Guía del usuario de

AWS Sign-In

AWS Sign-In: Guía del usuario de

Table of Contents

¿Qué es? AWS Sign-In?

Con esta guía, le resultará más fácil entender las diferentes formas en las que puede iniciar sesión en Amazon Web Services (AWS), según el tipo de usuario que sea. Para obtener más información sobre cómo iniciar sesión en función del tipo de usuario y los AWS recursos a los que desee acceder, consulte uno de los siguientes tutoriales.

- Inicie sesión en Consola de administración de AWS
- Inicia sesión en tu AWS acceda al portal
- Inicie sesión como una identidad federada
- Inicie sesión a través del AWS Command Line Interface
- Inicia sesión con ID de creador de AWS

Si tiene problemas para iniciar sesión en su Cuenta de AWS, consulteResolución de problemas Cuenta de AWS problemas de inicio de sesión. Para obtener ayuda con su ID de creador de AWS consultaSolución de problemas de AWS Builder ID. ¿Quieres crear un Cuenta de AWS? Inscríbase en AWS. Para obtener más información sobre cómo la inscripción AWS puede ayudarte a ti o a tu organización, consulta la sección Contáctanos.

Temas

- Terminología
- Disponibilidad regional para AWS Sign-In
- Sign-in registro de eventos
- Determine el tipo de usuario
- Determine la URL de inicio de sesión
- Dominios para agregar a la lista de permitidos
- Prácticas recomendadas de seguridad para Cuenta de AWS administradores

Terminología

Amazon Web Services (AWS) utiliza terminología común para describir el proceso de inicio de sesión. Le recomendamos que lea y asimile estos términos.

Administrador

También denominado Cuenta de AWS administrador o administrador de IAM. El administrador, que suele ser un empleado del departamento de TI, es una persona que supervisa una Cuenta de AWS. Los administradores tienen un nivel de permisos en la Cuenta de AWS superior respecto a otros miembros de la empresa. Los administradores establecen e implementan la configuración para. Cuenta de AWS También crean usuarios de IAM o de IAM Identity Center. El administrador proporciona a estos usuarios sus credenciales de acceso y una URL de inicio de sesión con la que poder iniciar sesión en la AWS.

Cuenta

Un estándar Cuenta de AWS contiene tanto sus AWS recursos como las identidades que pueden acceder a esos recursos. Las cuentas están asociadas a la dirección de correo electrónico y la contraseña del propietario de la cuenta.

Credenciales

También se denominan credenciales de acceso o credenciales de seguridad. En los procesos de autenticación y autorización, un sistema utiliza las credenciales para identificar quién realiza una llamada y decidir si se concede el acceso solicitado. Las credenciales son la información que los usuarios proporcionan AWS para iniciar sesión y acceder a AWS los recursos. Las credenciales de los usuarios humanos pueden ser, por ejemplo, una dirección de correo electrónico, un nombre de usuario, una contraseña definida por el usuario, un identificador o alias de cuenta, un código de verificación y un código de autenticación multifactor (MFA) de un solo uso. Para el acceso programático, también puede utilizar claves de acceso. Cuando sea posible, le recomendamos utilizar claves de acceso de corta duración.

Para obtener más información sobre las credenciales, consulte Credenciales de seguridad de AWS.

> **Note**
>
> El tipo de credenciales que debe enviar un usuario depende del tipo de usuario.

Credenciales de empresa

Las credenciales que proporcionan los usuarios al acceder a sus redes y recursos de empresa. El administrador corporativo puede configurarlo Cuenta de AWS para que utilice las mismas

credenciales que utiliza para acceder a la red y los recursos corporativos. El administrador o el empleado del servicio de asistencia le proporcionará estas credenciales.

Perfil

Cuando te registras para obtener un AWS Builder ID, creas un perfil. Dicho perfil incluye la información de contacto que proporcionó y la capacidad de gestionar los dispositivos de autenticación multifactor (MFA) y las sesiones activas. Puede obtener más información sobre la privacidad y cómo gestionamos sus datos en el perfil. Para obtener más información sobre su perfil y cómo interactúa con la Cuenta de AWS, consulte ID de creador de AWS y otras AWS credenciales.

Credenciales del usuario raíz

Las credenciales del usuario raíz son la dirección de correo electrónico y la contraseña que se han utilizado para crear la Cuenta de AWS. Es muy recomendable añadir una MFA a las credenciales del usuario raíz para mayor seguridad. Las credenciales de usuario raíz proporcionan acceso completo a todos los servicios y recursos de AWS de la cuenta. Para obtener más información sobre el usuario raíz, consulte Usuario raíz.

Usuario

Un usuario es una persona o aplicación que tiene permisos para realizar llamadas a la API a AWS los productos o acceder a AWS los recursos. Cada usuario tiene un conjunto único de credenciales de seguridad que no se comparten con nadie más. Estas credenciales son independientes de las credenciales de seguridad que se usan para la Cuenta de AWS. Para obtener más información, consulte Determine el tipo de usuario.

Código de verificación

Un código de verificación verifica su identidad durante el proceso de inicio de sesión mediante autenticación multifactor (MFA). Existen varios métodos de entrega para los códigos de verificación. Se pueden enviar por SMS o correo electrónico. Para obtener más información, consulte con su administrador.

Disponibilidad regional para AWS Sign-In

AWS Sign-in está disponible en varios de los más utilizados Regiones de AWS. Esta disponibilidad le facilita el acceso a los AWS servicios y las aplicaciones empresariales. Para ver una lista completa de las regiones Sign-in compatibles, consulta los AWS Sign-In puntos finales y las cuotas.

Sign-in registro de eventos

CloudTrail se activa automáticamente en usted Cuenta de AWS y registra los eventos cuando se produce una actividad. Los siguientes recursos resultan útiles para obtener más información sobre el registro y la supervisión de los eventos de inicio de sesión.

- CloudTrail registra los intentos de iniciar sesión en Consola de administración de AWS. Todos los eventos de inicio de sesión de usuarios de IAM, usuarios raíz y usuarios federados generan registros en CloudTrail los archivos de registro. Para obtener más información, consulte Eventos de inicio de sesión de Consola de administración de AWS en la Guía del usuario de AWS CloudTrail .
- Si utiliza un punto final regional para iniciar sesión en el Consola de administración de AWS, CloudTrail registra el `ConsoleLogin` evento en la región correspondiente al punto final. Para obtener más información sobre AWS Sign-In los puntos finales, consulte los AWS Sign-In puntos finales y las cuotas en la Guía de referencia AWS general.
- Para obtener más información sobre cómo se registran CloudTrail los eventos de inicio de sesión en el Centro de Identidad de IAM, consulte Descripción de los eventos de inicio de sesión en el Centro de Identidad de IAM en la Guía del usuario del Centro de Identidad de IAM.
- Para obtener más información sobre cómo se CloudTrail registra la diferente información de identidad de los usuarios en IAM, consulte Registrar las llamadas de IAM y AWS STS API en la Guía del usuario. AWS CloudTrailAWS Identity and Access Management

AWS Sign-In admite políticas basadas en recursos y políticas de control de recursos que permiten restringir el acceso a la consola en función de la ubicación de la red y la identidad principal. Para los usuarios root, la ubicación de la red se valida antes de que aparezca la solicitud de contraseña. Para todos los tipos principales, las políticas se evalúan antes y después de la autenticación. Para obtener más información, consulte Control del acceso a la consola con políticas basadas en recursos y políticas de control de recursos.

Determine el tipo de usuario

La forma de iniciar sesión depende del tipo de AWS usuario que sea. Puede gestionar una Cuenta de AWS como usuario raíz, un usuario de IAM, un usuario en IAM Identity Center o como identidad federada. Puedes usar un perfil de AWS Builder ID para acceder a determinados AWS servicios y herramientas. A continuación, se indican los distintos tipos de usuario.

Temas

- Usuario raíz
- Usuario de IAM
- Usuario de IAM Identity Center
- Identidad federada
- AWS Builder ID: usuario

Usuario raíz

También se denomina propietario de la cuenta o usuario raíz de la cuenta. Como usuario root, tiene acceso completo a todos los AWS servicios y recursos de su cuenta Cuenta de AWS. Cuando crea una por primera vez Cuenta de AWS, comienza con una identidad de inicio de sesión única que tiene acceso completo a todos los AWS servicios y recursos de la cuenta. Esta identidad es el usuario raíz AWS de la cuenta. Puede iniciar sesión como usuario raíz utilizando la dirección de correo electrónico y contraseña que usó al crear la cuenta. Los usuarios raíz inician sesión con el Consola de administración de AWS. Para obtener instrucciones paso a paso sobre cómo iniciar sesión, consulte Inicie sesión Consola de administración de AWS como usuario root.

> **Important**
>
> Al crear una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz, que tiene acceso completo a todos Servicios de AWS los recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Para obtener más información acerca de las identidades de IAM, incluyendo el usuario raíz, consulte Identidades IAM (usuarios, grupos de usuarios y roles).

Usuario de IAM

Un usuario de IAM es una entidad que se crea en AWS. Este usuario es simplemente una identidad en su Cuenta de AWS que tiene permisos personalizados específicos. Sus credenciales de usuario de IAM constan de un nombre y una contraseña que se utilizan para iniciar sesión en el Consola de

administración de AWS. Para obtener instrucciones paso a paso sobre cómo iniciar sesión, consulte Inicie sesión Consola de administración de AWS como usuario de IAM.

Para obtener más información acerca de las identidades de IAM, incluyendo el usuario de IAM, consulte Identidades de IAM (usuarios, grupos de usuarios y roles).

Usuario de IAM Identity Center

Un usuario del Centro de Identidad de IAM es miembro de AWS Organizations su portal de acceso Cuentas de AWS y se le puede conceder AWS acceso a varias aplicaciones. Si su empresa ha integrado Active Directory u otro proveedor de identidad en IAM Identity Center, los usuarios pueden utilizar sus credenciales corporativas para iniciar sesión en IAM Identity Center. IAM Identity Center también puede ser un proveedor de identidades en el que un administrador puede crear usuarios. Independientemente del proveedor de identidad, los usuarios del Centro de Identidad de IAM inician sesión mediante su portal de AWS acceso, que es una URL de inicio de sesión específica para su organización. Los usuarios de IAM Identity Center no pueden iniciar sesión a través de la URL de Consola de administración de AWS .

Los usuarios humanos del Centro de Identidad de IAM pueden obtener la URL del portal de AWS acceso de una de las siguientes maneras:

- Un mensaje de su administrador o empleado del servicio de asistencia
- Un correo electrónico AWS con una invitación para unirse al Centro de Identidad de IAM

> **Tip**
>
> Todos los correos electrónicos enviados por el servicio de IAM Identity Center proceden de la dirección no-reply@signin.aws 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.

Para obtener instrucciones paso a paso sobre cómo iniciar sesión, consulte Inicia sesión en tu AWS acceda al portal.

> **Note**
>
> Le recomendamos que añada a sus marcadores la URL de inicio de sesión específica de su organizción para el portal de acceso de AWS , de modo que pueda acceder a ella más adelante.

Para obtener más información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center?

Identidad federada

Una identidad federada es un usuario que puede iniciar sesión con un proveedor de identidades (IdP) externo conocido, como Login con Amazon, Facebook, Google o cualquier otro IdP compatible con OpenID Connect (OIDC). Con la federación de identidades web, puede recibir un token de autenticación y, después, cambiarlo por credenciales de seguridad temporales en AWS ese mapa por un rol de IAM con permisos para usar los recursos de su cuenta. Cuenta de AWS No inicias sesión en el portal Consola de administración de AWS ni AWS accedes a él. En su lugar, la identidad externa utilizada determina cómo se inicia sesión.

Para obtener más información, consulte Inicie sesión como una identidad federada.

AWS Builder ID: usuario

Como usuario de AWS Builder ID, inicia sesión específicamente en el AWS servicio o la herramienta a los que desea acceder. Un usuario de AWS Builder ID complementa cualquier usuario que ya Cuenta de AWS tenga o desee crear. Un AWS Builder ID lo representa como persona y puede usarlo para acceder a AWS servicios y herramientas sin necesidad de uno Cuenta de AWS. También tiene un perfil en el que puede ver y actualizar su información. Para obtener más información, consulte Inicia sesión con ID de creador de AWS.

AWS El Builder ID es independiente de la suscripción a AWS Skill Builder, un centro de aprendizaje en línea en el que puede aprender de AWS expertos y desarrollar habilidades relacionadas con la nube en línea. Para obtener más información sobre AWS Skill Builder, consulte AWS Skill Builder.

Determine la URL de inicio de sesión

Utilice una de las siguientes direcciones URL para acceder en AWS función del tipo de AWS usuario que sea. Para obtener más información, consulte Determine el tipo de usuario.

Temas

Cuenta de AWS URL de inicio de sesión del usuario raíz

El usuario raíz accede a ella Consola de administración de AWS desde la página de inicio de AWS sesión:. `https://console.aws.amazon.com/`

Esta página de inicio de sesión también tiene la opción de iniciar sesión como usuario de IAM.

AWS portal de acceso

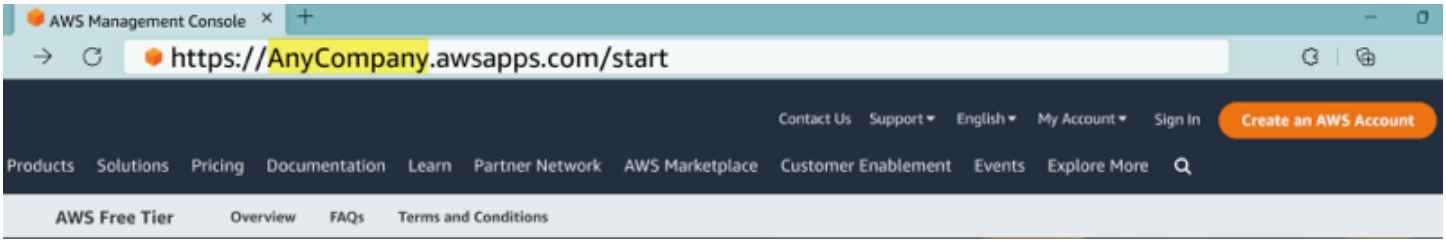
El portal de AWS acceso es una URL de inicio de sesión específica para que los usuarios del Centro de Identidad de IAM inicien sesión y accedan a su cuenta. Cuando un administrador crea el usuario en el Centro de Identidad de IAM, el administrador elige si el usuario recibe una invitación por correo electrónico para unirse al Centro de Identidad de IAM o un mensaje del administrador o empleado del servicio de asistencia que contiene una contraseña de un solo uso y AWS la URL del portal de acceso. El formato de la URL de inicio de sesión específica es parecido al de estos ejemplos:

```
https://d-xxxxxxxxxx.awsapps.com/start
```

o

```
https://your_subdomain.awsapps.com/start
```

La URL de inicio de sesión específica varía porque su administrador puede personalizarla. La URL de inicio de sesión específica puede empezar por la letra D seguida de 10 letras y números aleatorios. Es posible que también se emplee su subdominio en la URL de inicio de sesión, y que incluya el nombre de su empresa, como en el ejemplo siguiente:



> **Note**
>
> Le recomendamos que guarde en favoritos la URL de inicio de sesión específica de su portal de AWS acceso para poder acceder a ella más adelante.

Para obtener más información sobre su portal de AWS acceso, consulte Uso del portal de AWS acceso.

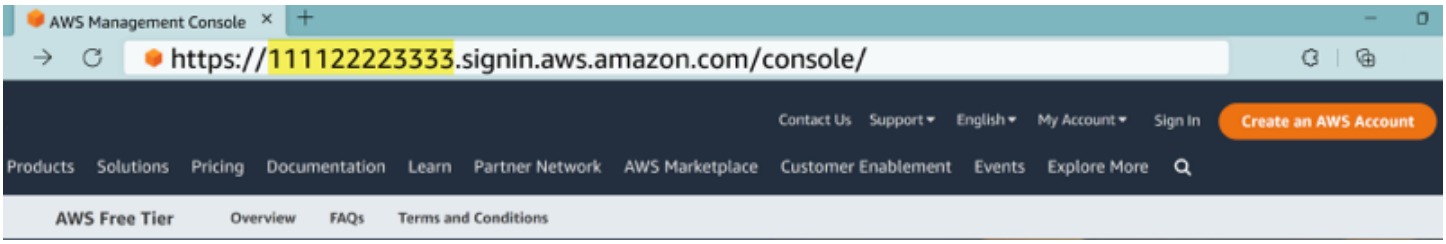
URL de inicio de sesión de usuario de IAM

Los usuarios de IAM pueden acceder a él Consola de administración de AWS con una URL de inicio de sesión de usuario de IAM específica. La URL de inicio de sesión de usuario de IAM combina su ID o alias y Cuenta de AWS `signin.aws.amazon.com/console`

