén de identidades: IdentityStoreArn
- centro de identidad: ApplicationArn
- centro de identidad: CredentialId
- centro de identidad: InstanceArn

almacén de identidades: UserId

Esta clave de contexto es la `UserId` del usuario del Centro de Identidad de IAM que es objeto de la afirmación de contexto emitida por el Centro de Identidad de IAM. La afirmación de contexto se pasa a. AWS STS Puede utilizar esta clave para comparar el identificador `UserId` del usuario del Centro de Identidad de IAM en nombre del que se realiza la solicitud con el identificador del usuario que especifique en la política.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud después de establecer una afirmación de contexto emitida por el Centro de Identidad de IAM, cuando se asume una función

mediante cualquier AWS STS `assume-role` comando de la operación AWS CLI o AWS STS `AssumeRole` de la API.

- Tipo de datos: cadena
- Tipo de valor: valor único

almacén de identidades: IdentityStoreArn

Esta clave de contexto es el ARN del almacén de identidades que está adjunto a la instancia de IAM Identity Center que emitió la afirmación de contexto. También es el almacén de identidades en el que puede buscar los atributos. `identitystore:UserID` Puede usar esta clave en las políticas para determinar si `identitystore:UserID` proviene de un ARN de almacén de identidades esperado.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud después de establecer una afirmación de contexto emitida por el Centro de Identidad de IAM, cuando se asume una función mediante cualquier AWS STS `assume-role` comando de la operación AWS CLI o AWS STS `AssumeRole` de la API.
- Tipo de datos: Arn, String
- Tipo de valor: valor único

centro de identidad: ApplicationArn

Esta clave de contexto es el ARN de la aplicación para la que IAM Identity Center emitió una afirmación de contexto. Puede usar esta clave en las políticas para determinar si `identitycenter:ApplicationArn` proviene de una aplicación esperada. El uso de esta clave puede ayudar a evitar que una aplicación inesperada acceda a un rol de IAM.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud de una operación de AWS STS `AssumeRole` API. El contexto de la solicitud incluye una afirmación de contexto emitida por IAM Identity Center.
- Tipo de datos: Arn, String
- Tipo de valor: valor único

centro de identidad: CredentialId

Esta clave de contexto es un identificador aleatorio para la credencial de rol con identidad mejorada y se utiliza únicamente para el registro. Como este valor clave es impredecible, le recomendamos que no lo utilice para hacer afirmaciones de contexto en las políticas.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud de una operación de AWS STS `AssumeRole` API. El contexto de la solicitud incluye una afirmación de contexto emitida por IAM Identity Center.
- Tipo de datos: cadena
- Tipo de valor: valor único

centro de identidad: InstanceArn

Esta clave de contexto es el ARN de la instancia de IAM Identity Center que emitió la afirmación de contexto para. `identitystore:UserID` Puede utilizar esta clave para determinar si la afirmación `identitystore:UserID` y el contexto provienen de un ARN de instancia de IAM Identity Center esperado.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud de una AWS STS `AssumeRole` operación de API. El contexto de la solicitud incluye una afirmación de contexto emitida por IAM Identity Center.
- Tipo de datos: Arn, String
- Tipo de valor: valor único

Registro y supervisión en IAM Identity Center

Como práctica recomendada, debe monitorear su organización para asegurarse de que los cambios queden registrados. Esto le ayuda a garantizar que se pueda investigar cualquier cambio inesperado y revertir los cambios no deseados. AWS IAM Identity Center actualmente admite dos AWS servicios que le ayudan a supervisar su organización y la actividad que se lleva a cabo en ella.

Temas

- Registrar las llamadas a la API de IAM Identity Center con AWS CloudTrail
- Amazon EventBridge

- Registro de errores de sincronización de AD y de sincronización de AD configurables

Registrar las llamadas a la API de IAM Identity Center con AWS CloudTrail

AWS IAM Identity Center está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en el Centro de Identidad de IAM. CloudTrail captura las llamadas a la API del Centro de Identidad de IAM como eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de IAM Identity Center y las llamadas de código a las operaciones de la API de IAM Identity Center. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos del IAM Identity Center. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó al Centro de Identidad de IAM, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía del AWS CloudTrail usuario.

Temas

- Información sobre el centro de identidad de IAM en CloudTrail
- Explicación de las entradas de los archivos de registros de IAM Identity Center
- Explicación de los eventos de inicio de sesión de IAM Identity Center

Información sobre el centro de identidad de IAM en CloudTrail

CloudTrail está habilitada en su cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en el Centro de Identidad de IAM, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos en su centro de identidad Cuenta de AWS, incluidos los eventos del IAM Identity Center, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS . La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar

más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Cuando el CloudTrail registro está activado en su cuenta Cuenta de AWS, las llamadas a la API realizadas a las acciones del Centro de Identidad de IAM se registran en los archivos de registro. Los registros del IAM Identity Center se escriben junto con otros registros de AWS servicio en un archivo de registro. CloudTrail determina cuándo crear y escribir en un nuevo archivo en función del período de tiempo y del tamaño del archivo.

Se admiten las siguientes CloudTrail operaciones del IAM Identity Center:

Operaciones de la API en la consola	Operaciones de la API públicas
`AssociateDirectory`	`AttachManagedPolicyToPermissionSet`
`AssociateProfile`	`CreateAccountAssignment`
`BatchDeleteSession`	`CreateInstanceAccessControlAttributeConfiguration`
`BatchGetSession`	`CreatePermissionSet`
`CreateApplicationInstance`	`DeleteAccountAssignment`
`CreateApplicationInstanceCertificate`	`DeleteInlinePolicyFromPermissionSet`
`CreatePermissionSet`	`DeleteInstanceAccessControlAttributeConfiguration`
`CreateProfile`	`DeletePermissionSet`

Operaciones de la API en la consola	Operaciones de la API públicas
DeleteApplicationInstance	DescribeAccountAssignmentCreationStatus
DeleteApplicationInstanceCertificate	DescribeAccountAssignmentDeletionStatus
DeletePermissionsPolicy	DescribeInstanceAccessControlAttributeConfiguration
DeletePermissionSet	DescribePermissionSet
DeleteProfile	DescribePermissionSetProvisioningStatus
DescribePermissionsPolicies	DetachManagedPolicyFromPermissionSet
DisassociateDirectory	GetInlinePolicyForPermissionSet
DisassociateProfile	ListAccountAssignmentCreationStatus
GetApplicationInstance	ListAccountAssignmentDeletionStatus
GetApplicationTemplate	ListAccountAssignments
GetMfaDeviceManagementForDirectory	ListAccountsForProvisionedPermissionSet
GetPermissionSet	ListInstances
GetSSOStatus	ListManagedPoliciesInPermissionSet
ImportApplicationInstanceServiceProviderMetadata	ListPermissionSetProvisioningStatus

Operaciones de la API en la consola	Operaciones de la API públicas
ListApplicationInstances	ListPermissionSets
ListApplicationInstanceCertificates	ListPermissionSetsProvisionedToAccount
ListApplicationTemplates	ListTagsForResource
ListDirectoryAssociations	ProvisionPermissionSet
ListPermissionSets	PutInlinePolicyToPermissionSet
ListProfileAssociations	TagResource
ListProfiles	UntagResource
ListSessions	UpdateInstanceAccessControlAttributeConfiguration
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	

Operaciones de la API en la consola	Operaciones de la API públicas
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	
UpdateProfile	

Para obtener más información sobre las operaciones de la API pública para IAM Identity Center, consulte la Guía de referencia de la API para IAM Identity Center.

Se admiten las siguientes CloudTrail operaciones del almacén de identidades del IAM Identity Center:

- AddMemberToGroup
- CompleteVirtualMfaDeviceRegistration
- CompleteWebAuthnDeviceRegistration
- CreateAlias
- CreateExternalIdPConfigurationForDirectory
- CreateGroup
- CreateUser
- DeleteExternalIdPConfigurationForDirectory
- DeleteGroup
- DeleteMfaDeviceForUser
- DeleteUser
- DescribeDirectory
- DescribeGroups
- DescribeUsers
- DisableExternalIdPConfigurationForDirectory
- DisableUser

- EnableExternalIdPConfigurationForDirectory
- EnableUser
- GetAWSSPConfigurationForDirectory
- ListExternalIdPConfigurationsForDirectory
- ListGroupsForUser
- ListMembersInGroup
- ListMfaDevicesForUser
- PutMfaDeviceManagementForDirectory
- RemoveMemberFromGroup
- SearchGroups
- SearchUsers
- StartVirtualMfaDeviceRegistration
- StartWebAuthnDeviceRegistration
- UpdateExternalIdPConfigurationForDirectory
- UpdateGroup
- UpdateMfaDeviceForUser
- UpdatePassword
- UpdateUser
- VerifyEmail

Se admiten las siguientes acciones OIDC CloudTrail del IAM Identity Center:

- CreateToken
- RegisterClient
- StartDeviceAuthorization

Se admiten las siguientes acciones del portal CloudTrail del IAM Identity Center:

- Authenticate
- Federate
- ListApplications
- ListProfilesForApplication

- `ListAccounts`
- `ListAccountRoles`
- `GetRoleCredentials`
- `Logout`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario raíz o de usuario AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento CloudTrail UserIdentity.

