IDENTIDAD FEDERADA

La identidad federada es un sistema de confianza entre dos partes para autenticar a los usuarios y transmitir la información necesaria a fin de autorizar el acceso a los recursos.

Los proveedores de identidad (IdP) son responsables de la autenticación de los usuarios.

Los proveedores de servicios (SP), como servicios o aplicaciones, son responsables de controlar el acceso a los recursos. A través de un acuerdo administrativo y configuración, el SP confía en el IdP para autenticar a los usuarios y les concede acceso a los recursos solicitados.

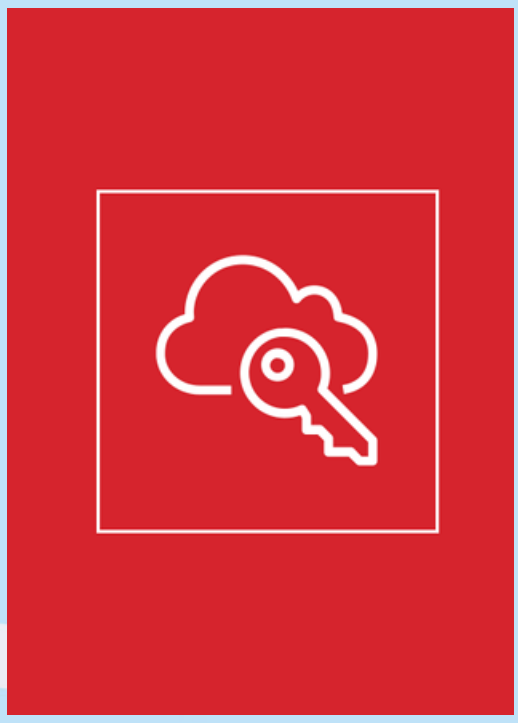
Hay dos servicios de AWS disponibles para proporcionar federación a cuentas y aplicaciones de AWS: AWS Single Sign-On (AWS SSO) e IAM. Si utiliza un único directorio centralizado, AWS SSO es una excelente opción para emplear.

Si utiliza un único directorio centralizado, AWS SSO es una excelente opción para emplear. Si utiliza varios directorios dentro de su organización o si desea utilizar permisos basados en atributos, considere IAM. Para más información, consulte Identidad federada en AWS

AWS Single Sign-On (AWS SSO)

- Cree o conecte identidades una vez y administre el acceso de forma centralizada en todas sus cuentas de AWS.
- AWS SSO proporciona una experiencia de administración unificada para definir, personalizar y asignar acceso detallado.
- A los usuarios se les proporciona un portal de usuario para acceder a todas sus cuentas de AWS o aplicaciones en la nube asignadas.
- Puede configurar el acceso de manera flexible para que se ejecute en paralelo o reemplace la administración de acceso a la cuenta de AWS mediante IAM.

Con AWS Single Sign-On(AWS SSO), puede crear o conectar identidades una vez en AWS y administrar de forma centralizada el acceso a todas sus cuentas de AWS. AWS SSOproporciona una experiencia de administración unificada para definir, personalizar y asignar permisos detallados de acuerdo con las funciones laborales comunes.



Los usuarios de su entorno de AWS SSO pueden utilizar sus credenciales de directorio para acceder a su portal de usuario. Los usuarios pueden acceder a todas sus cuentas de AWS o aplicaciones en la nube asignadas. Puede configurar el acceso de manera flexible para que se ejecute en paralelo o reemplace la administración de acceso a la cuenta de AWS mediante IAM. AWS SSOadmite aplicaciones en la nube de uso común, como Microsoft 365 y Salesforce. El servicio proporciona instrucciones de integración de aplicaciones que eliminan la necesidad de que los administradores aprendan los matices de configuración de cada aplicación en la nube.

Para más información, consulte What is AWS Single Sign-On? (¿Qué es AWS Single Sign-On?)