Un ejemplo de como sería la URL de inicio de sesión de un usuario de IAM:

```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

Si el ID de su cuenta es 111122223333, su URL de inicio de sesión sería:



Si tienes problemas para acceder a tu Cuenta de AWS URL de inicio de sesión de usuario de IAM, consulta Resilience in AWS Identity and Access Management para obtener más información.

URL de identidad federada

La URL de inicio de sesión para una identidad federada es distinta. La identidad externa o el proveedor de identidades (IdP) externo determinan la URL de inicio de sesión de las identidades

federadas. La identidad externa puede ser Windows Active Directory, Inicio de sesión con Amazon, Facebook o Google. Póngase en contacto con su administrador para obtener más información sobre cómo iniciar sesión como una identidad federada.

Para obtener más información acerca de las identidades federadas, consulte Acerca de la federación de identidades en la web.

AWS ID de Builder (URL)

La URL de tu perfil de AWS Builder ID eshttps://profile.aws.amazon.com/. Al usar tu ID de AWS Builder, la URL de inicio de sesión depende del servicio al que quieras acceder. Por ejemplo, para iniciar sesión en Amazon CodeCatalyst, ve ahttps://codecatalyst.aws/login.

Dominios para agregar a la lista de permitidos

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.

AWS Sign-In dominios a la lista de dominios permitidos

Si usted o la organización implementan el filtrado de IP o dominios, es posible que tenga que incluir dominios en la lista de permitidos para utilizar la Consola de administración de AWS. Se debe poder acceder a los siguientes dominios en la red desde la que se intenta acceder a la Consola de administración de AWS.

- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

AWS Sign-In dominios de administración para permitir

Si configura los controles de acceso a la consola mediante la AWS CLI, debe incluir en la lista de permisos el punto final del plano AWS Sign-In de control. Este punto final se encarga de la

administración de políticas y es distinto de los dominios de inicio de sesión de la consola descritos en la sección anterior.

- `signin.[Region].api.aws`

  *[Region]*Sustitúyalo por la AWS región a la que llamas. Disponible en todas las regiones comerciales. Ejemplo: `signin.us-east-1.api.aws`.

Portal de acceso a AWS dominios para incluir en la lista

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 agregar los siguientes dominios o puntos de enlace de URL a las listas de permisos de su solución de filtrado de contenido web. Si lo hace, podrá acceder a su. Portal de acceso a AWS

Las siguientes listas proporcionan los dominios IPv4 y de doble pila y los puntos finales de URL que debe añadir a las listas de permitidos de su solución de filtrado de contenido web. Para obtener más información sobre los puntos de enlace de doble pila, consulte Actualizar los firewalls y las puertas de enlace para permitir el acceso a ellos en la Guía del usuario del IAM Identity Center. Portal de acceso a AWS

Lista de IPv4 permitidos

- *[Directory ID or alias]*.awsapps.com
- *[IAM Identity Center instance ID]*.*[Region]*.portal.amazonaws.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

Dual-stack lista de permitidos

- *[IAM Identity Center instance ID]*.portal.*[Region]*.app.aws

- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

ID de creador de AWS dominios para incluir en la lista

Si usted o la organización implementan el filtrado de IP o dominios, es posible que tenga que incluir dominios en la lista de permitidos para crear y utilizar un ID de creador de AWS. Se debe poder acceder a los siguientes dominios en la red desde la que se intenta acceder a ID de creador de AWS.

- view.awsapps.com/start
- *.portal.*.app.aws
- *.aws.dev
- *.api.aws
- *.uis.awsstatic.com
- *.console.aws.a2z.com
- oidc.*.amazonaws.com
- oidc.*.api.aws
- *.sso.amazonaws.com
- *.sso.*.amazonaws.com
- *.sso-portal.*.amazonaws.com

- `sso.*.api.aws`
- `*.signin.aws`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`
- `profile.aws.amazon.com`

Prácticas recomendadas de seguridad para Cuenta de AWS administradores

Si eres el administrador de una cuenta y has creado una nueva Cuenta de AWS, te recomendamos que sigas los siguientes pasos para ayudar a tus usuarios a seguir las prácticas recomendadas de AWS seguridad al iniciar sesión.

1. Inicie sesión como usuario raíz para habilitar la autenticación multifactor (MFA) y cree AWS un usuario administrativo en IAM Identity Center si aún no lo ha hecho. A continuación, Proteja sus credenciales raíz y no las utilice para otras tareas cotidianas.
2. Inicie sesión como Cuenta de AWS administrador y configure las siguientes identidades:
   - Cree usuarios con Privilegios mínimos para otras personas.
   - Configure Credenciales temporales para las cargas de trabajo.
   - Cree claves de acceso solo para Casos de uso que requieran credenciales de larga duración.
3. Añada permisos para conceder acceso a esas identidades. Puede empezar con las políticas AWS administradas y avanzar hacia los permisos con privilegios mínimos.
   - Añada conjuntos de permisos a los usuarios AWS del IAM Identity Center (sucesor de Single AWS). Sign-On
   - Añada políticas basadas en la identidad a los roles de IAM utilizados para las cargas de trabajo.
   - Añada políticas basadas en identidades para los usuarios de IAM para los casos de uso que requieran credenciales de larga duración.
   - Para obtener más información sobre usuarios de IAM, consulte Prácticas recomendadas de seguridad en IAM.
4. Guarde y comparta información sobre Inicie sesión en Consola de administración de AWS. Esta información varía en función del tipo de identidad que creó.

5. Mantenga actualizados la dirección de correo electrónico del usuario raíz y el número de teléfono de contacto de la cuenta principal para asegurarse de que puede recibir notificaciones importantes relacionadas con la cuenta y la seguridad.

   - Modifique el nombre de la cuenta, la dirección de correo electrónico o la contraseña de Usuario raíz de la cuenta de AWS.
   - Acceda o actualice el contacto de la cuenta principal.

6. Consulte las Prácticas recomendadas de seguridad de IAM para obtener más información sobre otros consejos sobre la gestión de identidades y accesos.

7. Implemente controles de acceso basados en la red: utilice políticas Sign-in basadas en recursos o políticas de control de recursos (RCP) para restringir el inicio de sesión en la consola a las solicitudes procedentes de rangos de direcciones IP o VPC aprobados. Para los entornos que utilizan el acceso privado a la consola, configure las políticas de punto final de la VPC para controlar a qué cuentas se puede acceder a través de los puntos finales (consulte Acceso privado a la consola). En conjunto, las políticas Sign-in basadas en recursos, las RCP y las políticas de punto final de VPC proporcionan controles de red en capas en diferentes puntos de aplicación. En el caso de los usuarios raíz, Sign-in las políticas bloquean por completo la página de credenciales cuando se intenta acceder desde redes no autorizadas. AWS recomienda configurar los principales excluidos para el acceso de recuperación a fin de evitar el bloqueo de la cuenta, aunque esto es opcional. Para obtener más información, consulte Control del acceso a la consola con políticas basadas en recursos y políticas de control de recursos.

Inicie sesión en Consola de administración de AWS

Al iniciar sesión Consola de administración de AWS desde la URL de inicio de AWS sesión principal (https://console.aws.amazon.com/), debe elegir su tipo de usuario, usuario raíz o usuario de IAM. Si no está seguro del tipo de usuario que es, consulte Determine el tipo de usuario.

El usuario raíz tiene acceso ilimitado a la cuenta y está asociado a la persona que creó la Cuenta de AWS. A continuación, el usuario raíz crea otros tipos de usuarios, como los usuarios de IAM y usuarios en AWS IAM Identity Center, y les asigna credenciales de acceso.

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos personalizados específicos. Cuando un usuario de IAM inicia sesión, puede usar una URL de inicio de sesión que incluya su Cuenta de AWS alias, por ejemplo, `https://account_alias_or_id.signin.aws.amazon.com/console/` en lugar de la URL de inicio de AWS sesión principal. `https://console.aws.amazon.com/`

Puedes iniciar sesión con hasta 5 identidades diferentes de forma simultánea en un único navegador del. Consola de administración de AWS Pueden ser una combinación de usuarios raíz, usuarios de IAM o roles federados en cuentas diferentes o en la misma cuenta. Para obtener más información, consulte Cómo iniciar sesión en varias cuentas en la Guía de introducción a Consola de administración de AWS .

Tutoriales

- Inicie sesión Consola de administración de AWS como usuario root
- Inicie sesión Consola de administración de AWS como usuario de IAM

Si no está seguro del tipo de usuario que es, consulte Determine el tipo de usuario.

Tutoriales

- Inicie sesión Consola de administración de AWS como usuario root
- Inicie sesión Consola de administración de AWS como usuario de IAM

Inicie sesión Consola de administración de AWS como usuario root

Cuando creas una por primera vez Cuenta de AWS, comienzas con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se

denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta.

> **Important**
>
> Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del Usuario raíz y utilícelas solo para las tareas que solo el Usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Para iniciar sesión como usuario raíz

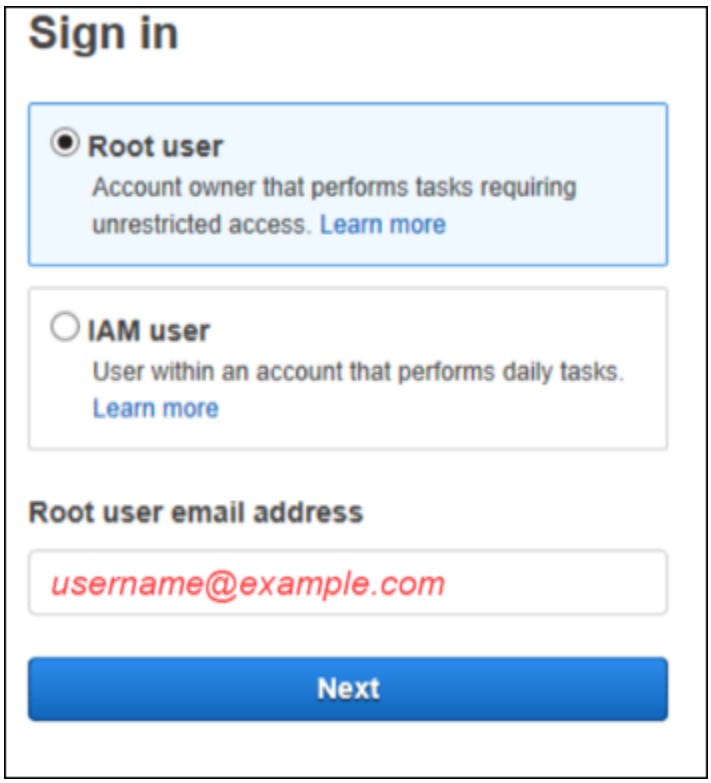
Puede iniciar sesión como usuario raíz cuando ya haya iniciado sesión con otra identidad en la Consola de administración de AWS. Para obtener más información, consulte Cómo iniciar sesión en varias cuentas en la Guía de introducción a Consola de administración de AWS .

Cuentas de AWS AWS Organizations Es posible que el uso administrado no tenga credenciales de usuario raíz y debe ponerse en contacto con un administrador para realizar acciones de usuario raíz en su cuenta de miembro. Si no puede iniciar sesión como usuario raíz, consulte Resolución de problemas Cuenta de AWS problemas de inicio de sesión.

1. Abre el Consola de administración de AWS chathttps://console.aws.amazon.com/.

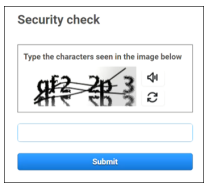
   > **Note**
   >
   > Si ha iniciado sesión anteriormente como usuario de IAM en este navegador, es posible que en su lugar aparezca la página de inicio de sesión del usuario de IAM. Seleccione Iniciar sesión con el correo electrónico del usuario raíz.

2. Elija Usuario raíz.



3. En Dirección de correo electrónico del usuario raíz, escriba la dirección de correo electrónico asociada a su usuario raíz. A continuación, seleccione Siguiente.
4. Si se le solicita que realice un control de seguridad, introduzca los caracteres que se muestran para continuar. Si no puede completar el control de seguridad, intente escuchar el audio o vuelva a cargar el control de seguridad para usar un conjunto de caracteres distinto.

> **Tip**
>
> Escriba los caracteres alfanuméricos que vea (u oiga) en orden y sin espacios.



5. Introduzca su contraseña.

6. Autentíquese con la MFA. La MFA se aplica de forma predeterminada al usuario raíz. Para los usuarios raíz de cuentas independientes y de miembros, debe habilitar de manera manual la MFA, una acción muy recomendable. Para obtener más información sobre la MFA, consulte Cuenta de AWS Autenticación multifactor para el usuario raíz de la en la Guía del usuario de AWS Identity and Access Management .

   > **Tip**
   >
   > Como práctica recomendada de seguridad, recomendamos eliminar todas las credenciales de los usuarios raíz de las cuentas de los miembros de su AWS organización para evitar el uso no autorizado. Si elige esta opción, las cuentas de miembro no podrán iniciar sesión como usuario raíz, recuperar la contraseña ni configurar la MFA. En este caso, solo el administrador de la cuenta de administración puede realizar una tarea que exige credenciales de usuario raíz en una cuenta de miembro. Para obtener más detalles, consulte Administrar de forma centralizada el acceso raíz de las cuentas de miembros en la Guía del usuario de AWS Identity and Access Management .

7. Seleccione Iniciar sesión. Consola de administración de AWS Aparece el.

Tras la autenticación, Consola de administración de AWS se abre en la página de inicio de la consola.

Información adicional

Si desea obtener más información sobre el usuario Cuenta de AWS root, consulte los siguientes recursos.

- Para obtener una descripción general del usuario raíz, consulte Usuario raíz de Cuenta de AWS.
- Para obtener más información sobre el uso del usuario raíz, consulte Uso del usuario Cuenta de AWS raíz.
- Para obtener step-by-step instrucciones sobre cómo restablecer la contraseña del usuario raíz, consulteHe olvidado la contraseña de mi usuario root Cuenta de AWS.

Inicie sesión Consola de administración de AWS como usuario de IAM

Un usuario de IAM es una identidad creada dentro de los AWS recursos y Cuenta de AWS que tiene permiso para interactuar con ellos. Los usuarios de IAM inician sesión con el ID de su cuenta o alias, su nombre de usuario y una contraseña. Su administrador configura los nombres de usuario de IAM. Los nombres de usuario de IAM pueden ser nombres descriptivos, por ejemplo, o direcciones de correo electrónico*Zhang*, por ejemplo. *zhang@example.com* Los nombres de usuario de IAM no pueden contener espacios, pero sí letras mayúsculas y minúsculas, números y los símbolos + = , . @ _ -.

> **Tip**
>
> Si su usuario de IAM tiene habilitada la autenticación multifactor (MFA), debe contar con acceso al dispositivo de autenticación. Para obtener más información, consulte Uso de dispositivos MFA con la página de inicio de sesión de IAM.

Para iniciar sesión como usuario de IAM

Puede iniciar sesión como usuario de IAM cuando ya haya iniciado sesión con otra identidad en la Consola de administración de AWS. Para obtener más información, consulte Cómo iniciar sesión en varias cuentas en la Guía de introducción a Consola de administración de AWS .

1. Abre el chat Consola de administración de AWS . https://console.aws.amazon.com/

2. Aparecerá la página de inicio de sesión principal. Ingrese el ID (12 dígitos) o alias de la cuenta, el nombre de usuario de IAM y la contraseña.

   > **Note**
   >
   > Es posible que no tenga que introducir el ID o el alias de su cuenta si ha iniciado sesión anteriormente como usuario de IAM con su navegador actual o si utiliza la URL de inicio de sesión de su cuenta.

3. Seleccione Iniciar sesión.
4. Si la MFA está habilitada para su usuario de IAM, AWS requiere que confirme su identidad con un autenticador. Para obtener más información, consulte Utilizar la autenticación multifactor (MFA) en AWS.

Tras la autenticación, Consola de administración de AWS se abre a la página de inicio de la consola.

Información adicional

Si desea obtener más información sobre los usuarios de IAM, consulte los siguientes recursos.

- Para obtener información general sobre IAM, consulte ¿Qué es Identity and Access Management?
- Para obtener más información sobre la AWS cuenta IDs, consulte el ID de su AWS cuenta y su alias.
- Para obtener step-by-step instrucciones sobre cómo restablecer la contraseña de usuario de IAM, consulteHe olvidado la contraseña de usuario de IAM para mi Cuenta de AWS.

Control del acceso a la consola con políticas basadas en recursos y políticas de control de recursos

> **Important**
>
> El acceso al inicio de sesión de la consola está habilitado de forma predeterminada. AWS Sign-In permite inicialmente el acceso sin restricciones a la consola. Para añadir restricciones, habilite la configuración de autorización de la consola para su cuenta u organización. Las declaraciones de permisos de recursos que cree no surtirán efecto hasta que habilite la autorización de la consola. Consulte Cómo empezar con el control de acceso a la consola mediante políticas de recursos.

AWS Sign-In admite políticas basadas en recursos y políticas de control de recursos (RCP) para controlar el acceso. AWS Sign-In Utilice estas políticas para verificar la identidad del usuario y la ubicación de la red durante el Consola de administración de AWS acceso: antes, durante y después de la autenticación. En el caso de los usuarios raíz, estas políticas validan la ubicación de la red y la identidad del usuario antes de que comience la recopilación de credenciales. Las credenciales solo se pueden introducir cuando el acceso se origina en las redes esperadas.

AWS Sign-In políticas basadas en recursos:

- Se aplican a cuentas individuales AWS .
- Permita que los administradores de cuentas restrinjan el acceso a la consola en función de los parámetros de la red y las identidades principales.

Políticas de control de recursos (RCP):

- Realice su solicitud en toda la organización a través de AWS Organizations.
- Proporcione un gobierno centralizado en todas las cuentas de los miembros.

Ambos tipos de políticas verifican el acceso antes de la autenticación. Esto impide que los directores accedan a la página de inicio de sesión desde redes inesperadas.

Estas políticas no sustituyen a las políticas de IAM basadas en la identidad, que siguen aplicándose.

> **Note**
>
> Para obtener la documentación completa sobre las políticas de control de recursos, incluidas la configuración y la administración a nivel de la organización, consulte las políticas de control de recursos en la Guía del usuario de AWS Organizations. Esta sección se centra principalmente en las políticas basadas en los AWS Sign-In recursos.

AWS Sign-In las políticas basadas en recursos y las RCP se aplican a los siguientes métodos de autenticación:

- Consola de administración de AWS— Inicio de sesión directo mediante la página de inicio de sesión de la consola.
- AWS IAM Identity Center: inicio de sesión en la consola mediante IAM Identity Center.
- Proveedores de identidad federados: Sign-in mediante la federación SAML o OIDC.
- Aplicaciones integradas con AWS Sign-In: Amazon Connect, Amazon QuickSight, AWS Health Dashboard, Amazon AppStream, Amazon Lightsail y AWS IQ.

Estos controles no se aplican al acceso programático mediante claves de acceso (AWS SDK o llamadas a la API firmadas con SiGv4).

Cómo AWS Sign-In evalúa las políticas basadas en los recursos

AWS Sign-In evalúa las políticas basadas en recursos o las políticas de control de recursos (RCP) aplicables en dos momentos durante el acceso a la consola: antes de la autenticación (la fase previa a la autenticación) y después de una autenticación correcta (la fase posterior a la autenticación). Cada evaluación comprueba las claves de condición definidas en su política. Las claves disponibles dependen de la fase y la acción. Para obtener más información, consulte Claves de condición admitidas.

> **Note**
>
> Al iniciar sesión como usuario root, se bloquea cualquier intento de acceso desde redes inesperadas antes de que aparezca la solicitud de contraseña. Esto impide el envío de credenciales desde redes inesperadas.

Tras la autenticación, la evaluación también considera las políticas del director basadas en la identidad. Una política de IAM que deniegue la acción de inicio de sesión correspondiente puede impedir que se conceda la sesión de consola, incluso cuando se cumplan las condiciones de la red.

Acciones admitidas

AWS Sign-In las políticas de recursos (políticas basadas en recursos y RCP) admiten las siguientes acciones:

`signin:Authenticate`

Se trata de una acción únicamente de evaluación (no exigible) que se evalúa cuando se recibe una solicitud de inicio de sesión. Se trata de una comprobación previa a la autenticación y se realiza cuando el director introduce las credenciales en la página de inicio de sesión (usuario raíz, usuario de IAM) o inicia el inicio de sesión en la consola con las credenciales de un proveedor de identidad o de AWS STS (usuario federado, rol).

Claves de condición compatibles:`aws:SourceIp`,,,,. `aws:SourceVpc` `aws:SourceVpce` `aws:VpcSourceIp` `aws:RequestedRegion` `signin:PrincipalArn`

Principal-based Las claves de condición globales (`aws:PrincipalArn`,`aws:PrincipalAccount`) no están disponibles para esta acción porque aún no se ha confirmado la identidad del usuario.

`signin:AuthorizeOAuth2Access`

Se utiliza para la generación del código de autorización de OAuth. Tras una autenticación correcta, esta acción se activa cuando el sistema genera un código de autorización de OAuth. En este punto, el usuario se autentica y están disponibles las claves de condición basadas en el código principal.

Claves de condición compatibles:`aws:SourceIp`,,`aws:SourceVpc`,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:Requeste`
`aws:PrincipalArn` `aws:PrincipalAccount`

`signin:CreateOAuth2Token`

Esta acción posterior a la autenticación se utiliza para crear e intercambiar el token de OAuth. Esta acción se activa al canjear códigos de autorización por fichas de acceso, al actualizar las fichas o al realizar operaciones de intercambio de fichas. Principal-based las claves de condición están disponibles durante esta fase.

Claves de condición compatibles:
`aws:SourceIpaws:SourceVpc,aws:SourceVpce,aws:VpcSourceIp,aws:RequestedRegion,aws`

> **Important**
>
> Al crear AWS Sign-In políticas (políticas basadas en recursos o RCP), incluya las tres acciones de la política: `signin:Authenticate` en una declaración previa a la autenticación `signin:AuthorizeOAuth2Access` y `signin:CreateOAuth2Token` en una declaración posterior a la autenticación. El inicio de sesión en la consola utiliza OAuth 2.0, que recorre las tres acciones de forma secuencial. Si tu política omite una acción, la fase correspondiente no está protegida. Para ver las acciones de política de puntos finales de la VPC`signin:CreateAccount`, consulte Acceso privado a la consola de administración de AWS.

Claves de condición admitidas

AWS Sign-In admite las siguientes claves de condición en las políticas basadas en recursos y en las políticas de control de recursos (RCP). Utilice estas teclas para controlar el acceso a la consola en función de la ubicación de la red y la identidad principal:

- Network-based (todas las acciones):`aws:SourceIp`,`aws:SourceVpc`,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:RequestedRe`
- Identity-based (acciones posteriores a la autenticación):`aws:PrincipalArn`,`aws:PrincipalAccount`.
- Service-specific (solo autenticación previa):. `signin:PrincipalArn`

Para ver las reglas de uso detalladas, la compatibilidad de los operadores, las restricciones de combinación y la matriz de disponibilidad por acción, consulteAWS Sign-In referencia de claves de condición.

Cómo empezar con el control de acceso a la consola mediante políticas de recursos

Requisitos previos

- AWS CLI instalada y configurada.
- Permisos de IAM adecuados (consulteAWS política gestionada: AWSSignInResourcePolicyManagement).
- Perímetros de red identificados (rangos de IP, VPC o puntos finales de VPC).
- Designe a los principales excluidos para conservar el acceso (recomendado pero opcional).
- Si su red utiliza el filtrado de salida, incluya en la lista de puntos finales del plano AWS Sign-In de control (consulte). AWS Sign-In dominios de administración para permitir

> **Important**
>
> Antes de habilitar la autorización de la consola en producción, se AWS recomienda configurar al menos un principal excluido para mantener el acceso de recuperación de emergencia. Todos los usuarios principales, incluido el usuario root, están sujetos a la política, a menos que se excluyan explícitamente. Los directores excluidos son opcionales, pero omitirlos aumenta el riesgo de bloqueo de la cuenta si las condiciones de la red cambian inesperadamente.

Especifique todas las operaciones `--region us-east-1` de escritura en las políticas. AWS Sign-In AWS replica las políticas de esta región a nivel mundial. Las operaciones de lectura pueden dirigirse a cualquier región.

Paso 1: Crear declaraciones de permiso de recursos

Cree declaraciones de permiso que definan sus controles de acceso. Todas las operaciones de escritura `--region us-east-1` son obligatorias (el AWS Sign-In servicio solo acepta cambios de política en esta región). Los parámetros restantes (`--source-vpc`,`--source-ip`,`--requested-region`,`--excluded-principal`) definen las condiciones de su política. Por ejemplo, `--requested-region us-west-2` añade una condición que restringe el inicio de sesión en el punto final de inicio de sesión regional us-west-2.

Ejemplo: restringir el acceso a la VPC corporativa:

```
aws signin put-resource-permission-statement \
  --source-vpc vpc-0abc123def456789 \
  --requested-region us-west-2 \
  --excluded-principal "arn:aws:iam::123456789012:user/EmergencyAdmin" \
```

```
  --client-token unique-request-id-12345 \
  --region us-east-1
```

Ejemplo: restringir el acceso a un rango de IP específico:

```
aws signin put-resource-permission-statement \
  --source-ip "IP_ADDRESS" \
  --excluded-principal "arn:aws:iam::123456789012:role/BreakGlassRole" \
  --region us-east-1
```

> **Note**
>
> El `--excluded-principal` parámetro designa un principal excluido que elude las restricciones de la red y preserva el acceso de emergencia en caso de que cambien las condiciones de la red.

Paso 2: Habilitar la configuración de autorización de la consola

El siguiente paso activa la aplicación de políticas para el proceso de inicio de sesión en la consola en su cuenta u organización. Las declaraciones de permisos de recursos se pueden crear en cualquier momento, pero no se evalúan hasta que se habilita la autorización de la consola.

> **Warning**
>
> Si se habilita la autorización de la consola, se pueden bloquear las entidades principales si las condiciones de la red están mal configuradas o si una política de control de servicios (SCP) o una política de control de recursos (RCP) existentes deniegan dichas acciones. AWS Sign-In Antes de activar la autorización de la consola, confirme que sus declaraciones de permiso son correctas y elimine o ajuste cualquier SCP o RCP que la deniegue, o. `signin:Authenticate` `signin:AuthorizeOAuth2Access` `signin:CreateOAuth2Token`

Para cuentas independientes:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

Para AWS Organizations:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-organization-id> \
  --region us-east-1
```

Verifique la configuración:

```
aws signin get-console-authorization-configuration \
  --target-id <your-target-id> \
  --region <your-region>
```

Elimine la configuración de autorización de la consola:

```
aws signin delete-console-authorization-configuration \
  --target-id <your-target-id> \
  --region us-east-1
```

Paso 3: Verifica tu política

Enumere todas las declaraciones de permiso:

```
aws signin list-resource-permission-statements \
  --max-results 50 \
  --region <your-region>
```

Recupere la política consolidada completa:

```
aws signin get-resource-policy \
  --region <your-region>
```

El `get-resource-policy` comando devuelve la política completa basada en los recursos, compuesta por todas las declaraciones de permiso. Revise esta política para confirmar que refleja los controles de acceso previstos antes de probar el acceso a la consola.