Explicación de las entradas de los archivos de registros de IAM Identity Center

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de CloudTrail registro para un administrador (samadams@example.com) que tuvo lugar en la consola del IAM Identity Center:


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "accessKeyId":"AKIAIIJM2K4example",
```

```
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro de una acción del usuario final (bobsmith@example.com) que tuvo lugar en el portal de AWS acceso:

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
```

```
        "sourceIPAddress":"203.0.113.0",
        "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
        "requestParameters":null,
        "responseElements":null,
        "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
        "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
        "eventType":"AwsApiCall",
        "recipientAccountId":"08966example"
      }
   ]
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro para una acción de un usuario final (bobsmith@example.com) que tuvo lugar en el IAM Identity Center OIDC:

```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "08966example",
        "userName": "bobsmith@example.com"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
```

```
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
          "accountId": "08966example",
          "type": "IdentityStoreId",
          "ARN": "d-1234example"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "08966example"
}
```

Explicación de los eventos de inicio de sesión de IAM Identity Center

AWS CloudTrail registra los eventos de inicio de sesión correctos y fallidos en todas las fuentes de identidad. AWS IAM Identity Center Las identidades de origen nativo de SSO y Active Directory (AD Connector y AWS Managed Microsoft AD) incluirán eventos de inicio de sesión adicionales que se capturarán cada vez que se pida a un usuario que resuelva un desafío o factor de credenciales específico, así como el estado de esa solicitud de verificación de credenciales en particular. Solo después de que un usuario haya completado todos los desafíos de credenciales requeridos, el usuario iniciará sesión, lo que provocará que se registre un evento `UserAuthentication`.

En la siguiente tabla se muestran los nombres de los CloudTrail eventos de inicio de sesión del IAM Identity Center, su finalidad y su aplicabilidad a las distintas fuentes de identidad.

Nombre de evento	Propósito del evento	Aplicabilidad de la fuente de identidad
`CredentialChallenge`	Se utiliza para notificar que IAM Identity Center ha solicitado al usuario que resuelva un desafío de credenciales específico y puntualiza el `CredentialType` que se requiere (por ejemplo, PASSWORD o TOTP).	Usuarios nativos del IAM Identity Center, AD Connector y AWS Managed Microsoft AD

Nombre de evento	Propósito del evento	Aplicabilidad de la fuente de identidad
`CredentialVerification`	Se utiliza para notificar que el usuario ha intentado resolver una solicitud de `CredentialChallenge` específica y precisa si la credencial se ha realizado correctamente o no.	Usuarios nativos del IAM Identity Center, AD Connector y AWS Managed Microsoft AD
`UserAuthentication`	Se utiliza para notificar que todos los requisitos de autenticación con los que se desafió al usuario se han completado con éxito y que el usuario ha iniciado sesión correctamente. Si los usuarios no completan correctamente los desafíos de credenciales requeridos, no se registrará ningún evento de *`UserAuthentication`* .	Todas las fuentes de identidad

En la siguiente tabla, se muestran otros campos de datos de eventos útiles incluidos en eventos de inicio de sesión CloudTrail específicos.

Nombre de evento	Propósito del evento	Aplicabilidad al evento de inicio de sesión	Valores de ejemplo
`AuthWorkflowID`	Se utiliza para correlacionar todos los eventos emitidos en una secuencia de inicio de sesión completa. Por cada inicio de sesión de	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	«AuthWorkflowID»: «9de74b32-8362-4a01-a524-de21df59fd83"

Nombre de evento	Propósito del evento	Aplicabilidad al evento de inicio de sesión	Valores de ejemplo
	usuario, IAM Identity Center puede emitir varios eventos.		
`CredentialType`	Se utiliza para especificar la credencial o el factor que se ha cuestiona do. Los eventos de `UserAuthe ntication` incluirán todos los valores de `CredentialType` que se hayan verificado correctam ente a lo largo de la secuencia de inicio de sesión del usuario.	`Credentia lChalleng e` , `Credentia lVerifica tion` , `UserAuthe ntication`	CredentialType«: «PASSWORD» o "«: «PASSWORD, TOTP» (los valores posibles incluyen: PASSWORD, TOTP, WEBAUTHN, CredentialType EXTERNAL_IDP, RESYNC_TOTP)
`DeviceEnr ollmentRe quired`	Se utiliza para especificar que el usuario debe registrar un dispositivo de MFA durante el inicio de sesión y que el usuario ha completad o correctamente la solicitud.	`UserAuthe ntication`	"«: «verdadero» DeviceEnrollmentRe quired

Nombre de evento	Propósito del evento	Aplicabilidad al evento de inicio de sesión	Valores de ejemplo
`LoginTo`	Se utiliza para especificar la ubicación de redirecci onamiento tras una secuencia de inicio de sesión correcta.	`UserAuthe ntication`	LoginTo«:" https://m ydirectory.awsapps .com/start/...»

Ejemplos de eventos para escenarios de inicio de sesión en IAM Identity Center

Los siguientes ejemplos muestran la secuencia de CloudTrail eventos esperada para diferentes escenarios de inicio de sesión.

Temas

- Inicio de sesión exitoso al autenticarse solo con contraseña
- Inicio de sesión correcto al autenticarse con un proveedor de identidad externo
- Inicio de sesión correcto al autenticarse con una contraseña y una aplicación de autenticación TOTP
- Inicio de sesión exitoso al autenticarse con una contraseña y se requiere un registro MFA forzado
- Inicio de sesión fallido al autenticarse solo con una contraseña

Inicio de sesión exitoso al autenticarse solo con contraseña

La siguiente secuencia de eventos muestra un ejemplo de un inicio de sesión exitoso solo con contraseña.

CredentialChallenge (Contraseña)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
```

```
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Exitoso CredentialVerification (contraseña)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
```

```
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

UserAuthentication Correcto (solo contraseña)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
```

```
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Inicio de sesión correcto al autenticarse con un proveedor de identidad externo

La siguiente secuencia de eventos muestra un ejemplo de un inicio de sesión correcto cuando se autentica mediante el protocolo SAML con un proveedor de identidad externo.

UserAuthentication Correcto (proveedor de identidad externo)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":""
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
```

```
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Inicio de sesión correcto al autenticarse con una contraseña y una aplicación de autenticación TOTP

La siguiente secuencia de eventos captura un ejemplo en el que se requería una autenticación multifactorial durante el inicio de sesión y el usuario inició sesión correctamente con una contraseña y una aplicación de autenticación TOTP.

CredentialChallenge (Contraseña)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
```

```
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Exitoso CredentialVerification (contraseña)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
```

```
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

CredentialChallenge (TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
```

```
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Exitoso CredentialVerification (TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
```

```
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

Exitoso UserAuthentication (contraseña + TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
```

```
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

Inicio de sesión exitoso al autenticarse con una contraseña y se requiere un registro MFA forzado

La siguiente secuencia de eventos captura un ejemplo de un inicio de sesión con contraseña correcto, pero el usuario tenía que registrar correctamente un dispositivo MFA antes de completar su inicio de sesión.

CredentialChallenge (Contraseña)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
```

```
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Exitoso CredentialVerification (contraseña)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

Exitoso UserAuthentication (se requiere contraseña y registro en MFA)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
   },
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
```

```
}
```

Inicio de sesión fallido al autenticarse solo con una contraseña

La siguiente secuencia de eventos captura un ejemplo de un inicio de sesión fallido con solo contraseña.

CredentialChallenge (Contraseña)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Error CredentialVerification (contraseña)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
   "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Failure"
   }
}
```


Amazon EventBridge

IAM Identity Center puede trabajar con Amazon EventBridge para generar eventos cuando se producen acciones especificadas por el administrador en una organización. Por ejemplo, por la sensibilidad de ese tipo de acciones, la mayoría de los administradores desean que se les

advierta cada vez que alguien crea una nueva cuenta en la organización o que un administrador de una cuenta miembro intenta salir de la organización. Puede configurar EventBridge reglas que busquen estas acciones y, a continuación, envíen los eventos generados a objetivos definidos por el administrador. El objetivo puede ser un tema de Amazon SNS que envíe un correo electrónico o un mensaje de texto a sus suscriptores. También puede crear una AWS Lambda función que registre los detalles de la acción para su posterior revisión.

Para obtener más información EventBridge, incluido cómo configurarlo y habilitarlo, consulta la Guía del EventBridge usuario de Amazon.