AWS Directory Service

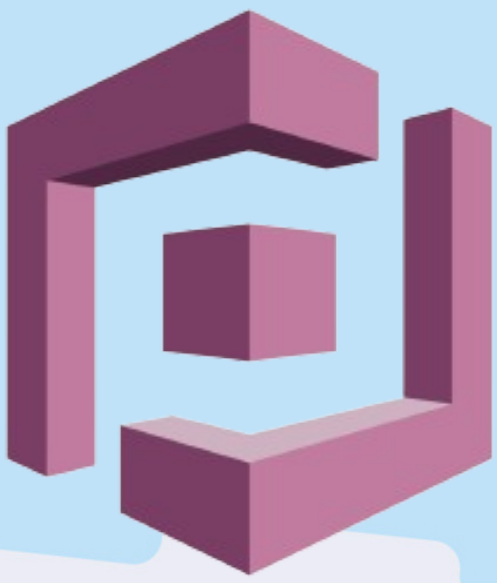
- AWS Directory Service para Microsoft Active Directory, también conocido como AWS Managed Microsoft AD
- Facilita las cargas de trabajo con reconocimiento de directorios y los recursos de AWS para utilizar Active Directory administrado en la nube de AWS.
- Proporciona la capacidad de extender su Active Directory existente a AWS mediante el uso de sus credenciales de usuario en las instalaciones existentes para acceder a los recursos en la nube.
- Admite SSO de Active Directory para aplicaciones de AWS mediante el uso de un único conjunto de credenciales.

AWS Directory Service para Microsoft Active Directory también se conoce comúnmente como AWS Managed Microsoft AD. AWS Managed Microsoft AD hace posible que la carga de trabajo con reconocimiento de directorios y los recursos de AWS utilicen Active Directory administrado en la nube de AWS. El servicio se basa en Microsoft Active Directory, lo que elimina el requisito de sincronizar o replicar sus datos existentes de Active Directory en la nube. Con este servicio, puede utilizar sus credenciales de usuario en las instalaciones existentes a fin de acceder a los recursos en la nube, lo que simplifica el proceso para extender su Active Directory existente a AWS.

Para más información, consulte AWS Directory Service: Microsoft Active Directory administrado en AWS

Amazon Cognito

- Integra el registro de usuario, inicio de sesión y control de acceso con aplicaciones web y móviles.
- Proporciona un almacén de identidades seguro que puede escalar a millones de usuarios con grupos de usuarios de Amazon Cognito.
- Ofrece un inicio de sesión de usuario mediante proveedores de identidad empresariales y sociales como Apple, Google, Facebook y Amazon.
- Proporciona la capacidad de crear identidades únicas para sus usuarios y federarlos con proveedores de identidad mediante grupos de identidades de Amazon Cognito.