Disponibilidad regional

Las API de autorización de consolas están disponibles en todas las regiones AWS comerciales. Puede llamar a estas API desde cualquier región en la que opere.

> **Important**
>
> Las operaciones de escritura (`put-console-authorization-configurationput-resource-permission-statement`,`delete-console-authorization-configuration`,,`delete-resource-permission-statement`) se deben realizar en la `us-east-1` región. Las políticas creadas en `us-east-1` se replican automáticamente a nivel mundial. Las operaciones de lectura (`get-console-authorization-configurationlist-resource-permission-statements`,,`get-resource-policy`) se pueden realizar desde cualquier región.

Comprender la estructura de las políticas

AWS Sign-In las políticas contienen dos declaraciones que protegen las distintas fases del flujo de inicio de sesión en la consola:

- Pre-authentication declaración (Acción:**`signin:Authenticate`**): se evalúa cuando se recibe la solicitud de inicio de sesión, antes de que se complete la autenticación. La clave global no `aws:PrincipalArn` está disponible en esta fase porque la identidad del principal no está confirmada. En esta fase `signin:PrincipalArn` está disponible para eximir a directores específicos de las restricciones de la red. Network-based Las claves de condición están disponibles para su evaluación en esta fase.
- Post-authentication declaración (Acción:**`signin:AuthorizeOAuth2Access`**,**`signin:CreateOAuth2Token`**): se evalúa después de la autenticación, durante el intercambio del token de OAuth. Se usa `aws:PrincipalArn` para eximir a directores específicos. Todas las claves de condición basadas en la red y en la identidad están disponibles para su evaluación en esta fase.

Ambas declaraciones son obligatorias porque el inicio de sesión en la consola utiliza OAuth 2.0, que realiza las tres acciones de forma secuencial. Una política con una sola declaración deja desprotegida la otra fase. `signin:PrincipalArn`admite los tipos principales de usuario root, usuario de IAM y rol. `aws:PrincipalArn`admite todos los tipos principales (usuario root, usuario de IAM, usuario federado, rol).

Ejemplos de políticas

Ejemplo 1: RCP con perímetro de red y principales excluidos

La siguiente política de control de recursos (RCP) deniega el Consola de administración de AWS inicio de sesión desde fuera de la red corporativa en todas las cuentas de la organización. Los directores excluidos designados están exentos del acceso de emergencia. Dado que los ID de VPC son únicos solo dentro de una región, la política incluye una tercera declaración que fija el VPC-based acceso a la región esperada.

La `EnforceNetworkPerimeterPreAuth` declaración se utiliza `signin:PrincipalArn` para eximir a los directores excluidos durante la fase previa a la autenticación. La `EnforceNetworkPerimeterPostAuth` declaración se utiliza `aws:PrincipalArn` para eximir a los directores excluidos después de la autenticación. La `EnforceSourceVPCRegion` declaración garantiza que la región de la solicitud coincida con la región de la VPC, lo que restringe el acceso a la región esperada para la VPC especificada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceNetworkPerimeterPreAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
```

```
      }
    },
    {
      "Sid": "EnforceNetworkPerimeterPostAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceSourceVPCRegion",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "signin:Authenticate",
        "signin:CreateOAuth2Token",
        "signin:AuthorizeOAuth2Access"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceVpc": "<my-vpc>"
        },
        "StringNotEqualsIfExists": {
          "aws:RequestedRegion": "<my-vpc-region>"
        }
      }
    }
```

```
  ]
}
```

Esta política:

- Denega el acceso a la página de inicio de sesión a menos que la solicitud se origine en el rango de IP corporativas o en la VPC corporativa. Las cuentas raíz excluidas y los usuarios de IAM están exentos mediante la autenticación previa. `signin:PrincipalArn`
- Denega el intercambio de token de OAuth a menos que provenga del rango de IP corporativas o de una VPC. Las cuentas raíz, los usuarios de IAM y los roles excluidos están exentos mediante `aws:PrincipalArn` la clave global posterior a la autenticación.
- Si una solicitud proviene de la VPC especificada pero la región no coincide, se deniega el acceso. AWS Los ID de VPC son únicos dentro de una región y el mismo ID de VPC puede existir en diferentes regiones.
- Se aplica a nivel mundial en toda su organización de AWS cuando se configura como RCP.

Ejemplo 2: Resource-based política de IP-based acceso con principal excluido

La siguiente política basada en los recursos deniega el acceso a la consola a todos los principales que realicen solicitudes desde fuera del rango de IP especificado, con la excepción del principal excluido. La política contiene dos declaraciones: una declaración previa a la autenticación que utiliza la `signin:PrincipalArn` clave específica del servicio y una declaración posterior a la autenticación que utiliza la clave global. `aws:PrincipalArn`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
```

```
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    }
  ]
}
```

Esta política:

- Niega el acceso a todos los principales a menos que se conecten desde el rango de IP. `<my-corporate-cidr>`
- Exime al principal excluido de las restricciones de uso de la red `signin:PrincipalArn` (autenticación previa) y `aws:PrincipalArn` (posterior a la autenticación).
- Se aplica solo a la cuenta específica en la que está configurada la política basada en recursos (identificada por). `<my-aws-account-id>`

Prácticas recomendadas

Configure los principales excluidos para el acceso de recuperación de emergencia

AWS recomienda configurar al menos un usuario excluido antes de aplicar las políticas de autorización de la consola en producción. En la fase previa a la autenticación, la clave de `signin:PrincipalArn` condición exime al usuario raíz, al usuario de IAM y a los directores de rol. En la fase posterior a la autenticación, la clave de `aws:PrincipalArn` condición exime a todos los tipos principales (usuario raíz, usuario de IAM, usuario federado, rol).

Los principales excluidos son opcionales, pero omitirlos aumenta el riesgo de bloqueo de la cuenta si las condiciones de la red cambian inesperadamente o si las políticas están mal configuradas.

Pasos de configuración recomendados para el principal excluido:

1. Cree una función de IAM excluida (por ejemplo,). `BreakGlassRole`
2. Para las funciones excluidas, exija el MFA en la política de confianza de funciones.
3. Otorgue a la identidad excluida solo los permisos mínimos necesarios para la recuperación de emergencia.
4. Incluya el ARN principal excluido en las declaraciones de política de autenticación previa (`signin:PrincipalArn`) y posterior a la autenticación (`aws:PrincipalArn`).
5. Documente el procedimiento de recuperación y guárdelo de forma segura en el exterior. AWS
6. Pruebe periódicamente el acceso principal excluido para confirmar que funciona cuando sea necesario.

Mantenga las rutas de acceso de recuperación

Además del principio excluido descrito anteriormente, asegúrese de que haya métodos de acceso alternativos en caso de que las políticas de autorización de la consola bloqueen el inicio de sesión de forma inesperada:

- Role-based Acceso programático: las políticas de autorización de la consola se aplican únicamente al inicio de sesión interactivo en la consola. No se aplican a las solicitudes de API firmadas con SiGv4. Si tienes acceso mediante programación (por ejemplo, claves de acceso existentes o un rol multicuenta), úsalo para invocar la política de restricción

`signin:DeleteConsoleAuthorizationConfiguration` y eliminarla. Las credenciales deben incluir el `signin:DeleteConsoleAuthorizationConfiguration` permiso (incluido en la política `AWSSignInResourcePolicyManagement` gestionada). AWS recomienda las credenciales temporales en lugar de las claves de acceso de los usuarios de IAM a largo plazo. `OrganizationAccountAccessRole`En el caso de las cuentas de miembros, los administradores de las cuentas de administración pueden utilizar la cuenta de miembro (`aws sts assume-role`) para obtener estas credenciales temporales.

- AWS soporte de recuperación: mantenga actualizados el correo electrónico y el número de teléfono de su cuenta de usuario raíz. Si el acceso principal excluido y el acceso programático no están disponibles, AWS Support puede proporcionar un enlace al portal de recuperación tras la verificación de identidad. Consulte Se bloquea el acceso a mi cuenta después de activar la autorización de la consola para ver el proceso de recuperación completo.

Realice pruebas antes del despliegue en producción

AWS recomienda no adjuntar RCP restrictivos a la raíz de la organización sin comprobar exhaustivamente el impacto que la política tiene en las cuentas. En su lugar, cree una unidad organizativa a la que pueda mover sus cuentas de una en una, o al menos en pequeñas cantidades, para asegurarse de no bloquear inadvertidamente el acceso de los usuarios a las cuentas clave.

Flujo de trabajo de pruebas:

1. Cree una declaración de permiso única con las restricciones de su red principal.
2. Habilita la autorización de la consola en una cuenta que no sea de producción.
3. Pruebe el acceso a la consola desde las redes permitidas y denegadas.
4. Revisa CloudTrail los registros de Amazon para confirmar el comportamiento de evaluación de las políticas.
5. Pruebe el acceso con su principal excluido.
6. Amplíe gradualmente a redes y cuentas adicionales.
7. Supervise antes de implantar las cuentas de producción.

Diseñe con una defensa en profundidad

Utilice las políticas AWS Sign-In basadas en los recursos y las políticas de control de los recursos como una capa dentro de una estrategia de seguridad más amplia. AWS Sign-In las políticas

restringen el acceso a la consola en función de la ubicación de la red y la identidad principal. Combínelas con otros tipos de políticas para crear controles de acceso integrales:

- AWS Sign-In políticas (políticas basadas en recursos y RCP): restrinjan el acceso a la consola en función de la ubicación de la red y la identidad principal antes, durante y después de la autenticación.
- Políticas de IAM: controlan las acciones que pueden realizar los usuarios después de iniciar sesión.
- Políticas de control de servicios (SCP): aplican barreras de permisos en toda la organización a todas las entidades principales.
- Políticas de puntos de enlace de VPC: controle a qué servicios y cuentas se puede acceder a través de puntos de enlace de VPC.

Supervise y audite continuamente

AWS CloudTrail registra automáticamente todas las evaluaciones AWS Sign-In de políticas y los cambios de configuración. Vea estos eventos en el historial de CloudTrail eventos durante un máximo de 90 días. Para una retención más prolongada, envíe los eventos a Amazon S3 mediante la creación de una ruta (consulte Creación de una ruta). Para recibir alertas en tiempo real, crea EventBridge reglas de Amazon que coincidan con AWS Sign-In los eventos, configura tu ruta para que se entregue a un grupo de CloudWatch registros para las alarmas basadas en filtros de métricas o reenvía los eventos a tu solución SIEM existente.

Casos de uso

Control del perímetro de la red

Restrinja el acceso a la consola a las VPC corporativas o a los rangos de IP aprobados. Utilice políticas basadas en recursos para cuentas individuales o políticas de control de recursos (RCP) para aplicarlas en toda la organización y garantizar que los usuarios solo puedan iniciar sesión desde ubicaciones de red confiables, lo que evitará el acceso no autorizado desde redes públicas o que no sean de confianza.

Ejemplo de escenario: una empresa exige que todo el acceso a la consola provenga de su red corporativa o de VPC aprobadas. AWS Configuran una política basada en los recursos para una sola cuenta, o un RCP en toda la organización, que deniega el acceso desde todas las

demás redes y, al mismo tiempo, mantiene el acceso de recuperación de emergencia para los administradores de emergencia.

Requisitos de conformidad

Cumpla con los requisitos reglamentarios para los controles de acceso basados en la red. Muchos marcos de cumplimiento exigen que las organizaciones restrinjan el acceso a los sistemas confidenciales en función de la ubicación de la red. AWS Sign-In las políticas proporcionan controles auditables y aplicables que demuestran el cumplimiento de estos requisitos.

Ejemplo de escenario: una empresa de servicios financieros debe cumplir con las normas que exigen el acceso a la consola únicamente desde redes aprobadas. Utilizan los RCP para hacer cumplir las restricciones de red en toda la organización y mantener AWS CloudTrail los registros como prueba del cumplimiento.

Multi-account gobernanza

Implemente políticas de acceso a la consola coherentes en AWS Organizations. Utilice los RCP para hacer cumplir las restricciones de red estándar en todas las cuentas de los miembros, garantizando una postura de seguridad uniforme sin necesidad de una configuración individual a nivel de cuenta.

Ejemplo de escenario: una empresa con más de 100 AWS cuentas utiliza los RCP para aplicar una política que exige que todo el acceso a la consola se origine desde los puntos finales de VPC de su organización, lo que confirma la coherencia de los controles de red en todas las cuentas.

Third-party control de acceso

Conceda acceso temporal a la consola a socios o contratistas de redes específicas. Las organizaciones pueden crear un acceso a la consola por tiempo limitado y restringido por la red para terceros sin comprometer la postura general de seguridad.

Ejemplo de escenario: una empresa debe conceder a una consultora un acceso temporal a la consola. Crean una política basada en los recursos que permite el acceso solo desde los rangos de IP conocidos de la consultora y solo para las funciones de IAM asignadas a los consultores.

Restrinja el acceso a la consola a entidades principales específicas

Permita que solo un conjunto definido de directores inicie sesión en ella y deniegue a todos los demás Consola de administración de AWS, independientemente de la ubicación de la red. Esto resulta útil para los clientes que no utilizan puntos de conexión de VPC y desean restricciones

de consola basadas en la identidad. Los directores a los que se deniega el inicio de sesión en la consola conservan su acceso mediante programación; AWS Sign-In las políticas solo limitan el inicio de sesión en la consola y solo los directores a los que se exima pueden iniciar sesión.

Escenario de ejemplo: una empresa quiere que solo sus administradores usen la consola. Configuran un RCP que deniega el inicio de sesión en la consola a todos los principales, excepto a los ARN principales del administrador. Un rol de instancia de Amazon EC2 con credenciales válidas no puede iniciar sesión en la consola porque no es un principal exento, aunque conserva sus permisos de programación. Esto resuelve el caso habitual en el que las credenciales de rol de instancia se utilizan para iniciar sesión en la consola.

Solución de problemas con el control de acceso a

No puedo iniciar sesión debido a las condiciones de la red en las políticas Sign-in basadas en recursos

Es posible que veas uno de los siguientes mensajes de error cuando una AWS Sign-In política deniega el acceso:

- «La información de autenticación es incorrecta. Inténtelo de nuevo». (denegación de la autenticación previa mediante una política basada en los recursos)
- «Error de autenticación, solicitud no válida» (denegación de autenticación previa por parte del RCP)
- «Error de autenticación: para acceder a esta cuenta, inicie sesión desde una red diferente o póngase en contacto con el administrador para obtener más información» (denegación posterior a la autenticación)

Si ve alguno de estos errores y cree que debería permitirse el acceso, póngase en contacto con su AWS administrador. Pueden revisar CloudTrail los registros para ver si hay `ConsoleLogin` eventos con las `errorMessage` palabras «Autorización denegada debido a una política basada en recursos» o «Autorización denegada debido a una política de control de recursos» para identificar qué declaración de política denegó el acceso.

Causas posibles:

- La dirección IP de origen no se encuentra en el rango de CIDR permitido.

- No está conectado a la VPC o al punto final de VPC requerido.
- Está accediendo a un punto final de inicio de sesión regional que no coincide con la región prevista en la política.
- Su ARN principal no aparece correctamente en los principales excluidos de la póliza.
- La política se actualizó recientemente y el cambio aún no se ha aplicado a nivel mundial.

Solución:

- Compruebe que está conectado a la red corporativa o a la VPN.
- Confirme que está accediendo a través del punto de enlace de la VPC correcto si están configuradas las restricciones basadas en el punto de enlace de la VPC.
- Póngase en contacto con el AWS administrador para verificar la configuración de la política y confirmar qué redes están autorizadas.
- Si está configurado como principal excluido, compruebe que su ARN principal esté correctamente configurado en la lista de principales excluidos.
- Si se han realizado cambios en la política recientemente, espere unos minutos hasta que se complete la replicación global.

Para los administradores que estén diagnosticando este problema:

- Revise AWS CloudTrail los registros de los eventos de evaluación de políticas para identificar qué declaración de política denegó el acceso.
- Se utiliza `aws signin get-resource-policy` para revisar la configuración de la política actual.
- Compruebe que la ubicación de red del usuario coincide con las condiciones de la política.
- Confirme que los principales excluidos estén configurados correctamente si el usuario debe estar exento de las restricciones de la red.

Se bloquea el acceso a mi cuenta después de activar la autorización de la consola

Si configuraste la autorización de la consola y ya no puedes acceder a tu cuenta, es posible que no hayas configurado las entidades excluidas antes de aplicar la política.

Existen varias rutas para recuperar el acceso, según el tipo de cuenta y las credenciales disponibles.

Opción 1: usar el acceso programático (AWS CLI o SDK)

Las políticas de autorización de la consola se aplican únicamente al inicio de sesión en la consola interactiva. No se aplican a las solicitudes de API firmadas con SiGv4. Si tienes acceso mediante programación (por ejemplo, claves de acceso existentes o un rol multicuenta), úsalo para invocar la política de restricción `signin:DeleteConsoleAuthorizationConfiguration` y eliminarla. Las credenciales que utilice deben tener permiso para llamar. `signin:DeleteConsoleAuthorizationConfiguration` La política `AWSSignInResourcePolicyManagement` gestionada incluye este permiso. AWS recomienda las credenciales temporales en lugar de las claves de acceso de los usuarios de IAM a largo plazo. `OrganizationAccountAccessRole`En el caso de las cuentas de los miembros, los administradores de las cuentas de administración pueden utilizar la cuenta del miembro para obtener credenciales temporales. Este rol no se crea automáticamente en las cuentas que fueron invitadas a unirse a la organización.

```
aws signin delete-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

O elimina declaraciones de permiso específicas:

```
# First, list statements to get the statement ID
aws signin list-resource-permission-statements \
  --region us-east-1

# Then delete the problematic statement
aws signin delete-resource-permission-statement \
  --statement-id <statement-id> \
  --region us-east-1
```

Opción 2: Contactar con AWS Support

Si no tiene acceso programático y no puede usarlo `OrganizationAccountAccessRole` para acceder a la cuenta, póngase en contacto con AWS Support para iniciar el proceso de recuperación del bloqueo.

El proceso de recuperación funciona de la siguiente manera:

1. Si no puede resolver el problema con las opciones anteriores, abra un caso de soporte en el AWS Support Center. AWS Support verificará tu identidad antes de examinar tu cuenta. Los métodos de verificación pueden incluir confirmar la dirección de correo electrónico de la cuenta raíz del usuario, responder a una llamada telefónica de verificación o responder a las preguntas de seguridad de la cuenta.
2. AWS Support confirma que el problema de acceso a la consola se debe a un bloqueo de políticas basado en los recursos.
3. AWS Support comparte un enlace al portal de recuperación. Utilice este enlace para iniciar sesión con un responsable de IAM en la cuenta que tenga el `signin:DeleteConsoleAuthorizationConfiguration` permiso. Este permiso permite al director eliminar la configuración de autorización de la consola que provoca el bloqueo.

> **Important**
>
> El portal de recuperación elimina toda la configuración de autorización de la consola de la cuenta, incluidas todas las declaraciones de permisos de los recursos. El portal de recuperación no permite la reconfiguración de las políticas basadas en AWS Sign-In recursos.

El enlace al portal de recuperación caduca 72 horas después de que AWS Support lo comparta. Si no completa la recuperación dentro de ese período, póngase en contacto con AWS Support para reiniciar el proceso.

Tras recuperar el acceso:

- Revise y actualice sus declaraciones de permisos de recursos para incluir los principales excluidos configurados correctamente.
- Pruebe el acceso a la consola desde las redes esperadas antes de volver a habilitar la autorización de la consola.
- Documente sus procedimientos de recuperación para consultarlos en el futuro.

Los cambios que realizo no están siempre visibles inmediatamente

Los cambios de política se replican a nivel mundial, pero la replicación puede tardar unos minutos.

Solución:

- Espere unos minutos después de realizar los cambios de política para que se complete la replicación global.
- Verifique los cambios mediante el `get-resource-policy` comando:

```
aws signin get-resource-policy --region <your-region>
```

- Compruebe AWS CloudTrail los registros de eventos de evaluación de políticas para confirmar que se está evaluando la nueva política.
- Confirme que está utilizando la región correcta para sus operaciones (las operaciones de escritura deben utilizar`us-east-1`).
- Si utiliza condiciones basadas en puntos de enlace de VPC, compruebe que las políticas de puntos de enlace de VPC también estén configuradas correctamente.

Problemas comunes de replicación de políticas:

- Página de inicio de sesión en caché: los navegadores pueden almacenar en caché la página de inicio de sesión. Borra la memoria caché del navegador o usa una ventana de incógnito para probar los cambios en las políticas.
- Declaraciones contradictorias: si tiene varias declaraciones de permiso, confirme que no entren en conflicto entre sí. Se utiliza `get-resource-policy` para revisar la política consolidada.
- Políticas de punto final de VPC: las AWS Sign-In políticas funcionan en conjunto con las políticas de punto final de VPC. Ambas deben permitir el acceso deseado.

AWS Sign-In referencia de claves de condición

Esta página enumera las claves de condición que puede usar en las políticas AWS Sign-In basadas en recursos y en las políticas de control de recursos (RCP), y muestra la fase de evaluación y la acción a las que se aplica cada clave. Solo `signin:PrincipalArn` es específica de AWS Sign-In; las demás son claves de condición AWS globales. Para ver las definiciones de las claves globales, consulte las claves de contexto de las condiciones AWS globales.

Para ver la lista completa de acciones y claves de condición en la Referencia de autorización de servicio, consulte Acciones, recursos y claves de condición de AWS Sign-In.

Network-based claves de condición

Estas claves de condición comprueban el origen de la solicitud. AWS Sign-In las evalúa para todas AWS Sign-In las acciones (`signin:Authenticatesignin:Authorize0Auth2Access`, `ysignin:Create0Auth2Token`) tanto en las políticas basadas en recursos como en las RCP.

Network-based claves de condición

Clave de condición	Operadores	Description (Descripción)	Reglas de uso
`aws:SourceIp`	`IpAddress` , `NotIpAddress`	Dirección IP pública o rango de CIDR	No está presente cuando una solicitud utiliza un punto final de VPC. Usa `IfExists` operadores al combinarlos con VPC-based condiciones de la misma declaración.
`aws:SourceVpc`	`StringEquals` , `StringNotEquals`	ID DE VPC () `vpc-xxxxxxxx`	Solo está presente cuando una solicitud utiliza un punto final de VPC. Úselo con `aws:RequestedRegion` para evitar colisiones de ID de VPC entre regiones.

Clave de condición	Operadores	Description (Descripción)	Reglas de uso
`aws:SourceVpce`	`StringEquals` , `StringNotEquals`	ID de punto final de VPC () `vpce-xxxxxxxx`	Solo está presente cuando una solicitud utiliza un punto final de VPC.
`aws:VpcSourceIp`	`IpAddress` , `NotIpAddress`	IP privada dentro de la VPC	Utilice siempre la clave de `aws:VpcSourceIp` condición junto con las claves de `aws:SourceVpce` condición `aws:SourceVpc` o.
`aws:RequestedRegion`	`StringEquals` , `StringNotEquals`	Código de AWS región objetivo	Se recomienda cuando se usa `aws:SourceVpc` para evitar colisiones de ID de VPC entre regiones. Se pueden especificar varias regiones.

> **Important**
>
> Una sola solicitud contiene `aws:SourceIp` (red pública) o `aws:SourceVpc` (punto final de VPC), no ambos. Al redactar políticas de denegación a menos que cubran ambas rutas, utilice `IfExists` operadores (por ejemplo`NotIpAddressIfExists`) o cree declaraciones independientes.

Identity-based claves de condición

Estas claves de condición comprueban quién hace la solicitud. Solo están disponibles para las acciones posteriores a la autenticación

(`signin:AuthorizeOAuth2Accessysignin:CreateOAuth2Token`), en las que se ha establecido la identidad principal.

Identity-based claves de condición

Clave de condición	Operadores	Description (Descripción)	Ejemplos
`aws:PrincipalArn`	`ArnEquals` , `ArnLike`, `ArnNotEquals` , `StringEquals` , `StringLike`	ARN del principal de IAM autenticado	`arn:aws:iam::123456789012:user/alice` , `arn:aws:iam::123456789012:role/Admin`
`aws:PrincipalAccount`	`StringEquals` , `StringNotEquals`	AWS ID de cuenta del principal	`123456789012`

Service-specific clave de condición: inicio de sesión: PrincipalArn

La siguiente clave de condición es específica AWS Sign-In y no es una AWS clave global. Solo está disponible durante la evaluación previa a la autenticación. Se utiliza `signin:PrincipalArn` para identificar el inicio de sesión principal antes de que se complete la autenticación. Es el equivalente a la autenticación previa`aws:PrincipalArn`, que no está disponible hasta después de la autenticación.

Operadores

Operadores ARN (`ArnEquals`,, `ArnLikeArnNotEquals`,`ArnNotLike`) y operadores de cadena (`StringEquals`,`StringLike`).

Disponibilidad.

AWS Sign-In incluye esta clave en el contexto de la solicitud durante la fase previa a la autenticación (la `signin:Authenticate` acción). No está disponible para las acciones posteriores a la autenticación (`signin:AuthorizeOAuth2Accessysignin:CreateOAuth2Token`).

Tipo de datos:

ARN. Utilice operadores ARN en lugar de operadores de cadena.

Tipo de valor

Single-valued.

Compatible con

Resource-based políticas y RCP.

Utilice los operadores ARN para comparar valores. Puede especificar los siguientes tipos principales:

- Cuenta de AWS usuario root (`arn:aws:iam::123456789012:root`)
- Usuario de IAM () `arn:aws:iam::123456789012:user/`*`user-name`*
- Función de IAM () `arn:aws:iam::123456789012:role/`*`role-name`*

Caso de uso: eximir a una identidad principal excluida de las restricciones de la red, evitando el bloqueo y, al mismo tiempo, aplicando los controles de red para todos los demás intentos de acceso.

Ejemplo: denegar el acceso previo a la autenticación desde redes no autorizadas, excepto al usuario root:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
```

```
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

Esta política deniega el acceso a la consola desde fuera del rango de `203.0.113.0/24` IP, excepto al usuario raíz de la cuenta. La declaración de autenticación previa se utiliza `signin:PrincipalArn` para eximir al usuario raíz antes de que se complete la autenticación. La declaración posterior a la autenticación se utiliza `aws:PrincipalArn` para eximir al mismo principal después de la autenticación, durante el intercambio del token de OAuth. Consulte Ejemplos de políticas.

Condicione la disponibilidad de la clave por acción

Condicione la disponibilidad de las claves por acción

Clave de condición	Iniciar sesión: autenticarse	inicio de sesión: Authorize OAuth2Access	iniciar sesión: CreateOAuth2Token
`aws:SourceIp`	Sí	Sí	Sí
`aws:SourceVpc`	Sí	Sí	Sí

Clave de condición	Iniciar sesión: autenticarse	inicio de sesión: Authorize OAuth2Access	iniciar sesión: CreateOAuth2Token
`aws:SourceVpce`	Sí	Sí	Sí
`aws:VpcSourceIp`	Sí	Sí	Sí
`aws:RequestedRegion`	Sí	Sí	Sí
`aws:PrincipalArn`	–	Sí	Sí
`aws:PrincipalAccount`	–	Sí	Sí
`signin:PrincipalArn`	Sí	–	–

> **Note**
>
> La `signin:CreateAccount` acción se usa exclusivamente en las políticas de puntos finales de la VPC para el acceso privado a la consola y no está disponible para las políticas basadas en recursos o los RCP. No está asociada a ninguna clave de condición específica del servicio. Consulte Acceso privado a la consola.

Información relacionada

- Control del acceso a la consola con políticas basadas en recursos y políticas de control de recursos
- Consola de administración de AWS Acceso privado
- Claves de contexto de condición global de AWS
- Claves de condiciones, recursos y acciones para AWS Sign-In

Inicia sesión en tu AWS acceda al portal

Un usuario del Centro de Identidad de IAM es miembro de AWS Organizations. Un usuario del Centro de Identidad de IAM puede acceder a múltiples aplicaciones Cuentas de AWS y aplicaciones empresariales iniciando sesión en su portal de AWS acceso con una URL de inicio de sesión específica. Para obtener más información acerca de las URL de inicio de sesión específicas, consulte AWS portal de acceso.

Antes de iniciar sesión Cuenta de AWS como usuario en el Centro de identidades de IAM, recopile la siguiente información obligatoria.

- Nombre de usuario de empresa
- Contraseña de empresa
- URL de inicio de sesión específica

> **Note**
>
> Una vez que inicie sesión, su sesión en el portal de AWS acceso será válida durante 8 horas. Una vez transcurridas esas 8 horas, deberá volver a iniciar sesión.

Para iniciar sesión en su AWS acceder al portal

1. En la ventana del navegador, pega la URL de inicio de sesión que te proporcionaron por correo electrónico, por ejemplo, `https://your_subdomain.awsapps.com/start` o el formato de URL de doble pila. `https://[IAM Identity Center instance ID].portal.[Region].app.aws` A continuación, pulse Intro.
2. Inicie sesión con sus credenciales de empresa (como un nombre de usuario y una contraseña).

> **Note**
>
> Si el administrador le envió una contraseña de un solo uso (OTP) por correo electrónico y es la primera vez que inicia sesión, escriba esa contraseña. Una vez que haya iniciado sesión, debe crear una contraseña nueva para poder acceder en el futuro.

3. Si se le pide un código de verificación, compruebe su correo electrónico. A continuación, copie y pegue el código en la página de inicio de sesión.

> **Note**
>
> Los códigos de verificación suelen enviarse por correo electrónico, pero el método de entrega puede variar. Si no ha recibido ninguno en su correo electrónico, póngase en contacto con el administrador para obtener más información sobre el código de verificación.

4. Si la MFA está habilitada para su usuario en IAM Identity Center, debe autenticarse con ella.
5. Tras la autenticación, podrá acceder a cualquier Cuenta de AWS aplicación que aparezca en el portal.

   a. Para iniciar sesión, Consola de administración de AWS elija la pestaña Cuentas y seleccione la cuenta individual que desee administrar.

      Aparece el rol de usuario. Elija el nombre del rol de la cuenta para abrir la Consola de administración de AWS. Elija Claves de acceso para obtener credenciales de acceso a la línea de comandos o mediante programación.

   b. Elija la pestaña Aplicaciones para ver las aplicaciones disponibles y seleccione el icono de la aplicación a la que desea acceder.

Al iniciar sesión como usuario en IAM Identity Center, obtendrá credenciales para acceder a los recursos durante un período de tiempo determinado, denominado sesión. De forma predeterminada, la sesión de un usuario en una Cuenta de AWS puede durar 8 horas. El administrador de IAM Identity Center puede especificar una duración diferente, que puede oscilar entre un mínimo de 15 minutos y un máximo de 90 días. Una vez finalizada la sesión, podrá iniciar sesión de nuevo.

Información adicional

Si desea obtener más información sobre los usuarios de IAM Identity Center, consulte los siguientes recursos.

- Para obtener una descripción general de IAM Identity Center, consulte ¿Qué es IAM Identity Center?
- Para obtener más información sobre su portal de AWS acceso, consulte Uso del portal de AWS acceso.

- Para obtener más información sobre las sesiones del IAM Identity Center, consulte Autenticaciones de usuarios.
- Para obtener instrucciones paso a paso sobre cómo restablecer la contraseña de usuario de IAM Identity Center, consulte He olvidado la contraseña del Centro de Identidad de IAM para mi Cuenta de AWS.
- Si usted o su organización implementan el filtrado de IP o dominio, es posible que necesite permitir que los dominios de la lista creen y usen su portal de AWS acceso. El IAM Identity Center admite puntos de conexión IPv4 y de doble pila. Si su red utiliza IPv6, utilice los dominios de punto final de doble pila. Para obtener más información sobre cómo permitir la inclusión de dominios en la lista, consulte Dominios para agregar a la lista de permitidos.

Inicie sesión a través del AWS Command Line Interface

Debe establecer cómo se AWS CLI autentica con AWS. Elija el método que mejor se adapte a sus requisitos de flujo de trabajo y seguridad.

- Inicie sesión con las credenciales de la consola (recomendado)si utiliza usuarios root, usuarios de IAM o una federación con IAM para el acceso a la AWS cuenta.
- Inicie sesión con las credenciales del IAM Identity Centersi usa Identity Center para acceder a la AWS cuenta.

Inicie sesión con las credenciales de la consola (recomendado)

Este método de autenticación le permite utilizar las credenciales de la consola con el AWS CLI, lo que facilita el inicio AWS mediante programación en cuestión de minutos después de configurar la cuenta. Puede obtener credenciales temporales que funcionan sin problemas en herramientas de desarrollo local como AWS CLI, y AWS SDKs . Herramientas de AWS para PowerShell

Requisitos previos

- Instale el AWS CLI. Para obtener más información, consulte Instalación o actualización de la versión más reciente de la AWS CLI. Se requiere una versión mínima de 2.32.0 para usar el comando `aws login`.
- Acceda para iniciar sesión Consola de administración de AWS como usuario root, usuario de IAM o mediante una federación con IAM. Si utiliza IAM Identity Center, vaya a Inicie sesión con las credenciales del IAM Identity Center en su lugar.
- Asegúrese de que la identidad de IAM tiene los permisos adecuados. Adjunta la política SignInLocalDevelopmentAccessgestionada a tu usuario, rol o grupo de IAM. Si inicia sesión como usuario raíz, no se requieren permisos adicionales.

Para iniciar sesión con las credenciales de la consola

1. Ejecute el siguiente comando para iniciar el proceso de autenticación basado en el navegador:

   ```
   $ aws login
   ```

   El `aws login` comando admite varios parámetros opcionales:

- `aws login --remote`- Para la autenticación multidispositivo cuando el dispositivo no es compatible con un navegador

> **Note**
>
> Puede controlar el acceso a la autenticación en el mismo dispositivo (`aws login`) y en varios dispositivos (`aws login --remote`). Utilice el siguiente recurso ARNs en cualquier política de IAM pertinente.
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost`: utilice este ARN para la autenticación en el mismo dispositivo con `aws login`.
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote`: utilice este ARN para la autenticación entre dispositivos con `aws login --remote`.

- `aws login --profile profile-name`- Para autenticarse con un perfil específico
- `aws login --region region`- Para autenticarse en una región específica

2. Sigue las instrucciones de tu terminal. El comando abrirá automáticamente tu navegador predeterminado y te guiará a través del proceso de autenticación. Tras la autenticación correcta, la AWS CLI sesión será válida durante un máximo de 12 horas.
3. Para finalizar la sesión, utilice:

```
$ aws logout
```

Si accede a los AWS servicios mediante programación mediante el uso de AWS Herramientas de AWS para PowerShell, consulte Autenticación de las herramientas de AWS con PowerShell AWS. Si lo utiliza AWS SDKs, consulte Autenticación y acceso mediante AWS SDKs y herramientas.

Inicie sesión con las credenciales del IAM Identity Center

El portal de AWS acceso facilita a los usuarios del Centro de Identidad de IAM la selección Cuenta de AWS y la obtención de credenciales de seguridad temporales para el. AWS CLI Para obtener más información sobre cómo obtener estas credenciales, consulte Disponibilidad regional para ID de creador de AWS. También puede configurarlo para autenticar a los usuarios AWS CLI directamente con el Centro de identidades de IAM.

Para iniciar sesión con las credenciales del IAM Identity Center

1. Compruebe que cumple los Requisitos previos.
2. Si es la primera vez que inicia sesión, configure su perfil con el asistente de `aws configure sso`.
3. Tras configurar el perfil, ejecute el siguiente comando y, a continuación, siga las instrucciones del terminal:

```
$ aws sso login --profile my-profile
```

Información adicional

Si quieres obtener más información sobre cómo iniciar sesión mediante la línea de comandos, consulta los siguientes recursos.

- Para obtener más información sobre el uso de las credenciales de la consola para iniciar sesión en el desarrollo AWS local, consulte Credenciales de autenticación y acceso para la AWS CLI.
- Para obtener más información sobre el proceso de AWS CLI inicio de sesión, consulte Autenticación con credenciales de corta duración para el. AWS CLI
- Para obtener más información sobre la configuración del Centro de Identidad de IAM, consulte Configuración del Centro de Identidad de IAM AWS CLI para usar el Centro de Identidad de IAM.

Inicie sesión como una identidad federada

Una identidad federada es un usuario que puede acceder a Cuenta de AWS recursos seguros con identidades externas. Las identidades externas pueden proceder de un almacén de identidades corporativas (por ejemplo, LDAP o Windows Active Directory) o de un tercero (como Login with Amazon, Facebook o Google). Las identidades federadas no inician sesión en el portal Consola de administración de AWS ni AWS acceden a él. El tipo de identidad externa que se utilice determina la manera en que inician sesión las identidades federadas.

Los administradores deben crear una URL personalizada que incluya `https://signin.aws.amazon.com/federation`. Para obtener más información, consulte Cómo habilitar el acceso del agente de identidades personalizado a la Consola de administración de AWS.

> **Note**
>
> Su administrador crea las identidades federadas. Póngase en contacto con su administrador para obtener más información sobre cómo iniciar sesión como una identidad federada.

Para obtener más información acerca de las identidades federadas, consulte Acerca de la federación de identidades en la web.

Inicia sesión con ID de creador de AWS

ID de creador de AWS es un perfil personal que proporciona acceso a herramientas y servicios seleccionados, como Amazon CodeCatalyst, Amazon Q Developer Formación de AWS y Certification. ID de creador de AWS lo representa como individuo y es independiente de las credenciales y los datos que pueda tener en AWS las cuentas existentes. Al igual que otros perfiles personales, ID de creador de AWS permanece contigo a medida que avanzas en tus objetivos personales, educativos y profesionales.

ID de creador de AWS Complementa cualquier Cuentas de AWS cosa que ya tengas o quieras crear. Si bien a Cuenta de AWS actúa como contenedor de los AWS recursos que usted crea y proporciona un límite de seguridad para esos recursos, usted lo ID de creador de AWS representa como individuo. Para obtener más información, consulte ID de creador de AWS y otras AWS credenciales.

ID de creador de AWS es gratis. Solo pagas por los AWS recursos que consumes en tu Cuentas de AWS. Para obtener más información sobre los precios, consulte Precios de AWS.

Si usted o la organización implementan el filtrado de IP o dominios, es posible que tenga que incluir dominios en la lista de permitidos para crear y utilizar un ID de creador de AWS. Para obtener más información sobre cómo permitir la inclusión de dominios en la lista, consulte Dominios para agregar a la lista de permitidos.

> **Note**
>
> AWS Builder ID es independiente de su suscripción a AWS Skill Builder, un centro de aprendizaje en línea donde puede aprender de AWS expertos y desarrollar sus habilidades en la nube en línea. Para obtener más información sobre AWS Skill Builder, consulte AWS Skill Builder.

Temas

- Edita tu ID de creador de AWS perfil
- Cambia tu ID de creador de AWS contraseña
- Elimine todas las sesiones activas de su ID de creador de AWS
- Elimine su ID de creador de AWS
- Gestione la autenticación ID de creador de AWS multifactor (MFA)
- Privacidad y datos en ID de creador de AWS
- ID de creador de AWS y otras AWS credenciales

Para iniciar sesión con ID de creador de AWS

1. Navegue hasta el ID de creador de AWS perfil o la página de inicio de sesión de la AWS herramienta o servicio al que desee acceder. Por ejemplo, para acceder a Amazon CodeCatalyst, vaya ahttps://codecatalyst.aws.
2. Elige cómo iniciar sesión en tu ID de creador de AWS
   - Ya poseo una cuenta existente
   - Tengo una cuenta de Google
   - Tengo una cuenta de Apple
   - Tengo una GitHub cuenta
   - Tengo una cuenta de Amazon

Ya poseo una cuenta existente

1. En el caso de las cuentas existentes, introduce el correo electrónico que utilizaste para crear la tuya ID de creador de AWS y selecciona Iniciar sesión.
2. Introduce el correo electrónico que utilizaste para crear la tuya ID de creador de AWS y selecciona Iniciar sesión.
3. En la página Iniciar sesión con su ID de creador de AWS, ingrese su contraseña.
4. (Opcional) Si desea que al iniciar sesión en este dispositivo en el futuro no se solicite una verificación adicional, marque la casilla situada junto a Este es un dispositivo de confianza.
5. Elija Continuar.
6. Si aparece una página indicando que Se requiere verificación adicional, siga las instrucciones de su navegador para proporcionar el código o la clave de seguridad necesarios.

> **Note**
>
> Para su seguridad, analizamos el navegador, la ubicación y el dispositivo de inicio de sesión. Si nos indica que debemos confiar en este dispositivo, no tendrá que proporcionar un código de autenticación multifactor (MFA) cada vez que inicie sesión. Para obtener más información, consulte Dispositivos de confianza.

Tengo una cuenta de Google

Si tu cuenta de Google ya está asociada a una ID de creador de AWS, debes usar una dirección de correo electrónico diferente para iniciar sesión en una aplicación. Para obtener más información, consulte No puedo iniciar sesión con Google.

1. Para usar tu cuenta de Google para iniciar sesión ID de creador de AWS, selecciona Continuar con Google.
2. En la página Iniciar sesión con Google, introduce la información de tu cuenta de Google para iniciar sesión.
3. Selecciona Continuar para cargar la página de inicio AWS de la aplicación.

Tengo una cuenta de Apple

Si tu cuenta de Apple ya está asociada a una ID de creador de AWS, debes usar una dirección de correo electrónico diferente para iniciar sesión en una aplicación. Para obtener más información, consulte No puedo iniciar sesión con Apple.

1. Para usar tu cuenta de Apple para iniciar sesión ID de creador de AWS, selecciona Continuar con Apple.
2. En la página Iniciar sesión con Apple, introduce la información de tu cuenta de Apple para iniciar sesión.
3. Selecciona Continuar para cargar la página de inicio AWS de la aplicación.

Tengo una GitHub cuenta

Si su GitHub cuenta ya está asociada a una ID de creador de AWS, debe utilizar una dirección de correo electrónico diferente para iniciar sesión en una solicitud. Para obtener más información, consulte No puedo iniciar sesión con GitHub.

1. Para usar tu GitHub cuenta para iniciar sesión ID de creador de AWS, selecciona Continuar con GitHub.
2. En la GitHub página Iniciar sesión con, introduce la información de tu GitHub cuenta para iniciar sesión.
3. Selecciona Continuar para cargar la página de inicio AWS de la aplicación.

Tengo una cuenta de Amazon

Si tu cuenta de Amazon ya está asociada a una ID de creador de AWS, debes usar una dirección de correo electrónico diferente para iniciar sesión en una aplicación. Para obtener más información, consulte No puedo iniciar sesión con Amazon.

1. Para usar tu cuenta de Amazon para iniciar sesión ID de creador de AWS, selecciona Continuar con Amazon.
2. En la página Iniciar sesión con Amazon, introduce la información de tu cuenta de Amazon para iniciar sesión.
3. Selecciona Continuar para cargar la página de inicio AWS de la aplicación.

Disponibilidad regional para ID de creador de AWS

ID de creador de AWS está disponible en las siguientes ubicaciones Regiones de AWS. Las aplicaciones que utilice ID de creador de AWS pueden funcionar en otras regiones.

Name	Código
Este de EE. UU. (Norte de Virginia)	us-east-1

Crea tu ID de creador de AWS

Usted crea el suyo ID de creador de AWS al suscribirse a una de las AWS herramientas y servicios que lo utilizan. Regístrese con su dirección de correo electrónico, nombre y contraseña como parte del proceso de registro en una AWS herramienta o servicio.

La contraseña debe cumplir los siguientes requisitos:

- 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.

> **Note**
>
> Las herramientas y los servicios que utilizas ID de creador de AWS te permiten crear y usar los tuyos ID de creador de AWS cuando los necesites.

Para crear tu ID de creador de AWS

1. Navegue hasta el ID de creador de AWS perfil o la página de registro de la AWS herramienta o servicio al que desee acceder. Por ejemplo, para acceder a Amazon CodeCatalyst, vaya ahttps://codecatalyst.aws.
2. Elige cómo crear tu ID de creador de AWS
   - Para usar tu cuenta de Google, selecciona Continuar con Google y sigue las instrucciones para completar el proceso de registro. Esto omite los pasos 3 a 8 que se indican a continuación. Ve al paso 9.

- Para usar tu cuenta de Apple, selecciona Continuar con Apple y sigue las instrucciones para completar el proceso de registro. Esto omite los pasos 3 a 8 que se indican a continuación. Ve al paso 9.

  > **Note**
  >
  > Si decides activar la función «Ocultar mi correo electrónico» de iCloud+ para iniciar sesión con Apple, se te creará con la dirección de Ocultar mi correo electrónico indicada en tu ID de creador de AWS cuenta de Apple en lugar de con tu dirección de correo electrónico real. No podrás cambiar esta dirección de correo electrónico, pero tu nombre y apellidos seguirán siendo editables. Si necesitas iniciar sesión ID de creador de AWS, debes usar tu dirección de Hide My Email. ID de creador de AWS utilizará tu dirección de Hide My Email para enviarte comunicaciones por correo electrónico. Para obtener más información, consulta Cómo usar Ocultar mi correo electrónico con el inicio de sesión con Apple.

- Para usar tu GitHub cuenta, selecciona Continuar con GitHub y sigue las instrucciones para completar el proceso de registro. Esto omite los pasos 3 a 8 que se indican a continuación. Ve al paso 9.
- Para usar tu cuenta de Amazon, selecciona Continuar con Amazon y sigue las instrucciones para completar el proceso de registro. Esto omite los pasos 3 a 8 que se indican a continuación. Ve al paso 9.
- Para crear una cuenta con correo electrónico y contraseña, continúe con los siguientes pasos.

3. En la página Crear ID de creador de AWS, introduzca Su dirección de correo electrónico. Le recomendamos que utilice un correo electrónico personal.
4. Elija Siguiente.
5. Escriba Su nombre y, a continuación, elija Siguiente.
6. En la página de Verificación del correo electrónico, introduzca el código de verificación que le enviamos a su dirección de correo electrónico. Seleccione Verificar. En función de su proveedor de correo electrónico, es posible que el mensaje tarde unos minutos en recibirse. Busque el código en sus carpetas de correo no deseado y spam. Si no ves el correo electrónico AWS transcurrido cinco minutos, selecciona Reenviar código.
7. Después de verificar su correo electrónico, en la página Elija una contraseña, introduzca una Contraseña y Confirme la contraseña.

8. Si aparece un captcha como medida de seguridad adicional, introduzca los caracteres que aparecen.
9. Seleccione Crear ID de creador de AWS.

Dispositivos de confianza

Después de seleccionar la opción Este es un dispositivo de confianza en la página de inicio de sesión, consideraremos que todos los inicios de sesión futuros desde ese navegador web en ese dispositivo están autorizados, con lo que no tendrá que proporcionar en él un código MFA. Sin embargo, si su navegador, las cookies o la dirección IP cambian, es posible que deba usar su código MFA para llevar a cabo una verificación adicional.

AWS herramientas y servicios que utilizan ID de creador de AWS

Puede iniciar sesión con su cuenta ID de creador de AWS para acceder a las siguientes AWS herramientas y servicios. El acceso a las capacidades o beneficios que se ofrecen por un cargo requiere un Cuenta de AWS.

De forma predeterminada, cuando inicias sesión en una AWS herramienta o servicio con tu ID de creador de AWS, la duración de la sesión es de 30 días, excepto para Amazon Q Developer, que tiene una duración de sesión de 90 días. Una vez finalizada la sesión, deberá iniciar sesión de nuevo.

AWS Comunidad en la nube

Community.aws es una plataforma creada por y para la comunidad de AWS creadores a la que puede acceder con su. ID de creador de AWS Es el lugar ideal para descubrir contenidos educativos, compartir ideas y proyectos personales, comentar las publicaciones de otros y seguir a sus creadores favoritos.

Amazon CodeCatalyst

ID de creador de AWS Cuando comiences a usar Amazon, crearás un alias CodeCatalyst y elegirás un alias que se asociará a actividades como problemas, confirmaciones de código y solicitudes de cambios. Invita a otras personas a tu CodeCatalyst espacio de Amazon, que incluye las herramientas, la infraestructura y los entornos que tu equipo necesita para crear tu próximo proyecto exitoso. Necesitarás Cuenta de AWS implementar un nuevo proyecto en la nube.

AWS Migration Hub

Acceda AWS Migration Hub(Migration Hub) con su ID de creador de AWS. Migration Hub ofrece un único lugar para descubrir los servidores existentes, planificar migraciones y realizar un seguimiento del estado de cada una de las migraciones de aplicaciones.

Amazon Q Developer

Amazon Q Developer es un asistente conversacional generativo basado en inteligencia artificial que puede ayudarlo a comprender, crear, ampliar y operar aplicaciones. AWS Para obtener más información, consulte ¿Qué es Amazon Q Developer? en la Guía del usuario de Amazon Q Developer.

AWS re:Post

AWS re:Post le proporciona orientación técnica para que pueda innovar más rápido y mejorar la eficiencia operativa mediante los servicios de AWS . Puedes iniciar sesión con tu comunidad ID de creador de AWS y unirte a la comunidad de Re:post sin necesidad de una tarjeta de crédito. Cuenta de AWS

AWS Startups

ID de creador de AWS Utilízalo para unirte a AWS Startups, donde podrás utilizar el contenido de aprendizaje, las herramientas, los recursos y el apoyo para hacer crecer tu empresa emergente AWS.

Formación de AWS y certificación

Puede utilizar su certificación ID de creador de AWS para acceder Formación de AWS a una certificación, donde podrá desarrollar sus Nube de AWS habilidades con AWS Skill Builder, aprender de AWS los expertos y validar su experiencia en la nube con una credencial reconocida en el sector.

Kiro

Kiro es un IDE de agencia que le ayuda a pasar del prototipo a la producción con un desarrollo basado en especificaciones. Desde tareas sencillas a complejas, Kiro trabaja junto a usted para convertir las peticiones en especificaciones detalladas y, después, en código de trabajo, documentos y pruebas. Con Kiro, lo que construye es exactamente lo que desea, y está listo para compartirlo con el equipo. Los agentes de Kiro ayudan a resolver problemas complejos y a automatizar tareas tales como la generación de documentación y las pruebas unitarias. Con Kiro, puede construir más allá de los prototipos y, al mismo tiempo, controlar cada etapa del proceso.

Portal de registro de sitios web (WRP)

Puede utilizar su ID de creador de AWS identidad de cliente permanente y su perfil de registro para el sitio web de AWS marketing. Para registrarse en nuevos seminarios web y ver todos los seminarios web a los que se ha registrado o a los que ha asistido, consulte Mis seminarios web.

Edita tu ID de creador de AWS perfil

Puede cambiar la información de su perfil en cualquier momento. Puedes editar la dirección de correo electrónico y el nombre que utilizaste para crear una ID de creador de AWS, así como tu apodo. Al utilizar inicios de sesión en redes sociales como Google o Apple, solo se pueden editar el nombre y el apodo.

Su Nombre es el que se usará para dirigirse a usted en las herramientas y servicios cuando interactúe con otras personas. Tu apodo indica cómo quieres que te conozcan tus amigos y otras personas con las que colaboras estrechamente. AWS

> **Note**
>
> Las herramientas y los servicios que ID de creador de AWS utilizas te permiten crear y usar el tuyo ID de creador de AWS cuando lo necesites.

Para editar la información de su perfil

1. Inicie sesión en su ID de creador de AWS perfil enhttps://profile.aws.amazon.com.
2. Seleccione Mis datos.
3. En la página Mis datos, seleccione el botón Editar situado junto a Perfil.
4. En la página Editar perfil, realice los cambios que desee en su Nombre y Apodo.
5. Elija Guardar cambios. Un mensaje de confirmación verde aparece en la parte superior de la página para indicarle que ha actualizado su perfil.

> **Note**
>
> Si cambia su nombre y apodo con uno de nuestros otros socios de inicio de sesión, no se actualizarán los mismos ajustes de su ID de creador de AWS.

Para editar la información de contacto

1. Inicie sesión en su ID de creador de AWS perfil enhttps://profile.aws.amazon.com.
2. Seleccione Mis datos.
3. En la página Mis datos, seleccione el botón Editar situado junto a Información de contacto.
4. En la página Editar información de contacto, cambie su Dirección de correo electrónico.
5. Seleccione Verificar correo electrónico. Aparecerá un cuadro de diálogo.
6. En el cuadro de diálogo Verificar correo electrónico, después de recibir el código en el correo electrónico, introdúzcalo en Código de verificación. Seleccione Verificar.

Cambia tu ID de creador de AWS contraseña

La contraseña debe cumplir los siguientes requisitos:

- 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.

> **Note**
>
> Los cambios de contraseña no están disponibles para ID de creador de AWS las cuentas que utilizan inicios de sesión en redes sociales, como Google o Apple. Si iniciaste sesión con un inicio de sesión social, administrarás tu contraseña a través de tu cuenta de inicio de sesión social. Para cambiar la contraseña de un inicio de sesión en una red social, sigue estos pasos:
>
> - Para una cuenta de Google, consulta Cambiar o restablecer tu contraseña (de Google).
> - Para una cuenta de Apple, consulta Cambiar la contraseña de tu cuenta de Apple.
> - Para crear una GitHub cuenta, consulta Actualizar tus credenciales de GitHub acceso.

- Para una cuenta de Amazon, consulta Cómo cambiar la contraseña de Amazon.

Para cambiar tu ID de creador de AWS contraseña

1. Inicia sesión en tu ID de creador de AWS perfil enhttps://profile.aws.amazon.com.
2. Elija Seguridad.
3. En la página Seguridad, seleccione Cambiar contraseña. Esto le llevará a una nueva página.
4. En la página Vuelva a introducir su contraseña, en la sección Contraseña, introduzca su contraseña actual. A continuación, seleccione Iniciar sesión.
5. En la página Cambiar contraseña, en la sección Nueva contraseña, introduzca la nueva contraseña que desee usar. A continuación, en la sección Confirmar contraseña, vuelva a escribir la nueva contraseña que desea usar.
6. Elija Cambiar contraseña. Se le redirigirá a su perfil de ID de creador de AWS .

Elimine todas las sesiones activas de su ID de creador de AWS

En Dispositivos con sesión iniciada, puede ver todos los dispositivos en los que tiene una sesión iniciada en este momento. Si no reconoce un dispositivo, como práctica recomendada de seguridad, cambie su contraseña antes de nada y, a continuación, cierre sesión en todas partes. Puede cerrar sesión en todos los dispositivos cerrando todas las sesiones activas en la página Seguridad de su ID de creador de AWS.