Registro de errores de sincronización de AD y de sincronización de AD configurables

Puedes activar el registro en tu sincronización de Active Directory (AD) y en las configuraciones configurables de sincronización de AD para recibir registros con información sobre los errores que pueden producirse durante el proceso de sincronización. Con estos registros, puedes supervisar si hay algún problema con la sincronización de AD y la sincronización de AD configurable y tomar las medidas necesarias. Puede enviar sus registros a un grupo de registros de Amazon CloudWatch Logs, a un depósito de Amazon Simple Storage Service (Amazon S3) o a un Amazon Data Firehose, y se admite la entrega entre cuentas para los depósitos de Amazon S3 y Firehose.

Para obtener más información sobre las limitaciones, los permisos y los registros vendidos, consulte Habilitar el registro desde. Servicios de AWS

> **Note**
>
> Se le cobrará por el registro. Para obtener más información, consulta Vended Logs en la página de CloudWatch precios de Amazon.

Para habilitar la sincronización de AD y los registros de errores de sincronización de AD configurables

1. Inicie sesión en la consola del IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, elija Administrar registros.
4. Selecciona Añadir entrega de registros y uno de los siguientes tipos de destino.

a. Elige Amazon CloudWatch Logs. A continuación, elija o introduzca el grupo de registros de destino.
b. Elija Amazon S3. A continuación, elija o introduzca el depósito de destino.
c. Elige Firehose. A continuación, elija o introduzca el flujo de entrega de destino.

5. Seleccione Submit (Enviar).

Para deshabilitar la sincronización de AD y los registros de errores de sincronización de AD configurables

1. Inicie sesión en la consola del IAM Identity Center.
2. Elija Configuración.
3. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, elija Administrar registros.
4. Selecciona Eliminar para el destino que deseas eliminar.
5. Seleccione Submit (Enviar).

Campos de registro de errores de sincronización de AD y sincronización de AD configurables

Consulta la siguiente lista para ver los posibles campos del registro de errores.

`sync_profile_name`

El nombre del perfil de sincronización.

`error_code`

El código de error que representa el tipo de error que se ha producido.

`error_message`

Un mensaje que contiene información detallada sobre el error que se ha producido.

`sync_source`

La fuente de sincronización es el lugar desde el que se sincronizan las entidades. En el caso del IAM Identity Center, se trata de un Active Directory (AD) gestionado por. AWS Directory Service La fuente de sincronización contiene el dominio y el ARN del directorio afectado.

`sync_target`

El destino de sincronización es el destino en el que se guardan las entidades. En el caso del IAM Identity Center, se trata de un almacén de identidades. El destino de sincronización contiene el ARN del almacén de identidades afectado.

`source_entity_id`

Un identificador único de la entidad que está causando el error. En el caso del IAM Identity Center, este es el SID de la entidad.

`source_entity_type`

El tipo de entidad que provoca el error. El valor puede ser `USER` o `GROUP`.

`eventTimestamp`

La marca de tiempo en que se produjo el error.

Ejemplos de registros de errores de sincronización de AD y sincronización de AD configurable

Ejemplo 1: registro de errores de una contraseña caducada de un directorio de AD

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "InvalidDirectoryCredentials",
        "error_message": "The password for your AD directory has expired. Please reset
 the password to allow Identity Sync to access the directory."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
}
```

Ejemplo 2: Un registro de errores para un usuario con un nombre de usuario que no es único

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
```

```
        "error_code": "ConflictError",
        "error_message": "The source entity has a username conflict with the sync
 target. Please verify that the source identity has a unique username in the target."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "sync_target": {
        "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
    },
    "source_entity_id": "SID-1234",
    "source_entity_type": "USER",
    "eventTimestamp": "1683355579981"
}
```

Validación de la conformidad en IAM Identity Center

Los auditores externos evalúan la seguridad y el cumplimiento de Servicios de AWS dichos programas, por ejemplo AWS IAM Identity Center , como parte de varios programas de AWS cumplimiento.

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

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

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Estándares de conformidad admitidos

IAM Identity Center ha sido sometido a auditorías para los siguientes estándares y puede utilizarse en soluciones para las que se exija certificación de conformidad.

AWS ha ampliado su programa de cumplimiento de la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) para incluir el Centro de Identidad de IAM como un servicio que cumple con los requisitos de la HIPAA.

AWS ofrece un documento técnico centrado en la HIPAA para los clientes que desean obtener más información sobre cómo procesar y almacenar la información de salud. Servicios de AWS Para obtener más información, consulte Conformidad con HIPAA.

El Programa de Asesores Registrados de Seguridad de la Información (IRAP) permite a los clientes del Gobierno australiano garantizar que existen controles apropiados, así como determinar el modelo de responsabilidad adecuado para abordar los requisitos del Manual de Seguridad de la Información (ISM) del Gobierno australiano, elaborado por el Centro Australiano de Ciberseguridad (ACSC). Para obtener más información, consulte Recursos de IRAP.

IAM Identity Center dispone de una declaración de conformidad para el estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS) versión 3.2 de nivel de proveedor de servicios 1.

Los clientes que utilizan AWS productos y servicios para almacenar, procesar o transmitir datos de titulares de tarjetas pueden utilizar las siguientes fuentes de identidad en el Centro de Identidad de IAM para gestionar su propia certificación de conformidad con la PCI DSS:

- Active Directory
- Proveedor de identidades externo

	La fuente de identidad de IAM Identity Center actualmente no cumple con el estándar PCI DSS. Para obtener más información sobre PCI DSS, incluida la forma de solicitar una copia del PCI AWS Compliance Package, consulte PCI DSS nivel 1.
	Los informes de control de organizaciones y sistemas (SOC) son informes de análisis independientes de terceros que muestran cómo IAM Identity Center cumple los controles y objetivos clave de conformidad. Estos informes ayudan tanto a sus auditores como a usted a comprender cómo los controles respaldan las operaciones y la conformidad. Existen 3 tipos de informes de SOC: • AWS Informe SOC 1: Descargar con Artifact AWS • AWS SOC 2: Informe de seguridad, disponibilidad y confidencialidad: descarga con Artifact AWS • AWS SOC 3: Informe de seguridad, disponibilidad y confidencialidad El IAM Identity Center está dentro del ámbito de aplicació n de los AWS informes SOC 1, SOC 2 y SOC 3. Para obtener más información, consulte Conformidad con SOC.

Resiliencia en IAM Identity Center

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

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte la infraestructura global.AWS

Para obtener más información sobre AWS IAM Identity Center la resiliencia, consulteDiseño de resiliencia y comportamiento regional.

Seguridad de la infraestructura en IAM Identity Center

Como servicio gestionado, AWS IAM Identity Center está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utilice las llamadas a la API AWS publicadas para acceder al IAM Identity Center a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Etiquetado de recursos de AWS IAM Identity Center

Una etiqueta es una designación de atributo personalizada que añade a un recurso de AWS para facilitar la identificación, la organización y la búsqueda de recursos. Cada etiqueta tiene dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta pueden tener 128 caracteres como máximo y distingue entre mayúsculas y minúsculas.
- Un valor de etiqueta (por ejemplo, `111122223333` o `Production`). Los valores de etiqueta pueden tener una longitud de hasta 256 caracteres y, al igual que las claves de etiqueta, distinguen mayúsculas y minúsculas. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Omitir el valor de etiqueta es lo mismo que utilizar una cadena vacía.

Las etiquetas le ayudan a identificar y organizar los recursos de AWS. Muchos servicios de AWS admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados. Por ejemplo, puede asignar la misma etiqueta a un conjunto de permisos específico en su instancia de IAM Identity Center. Para obtener más información sobre las estrategias de etiquetado, consulte Etiquetado de los recursos de AWS en la GuíaReferencia general de AWS y en Prácticas recomendadas de etiquetado.

Además de identificar, organizar y realizar el seguimiento de sus recursos de AWS con etiquetas, puede utilizar etiquetas en las políticas de IAM para ayudar a controlar quién puede ver e interactuar con los recursos. Para obtener más información sobre el uso de etiquetas para controlar el acceso, consulte Control del acceso a los recursos de AWS mediante etiquetas en la Guía del usuario de IAM. Por ejemplo, puede permitir que un usuario actualice un conjunto de permisos de IAM Identity Center, pero solo si este conjunto tiene una etiqueta de `owner` con un valor del nombre de ese usuario.

Por el momento, solo puede aplicar etiquetas a conjuntos de permisos. No puede aplicar etiquetas a los roles correspondientes que IAM Identity Center crea en Cuentas de AWS. Puede utilizar la consola de IAM Identity Center, AWS CLI o las API del IAM Identity Center para agregar, editar o eliminar las etiquetas de un conjunto de permisos.

En las siguientes secciones se ofrece más información acerca de las etiquetas para IAM Identity Center.