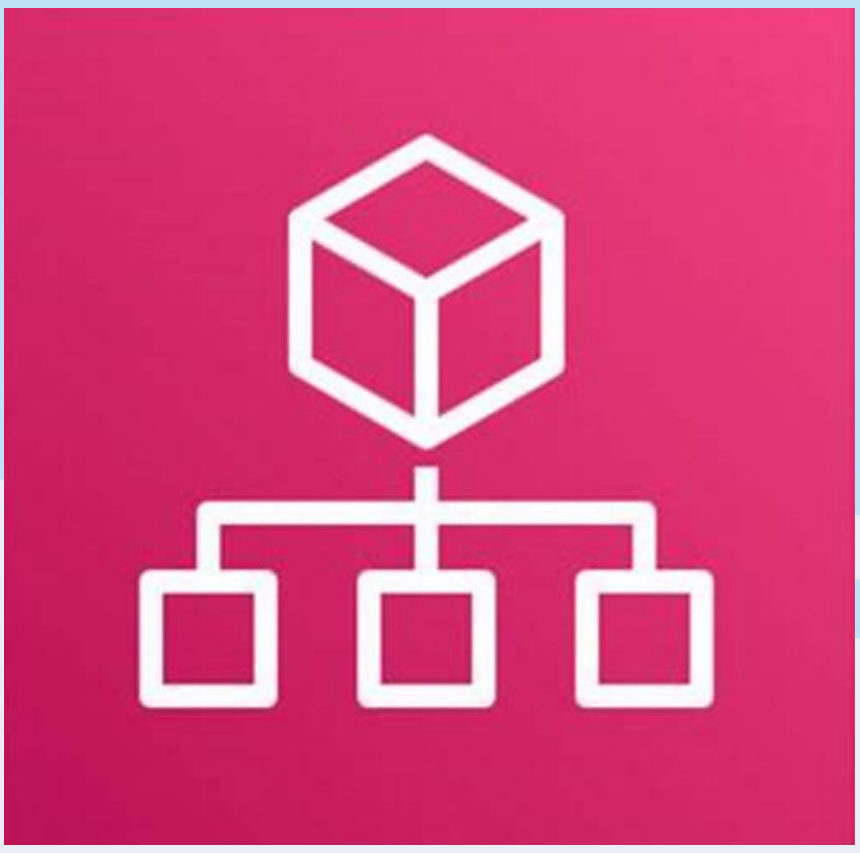


Amazon Cognito es un servicio que proporciona autenticación, autorización y administración de usuarios (registro, inicio de sesión y control de acceso) para aplicaciones móviles y web. El servicio proporciona un almacén de identidades seguro, que puede ayudarle a escalar de manera efectiva para millones de usuarios. Amazon Cognito admite el inicio de sesión directo mediante un nombre de usuario y contraseña. Pero también admite la autenticación de terceros mediante proveedores de identidad sociales, como Apple, Google, Facebook y Amazon.

Amazon Cognito se basa en dos componentes principales para proporcionar le sus servicios: grupos de usuarios y grupos de identidades. Los grupos de usuarios son directorios que proporcionan opciones de registro e inicio de sesión para los usuarios de su aplicación. Esto se integra con los proveedores de identidad social y admite funciones de seguridad como la MFA y verificación telefónica. Con los grupos de identidades, puede conceder a sus usuarios acceso a los servicios de AWS mediante credenciales de AWS temporales con privilegios limitados.

AWS Organizations

- Servicio de administración de cuentas que puede utilizar para consolidar varias cuentas de AWS en una organización administrada de forma centralizada.
- Incluye la creación y administración de cuentas, así como capacidades de facturación unificada.
- Proporciona la agrupación jerárquica de cuentas.
- Admite el control de políticas centralizado sobre los servicios de AWS y las acciones de la API mediante políticas de control de servicios (SCP).
- Se integra con IAM y otros servicios.



AWS Organizations es un servicio de administración de cuentas que se puede utilizar para crear una organización donde se pueden consolidar varias cuentas y administrarlas de forma centralizada. AWS Organizations proporciona creación y administración de cuentas centralizadas, así como capacidades de facturación unificadas. Con estas funciones, puede administrar sus necesidades de seguridad, cumplimiento y presupuesto de forma más eficiente. Organizations también proporciona la capacidad de agrupar de forma jerárquica sus cuentas en unidades organizativas (OU)y adjuntar diferentes políticas de acceso a cada una. Esto otorga la capacidad de crear y personalizar políticas detalladas, que puede orientar a una sola OUo adjuntar a varias OU. Puede anidar OU dentro de otras OU hasta una profundidad de cinco niveles, lo que le ayuda a estructurar su jerarquía como prefiera.

EJEMPLO: SCP

Evite que las cuentas de los miembros abandonen la organización:

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

Este ejemplo de SCP evita que las cuentas de miembros abandonen la organización.

El efecto del enunciado de política es denegar de forma explícita la acción organizations:Leave Organization, lo que evita que las cuentas de miembros se retiren.

Para más información, consulte Políticas de control de servicios (SCP) en la Guía del usuario de AWS Organizations

EN ESTA UNIDAD, APRENDIÓ A HACER LO SIGUIENTE:

Autorizar el acceso a los servicios de AWS mediante usuarios, grupos y roles de IAM

Diferenciar los diferentes tipos de credenciales de seguridad en IAM

Autorizar el acceso a los servicios de AWS mediante políticas basadas en identidades y recursos

Identificar otros servicios de AWS que proporcionan servicios de autenticación y administración de acceso

Administrar y aplicar políticas de manera centralizada para varias cuentas de AWS.