> **Note**
>
> ID de creador de AWS admite sesiones ampliadas de 90 días para Amazon Q Developer en un IDE. Podrá ver dos entradas de sesión por cada nuevo inicio de sesión en el IDE. Tras cerrar sesión del IDE, es posible que aún aparezcan sesiones del IDE en la lista de Dispositivos conectados, aunque ya no sean válidas. Estas sesiones desaparecerán una vez transcurridos los 90 días.

Para eliminar todas las sesiones activas

1. Inicie sesión en su ID de creador de AWS perfil enhttps://profile.aws.amazon.com.
2. Elija Seguridad.

3. En la página Seguridad, seleccione Eliminar todas las sesiones activas.
4. En el cuadro de diálogo Eliminar todas las sesiones, seleccione Eliminar todo. Al eliminar todas tus sesiones, cierras sesión en todos los dispositivos en los que hayas iniciado sesión con tu navegador ID de creador de AWS, incluidos los distintos navegadores. A continuación, seleccione Eliminar todas las sesiones.

> **Note**
>
> Al utilizar una cuenta de inicio de sesión social como Google o Apple, al eliminar ID de creador de AWS las sesiones activas no se cerrará la sesión de su cuenta de inicio de sesión social.

Elimine su ID de creador de AWS

El siguiente procedimiento describe cómo eliminar su ID de creador de AWS cuenta.

> **Warning**
>
> Si eliminas la tuya, se ID de creador de AWS producirá lo siguiente:
>
> - Pérdida de acceso: ya no puede acceder a AWS las herramientas y servicios a los que accedía anteriormente ID de creador de AWS. ID de creador de AWS La suya es independiente de cualquier AWS cuenta que pueda tener, y la eliminación de la suya no ID de creador de AWS cerrará su AWS cuenta.
> - Eliminación de contenido: se ID de creador de AWS eliminará cualquier contenido restante que esté asociado únicamente a usted y ya no podrá acceder a él ni recuperarlo de las aplicaciones que utilicen su ID de creador de AWS.
> - Eliminación de información personal: se eliminará cualquier información personal que haya proporcionado en relación con su ID de creador de AWS creación y administración, excepto si se conserva la información personal según lo exija o permita la ley, como los registros de su solicitud de eliminación o los datos en un formulario que no lo identifique. AWS
>
>   Puede obtener más información sobre cómo gestionamos su información en el Aviso de privacidad de AWS. Puede actualizar sus preferencias de AWS comunicación o cancelar la suscripción visitando el Centro de preferencias de comunicaciones de AWS.

- Las cuentas de inicio de sesión social permanecen sin cambios: si utiliza un inicio de sesión social, como Google o Apple, al eliminarlas ID de creador de AWS no se elimina nada relacionado con su cuenta de inicio de sesión social. Consulta la documentación de tu proveedor de acceso a redes sociales para obtener información sobre cómo eliminar esas cuentas. Si eliminas la ID de creador de AWS conexión de tu cuenta de inicio de sesión en una red social, no se elimina la ID de creador de AWS cuenta, pero ya no podrás acceder a tu ID de creador de AWS perfil.

Para eliminar tu ID de creador de AWS

1. Inicia sesión en tu ID de creador de AWS perfil enhttps://profile.aws.amazon.com.
2. Seleccione Privacidad y datos.
3. En la página Privacidad y datos, en la sección Eliminar ID de creador de AWS, seleccione Eliminar ID de creador de AWS.
4. Seleccione la casilla de verificación situada junto a cada aviso de exención de responsabilidad para confirmar que está listo para continuar.
5. Elija Eliminar ID de creador de AWS.

Gestione la autenticación ID de creador de AWS multifactor (MFA)

La autenticación multifactor (MFA) es un mecanismo simple y eficaz para mejorar la seguridad. El primer factor, 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 su ID de creador de AWS.

Puede registrar un autenticador integrado y también una clave de seguridad que guarde en un lugar físico seguro. Si no puede utilizar el autenticador integrado, puede utilizar su clave de seguridad registrada. En el caso de las aplicaciones de autenticación, también puede habilitar la característica de copia de seguridad o sincronización en la nube en esas aplicaciones. Este sistema lo ayuda a evitar que pierda el acceso a su perfil si extravía su dispositivo MFA o este se rompe.

Puntos clave

- Le recomendamos que registre varios dispositivos MFA. Si pierde el acceso a todos los dispositivos MFA registrados, no podrá recuperar su ID de creador de AWS.
- Le recomendamos que revise periódicamente sus dispositivos MFA registrados para asegurarse de que están actualizados y funcionan. Además, debe guardar esos dispositivos en un lugar que sea físicamente seguro cuando no los utilice.
- Si creó su cuenta mediante Continuar con Google, puede habilitar la autenticación multifactorial a través de su cuenta de Google. Para obtener más información, consulte Cómo activar la verificación en dos pasos.
- Si creaste tu cuenta con Continuar con Apple, es probable que la autenticación multifactorial ya esté habilitada en tu cuenta de Apple. Si no es así, para obtener más información sobre cómo activarla, consulta Autenticación de dos factores para la cuenta de Apple.
- Si creaste tu cuenta con Continuar con GitHub, puedes habilitar la autenticación multifactorial a través de tu GitHub cuenta. Para obtener más información, consulte Configurar (GitHub) la autenticación de dos factores.
- Si creaste tu cuenta con Continue with Amazon, puedes activar la autenticación multifactorial a través de tu cuenta de Amazon. Para obtener más información, consulta ¿Qué es la verificación en dos pasos? .

Tipos de MFA disponibles para ID de creador de AWS

ID de creador de AWS admite los siguientes tipos de dispositivos de autenticación multifactor (MFA).

FIDO2 autenticadores

FIDO2es un estándar que incluye CTAP2 WebAuthny se basa en la 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 dispositivos tienen autenticadores integrados, como TouchID on MacBook o una cámara compatible con Windows Hello. Si tu dispositivo es compatible con los protocolos FIDO, por ejemplo WebAuthn, puedes usar tu huella digital o tu rostro como segundo factor. Para obtener más información, consulte Autenticación FIDO.

Claves de seguridad

Puedes comprar una llave FIDO2 de seguridad externa compatible con USB, BLE o NFC. Cuando se te pida un dispositivo MFA, toca el sensor de la tecla. YubiKey o Feitian fabrica dispositivos compatibles. Para obtener una lista de todas las llaves de seguridad compatibles, 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

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, 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.

Puede elegir entre las siguientes aplicaciones de autenticación de terceros conocidas. Sin embargo, cualquier aplicación compatible con TOTP funciona con ID de creador de AWS MFA.

Sistema operativo	Aplicación de autenticación probada
Android	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

Registre su ID de creador de AWS dispositivo MFA

> **Note**
>
> Después de registrar una MFA, cerrar sesión e iniciar sesión en el mismo dispositivo, es posible que no se le pida una MFA en dispositivos de confianza.

Para registrar su dispositivo MFA mediante una aplicación de autenticación

1. Inicie sesión en su ID de creador de AWS perfil enhttps://profile.aws.amazon.com.
2. Elija Seguridad.
3. En la página Seguridad, seleccione Registrar dispositivo.
4. En la página Registrar dispositivo MFA, elija la App Authenticator.

5. ID de creador de AWS opera y muestra información de configuración, incluido un gráfico de código QR. El gráfico es una representación de la “clave de configuración secreta” que se puede introducir manualmente en aplicaciones de autenticación que no admiten códigos QR.
6. Abra su aplicación de autenticación. Para obtener una lista de aplicaciones, consulte Aplicaciones de autenticación.

   Si la aplicación de autenticación admite varios dispositivos o cuentas de MFA, elija la opción de crear un nuevo dispositivo o cuenta de MFA virtual.
7. Determine si la aplicación de MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones en la página Aplicación para configurar un autenticador

   1. 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.
   2. Seleccione Mostrar clave secreta y, a continuación, introduzca esa clave secreta en su aplicación de MFA.

   Cuando termine, la aplicación de autenticación generará y mostrará una contraseña de un solo uso.
8. En el cuadro del Código de autenticación, introduzca la contraseña de un solo uso que aparece actualmente en la aplicación de autenticación. Elija Asignar MFA.

   > **Important**
   >
   > Envíe su solicitud inmediatamente después de generar el código. Si generas el código y esperas demasiado para enviar la solicitud, el dispositivo MFA se asociará correctamente al tuyo ID de creador de AWS, pero el dispositivo MFA 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. Para obtener más información, consulte Cuando intento registrarme o iniciar sesión con una aplicación de autenticación, aparece el mensaje “Se ha producido un error inesperado”.
9. Para asignar un nombre descriptivo a tu dispositivo ID de creador de AWS, selecciona Cambiar nombre. Este nombre lo ayuda a distinguir este dispositivo de los demás que registre.

El dispositivo MFA ya está listo para usarse con. ID de creador de AWS

Registre una clave de seguridad como dispositivo ID de creador de AWS MFA

Para registrar su dispositivo MFA mediante una clave de seguridad

1. Inicie sesión en su ID de creador de AWS perfil enhttps://profile.aws.amazon.com.
2. Elija Seguridad.
3. En la página Seguridad, seleccione Registrar dispositivo.
4. En la página Registrar dispositivo MFA, elija Clave de seguridad.
5. Asegúrese de que su clave de seguridad esté habilitada. Si utiliza una clave de seguridad física independiente, conéctela a su equipo.
6. Siga las instrucciones que aparecen en pantalla. Los pasos cambian según el sistema operativo y el navegador.
7. Para asignar un nombre descriptivo a tu dispositivo ID de creador de AWS, selecciona Cambiar nombre. Este nombre lo ayuda a distinguir este dispositivo de los demás que registre.

El dispositivo MFA ya está listo para usarse con. ID de creador de AWS

Cambie el nombre de su dispositivo ID de creador de AWS MFA

Para cambiar el nombre del dispositivo MFA

1. Inicie sesión en su ID de creador de AWS perfil en. https://profile.aws.amazon.com
2. Elija Seguridad. Cuando llegue a la página, verá que Cambiar nombre aparece atenuado.
3. Seleccione el dispositivo MFA que desea cambiar. Esto le permite elegir Cambiar nombre. A continuación, aparece un cuadro de diálogo.
4. En el mensaje que se abre, introduzca el nuevo nombre en Nombre del dispositivo MFA y elija Cambiar nombre. El dispositivo renombrado aparece en Dispositivos de autenticación multifactor (MFA).

Eliminar su dispositivo MFA

Se recomienda mantener dos o más dispositivos MFA activos. Antes de eliminar un dispositivo, consulte Registre su ID de creador de AWS dispositivo MFA para registrar un dispositivo MFA de sustitución. Para deshabilitar la autenticación multifactor para usted ID de creador de AWS, elimine todos los dispositivos MFA registrados de su perfil.

Para eliminar un dispositivo MFA

1. Inicie sesión en su ID de creador de AWS perfil en. https://profile.aws.amazon.com
2. Elija Seguridad.
3. Seleccione el dispositivo MFA que desee eliminar y seleccione Eliminar.
4. En la sección ¿Eliminar dispositivo MFA?, siga las instrucciones para eliminar su dispositivo.
5. Elija Eliminar

El dispositivo eliminado ya no aparece en los Dispositivos de autenticación multifactor (MFA).

Privacidad y datos en ID de creador de AWS

El Aviso de privacidad de AWS describe cómo gestionamos sus datos personales. Para obtener información sobre cómo eliminar su ID de creador de AWS perfil, consulteElimine su ID de creador de AWS.

Solicita tus ID de creador de AWS datos

Puede solicitar y ver la información personal asociada a usted y a las AWS aplicaciones ID de creador de AWS y servicios a los que accedió con su ID de creador de AWS. Para obtener más información sobre el ejercicio de sus derechos como sujeto de datos, incluida la información personal proporcionada en relación con otros AWS sitios web, aplicaciones, productos, servicios, eventos y experiencias, consultehttps://aws.amazon.com/privacy.

Para solicitar sus datos

1. Inicie sesión en su ID de creador de AWS perfil enhttps://profile.aws.amazon.com.
2. Selecciona Mis ID de creador de AWS datos.
3. En la página Mis ID de creador de AWS datos, en Eliminar ID de creador de AWS, selecciona Solicitar tus datos.

4. Aparece un mensaje de confirmación verde en la parte superior de la página en el que se indica que hemos recibido su solicitud y que la completaremos en un plazo de 30 días.
5. Cuando reciba un correo electrónico en el que se indique que la solicitud se ha procesado, vuelva a la página Privacidad y datos de su perfil de ID de creador de AWS . Seleccione el nuevo botón disponible Descargar archivo ZIP con sus datos.

   Mientras la solicitud de sus datos esté pendiente, no podrá eliminar su ID de creador de AWS.

ID de creador de AWS y otras AWS credenciales

ID de creador de AWS La suya es independiente de cualquier Cuenta de AWS otra credencial de inicio de sesión. Puede usar el mismo correo electrónico para su correo electrónico ID de creador de AWS y para el del usuario raíz de un Cuenta de AWS.

Y ID de creador de AWS:

- Le permite acceder a las herramientas y servicios que utiliza ID de creador de AWS.
- No afecta a los controles de seguridad existentes, como las políticas y configuraciones que haya especificado en sus Cuentas de AWS aplicaciones.
- No sustituye a ningún usuario, credencial o cuenta raíz, del IAM Identity Center o usuario de IAM existente.
- No se pueden obtener las credenciales de AWS IAM para acceder al Consola de administración de AWS AWS CLI AWS SDKs, o al kit de AWS herramientas.

An Cuenta de AWS es un contenedor de recursos con información de contacto y pago. Establece un límite de seguridad en el que operar los AWS servicios facturados y medidos, como S3, EC2 o Lambda. Los propietarios de las cuentas pueden iniciar sesión y en. Cuenta de AWS Consola de administración de AWS Para obtener más información, consulte Inicio de sesión en la Consola de administración de AWS.

¿Cómo ID de creador de AWS se relaciona con su identidad actual en el Centro de Identidad de IAM

Como persona propietaria de la identidad, usted administra el ID de creador de AWS. Esta identidad no está relacionada con ninguna otra que pueda tener para otra organización, como la escuela o el trabajo. Puede utilizar una identidad de personal en el Centro de Identidad de IAM para representar

su identidad laboral y otra ID de creador de AWS para representar su identidad privada. Estas identidades funcionan de forma independiente.

Los usuarios del AWS IAM Identity Center (sucesor del AWS Single Sign-On) están gestionados por un administrador corporativo de TI o de la nube, o por el administrador del proveedor de identidad de la organización, como Okta, Ping o Azure. Los usuarios del IAM Identity Center pueden acceder a los recursos de varias cuentas en AWS Organizations.

Varios perfiles ID de creador de AWS

Puedes crear más de uno ID de creador de AWS siempre que cada ID utilice una dirección de correo electrónico única. Sin embargo, usar más de uno ID de creador de AWS puede hacer que sea difícil recordar cuál ID de creador de AWS usó para qué propósito. Siempre que sea posible, le recomendamos que utilice una sola herramienta ID de creador de AWS para todas sus actividades en AWS herramientas y servicios.

Cerrar sesión en AWS

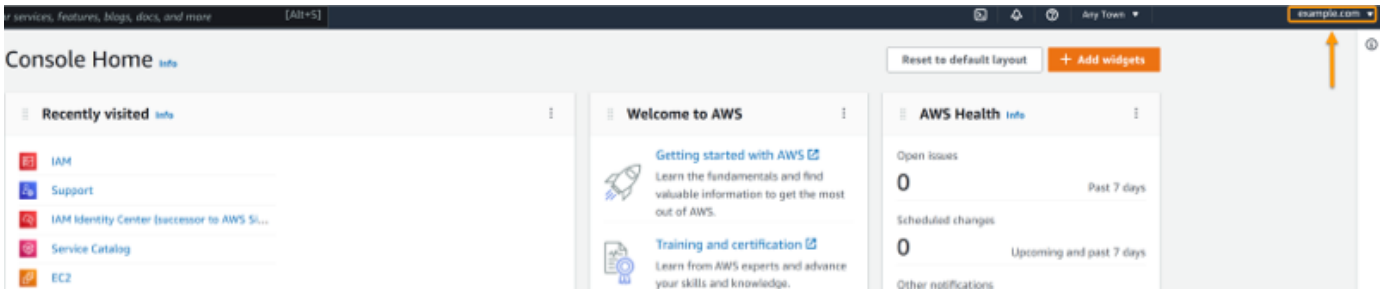
La forma de cerrar sesión Cuenta de AWS depende del tipo de AWS usuario que sea. Puede ser un usuario raíz de una cuenta, un usuario de IAM, un usuario del Centro de Identidad de IAM, una identidad federada o un usuario de AWS Builder ID. Si no está seguro del tipo de usuario que es, consulte Determine el tipo de usuario.

Temas

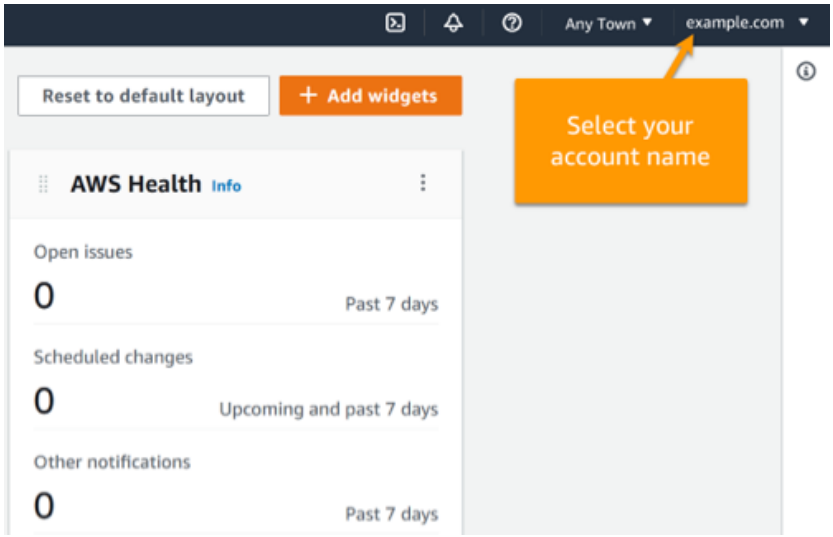
Cierre sesión en Consola de administración de AWS

Para cerrar sesión en Consola de administración de AWS

1. Cuando hayas iniciado sesión en Consola de administración de AWS, llegarás a una página similar a la que se muestra en la siguiente imagen. El nombre de su cuenta o el nombre de usuario de IAM se muestra en la esquina superior derecha.



2. En la barra de navegación de la parte superior derecha, elija su nombre de usuario.



3. Elija una opción de cierre de sesión. Las opciones de los botones varían según el número de cuentas en las que ha iniciado sesión.

   - Seleccione Cerrar sesión si solo ha iniciado sesión en una cuenta.
   - Seleccione Cerrar sesión en todas las sesiones para cerrar sesión en todas sus identidades al mismo tiempo.
   - Seleccione Cerrar sesión actual para cerrar sesión en la identidad que ha seleccionado.

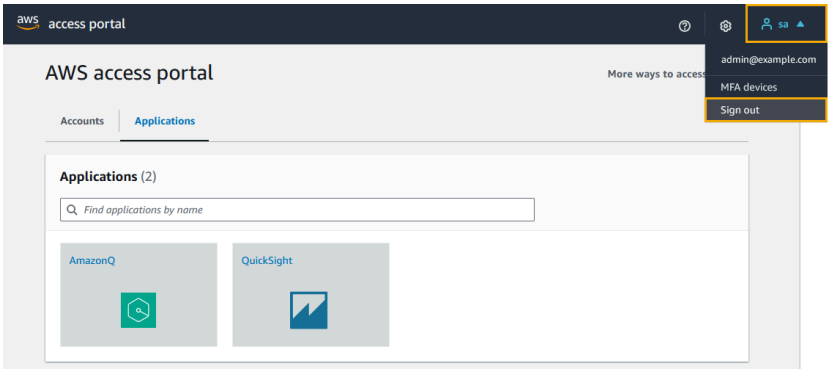
4. Volverá a la Consola de administración de AWS página web.

Para obtener más información sobre cómo iniciar sesión en varias cuentas, consulte Iniciar sesión en varias cuentas en la Guía de introducción de la Consola de administración de AWS .

Cierre sesión en su portal de AWS acceso

Para cerrar sesión en su portal de AWS acceso

1. En la barra de navegación de la parte superior derecha, elija su nombre de usuario.
2. Seleccione Cerrar sesión como se muestra la siguiente imagen.



3. Si cierra sesión correctamente, ahora verá la página de inicio de sesión de su portal de AWS acceso.

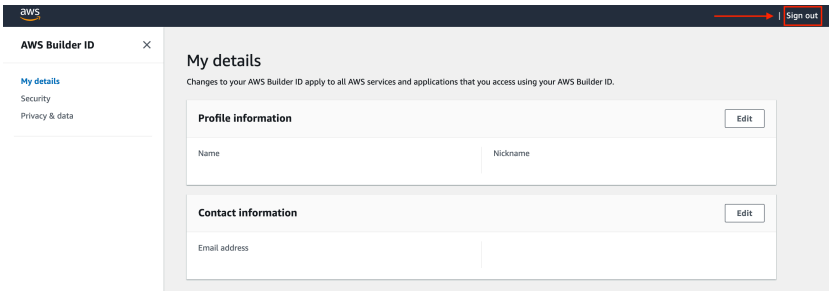
Si utiliza un proveedor de identidades (IdP) externo como origen de identidad, la sesión activa de sus credenciales no finalizará cuando cierre sesión. Si vuelve al portal de acceso de AWS , es posible que inicie sesión automáticamente sin tener que proporcionar sus credenciales.

Cierre sesión en AWS Builder ID

Para cerrar sesión en un AWS servicio al que haya accedido con su ID de AWS Builder, debe cerrar sesión en el servicio. Si quieres cerrar sesión en tu perfil de AWS Builder ID, consulta el siguiente procedimiento.

Para cerrar sesión en su perfil de AWS Builder ID

1. Tras iniciar sesión en tu perfil de AWS Builder ID enhttps://profile.aws.amazon.com/, accederás a Mis datos.
2. En la parte superior derecha de tu página de perfil de AWS Builder ID, selecciona Cerrar sesión.



3. Se cierra la sesión cuando ya no ves tu perfil de AWS Builder ID.

Resolución de problemas Cuenta de AWS problemas de inicio de sesión

Usa esta información para ayudarte a solucionar problemas relacionados con el inicio de sesión y otros Cuenta de AWS problemas. Para obtener instrucciones paso a paso sobre cómo iniciar sesión en un dispositivo Cuenta de AWS, consulte. Inicie sesión en Consola de administración de AWS

Si ninguno de los temas de solución de problemas te ayuda a solucionar tu problema de inicio de sesión, puedes crear un caso Soporte rellenando este formulario: Soy un AWS cliente y estoy buscando asistencia en materia de facturación o de cuentas. Como práctica recomendada de seguridad, no Soporte puedes hablar de los detalles de ninguna Cuenta de AWS otra cuenta que no sea la cuenta en la que has iniciado sesión. AWS Support tampoco puede cambiar las credenciales asociadas a una cuenta por ningún motivo.

> **Note**
>
> Soporte no publica un número de teléfono directo para contactar con un representante de soporte.