Restricciones de las etiquetas

Las siguientes restricciones básicas se aplican a las etiquetas en recursos de IAM Identity Center:

- El número máximo de etiquetas que puede asignar a un recurso es 50.
- La longitud máxima de la clave es de 128 caracteres Unicode.
- La longitud máxima del valor es de 256 caracteres Unicode.
- Los caracteres válidos para una clave y un valor de etiqueta son:

  a-z, A-Z, 0-9, espacio y los siguientes caracteres: _ . : / = + - y @
- Las claves y los valores distinguen entre mayúsculas y minúsculas.
- No utilice `aws:` como prefijo para claves, ya que está reservado para AWS.

Administre las etiquetas a través de la consola de IAM Identity Center

Puede utilizar la consola de IAM Identity Center para agregar, editar y eliminar etiquetas asociadas a sus conjuntos de instancias o permisos.

Administración de etiquetas de conjuntos de permisos para una consola de IAM Identity Center

1. Abra la consola del IAM Identity Center
2. Elija Conjuntos de permisos.
3. Elija el nombre del conjunto de permisos que tiene las etiquetas que desea administrar.
4. En la pestaña Permisos de la sección Etiquetas, realice una de las siguientes acciones y, a continuación, continúe con el paso siguiente:

   a. Si ya hay etiquetas asignadas a este conjunto de permisos, elija Edite etiquetas.

   b. Si no hay ninguna etiqueta asignada a este conjunto de permisos, elija Agregar etiquetas.
5. Para cada etiqueta nueva, escriba los valores en las columnas Clave y Valor (opcional). Cuando haya finalizado, elija Guardar cambios.

Para eliminar una etiqueta, seleccione la X en la columna Eliminar situada junto a la etiqueta que deseas eliminar.

Administración de etiquetas para una instancia de IAM Identity Center

1. Abra la Consola de IAM Identity Center.
2. Elija Configuración.
3. Elija la pestaña Etiquetas.
4. Para cada etiqueta, escriba los valores en los campos Clave y Valor (opcional). Cuando haya terminado, seleccione el botón Agregar nueva etiqueta.

Para eliminar una etiqueta, seleccione el botón Eliminar junto a la etiqueta que desee eliminar.

Ejemplos de Lambda

La AWS CLI proporciona comandos que puede utilizar para administrar las etiquetas que asigna a su conjunto de permisos.

Asignación de etiquetas

Utilice los siguientes comandos para asignar etiquetas a su conjunto de permisos.

Example Comando **`tag-resource`** para un conjunto de permisos

Asigne etiquetas a un conjunto de permisos mediante el uso de `tag-resource` en el conjunto de comandos de `sso`:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

Este comando incluye los siguientes parámetros:

- `instance-arn`: el nombre de recurso de Amazon (ARN) de la instancia de IAM Identity Center en la que se ejecutará la operación.
- `resource-arn`: el ARN del recurso con las etiquetas que se van a enumerar.
- `tags`: los pares de clave-valor de las etiquetas.

Para asignar varias etiquetas a la vez, especifíquelas en una lista separada por comas:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Visualización de etiquetas

Utilice los siguientes comandos para visualizar las etiquetas que ha asignado a su conjunto de permisos.

Example Comando **`list-tags-for-resource`** para un conjunto de permisos

Visualice las etiquetas que están asignadas a un conjunto de permisos mediante el uso de `list-tags-for-resource` en el conjunto de comandos de `sso`:

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

Eliminación de etiquetas

Utilice los siguientes comandos para eliminar etiquetas de un conjunto de permisos.

Example Comando **`untag-resource`** para un conjunto de permisos

Elimine etiquetas de un conjunto de permisos mediante el uso de `untag-resource` en el conjunto de comandos de `sso`:

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

Para el parámetro `--tag-keys`, especifique una o más claves de etiquetas y no incluya los valores de etiqueta.

Cómo aplicar etiquetas al crear un conjunto de permisos

Utilice los siguientes comandos para asignar etiquetas al crear un conjunto de permisos.

Example Comando **`create-permission-set`** con etiquetas

Cuando se crea un conjunto de permisos a través del comando `create-permission-set`, es posible especificar etiquetas con el parámetro `--tags`:

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Administre etiquetas mediante el uso de la API de IAM Identity Center

Puede utilizar las siguientes acciones de la API de IAM Identity Center para administrar las etiquetas de su conjunto de identidades.

Acciones de la API para etiquetas de instancia de IAM Identity Center

Utilice las siguientes acciones de la API para asignar, ver y eliminar etiquetas para un conjunto de permisos o instancia de IAM Identity Center.

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

Integración de CLI de AWS con IAM Identity Center

La integración de la versión 2 de la interfaz de la línea de comandos (CLI) AWS con IAM Identity Center simplifica el proceso de inicio de sesión. Los desarrolladores pueden iniciar sesión directamente en el AWS CLI con las mismas credenciales de Active Directory o IAM Identity Center que utilizan normalmente para iniciar sesión en el IAM Identity Center y acceder a las cuentas y funciones que se les asignen. Por ejemplo, después de que un administrador configure IAM Identity Center con el fin de que use Active Directory para la autenticación, el desarrollador puede iniciar sesión en el AWS CLI directamente con sus credenciales de Active Directory.

La integración de CLI de AWS con IAM Identity Center ofrece las siguientes ventajas:

- Las empresas pueden permitir que sus desarrolladores inicien sesión con las credenciales del IAM Identity Center o Active Directory conectando el IAM Identity Center a su Active Directory mediante AWS Directory Service.
- Los desarrolladores pueden iniciar sesión desde la CLI para un acceso más rápido.
- Los desarrolladores pueden enumerar las cuentas y los roles a los que tienen acceso asignado y cambiar de una cuenta a otra.
- Los desarrolladores pueden generar y guardar automáticamente perfiles de rol con nombre en su configuración de CLI y hacer referencia a ellos en la CLI para ejecutar comandos en las cuentas y roles deseados.
- La CLI administra automáticamente las credenciales a corto plazo para que los desarrolladores puedan iniciar y permanecer en la CLI de forma segura y sin interrupciones, y ejecutar scripts de larga duración.

Cómo integrar la CLI de AWS con IAM Identity Center

Para utilizar la integración de la CLI de AWS con IAM Identity Center, debe descargar, instalar y configurar la versión 2 de AWS Command Line Interface. Para ver los pasos detallados sobre cómo descargar e integrar el AWS CLI con IAM Identity Center, consulte Configurar la CLI de AWS para usar IAM Identity Center en la AWS Command Line InterfaceGuía del usuario.

AWS IAM Identity Center Disponibilidad regional

El IAM Identity Center está disponible en varios de los más utilizados Regiones de AWS. Esta disponibilidad facilita la configuración del acceso de los usuarios a múltiples aplicaciones Cuentas de AWS y aplicaciones empresariales. Cuando los usuarios inician sesión en el portal de AWS acceso, pueden seleccionar aquello Cuenta de AWS para lo que tienen permisos y, a continuación, acceder al AWS Management Console. Para obtener una lista completa de los dispositivos compatibles con el Regiones de AWS Centro de Identidad de IAM, consulte los puntos finales y las cuotas del Centro de Identidad de IAM.

Datos regionales de IAM Identity Center

Al habilitar IAM Identity Center por primera vez, todos los datos que configure en él se almacenarán en la región en la que los configuró. Estos datos incluyen configuraciones de directorios, conjuntos de permisos, instancias de aplicaciones y asignaciones de usuarios a las aplicaciones. Cuenta de AWS Si utiliza el almacén de identidades de IAM Identity Center, todos los usuarios y grupos que cree en IAM Identity Center también se almacenan en la misma región. Le recomendamos que instale IAM Identity Center en una región que desee mantener disponible para los usuarios, no en una región que pueda tener que deshabilitar.

AWS Organizations solo admite uno Región de AWS a la vez. Si desea que el Centro de identidades de IAM esté disponible en una región diferente, primero debe eliminar la configuración actual del Centro de identidades de IAM. Al cambiar a una región diferente, también se cambia la URL del portal de AWS acceso, por lo que debe volver a configurar todos los conjuntos de permisos y las asignaciones.

Llamadas entre regiones

IAM Identity Center utiliza Amazon Simple Email Service (Amazon SES) para enviar correos electrónicos a los usuarios finales cuando estos intentan iniciar sesión con una contraseña de un solo uso (OTP) como segundo factor de autenticación. Estos correos electrónicos también se envían para determinados eventos de administración de identidades y credenciales, como cuando se invita al usuario a configurar una contraseña inicial, verificar una dirección de correo electrónico y restablecer la contraseña. Amazon SES está disponible en un subconjunto de los Regiones de AWS que admite IAM Identity Center.

IAM Identity Center llama a los puntos de conexión locales de Amazon SES cuando Amazon SES está disponible localmente en una Región de AWS. Cuando Amazon SES no está disponible

localmente, IAM Identity Center llama a los puntos de conexión de Amazon SES que se encuentren en una Región de AWS diferente, como se indica en la siguiente tabla.

Los códigos de región de Amazon SES se enumeran en la tabla siguiente.

Código de región de IAM Identity Center	Nombre de región de IAM Identity Center	Código de región de Amazon SES	Nombre de región de Amazon SES
us-gov-east-1	AWS GovCloud (Este de EE. UU.)	us-gov-west-1	AWS GovCloud (Estados Unidos-Oeste)
ap-east-1	Asia-Pacífico (Hong Kong)	ap-northeast-2	Asia-Pacífico (Seúl)
ap-southeast-4	Asia-Pacífico (Melbourne)	ap-southeast-2	Asia-Pacífico (Sídney)
ap-south-2	Asia-Pacífico (Hyderabad)	ap-south-1	Asia-Pacífico (Bombay)
eu-central-2	Europa (Zúrich)	eu-central-1	Europa (Fráncfort)
eu-south-2	Europa (España)	eu-west-3	Europa (París)
me-central-1	Medio Oriente (EAU)	eu-central-1	Europa (Fráncfort)

En estas llamadas entre regiones, IAM Identity Center puede enviar los siguientes atributos de usuario:

- Dirección de correo electrónico
- Nombre
- Apellido
- Cuenta en AWS Organizations
- AWS URL del portal de acceso
- Nombre de usuario
- ID de directorio

- ID de usuario

Administrar el centro de identidad de IAM en una región opcional (región que está deshabilitada de forma predeterminada)

La mayoría Regiones de AWS están habilitadas para operar en todos los AWS servicios de forma predeterminada. Estas regiones se activan automáticamente para su uso con IAM Identity Center. Las siguientes Regiones de AWS son regiones opcionales y debe habilitarlas:

- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Hyderabad)
- Europa (Milán)
- Europa (Zúrich)
- Europa (España)
- Israel (Tel Aviv)
- Medio Oriente (Baréin)
- Medio Oriente (EAU)

Al habilitar el Centro de Identidad de IAM para una cuenta de administración mediante una suscripción voluntaria Región de AWS, los siguientes metadatos del Centro de Identidad de IAM para cualquier cuenta de miembro se almacenan en la región.

- ID de cuenta
- Nombre de cuenta
- Correo electrónico de la cuenta
- Nombres de recurso de Amazon (ARN) de los roles de IAM que IAM Identity Center crea en la cuenta miembro

Si deshabilita una región en la que IAM Identity Center está instalado, este también se deshabilitará. Una vez que el Centro de identidad de IAM esté desactivado en una región, los usuarios de esa

región no tendrán acceso mediante un inicio de sesión único a las aplicaciones. Cuentas de AWS AWS conserva los datos de la configuración del centro de identidad de IAM durante al menos 10 días. Si vuelve a activar IAM Identity Center dentro de este plazo, sus datos de configuración anteriores seguirán estando disponibles en la región.

Para volver a activar el Centro de Identidad de IAM de forma opcional Regiones de AWS, debe volver a activar la región. IAM Identity Center debe volver a procesar todos los eventos pausados, por lo que volver a habilitarlo puede llevar algún tiempo.

> **Note**
>
> El Centro de Identidad de IAM solo puede gestionar el acceso a aquellos Cuentas de AWS que estén habilitados para su uso en un. Región de AWS Para gestionar el acceso a todas las cuentas de su organización, active el Centro de identidad de IAM en la cuenta de gestión de forma Región de AWS que se active automáticamente para su uso con el Centro de identidades de IAM.

Para obtener más información sobre la activación y la desactivación Regiones de AWS, consulte Gestión Regiones de AWS en la AWS referencia general.

Eliminación de la configuración de IAM Identity Center

Cuando se elimina una configuración de IAM Identity Center, se eliminan todos los datos de esa configuración y no se pueden recuperar. En la siguiente tabla se describen los datos que se eliminan en función del tipo de directorio que está configurado actualmente en IAM Identity Center.

¿Qué datos se eliminan?	Directorio conectado (AWS Managed Microsoft AD o conector AD)	Almacén de identidades de IAM Identity Center
Todos los conjuntos de permisos para los que ha configurado Cuentas de AWS	✓	✓

¿Qué datos se eliminan?	Directorio conectado (AWS Managed Microsoft AD o conector AD)	Almacén de identidades de IAM Identity Center
Todas las aplicaciones que ha configurado en IAM Identity Center	✓	✓
Todas las asignaciones de usuarios Cuentas de AWS y aplicaciones que haya configurado	✓	✓
Todos los usuarios y grupos del directorio o almacén	N/D	✓

Siga el siguiente procedimiento cuando necesite eliminar la configuración actual de IAM Identity Center.

Cómo eliminar la configuración de IAM Identity Center

1. Abra la consola de IAM Identity Center.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página Configuración, seleccione la pestaña Administración.
4. En la sección Eliminar la configuración de IAM Identity Center, seleccione Eliminar.
5. En el cuadro de diálogo Eliminar la configuración de IAM Identity Center, marque todas las casillas de verificación para confirmar que entiende que los datos se van a eliminar. Escriba su instancia de IAM Identity Center en el cuadro de texto y, a continuación, seleccione Confirmar.

AWS IAM Identity Center cuotas

En las siguientes tablas se describen las cuotas de IAM Identity Center. Las solicitudes de aumento de cuota deben provenir de una cuenta de administración o de administrador delegado. Para solicitar un aumento de cuota, consulte Solicitar un aumento de cuota.

> **Note**
>
> Recomendamos usar la AWS CLI y las API si tiene más de 50 000 usuarios, 10 000 grupos o 500 conjuntos de permisos. Para obtener más información acerca de la CLI, consulte Integración de CLI de AWS con IAM Identity Center. Para obtener más información sobre API, consulte Welcome to the IAM Identity Center API Reference.

Cuotas de aplicaciones

Recurso	Cuota predeterminada	Se puede aumentar
Tamaño del archivo de los certificados SAML de proveedores de servicios (en formato PEM)	2 KB	No
Límite de aserciones de SAML	50 000 caracteres	No
Límite de tamaño de archivo del certificado de IdP cargado en el Centro de Identidad de IAM	2500 caracteres (UTF-8)	No
Ámbitos de acceso por aplicación	25	No

Cuenta de AWS cuotas

Recurso	Cuota predeterminada	Se puede aumentar
Número de conjuntos de permisos permitidos en IAM Identity Center	2000	Sí
Número de conjuntos de permisos aprovisionados permitidos por Cuenta de AWS	250	Sí
Número de políticas insertadas por conjunto de permisos	1	No
Número de políticas AWS administradas y administradas por el cliente por conjunto de permisos	20 [1]	No
Tamaño máximo de la política insertada por conjunto de permisos	32 768 bytes. El tamaño máximo de los caracteres que no son espacios en blanco en la política insertada por conjunto de permisos es de 10 240 bytes.	No
Número de funciones de IAM (conjuntos de permisos) Cuenta de AWS que se pueden actualizar a la vez	1	No

[1]AWS Identity and Access Management (IAM) establece una cuota de 10 políticas gestionadas por función. Para aprovechar esta cuota, solicite un aumento de la cuota de IAM en las políticas

gestionadas asociadas a una función de IAM en la consola de Service Quotas para cada uno de los Cuenta de AWS lugares en los que desee implementar el conjunto de permisos.

> **Note**
>
> Conjuntos de permisosse aprovisionan Cuentas de AWS como funciones de IAM o utilizan las funciones de IAM existentes y, por lo tanto Cuentas de AWS, respetan las cuotas de IAM. Para obtener más información sobre las cuotas asociadas a los roles de IAM, consulte Cuotas de IAM y STS.

Cuotas de Active Directory

Recurso	Cuota predeterminada	Se puede aumentar
Número de directorios conectados que se puede tener de forma simultánea	1	No

Cuotas de almacén de identidades de IAM Identity Center

Recurso	Cuota predeterminada	Se puede aumentar
Número de usuarios admitidos en IAM Identity Center	100000	Sí
Número de grupos admitidos en IAM Identity Center	100000	No
Número de grupos únicos que se pueden utilizar para evaluar los permisos de un usuario	1 000	No

Límites de solicitudes de IAM Identity Center

Recurso	Cuota predeterminada
API de IAM Identity Center	Las API de IAM Identity Center tienen un máximo de solicitudes colectivas de 20 transacciones por segundo (TPS). CreateAccountAssignmentTiene una tasa máxima de 10 llamadas asíncronas pendientes. Estas cuotas no pueden cambiarse.

Cuotas adicionales

Recurso	Cuota predeterminada	Se puede aumentar
Número total de Cuentas de AWS aplicaciones que se pueden configurar*	3 000	Sí
Total de instancias de IAM Identity Center por cuenta	1	No
Total de emisores de tokens de confianza	10	No

* Se admiten hasta 3000 Cuentas de AWS aplicaciones (en total combinadas). Por ejemplo, puede configurar 2750 cuentas y 250 aplicaciones, lo que da como resultado un total de 3000 cuentas y aplicaciones.