Para obtener más ayuda sobre cómo solucionar tus problemas de inicio de sesión, consulta ¿Qué hago si tengo problemas para iniciar sesión o acceder a mi? Cuenta de AWS Si tienes problemas para iniciar sesión Amazon.com, consulta el Servicio de atención al cliente de Amazon en lugar de esta página.

Temas

- ¿Cómo puedo encontrar mi Cuenta de AWS ID o alias
- Necesito el código de verificación de mi cuenta
- He olvidado la contraseña de mi usuario root Cuenta de AWS
- He olvidado la contraseña de usuario de IAM para mi Cuenta de AWS
- He olvidado la contraseña de mi identidad federada Cuenta de AWS
- No puedo iniciar sesión en mi cuenta actual Cuenta de AWS y no puedo crear una nueva Cuenta de AWS con la misma dirección de correo
- Necesito reactivar mi cuenta suspendida Cuenta de AWS
- Necesito ponerme en contacto Soporte para problemas de inicio de sesión
- Necesito ponerme en contacto AWS Billing por problemas de facturación
- Tengo una pregunta relacionada con un pedido
- Necesito ayuda para administrar mi Cuenta de AWS
- Mi AWS las credenciales del portal de acceso no funcionan
- He olvidado la contraseña del Centro de Identidad de IAM para mi Cuenta de AWS
- Recibo un error que dice “No es usted, somos nosotros” al intentar iniciar sesión en la consola de IAM Identity Center

¿Mi Consola de administración de AWS las credenciales no funcionan

Si recuerda su nombre de usuario y contraseña, pero sus credenciales no funcionan, es posible que se encuentre en la página equivocada. Intente iniciar sesión en otra página:

Página de inicio de sesión del usuario raíz

- Si ha creado o es propietario de una Cuenta de AWS y está realizando una tarea que requiere credenciales de usuario root, introduzca la dirección de correo electrónico de su cuenta en Consola de administración de AWS. Para obtener información sobre cómo acceder al usuario raíz, consulte Para iniciar sesión como usuario raíz. Si ha olvidado la contraseña de usuario raíz, puede restablecerla. Para obtener más información, consulte He olvidado la contraseña de mi usuario root Cuenta de AWS. Si ha olvidado la dirección de correo electrónico de su usuario raíz, busque en su bandeja de entrada un correo electrónico de AWS.
- Si intentó iniciar sesión en su cuenta de usuario raíz y recibió el siguiente error: La recuperación de la contraseña está deshabilitada para mi cuenta de usuario raíz, significa que no tiene credenciales

de usuario raíz. No puedes iniciar sesión como usuario root ni recuperar la contraseña del usuario root de tu cuenta. AWS es AWS Organizations posible que las cuentas de los miembros administradas mediante una contraseña de usuario raíz, claves de acceso, certificados de firma o autenticación multifactor (MFA) activa.

Solo la cuenta de administración o el administrador delegado de IAM pueden realizar acciones de usuario raíz en su cuenta de miembro. Póngase en contacto con su administrador si necesita realizar una tarea que requiera credenciales de usuario raíz. Para obtener más información, consulte Administrar de forma centralizada el acceso raíz de las cuentas de miembros en la Guía del usuario de AWS Identity and Access Management .

Página de inicio de sesión del usuario de IAM

- Si tú u otra persona creaste un usuario de IAM dentro de un Cuenta de AWS, debes conocer ese Cuenta de AWS ID o alias para iniciar sesión. Introduzca el ID o alias de la cuenta, el nombre de usuario y la contraseña en la Consola de administración de AWS. Para obtener información sobre cómo acceder a la página de inicio de sesión del usuario de IAM, consulte Para iniciar sesión como usuario de IAM. Si ha olvidado su contraseña de usuario de IAM, consulte He olvidado la contraseña de usuario de IAM para mi Cuenta de AWS para obtener información sobre cómo restablecerla. Si ha olvidado el número de cuenta, compruebe su correo electrónico, los favoritos del navegador o el historial del navegador en busca de una URL que incluya `signin.aws.amazon.com/`. El ID o alias de la cuenta seguirá el texto de la `"account="` en la URL. Si no encuentras el seudónimo o el seudónimo de tu cuenta, ponte en contacto con tu administrador. Soporte no puede ayudarte a recuperar esta información. No puede ver el ID ni el alias de la cuenta hasta que inicie sesión.

Se requiere restablecer la contraseña del usuario raíz

Como medida de protección de la cuenta, es posible que reciba el siguiente mensaje cuando intente iniciar sesión en Consola de administración de AWS:

Es necesario restablecer la contraseña. Por motivos de seguridad, es necesario que restablezca la contraseña. Para proteger la cuenta, debe seleccionar Olvidé la contraseña a continuación y restablecerla.

Además de este mensaje, AWS también te notifica cuando identificamos un posible problema a través del correo electrónico asociado a tu cuenta. En el mensaje de correo electrónico se indica

el motivo por el cual es necesario restablecer la contraseña. Por ejemplo, cuando detectamos una actividad de inicio de sesión inusual Cuenta de AWS o las credenciales asociadas a ella Cuenta de AWS están disponibles públicamente en línea.

Actualice la contraseña para proteger las credenciales de usuario raíz. Para obtener información sobre cómo restablecer la contraseña de usuario raíz, consulte Olvidé la contraseña de usuario raíz de la Cuenta de AWS.

No tengo acceso al correo electrónico de mi Cuenta de AWS

Al crear una Cuenta de AWS, proporciona una dirección de correo electrónico y una contraseña. Estas son las credenciales del Usuario raíz de la cuenta de AWS. Si no está seguro de la dirección de correo electrónico asociada a la suya Cuenta de AWS, busque la correspondencia guardada que termine en @signin .aws o @verify .signin.aws dirigida a cualquier dirección de correo electrónico de su organización que pueda haber sido utilizada para abrir la. Cuenta de AWS Pregúntele a otros miembros de su equipo, empresa o familia. Si la cuenta la creó alguien que conoce, puede ayudarlo a acceder.

Si conoce la dirección de correo electrónico pero ya no tiene acceso a dicho correo electrónico, intente recuperar el acceso al correo electrónico mediante una de las siguientes opciones:

- Si es el propietario del dominio de la dirección de correo electrónico, puede restaurar una dirección de correo electrónico eliminada. De forma alternativa, puede configurar un catch-all para su cuenta de correo electrónico. El catch-all captura todos los mensajes enviados a direcciones de correo electrónico que ya no existen en el servidor de correo y los redirige a otra dirección de correo electrónico.
- Si la dirección de correo electrónico de la cuenta forma parte de su sistema de correo electrónico de la empresa, le recomendamos que se ponga en contacto con los administradores del sistema de TI. Estos administradores podrían ayudarlo a recuperar el acceso al correo electrónico.

Si sigues sin poder iniciar sesión en tu Cuenta de AWS, ponte en contacto con nosotros para buscar otras opciones de asistencia. Soporte

Mi dispositivo MFA se ha perdido o ha dejado de funcionar

Si se ha perdido su dispositivo de MFA, se ha averiado o no funciona, no recibirá un código de acceso de un solo uso (OTP) cuando envíe una solicitud de verificación de MFA.

Usuarios de IAM

Puede iniciar sesión con otro dispositivo de MFA registrado para el mismo usuario de IAM.

Los usuarios de IAM deben ponerse en contacto con un administrador para desactivar un dispositivo de MFA que no está funcionando. Estos usuarios no pueden recuperar su dispositivo MFA sin la ayuda del administrador. El administrador suele ser un miembro del personal de tecnología de la información (TI) que tiene un nivel de permisos Cuenta de AWS superior al de otros miembros de la organización. Esta persona creó su cuenta y proporciona a los usuarios sus credenciales de acceso para iniciar sesión.

Usuarios raíz

Para recuperar el acceso al usuario raíz, debe iniciar sesión con otro dispositivo de MFA registrado con el mismo usuario raíz. A continuación, revise las siguientes opciones para recuperar o actualizar su dispositivo de MFA:

- Si desea obtener instrucciones paso a paso para recuperar un dispositivo MFA, consulte ¿Qué sucede si un dispositivo MFA se pierde o deja de funcionar?
- Para obtener instrucciones paso a paso sobre cómo actualizar el número de teléfono de un dispositivo MFA, consulte ¿Cómo actualizo mi número de teléfono para restablecer mi dispositivo MFA perdido?
- Para obtener instrucciones paso a paso sobre cómo activar los dispositivos MFA, consulte Habilitar dispositivos MFA para los usuarios en. AWS
- Si no puede recuperar su dispositivo MFA, póngase en contacto con Soporte.

> **Note**
>
> Los usuarios de IAM deben ponerse en contacto con su administrador para obtener ayuda con los dispositivos MFA. Soporte no puede ayudar a los usuarios de IAM con problemas con los dispositivos MFA.

No puedo acceder al Consola de administración de AWS página de inicio de sesión

Si no puede ver la página de inicio de sesión, es posible que un firewall esté bloqueando el dominio. Póngase en contacto con el administrador de la red para añadir los siguientes dominios o puntos de

enlace URL a las listas de permitidos en las opciones de filtrado de contenido web, en función del tipo de usuario que sea y del método que use para iniciar sesión.

Usuario raíz y usuarios de IAM	*.signin.aws.amazon.com
Amazon.com inicio de sesión en la cuenta	: www.amazon.com
Inicio de sesión de usuarios de IAM Identity Center y de aplicaciones propias	• *.awsapps.com () http://awsapps.com/ • *.signin.aws

No puedo iniciar sesión debido a las condiciones de la red en las políticas basadas en recursos Sign-in

Si aparece uno de los siguientes mensajes de error, es posible que una política Sign-in basada en recursos o una política de control de recursos (RCP) restrinja el acceso en función de la ubicación de la red:

- «La información de autenticación es incorrecta. Inténtelo de nuevo».
- «Falló la autenticación. Solicitud no válida»
- «Error de autenticación: para acceder a esta cuenta, inicia sesión desde una red diferente o ponte en contacto con el administrador para obtener más información»

Póngase en contacto con su administrador o consulte No puedo iniciar sesión debido a las condiciones de la red en las políticas Sign-in basadas en recursos los pasos detallados de solución de problemas.

Se bloquea el acceso a mi cuenta después de activar la autorización de la consola

Si configuraste la autorización de la consola y ya no puedes acceder a tu cuenta, es posible que no hayas configurado el acceso principal excluido o el acceso de recuperación de emergencia antes de aplicar la política. Para conocer los pasos de resolución, incluidas las opciones de autoservicio de AWS CLI`OrganizationAccountAccessRole`, y AWS Support, consulteSe bloquea el acceso a mi cuenta después de activar la autorización de la consola.

Los cambios de mi política no están surtiendo efecto

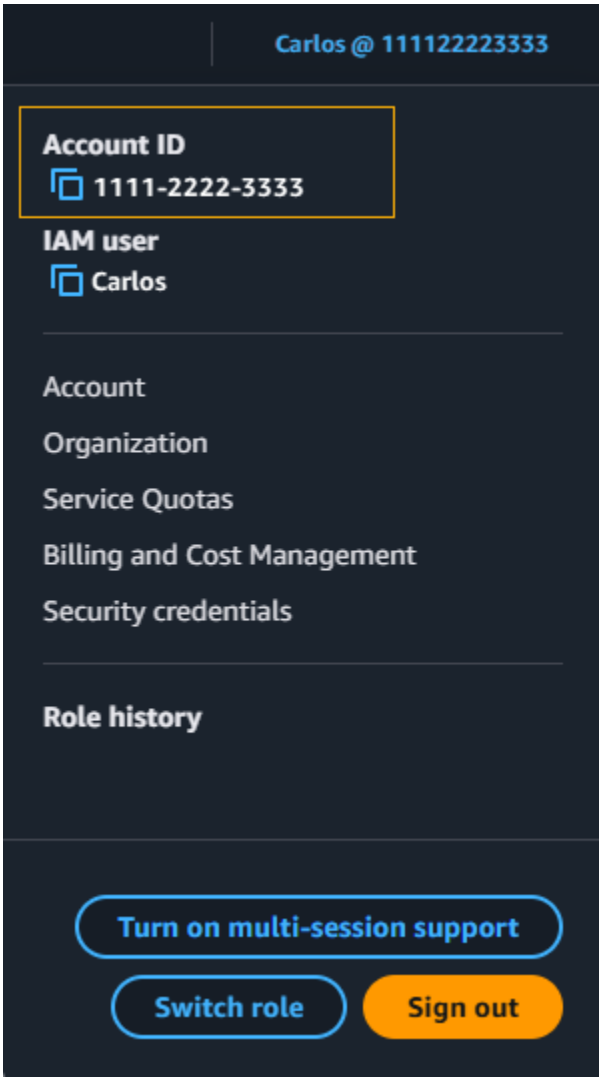
Los cambios en la configuración de autorización de la consola y en las declaraciones de permiso de los recursos se replican de forma global y pueden tardar unos minutos en surtir efecto. Si los cambios no están visibles después de esperar, consulte los pasos Los cambios que realizo no están siempre visibles inmediatamente de solución de problemas.

¿Cómo puedo encontrar mi Cuenta de AWS ID o alias

Si es usuario de IAM y no ha iniciado sesión, solicite al administrador el ID o el alias de Cuenta de AWS . El administrador suele ser un miembro del personal de tecnología de la información (TI) que tiene un nivel de permisos Cuenta de AWS superior al de los demás miembros de la organización. Esta persona creó su cuenta y proporciona a los usuarios sus credenciales de acceso para iniciar sesión.

Si es un usuario de IAM con acceso a Consola de administración de AWS, el ID de su cuenta se encuentra en la URL de inicio de sesión. Compruebe la URL de inicio de sesión en los correos electrónicos de su administrador. El ID de la cuenta son los doce primeros dígitos de la URL de inicio de sesión. Por ejemplo, en la siguiente URL`https://111122223333.signin.aws.amazon.com/console`, tu Cuenta de AWS ID es 111122223333.

Tras iniciar sesión en Consola de administración de AWS, encontrarás la información de tu cuenta en la barra de navegación situada junto a tu región. Por ejemplo, en la siguiente captura de pantalla, el usuario de IAM Carlos tiene un número Cuenta de AWS 1111-2222-3333.



Para obtener más información sobre tu Cuenta de AWS ID y tu alias y cómo encontrarlos, consulta Tu ID y su Cuenta de AWS alias.

Necesito el código de verificación de mi cuenta

Si has proporcionado la dirección de correo electrónico y la contraseña de tu cuenta, a AWS veces es necesario que proporciones un código de verificación único. Para recuperar el código de verificación, comprueba si hay algún mensaje de Amazon Web Services en el correo electrónico asociado al tuyo. Cuenta de AWS La dirección de correo electrónico termina en @signin.aws o @verify.signin.aws. Siga las indicaciones del mensaje. Si no ve el mensaje en su cuenta, compruebe las carpetas de correo basura y spam. Si ya no tiene acceso al correo electrónico, consulte No tengo acceso al correo electrónico de mi Cuenta de AWS.

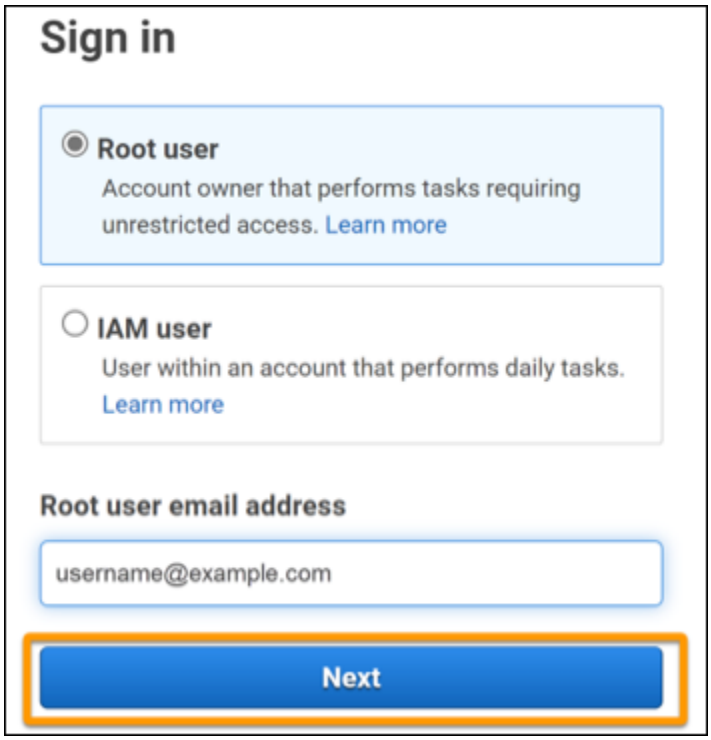
He olvidado la contraseña de mi usuario root Cuenta de AWS

Si es un usuario root y ha perdido u olvidado su contraseña Cuenta de AWS, puede restablecerla seleccionando el enlace «He olvidado mi contraseña» en el Consola de administración de AWS. Debe conocer la dirección de correo electrónico de su AWS cuenta y debe tener acceso a la cuenta de correo electrónico. Se le enviará por correo electrónico un enlace durante el proceso de recuperación de la contraseña para restablecerla. El enlace se enviará a la dirección de correo electrónico que utilizó para crear la suya Cuenta de AWS.

Para restablecer la contraseña de una cuenta que creó con AWS Organizations, consulte Acceder a una cuenta de miembro como usuario raíz.

Para restablecer la contraseña de su usuario raíz

1. Utilice su dirección de AWS correo electrónico para empezar a iniciar sesión en la Consola de AWS administración como usuario raíz. A continuación, elija Siguiente.

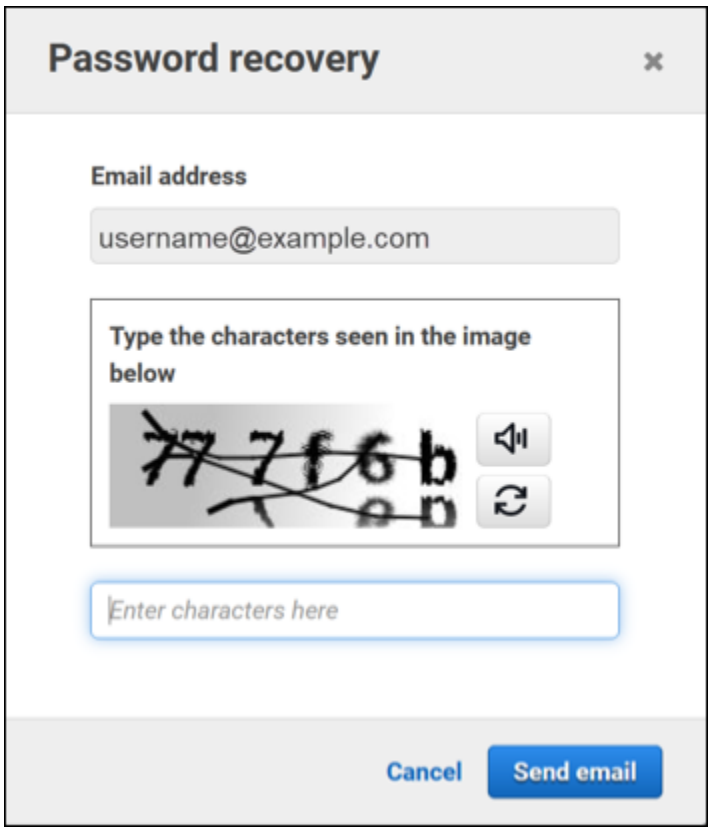


> **Note**
>
> Si ha iniciado sesión en la Consola de administración de AWS con las credenciales de usuario de IAM, debe cerrar la sesión para poder restablecer la contraseña de usuario raíz. Si ves la página de inicio de sesión del usuario de IAM específica de la cuenta,

elige Sign-in usar las credenciales de la cuenta raíz en la parte inferior de la página. Si es necesario, proporcione la dirección de correo electrónico de la cuenta y elija Siguiente para acceder a la página Inicio de sesión de usuario raíz.

2. Elija ¿Ha olvidado su contraseña?

3. Siga los pasos para recuperar la contraseña. Si no puede completar el control de seguridad, intente escuchar el audio o vuelva a cargar el control de seguridad para usar un conjunto de caracteres distinto. En la siguiente imagen se muestra un ejemplo de una página de recuperación de contraseña.

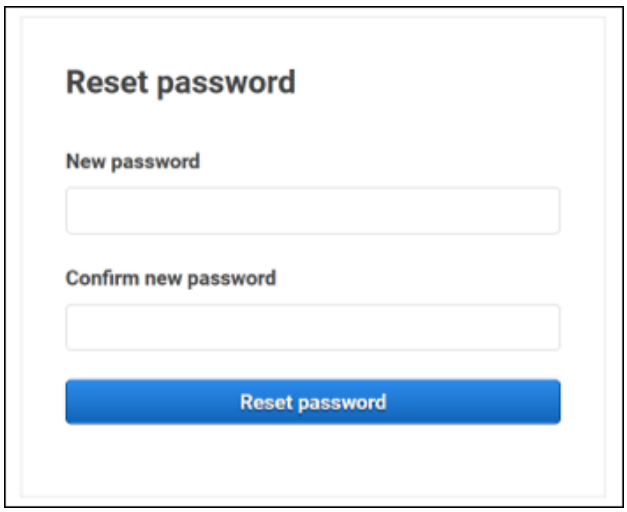


4. Tras completar los pasos de recuperación de la contraseña, recibirá un mensaje indicándole que se han enviado más instrucciones a la dirección de correo electrónico asociada a su cuenta de Cuenta de AWS.

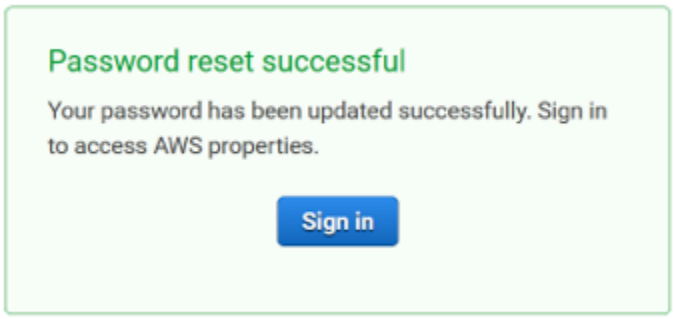
   Se enviará un correo electrónico con un enlace para restablecer la contraseña a la dirección de correo electrónico utilizada para crear la Cuenta de AWS.

   > **Note**
   >
   > El correo electrónico procederá de una dirección que termina en @signin.aws o @verify.aws.

5. Selecciona el enlace que aparece en el AWS correo electrónico para restablecer la contraseña de usuario AWS root.
6. El enlace le dirige a una nueva página web para crear una nueva contraseña de usuario raíz.



Recibirá un mensaje confirmando que la contraseña se ha restablecido correctamente. En la siguiente imagen se muestra un restablecimiento correcto de la contraseña.



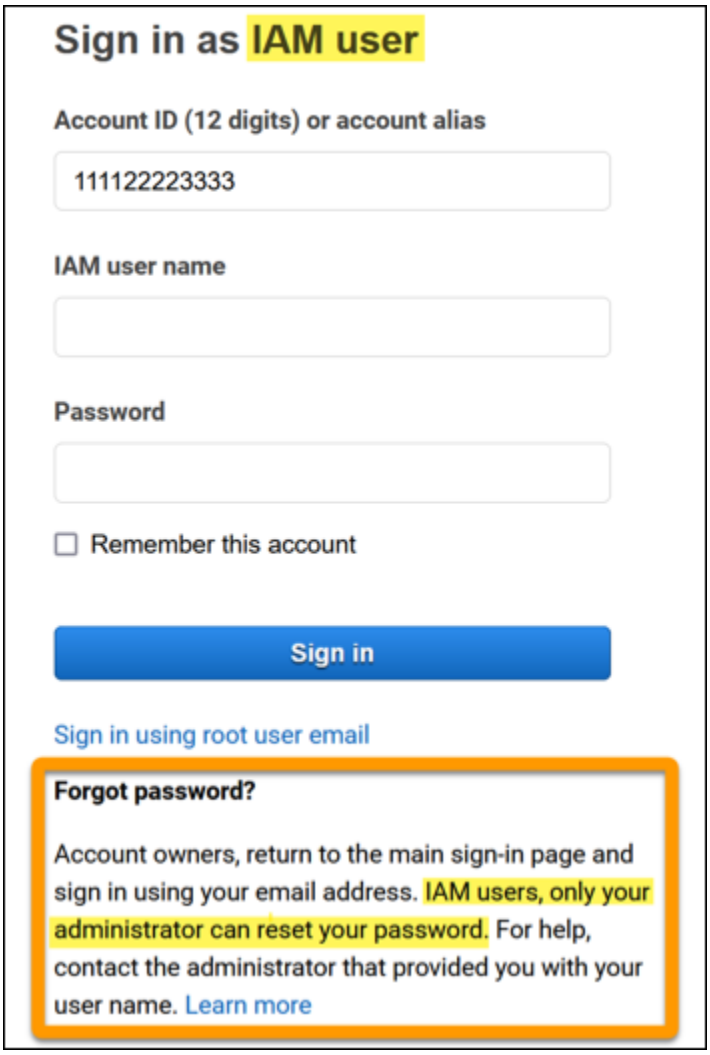
Para obtener más información sobre cómo restablecer la contraseña del usuario root, consulta ¿Cómo puedo recuperar una AWS contraseña perdida u olvidada?

He olvidado la contraseña de usuario de IAM para mi Cuenta de AWS

Para cambiar la contraseña de usuario de IAM, debe tener los permisos adecuados. Para obtener más información sobre cómo restablecer la contraseña de usuario de IAM, consulte Cómo un usuario de IAM puede cambiar su propia contraseña.

Si no tiene permiso para restablecer la contraseña, solo el administrador de IAM puede restablecer la contraseña de usuario de IAM. Los usuarios de IAM deben ponerse en contacto con su administrador de IAM para restablecer su contraseña. El administrador suele ser un miembro del personal de tecnología de la información (TI) que tiene un nivel de permisos superior al de los demás miembros

de la organización. Cuenta de AWS Esta persona creó su cuenta y proporciona a los usuarios sus credenciales de acceso para iniciar sesión.



Por motivos de seguridad, Soporte no tiene acceso para ver, proporcionar o cambiar sus credenciales.

Para obtener más información sobre cómo restablecer la contraseña de usuario de IAM, consulte ¿Cómo recupero una contraseña perdida u olvidada AWS?

Para obtener información sobre cómo un administrador puede administrar su contraseña, consulte Gestión de contraseñas para usuarios de IAM.

He olvidado la contraseña de mi identidad federada Cuenta de AWS

Las identidades federadas inician sesión para acceder Cuentas de AWS con identidades externas. El tipo de identidad externa que se utilice determina la manera en que inician sesión las identidades federadas. Su administrador crea las identidades federadas. Consulte a su administrador para obtener más información sobre cómo restablecer su contraseña. El administrador suele ser un miembro del personal de tecnología de la información (TI) que tiene un nivel de permisos más alto Cuenta de AWS que el de otros miembros de la organización. Esta persona creó su cuenta y proporciona a los usuarios sus credenciales de acceso para iniciar sesión.

No puedo iniciar sesión en mi cuenta actual Cuenta de AWS y no puedo crear una nueva Cuenta de AWS con la misma dirección de correo

Únicamente puede asociar una dirección de correo electrónico a cada Usuario raíz de la cuenta de AWS. Si cierra su cuenta de usuario raíz y permanece cerrada durante más de 90 días, no podrá volver a abrir su cuenta ni crear una nueva Cuenta de AWS con la dirección de correo electrónico asociada a esta cuenta.

Para solucionar este problema, puede usar una subdirección en la que añada un signo más (+) después de u dirección de correo electrónico habitual cuando abra una cuenta nueva. El signo más (+) puede ir seguido de letras mayúsculas o minúsculas, números u otros caracteres compatibles con el protocolo simple de transferencia de correo (SMTP). Por ejemplo, puede usar `email+1@yourcompany.com` o `email+tag@yourcompany.com` si su correo electrónico habitual es `email@yourcompany.com`. Se considera una dirección nueva aunque esté conectada a la misma bandeja de entrada que su dirección de correo electrónico habitual. Antes de crear una cuenta nueva, le recomendamos que envíe un mensaje de prueba a la dirección de correo electrónico adjunta para confirmar que su proveedor admite subdirecciones.

Necesito reactivar mi cuenta suspendida Cuenta de AWS