Resolución de problemas de IAM Identity Center

La siguiente información puede ayudarle a solucionar algunos problemas comunes que puede encontrarse a la hora de configurar o utilizar la consola de IAM Identity Center.

Problemas al crear una instancia de cuenta de IAM Identity Center

Es posible que se apliquen varias restricciones al crear una instancia de cuenta de IAM Identity Center. Si no puede crear una instancia de cuenta a través de la consola del IAM Identity Center o de la experiencia de configuración de una aplicación AWS gestionada compatible, compruebe los siguientes casos de uso:

- Marque otras Regiones de AWS Cuenta de AWS en las que esté intentando crear la instancia de cuenta. Tiene un límite de una instancia de IAM Identity Center por Cuenta de AWS. Para habilitar la aplicación, cambie a la Región de AWS instancia de IAM Identity Center o cambie a una cuenta sin una instancia de IAM Identity Center.
- Si su organización habilitó el Centro de identidad de IAM antes del 14 de septiembre de 2023, es posible que su administrador deba optar por la creación de instancias de cuenta. Trabaje con el administrador para habilitar la creación de instancias de cuenta desde la consola de IAM Identity Center en la cuenta de administración.
- Es posible que el administrador haya creado una política de control de servicio para limitar la creación de instancias de cuenta de IAM Identity Center. Trabaje con el administrador para agregar su cuenta a la lista de permitidos.

Recibe un error al intentar ver la lista de aplicaciones en la nube que están preconfiguradas para funcionar con IAM Identity Center

El siguiente error se produce cuando tiene una política que permite `sso:ListApplications`, pero no otras API de IAM Identity Center. Actualice la política para resolver este error.

El permiso `ListApplications` autoriza varias API:

- La API `ListApplications`.
- Una API interna similar a la API `ListApplicationProviders` utilizada en la consola de IAM Identity Center.

Para ayudar a resolver la duplicación, la API interna ahora también autoriza el uso de la acción `ListApplicationProviders`. Para permitir la API pública `ListApplications`, pero denegar la API interna, la política debe incluir una instrucción que deniegue la acción `ListApplicationProviders`:

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

Para permitir la API interna, pero denegar `ListApplications`, la política tiene que permitir solo `ListApplicationProviders`. La API `ListApplications` se deniega si no se permite explícitamente.

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    }
]
```

Cuando se actualicen sus políticas, póngase en contacto con nosotros AWS Support para que eliminen esta medida proactiva.

Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center

El Centro de Identidad de IAM ofrece una experiencia de depuración basada en la web para las afirmaciones de SAML creadas y enviadas por el Centro de Identidad de IAM, incluidos los atributos de estas afirmaciones, al acceder a Cuentas de AWS las aplicaciones de SAML desde el portal de acceso. AWS Para visualizar los detalles de una confirmación de SAML que genera IAM Identity Center, siga estos pasos:

1. Inicie sesión en el portal de acceso. AWS
2. Mientras está conectado al portal, mantenga pulsada la tecla Mayúscula, elija el mosaico de aplicaciones y suelte la tecla Mayúscula.
3. Revise la información de la página titulada You are now in administrator mode (Ahora está en modo administrador). Para conservar esta información y poder consultarla en el futuro, elija Copy XML (Copiar XML) y pegue el contenido en otro lugar.
4. Seleccione Enviar a <application> para continuar. Esta opción envía la confirmación al proveedor del servicio.

> **Note**
>
> Es posible que algunas configuraciones de navegadores y sistemas operativos no admitan este procedimiento. Este procedimiento se ha probado en Windows 10 con los navegadores Firefox, Chrome y Edge.

Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo

Si la sincronización SCIM se realiza correctamente para un subconjunto de usuarios configurados en su proveedor de identidades para el aprovisionamiento en IAM Identity Center, pero falla para otros, es posible que su proveedor de identidades muestre un error similar a `'Request is unparsable, syntactically incorrect, or violates schema'`. También puede ver mensajes detallados sobre los errores de aprovisionamiento en AWS CloudTrail.

Este problema suele indicar que el usuario de su IdP está configurado de un modo que IAM Identity Center no admite. Encontrará toda la información sobre la implementación del SCIM de IAM Identity Center, incluidas las especificaciones de los parámetros y operaciones obligatorios, opcionales y prohibidos para los objetos de usuario, en la Guía para desarrolladores de la implementación del SCIM de IAM Identity Center. La Guía para desarrolladores del SCIM se debe considerar como fidedigna para obtener información sobre los requisitos del SCIM. Sin embargo, los siguientes motivos son algunos de los más comunes de este error:

1. El objeto de usuario del IdP carece de un nombre (de pila), un apellido o un nombre para mostrar.

   - Solución: agregue un nombre (de pila), un apellido y un nombre para el objeto de usuario. Además, asegúrese de que las asignaciones de aprovisionamiento de SCIM para los objetos de usuario de su IdP estén configuradas para enviar valores no vacíos a todos estos atributos.

2. Se está enviando al usuario más de un valor para un único atributo (también conocidos como “atributos de valores múltiples”). Por ejemplo, el usuario puede tener un número de teléfono fijo y laboral especificado en el IdP, o varios correos electrónicos o direcciones físicas, y su IdP está configurado para intentar sincronizar varios o todos los valores de ese atributo.

   - Opciones de solución:

     i. Actualice las asignaciones de aprovisionamiento de SCIM para los objetos de usuario de su IdP para enviar solo un valor único para un atributo determinado. Por ejemplo, configure una asignación que envíe solo el número de teléfono laboral de cada usuario.

     ii. Si los atributos adicionales se pueden eliminar de forma segura del objeto de usuario del IdP, puede eliminar los valores adicionales y dejar uno o cero valores establecidos para ese atributo del usuario.

     iii. Si el atributo no es necesario para realizar ninguna acción AWS, elimine la asignación de ese atributo de las asignaciones de aprovisionamiento de SCIM para objetos de usuario en su IdP.

3. Su IdP intenta hacer coincidir a los usuarios del objetivo (en este caso, IAM Identity Center) en función de varios atributos. Como se garantiza que los nombres de usuario sean únicos en una instancia determinada de IAM Identity Center, solo tiene que especificar `username` como atributo utilizado para la coincidencia.

- Solución: asegúrese de que la configuración de SCIM de su IdP utilice solo un atributo para coincidir con los usuarios de IAM Identity Center. Por ejemplo, la asignación de `username` o `userPrincipalName` del IdP al atributo `userName` de SCIM para el aprovisionamiento en IAM Identity Center será correcto y suficiente para la mayoría de las implementaciones.

Los usuarios no pueden iniciar sesión cuando su nombre de usuario está en formato UPN

Es posible que los usuarios no puedan iniciar sesión en el portal de AWS acceso en función del formato que utilizan para introducir su nombre de usuario en la página de inicio de sesión. En la mayoría de los casos, los usuarios pueden iniciar sesión en el portal de usuarios con su nombre de usuario normal, su nombre de inicio de sesión de nivel inferior (DOMAIN\UserName) o su nombre de inicio de sesión UPN (). `UserName@Corp.Example.com` La excepción a esto se produce cuando IAM Identity Center utiliza un directorio conectado que se ha habilitado con MFA y el modo de verificación se ha establecido en Context-aware o en Always-on. En este escenario, los usuarios deben iniciar sesión con su nombre de inicio de sesión de nivel inferior (DOMAIN\). UserName Para obtener más información, consulte Autenticación multifactor para usuarios de Identity Center. Para obtener información general sobre los formatos de nombre de usuario que se utilizan para iniciar sesión en Active Directory, consulte Formatos de nombre de usuario en el sitio web de documentación de Microsoft.

Al modificar un rol de IAM, aparece el error: “No se puede realizar la operación en el rol protegido”.

Al revisar las funciones de IAM en una cuenta, es posible que veas que los nombres de las funciones comienzan por «_». AWSReservedSSO Se trata de los roles que el servicio de IAM Identity Center ha creado en la cuenta y provienen de la asignación de un conjunto de permisos a la cuenta. Si se intenta modificar estos roles desde la consola de IAM, se producirá el siguiente error:

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

Estas funciones solo se pueden modificar desde la consola de administración de IAM Identity Center, que se encuentra en la cuenta de administración de. AWS Organizations Una vez modificado, puede transferir los cambios a las cuentas de AWS a las que esté asignado.

Los usuarios del directorio no pueden restablecer su contraseña

Cuando un usuario del directorio restablece su contraseña mediante la opción ¿Ha olvidado su contraseña? al iniciar sesión en el portal de AWS acceso, su nueva contraseña debe cumplir con la política de contraseñas predeterminada, tal como se describe en. Requisitos de contraseñas para administrar identidades en IAM Identity Center

Si un usuario introduce una contraseña que cumple con la política y, a continuación, recibe el error`We couldn't update your password`, compruebe si AWS CloudTrail se ha registrado el error. Para ello, busque en la consola del historial de eventos o CloudTrail utilice el siguiente filtro:

```
"UpdatePassword"
```

Si el mensaje indica lo siguiente, es posible que deba ponerse en contacto con el servicio de asistencia:

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

Otra posible causa de este problema está en la convención de nomenclatura que se aplicó al valor del nombre de usuario. Las convenciones de nomenclatura deben seguir patrones específicos, como “surname.givenName”. Sin embargo, algunos nombres de usuario pueden ser bastante largos o contener caracteres especiales, lo que puede provocar que se eliminen caracteres en la llamada a la API y, por lo tanto, se produzca un error. Puede intentar restablecer la contraseña con un usuario de prueba de la misma manera para comprobar si es así.

Si el problema persiste, póngase en contacto con el centro de soporte de AWS.

En un conjunto de permisos se hace referencia a mi usuario, pero no puede acceder a las cuentas o aplicaciones asignadas

Este problema se puede producir si utilizas el Sistema de administración de identidades entre dominios (SCIM) para el aprovisionamiento automático con un proveedor de identidad externo. En concreto, cuando se elimina un usuario o el grupo al que pertenecía el usuario y se vuelve a crear con el mismo nombre de usuario (para los usuarios) o nombre (para los grupos) en el proveedor de identidad, se crea un nuevo identificador interno único para el nuevo usuario o grupo en IAM Identity Center. Sin embargo, IAM Identity Center aún conserva una referencia al identificador anterior en

su base de datos de permisos, de modo que el nombre del usuario o grupo sigue apareciendo en la interfaz de usuario, pero se produce un error en el acceso. Esto se debe a que el ID de usuario o grupo subyacente al que hace referencia la interfaz de usuario ya no existe.

Para restablecer el Cuenta de AWS acceso en este caso, puede eliminar el acceso del usuario o grupo anterior de los Cuenta de AWS lugares a los que estaba asignado originalmente y, a continuación, volver a asignar el acceso al usuario o grupo. Esto actualiza el conjunto de permisos con el identificador correcto para el nuevo usuario o grupo. Del mismo modo, para restablecer el acceso a la aplicación, puede eliminar el acceso del usuario o grupo de la lista de usuarios asignados a esa aplicación y, a continuación, volver a agregar el usuario o grupo.

También puede comprobar si se AWS CloudTrail ha registrado el error buscando en los CloudTrail registros los eventos de sincronización de SCIM que hagan referencia al nombre del usuario o grupo en cuestión.

No puedo configurar correctamente mi aplicación del catálogo de aplicaciones

Si ha agregado una aplicación del catálogo de aplicaciones en IAM Identity Center, tenga en cuenta que cada proveedor de servicios proporciona su propia documentación detallada. Puede acceder a esta información desde la pestaña Configuración de la aplicación en la consola de IAM Identity Center.

Si el problema está relacionado con la configuración de la confianza entre la aplicación del proveedor de servicios y IAM Identity Center, consulte el manual de instrucciones para conocer los pasos a seguir para la resolución de problemas.

Error: “Se ha producido un error inesperado” cuando un usuario intenta iniciar sesión con un proveedor de identidad externo

Este error puede producirse por varios motivos, pero uno de los más comunes es la falta de coincidencia entre la información del usuario incluida en la solicitud de SAML y la información del usuario en IAM Identity Center.

Para que un usuario de IAM Identity Center inicie sesión correctamente al utilizar un IdP externo como fuente de identidad, debe cumplirse lo siguiente:

- El formato de nameID de SAML (configurado en su proveedor de identidad) debe ser “correo electrónico”
- El valor de nameID debe ser una cadena con (RFC2822) el formato correcto (usuario@dominio.com)
- El valor del nameID debe coincidir exactamente con el nombre de usuario de un usuario existente en IAM Identity Center (no importa si la dirección de correo electrónico en IAM Identity Center coincide o no; la coincidencia entrante se basa en el nombre de usuario)
- La implementación de la federación SAML 2.0 en IAM Identity Center solo admite una confirmación en la respuesta de SAML entre el proveedor de identidades y IAM Identity Center. No admite las confirmaciones de SAML cifradas.
- Si los Atributos para controlar el acceso están habilitados en su cuenta de IAM Identity Center, se aplican las siguientes confirmaciones:
  - El número de atributos asignados en la solicitud de SAML debe ser 50 o inferior.
  - La solicitud de SAML no debe contener atributos con varios valores.
  - La solicitud de SAML no debe contener varios atributos con el mismo nombre.
  - El atributo no debe contener XML estructurado como valor.
  - El formato del nombre debe ser un formato especificado por SAML y no un formato genérico.

> **Note**
>
> IAM Identity Center no crea usuarios o grupos “justo a tiempo” para nuevos usuarios o grupos mediante la federación SAML. Esto significa que el usuario debe haber sido creado previamente en IAM Identity Center, ya sea de forma manual o mediante un aprovisionamiento automático, para poder iniciar sesión en IAM Identity Center.

Este error también se puede producir cuando el punto de conexión del Servicio de Consumidor de Aserción (ACS) configurado en su proveedor de identidad no coincide con la URL de ACS proporcionada por su instancia de IAM Identity Center. Asegúrese de que estos 2 valores coincidan exactamente.

Además, puede solucionar aún más los errores de inicio de sesión de un proveedor de identidad externo AWS CloudTrail consultando el nombre del evento P. ExternalId DirectoryLogin

Error: “No se pudieron habilitar los atributos del control de acceso”

Este error se puede producir si el usuario que habilita ABAC no tiene los permisos de `iam:UpdateAssumeRolePolicy` necesarios para habilitar Atributos para controlar el acceso.

El mensaje “El navegador no es compatible” aparece cuando intento registrar un dispositivo para MFA

WebAuthn actualmente es compatible con los navegadores web Google Chrome, Mozilla Firefox, Microsoft Edge y Apple Safari, así como con las plataformas Windows 10 y Android. Algunos componentes de la WebAuthn compatibilidad pueden variar, como la compatibilidad con el autenticador de plataforma en los navegadores macOS e iOS. Si los usuarios intentan registrar WebAuthn dispositivos en un navegador o una plataforma no compatibles, verán determinadas opciones que no son compatibles o recibirán un mensaje de error que indica que no se admiten todos los métodos compatibles. En estos casos, consulte FIDO2: Web Authentication (WebAuthn) para obtener más información sobre la compatibilidad entre navegadores y plataformas. Para obtener más información sobre el Centro de identidades de WebAuthn IAM, consulte. Autenticadores FIDO2

El grupo “Usuarios de dominio” de Active Directory no se sincroniza correctamente con IAM Identity Center

El grupo de usuarios de dominio de Active Directory es el “grupo principal” predeterminado para los objetos de usuario de AD. IAM Identity Center no puede leer los grupos principales de Active Directory ni sus membrecías. Al asignar el acceso a los recursos o aplicaciones de IAM Identity Center, utilice grupos distintos del grupo de usuarios del dominio (u otros grupos asignados como grupos principales) para que la membrecía a los grupos se refleje correctamente en el almacén de identidades de IAM Identity Center.

Error de credenciales de MFA no válidas

Este error se puede producir cuando un usuario intenta iniciar sesión en IAM Identity Center con una cuenta de un proveedor de identidad externo (por ejemplo, Okta o Microsoft Entra ID) antes de que su cuenta esté completamente aprovisionada en IAM Identity Center mediante el protocolo SCIM. Una vez que la cuenta de usuario se aprovisione en IAM Identity Center, este problema debería resolverse. Confirme que la cuenta se haya aprovisionado en IAM Identity Center. Si no es así, compruebe los registros de aprovisionamiento en el proveedor de identidades externo.

El mensaje “Se ha producido un error inesperado” aparece cuando intento registrarme o iniciar sesión con una aplicación de autenticación

Los sistemas de contraseña temporal de un solo uso (TOTP) basados en el tiempo, como los que utiliza IAM Identity Center en combinación con las aplicaciones de autenticación basadas en código, se basan en la sincronización horaria entre el cliente y el servidor. Asegúrese de que el dispositivo en el que está instalada la aplicación de autenticación esté sincronizado correctamente con una fuente horaria fiable o configure manualmente la hora del dispositivo para que coincida con una fuente fiable, como, por ejemplo, NIST (https://www.time.gov/) u otras fuentes equivalentes locales o regionales.

Aparece el mensaje de error «No eres tú, somos nosotros» cuando intento iniciar sesión en el Centro de Identidad de IAM

Este error indica que hay un problema de configuración con su instancia de IAM Identity Center o con el proveedor de identidad externo (IdP) que IAM Identity Center utiliza como fuente de identidad. Le recomendamos que compruebe lo siguiente:

- Verifica la configuración de fecha y hora del dispositivo que utilizas para iniciar sesión. Te recomendamos que configures la fecha y la hora para que se configuren automáticamente. Si no está disponible, le recomendamos que sincronice la fecha y la hora con un servidor de protocolo de hora de red (NTP) conocido.
- Compruebe que el certificado de IdP cargado en el Centro de Identidad de IAM es el mismo que el que proporcionó su IdP. Para comprobar el certificado desde la consola del IAM Identity Center, vaya a Configuración. En la pestaña Origen de identidad, elija Acción y, a continuación, elija Administrar autenticación. Si los certificados del IdP y del Centro de Identidad de IAM no coinciden, importe un certificado nuevo al Centro de Identidad de IAM.
- Asegúrese de que el formato NameID del archivo de metadatos de su proveedor de identidad sea el siguiente:
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- Si utiliza AD Connector de AWS Directory Service como proveedor de identidad, compruebe que las credenciales de la cuenta de servicio son correctas y no han caducado. Consulte Actualizar las credenciales de la cuenta de servicio de AD Connector en AWS Directory Service para obtener más información.

Mis usuarios no reciben correos electrónicos de IAM Identity Center

Todos los correos electrónicos enviados por el servicio de IAM Identity Center procederán de una de estas direcciones: `no-reply@signin.aws` o `no-reply@login.awsapps.com`. El sistema de correo debe estar configurado de modo que acepte los correos de estas direcciones de correo electrónico de los remitentes y no los trate como correo basura o spam.

Error: “No puede eliminar/modificar/quitar/asignar el acceso a los conjuntos de permisos proporcionados en la cuenta de administración”

Este mensaje indica que la Administración delegada función está habilitada y que la operación que intentó anteriormente solo la puede realizar correctamente una persona que tenga permisos de cuenta de administración en ella AWS Organizations. Para resolver este problema, inicie sesión como usuario con estos permisos e intente volver a realizar la tarea o asigne esta tarea a alguien que tenga los permisos correctos. Para obtener más información, consulte Registro de una cuenta miembro.

Error: no se encontró el token de sesión o no es válido

Este error puede producirse cuando un cliente, como un navegador web AWS Toolkit AWS CLI, o intenta utilizar una sesión revocada o invalidada en el servidor. Para corregir este problema, vuelva a la aplicación cliente o al sitio web e inténtelo de nuevo, incluso vuelva a iniciar sesión si se le solicita. A veces, esto puede requerir que también canceles las solicitudes pendientes, como un intento de conexión pendiente AWS Toolkit desde tu IDE.

Historial del documento

En la siguiente tabla se describen las adiciones importantes a la AWS IAM Identity Center documentación. Actualizamos la documentación con frecuencia para dar respuesta a los comentarios que se nos envía.

- Última actualización importante de la documentación: 23 de septiembre de 2022

Cambio	Descripción	Fecha
Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestionada.	17 de mayo de 2024
Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestionada.	30 de abril de 2024
Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSSSOMasterAccountAdministrator` AWS gestionada.	26 de abril de 2024
Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSSSOMemberAccountAdministrator` AWS gestionada.	26 de abril de 2024
Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSSSOReadOnly` AWS gestionada.	26 de abril de 2024

Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestionada.	26 de abril de 2024
Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestionada.	24 de abril de 2024
Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestionada.	19 de abril de 2024
Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestionada.	11 de abril de 2024
Actualizaciones de la política AWS gestionada	Permisos actualizados para la política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestionada.	26 de noviembre de 2023
Nuevo tema de política AWS gestionada	Se han añadido detalles para la política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestionada.	15 de noviembre de 2023

Guía de introducción mejorada sobre el uso de IAM Identity Center	Contenido nuevo agregado para empezar a utilizar IAM Identity Center y crear un usuario administrativo	23 de septiembre de 2022
Usuarios y grupos actualizados en la referencia de la API de Identity Center	Esta actualización incluye referencias a las nuevas API de creación, actualización y eliminación en la Guía de referencia de las API de Identity Center.	31 de agosto de 2022
AWS Se ha cambiado el nombre de Single Sign-On (AWS SSO) a AWS IAM Identity Center	AWS presenta. AWS IAM Identity Center IAM Identity Center amplía las capacidades de AWS Identity and Access Management (IAM) para ayudarle a gestionar de forma centralizada las cuentas y el acceso a las aplicaciones para los usuarios de su plantilla . Las características de IAM Identity Center incluyen la asignación de aplicaciones, los permisos para varias cuentas y un portal de acceso AWS .	26 de julio de 2022
Compatibilidad con límites de permisos y política administrada por el cliente en los conjuntos de permisos	Se agregó contenido para usar políticas AWS administradas y administradas por el cliente AWS Identity and Access Management (IAM) con conjuntos de permisos.	14 de julio de 2022

Support para AWS regiones habilitadas manualmente	Contenido agregado para utilizar IAM Identity Center en regiones habilitadas de forma manual.	15 de junio de 2022
Actualizaciones para las políticas AWS gestionadas	Permisos actualizados para la política `AWSSSOServiceRolePolicy` AWS gestionada.	11 de mayo de 2022
Compatibilidad con la administración delegada	Contenido agregado para la característica de administración delegada.	11 de mayo de 2022
Actualizaciones de las políticas AWS gestionadas	Se actualizaron los permisos para las `AWSSSOMasterAccountAdministrator` políticas `AWSSSOMemberAccountAdministrator` administradas y las políticas `AWSSSOReadOnly` AWS administradas.	28 de abril de 2022
Compatibilidad con la sincronización con AD configurable	Contenido agregado para la característica de sincronización con AD configurable.	14 de abril de 2022
Nuevo tema sobre políticas AWS administradas	Se han añadido detalles para la política `AWSSSOMasterAccountAdministrator` AWS gestionada.	4 de agosto de 2021
Actualizaciones para cuotas	Ajustes en las tablas de cuotas.	21 de diciembre de 2020

Nuevos ejemplos de políticas	Nuevos ejemplos agregados de políticas administradas por el cliente y actualizaciones a la sección de permisos requeridos.	21 de diciembre de 2020
Compatibilidad con el control de acceso basado en atributos (ABAC)	Contenido agregado para la característica ABAC.	24 de noviembre de 2020
Compatibilidad con inscripción forzosa de MFA	Actualizaciones para exigir a los usuarios que inscriban un dispositivo MFA al iniciar sesión.	23 de noviembre de 2020
Support para WebAuthn	Contenido agregado para la nueva característica WebAuthn.	20 de noviembre de 2020
Compatibilidad con Ping Identity	Contenido agregado para integrarlo con productos de Ping Identity en calidad de proveedor de identidad externo compatible.	26 de octubre de 2020
Support para OneLogin	Contenido agregado para integrarlo con OneLogin en calidad de proveedor de identidad externo compatible.	31 de julio de 2020
Compatibilidad con Okta	Contenido agregado para integrarlo con Okta en calidad de proveedor de identidad externo compatible.	28 de mayo de 2020

Compatibilidad con proveedores de identidad externos	Referencias modificadas del directorio a la fuente de identidad y contenido agregado para admitir a los proveedores de identidad externos.	26 de noviembre de 2019
Nueva configuración de MFA	Tema de la verificación en 2 pasos eliminado y nuevo tema de MFA agregado en su lugar.	24 de octubre de 2019
Nueva configuración para agregar la verificación en 2 pasos	Contenido agregado sobre cómo habilitar la verificación en dos pasos para los usuarios.	16 de enero de 2019
Support para la duración de la sesión en AWS las cuentas	Se agregó contenido sobre cómo configurar la duración de la sesión de una AWS cuenta.	30 de octubre de 2018
Nueva opción para usar el directorio de Identity Center	Contenido agregado para elegir un directorio de Identity Center o conectarse a un directorio existente en Active Directory.	17 de octubre de 2018
Compatibilidad con el estado de retransmisión y la duración de la sesión en aplicaciones	Se ha agregado contenido sobre el estado de retransmisión y la duración de la sesión para las aplicaciones.	10 de octubre de 2018

Compatibilidad adicional con las nuevas aplicaciones	Se agregó 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvaInSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, y UserEcho al catálogo de aplicaciones.	3 de agosto de 2018
Compatibilidad con el acceso de cuentas múltiples a cuentas de administración	Contenido agregado sobre cómo delegar a los usuarios el acceso de múltiples cuentas a una cuenta de administración.	9 de julio de 2018
Compatibilidad con las nuevas aplicaciones	Se agregó DocuSign, Keeper Security, y SugarCRM al catálogo de aplicaciones.	16 de marzo de 2018
Obtener credenciales temporales para acceder a la CLI	Se agregó información sobre cómo obtener credenciales temporales para ejecutar AWS CLI comandos.	22 de febrero de 2018
Nueva guía	Esta es la primera versión de la Guía del usuario de IAM Identity Center.	7 de diciembre de 2017

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

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.