Si Cuenta de AWS está suspendido y quiere restablecerlo, consulte ¿Cómo puedo reactivar mi suspensión? Cuenta de AWS

Necesito ponerme en contacto Soporte para problemas de inicio de sesión

Si lo has intentado todo, puedes obtener ayuda Soporte completando la solicitud de Billing and Account Support.

Necesito ponerme en contacto AWS Billing por problemas de facturación

Si no puedes iniciar sesión en tu cuenta Cuenta de AWS y deseas ponerte en contacto con nosotros AWS Billing por problemas de facturación, puedes hacerlo mediante una solicitud de Billing and Account Support. Para obtener más información Administración de facturación y costos de AWS, incluidos los cargos y los métodos de pago, consulta Cómo obtener ayuda con AWS Billing.

Tengo una pregunta relacionada con un pedido

Si tiene algún problema con su cuenta de www.amazon.com o tiene alguna pregunta sobre un pedido, consulte Opciones de asistencia y contacto.

Necesito ayuda para administrar mi Cuenta de AWS

Si necesitas ayuda para cambiar tu tarjeta de crédito Cuenta de AWS, denunciar una actividad fraudulenta o cerrar la tuya Cuenta de AWS, consulta Solución de problemas con Cuentas de AWS.

Mi AWS las credenciales del portal de acceso no funcionan

Cuando no pueda iniciar sesión en su portal de AWS acceso, intente recordar cómo accedió anteriormente AWS.

Si no recuerda haber utilizado una contraseña

Es posible que haya accedido anteriormente AWS sin usar AWS credenciales. Esto es común para el inicio de sesión único empresarial a través del Centro de identidades de IAM. Al acceder de AWS esta forma, se utilizan las credenciales corporativas para acceder a AWS las cuentas o aplicaciones sin necesidad de introducir las credenciales.

- AWS portal de acceso: si un administrador le permite usar credenciales externas AWS para acceder AWS, necesitará la URL de su portal. Compruebe su correo electrónico, los favoritos del navegador o el historial del navegador en busca de una URL que incluya `awsapps.com/start` o `signin.aws/platform/login`.

  Por ejemplo, la URL personalizada puede incluir un ID o un dominio, como `https://d-1234567890.awsapps.com/start`. Si no encuentra el enlace al portal, póngase en contacto con el administrador. Soporte no puede ayudarlo a recuperar esta información.

Si recuerda su nombre de usuario y contraseña, pero sus credenciales no funcionan, es posible que se encuentre en la página equivocada. Comprueba la URL de tu navegador web si es https://signin.aws.amazon.com/ un usuario federado o si un usuario del IAM Identity Center no puede iniciar sesión con sus credenciales.

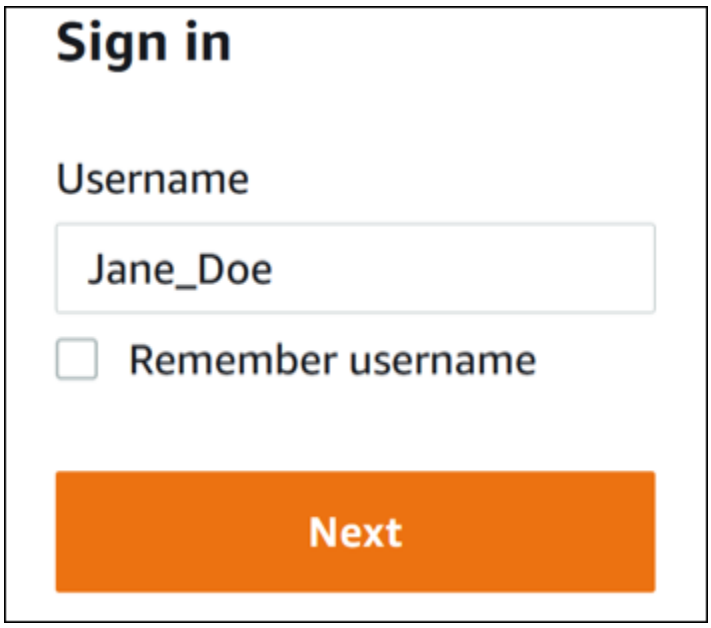
- AWS portal de acceso: si un administrador configuró una fuente de identidad del AWS IAM Identity Center (sucesor de AWS Single Sign-On) AWS, debe iniciar sesión con su nombre de usuario y contraseña en el portal de AWS acceso de su organización. Para localizar la URL que se usará en el portal, compruebe su correo electrónico, el almacenamiento seguro de contraseñas, los favoritos del navegador o el historial del navegador en busca de una URL que incluya `awsapps.com/start` o `signin.aws/platform/login`. Por ejemplo, la URL personalizada puede incluir un ID o un dominio, por ejemplo, `https://d-1234567890.awsapps.com/start.` si no encuentra el enlace al portal, póngase en contacto con su administrador. Soporte no puede ayudarte a recuperar esta información.

He olvidado la contraseña del Centro de Identidad de IAM para mi Cuenta de AWS

Si usted es un usuario de IAM Identity Center y ha perdido u olvidado la contraseña de la Cuenta de AWS, puede restablecerla. Debe conocer la dirección de correo electrónico utilizada para la cuenta del IAM Identity Center y poder acceder a ella. Se enviará a la correo electrónico asociada a su Cuenta de AWS un enlace para restablecer la contraseña.

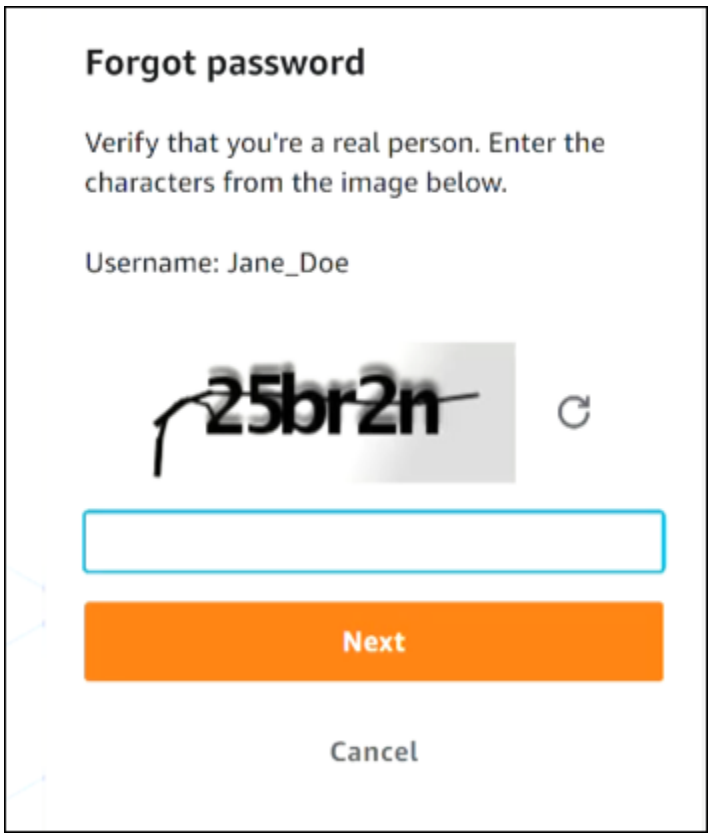
Para restablecer la contraseña de usuario en el IAM Identity Center

1. Utilice el enlace URL del portal de AWS acceso e introduzca su nombre de usuario. A continuación, elija Siguiente.

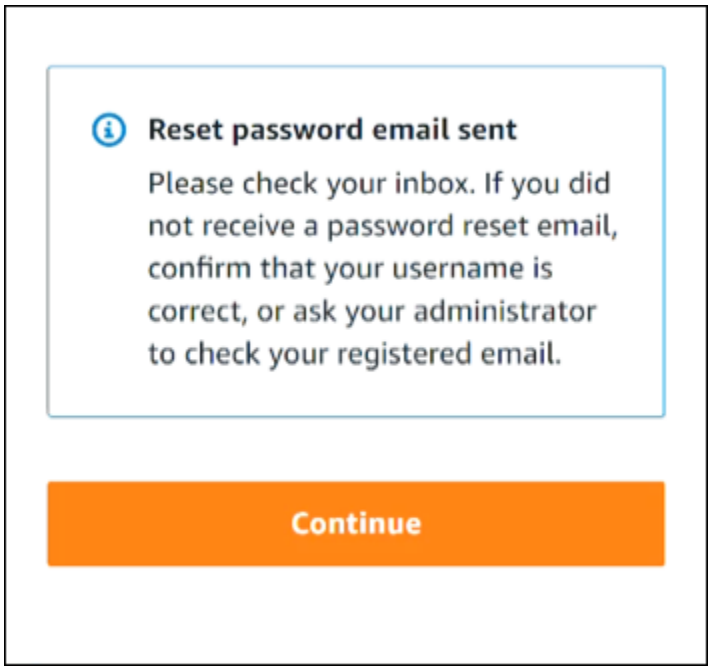


2. Seleccione ¿Ha olvidado su contraseña?, tal y como se muestra en la imagen siguiente.

3. Siga los pasos para recuperar la contraseña.



4. Tras completar los pasos de la recuperación de la contraseña, recibirá el siguiente mensaje confirmando que se le ha enviado un mensaje de correo electrónico que puede utilizar para restablecer la contraseña.



Se envía un mensaje con un enlace para restablecer la contraseña al correo electrónico asociado a la cuenta de usuario de IAM Identity Center. Seleccione el enlace que aparece en el AWS correo electrónico para restablecer la contraseña. El enlace le dirige a una nueva página web para crear una nueva contraseña. Tras crear una nueva contraseña, recibirá la confirmación de que se ha restablecido correctamente.

Si no ha recibido un correo electrónico para restablecer la contraseña, pida al administrador que confirme cuál es el correo electrónico que está registrado con su usuario en IAM Identity Center.

Recibo un error que dice “No es usted, somos nosotros” al intentar iniciar sesión en la consola de IAM Identity Center

Este error indica que hay un problema de configuración con la instancia de IAM Identity Center o con el proveedor de identidades externo (IdP) que utiliza como origen de identidades. Recomendamos que verifique lo siguiente:

- Revise la configuración de fecha y hora en del dispositivo que utiliza para iniciar sesión. Recomendamos que permita que la fecha y la hora se ajusten automáticamente. Si esa opción no está disponible, recomendamos que sincronice la fecha y la hora con un servidor de protocolo de hora de red (NTP) conocido.
- Verifique que el certificado de IdP cargado en IAM Identity Center sea el mismo que el proporcionado por el proveedor de identidades. Puede revisar el certificado desde la consola de IAM Identity Center. Para ello, vaya a Configuración. En la pestaña Origen de identidad, en Acción, seleccione Administrar la autenticación. Es posible que tenga que importar un nuevo certificado.
- En el archivo de metadatos SAML del IdP, asegúrese de que el formato NameID sea `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.
- Si utiliza el Conector de AD, revise que las credenciales de la cuenta de servicio sean correctas y no hayan caducado. Para obtener más información, consulte Actualizar las credenciales de la cuenta de servicio de AD Connector en Directory Service.

Solución de problemas de AWS Builder ID

Utilice la información que aparece aquí para solucionar problemas que pueda tener con su ID de creador de AWS.

Temas

- Cuando intento iniciar sesión en Builder ID, aparece el mensaje «No eres tú, somos nosotros» AWS
- Cerrar sesión no significa que se cierre mi sesión por completo
- Sigo intentando resolver mi problema

Mi correo electrónico ya está en uso

Si el correo electrónico que has introducido ya está en uso y lo reconoces como propio, es posible que ya te hayas registrado para obtener un AWS Builder ID. Intente iniciar sesión con esa dirección de correo electrónico. Si no recuerda su contraseña, consulte He olvidado mi contraseña.

No puedo completar la verificación de correo

Si te has registrado en AWS Builder ID pero no has recibido el correo electrónico de verificación, completa las siguientes tareas de solución de problemas.

1. Revise su carpeta de correo no deseado, correo basura y elementos eliminados.

   > **Note**
   >
   > Este correo electrónico de verificación proviene de la dirección no-reply@signin.aws o no-reply@login.awsapps.com. Le recomendamos que configure su sistema de correo para que acepte los mensajes con estas direcciones de correo electrónico como remitente y no los trate como correo basura o spam.

2. Seleccione Reenviar código, actualice la bandeja de entrada y vuelva a revisar las carpetas de correo no deseado, correo basura y elementos eliminados.
3. Si sigues sin ver el correo electrónico de verificación, comprueba que no haya errores tipográficos en tu dirección de correo electrónico de AWS Builder ID. Si ha introducido una dirección de correo electrónico incorrecta, vuelva a registrarse con una dirección de correo electrónico que sí sea suya.

No puedo iniciar sesión con Google

Si ya tienes un ID de creador de AWS perfil con la misma dirección de correo electrónico que tu cuenta de Google, usa tu ID de creador de AWS contraseña para iniciar sesión en tu cuenta. Si no recuerda su contraseña, consulte He olvidado mi contraseña.

Si necesita ayuda para iniciar sesión con su contraseña de Google, consulte No puedo iniciar sesión en mi cuenta de Google.

No puedo iniciar sesión con Apple

Si ya tienes un ID de creador de AWS perfil con la misma dirección de correo electrónico que tu cuenta de Apple, usa tu ID de creador de AWS contraseña para iniciar sesión en tu cuenta. Si no recuerda su contraseña, consulte He olvidado mi contraseña.

Si necesitas ayuda para iniciar sesión con tu contraseña de Apple, consulta Si no puedes iniciar sesión en tu cuenta de Apple.

No puedo iniciar sesión con GitHub

Si ya tienes un ID de creador de AWS perfil con la misma dirección de correo electrónico que tu GitHub cuenta, usa tu ID de creador de AWS contraseña para iniciar sesión en tu cuenta. Si no recuerda su contraseña, consulte He olvidado mi contraseña.

Si necesitas ayuda para iniciar sesión con tu GitHub contraseña, consulta Unable to sign in - GitHub Support.

No puedo iniciar sesión con Amazon

Si ya tienes un ID de creador de AWS perfil con la misma dirección de correo electrónico que tu cuenta de Amazon, usa tu ID de creador de AWS contraseña para iniciar sesión en tu cuenta. Si no recuerda su contraseña, consulte He olvidado mi contraseña.

Si necesitas ayuda para iniciar sesión con tu contraseña de Amazon, consulta Ayuda para iniciar sesión.

Recibí un error al iniciar sesión cuando intentaba registrarme para ID de creador de AWS usar Continúe con Google

Esto significa que ya tienes una que ID de creador de AWS utiliza la misma dirección de correo electrónico que tu cuenta de Google o que la dirección de correo electrónico asociada a tu cuenta de Google no está verificada. En cualquier caso, intente registrarse de nuevo con su dirección de correo electrónico y una contraseña.

Recibí un error al iniciar sesión cuando intentaba registrarme para seguir ID de creador de AWS usando Apple

Esto significa que ya tienes una dirección de correo electrónico ID de creador de AWS con la misma que tu cuenta de Apple o que la dirección de correo electrónico asociada a tu cuenta de Apple no está verificada ni gestionada por tu empresa con Apple Business Manager o por tu centro educativo con Apple School Manager. En cualquier caso, intente registrarse de nuevo con su dirección de correo electrónico y una contraseña.

Recibí un error al iniciar sesión cuando intentaba registrarme para ID de creador de AWS usar Continuar con GitHub

Esto significa que ya tienes una que ID de creador de AWS utiliza la misma dirección de correo electrónico que tu GitHub cuenta o que la dirección de correo electrónico asociada a tu GitHub cuenta no está verificada. En cualquier caso, intente registrarse de nuevo con su dirección de correo electrónico y una contraseña.

Recibí un error de inicio de sesión cuando intentaba registrarme para ID de creador de AWS usar Continuar con Amazon

Esto significa que ya tienes una que ID de creador de AWS utiliza la misma dirección de correo electrónico que tu cuenta de Amazon o que la dirección de correo electrónico asociada a tu cuenta de Amazon no está verificada. En cualquier caso, intente registrarse de nuevo con su dirección de correo electrónico y una contraseña.

Recibo un mensaje de error que dice «No eres tú, somos nosotros» cuando intento iniciar sesión con mi ID de creador de AWS

Si recibe este mensaje de error cuando intenta iniciar sesión, es posible que haya un problema con la configuración local o la dirección de correo electrónico.

- Revise la configuración de fecha y hora en del dispositivo que utiliza para iniciar sesión. Recomendamos que permita que la fecha y la hora se ajusten automáticamente. Si esa opción no está disponible, recomendamos que sincronice la fecha y la hora con un servidor de protocolo de hora de red (NTP) conocido.
- Revise su dirección de correo electrónico para ver si hay errores de formato. Los siguientes problemas devolverán un error al intentar iniciar sesión con su ID de creador de AWS.
  - Espacio en una dirección de correo electrónico
  - Barra diagonal (/) en una dirección de correo electrónico
  - Dos puntos (.) en una dirección de correo electrónico
  - Dos arrobas (@) en una dirección de correo electrónico
  - Una coma (,) al final de una dirección de correo electrónico
  - Corchetes (]) al final de una dirección de correo electrónico

He olvidado mi contraseña

Restablecer contraseña olvidada

1. En la página Iniciar sesión con el ID de AWS Builder, introduce el correo electrónico que utilizaste para crear tu AWS Builder ID en la dirección de correo electrónico. Elija Siguiente.
2. Elija ¿Ha olvidado su contraseña? Te enviamos un enlace a la dirección de correo electrónico asociada a tu ID de AWS constructor, donde podrás restablecer tu contraseña.
3. Siga las instrucciones que se detallan en el correo electrónico.

No puedo establecer una contraseña nueva

Por su seguridad, debe seguir estos requisitos siempre que establezca o cambie 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 contraseñas más recientes no se pueden volver a usar.
- 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.

Mi contraseña no funciona

Si recuerdas tu contraseña, pero no funciona cuando inicias sesión con AWS Builder ID, asegúrate de lo siguiente:

- El bloqueo de mayúsculas está desactivado.
- No está usando una contraseña antigua.
- Estás usando tu contraseña de AWS Builder ID y no una como contraseña Cuenta de AWS.

Si compruebas que tu contraseña es correcta up-to-date y la has introducido correctamente, pero sigue sin funcionar, sigue las instrucciones He olvidado mi contraseña para restablecerla.

Mi contraseña no funciona y ya no puedo acceder a los correos electrónicos enviados a mi dirección de correo electrónico de AWS Builder ID

Si aún puedes iniciar sesión con tu ID de AWS Builder, usa la página de perfil para actualizar el correo electrónico de tu AWS Builder ID a tu nueva dirección de correo electrónico. Tras completar la verificación del correo electrónico, podrás iniciar sesión AWS y recibir comunicaciones en tu nueva dirección de correo electrónico.

Si utilizó una dirección de correo electrónico profesional o universitaria, y ha dejado la empresa o el centro educativo, por lo que no puede recibir ningún correo electrónico enviado a esa dirección,

póngase en contacto con el administrador de ese sistema de correo electrónico. Es posible que puedan reenviar su correo electrónico a una nueva dirección, concederle acceso temporal o compartir contenido de su buzón.

No puedo habilitar la MFA

Para habilitar la MFA, añada uno o más dispositivos MFA a su perfil siguiendo los pasos que se indican en Gestione la autenticación ID de creador de AWS multifactor (MFA).

No puedo añadir una aplicación de autenticación como dispositivo de MFA

Si ve que no puede añadir otro dispositivo MFA, es posible que haya alcanzado el límite de dispositivos MFA que puede registrar en esa aplicación. Intente quitar un dispositivo MFA que no esté utilizando, o bien emplee una aplicación de autenticación diferente.

No puedo quitar un dispositivo MFA

Si tiene intención de deshabilitar la MFA, quite el dispositivo MFA siguiendo los pasos que se indican en Eliminar su dispositivo MFA. Sin embargo, si desea mantener la MFA habilitada, debe añadir otro dispositivo MFA antes de intentar eliminar un dispositivo MFA existente. Para obtener más información acerca de la adición de dispositivos MFA, consulte Gestione la autenticación ID de creador de AWS multifactor (MFA).

Cuando intento registrarme o iniciar sesión con una aplicación de autenticación, aparece el mensaje “Se ha producido un error inesperado”

Un sistema de contraseñas de un solo uso (TOTP) basado en el tiempo, como el que utiliza AWS Builder ID en combinación con una aplicación de autenticación basada en código, se basa 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 el NIST u otras equivalentes. local/regional

Cuando intento iniciar sesión en Builder ID, aparece el mensaje «No eres tú, somos nosotros» AWS

Compruebe la configuración de fecha y hora del dispositivo que utiliza para iniciar sesión. Recomendamos que establezca que la fecha y la hora se ajusten automáticamente. Si esa opción no está disponible, recomendamos que sincronice la fecha y la hora con un servidor de protocolo de hora de red (NTP) conocido.

Cerrar sesión no significa que se cierre mi sesión por completo

El sistema está diseñado para cerrar sesión inmediatamente, pero cerrar la sesión por completo puede llevar hasta una hora.

> **Note**
>
> Al utilizar una cuenta de inicio de sesión social como Google o Apple, al eliminar ID de creador de AWS las sesiones activas no se cerrará la sesión de su cuenta de inicio de sesión social.

Sigo intentando resolver mi problema

Puede rellenar el formulario de comentarios para el equipo de asistencia. En la sección Solicitar información, en Cómo podemos ayudarte, indica que estás utilizando AWS Builder ID. Proporcione la mayor cantidad de detalles posible para que podamos estudiar su problema de mejor manera posible.

AWS políticas gestionadas para AWS Sign-In

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

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

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

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

AWS política gestionada: AmazonManagedSignUpServicePolicy

La `AmazonManagedSignUpServicePolicy` política otorga los permisos necesarios para completar los procesos de registro de AWS cuentas.

Puede asociar `AmazonManagedSignUpServicePolicy` a los usuarios, grupos y roles.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- Verificación del cliente: permite crear, recuperar y actualizar los detalles de verificación del cliente y su estado de elegibilidad, incluida la creación de direcciones URL de carga para los documentos de verificación.

Para ver más detalles sobre la política, incluyendo la última versión del documento de política JSON, consulte AmazonManagedSignUpServicePolicy en la Guía de referencia de políticas administradas de AWS .

AWS política gestionada: ApplicationProvisioningPolicy

La ApplicationProvisioningPolicy política otorga permisos integrales para las operaciones de aprovisionamiento de aplicaciones y administración de identidades, incluida la administración de roles y políticas de IAM, la configuración del SSO y las operaciones de almacenamiento de identidades.

Puede asociar `ApplicationProvisioningPolicy` a los usuarios, grupos y roles.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- Administración de IAM: permite realizar operaciones de IAM integrales, como la creación, actualización y eliminación de roles y políticas, la administración de las conexiones de roles y la creación de funciones vinculadas a los servicios.
- Estudio de investigación e ingeniería en AWS: permite realizar todas las operaciones con los recursos de Estudio de investigación e ingeniería en AWS .
- Transferencia de roles: permite transferir roles de IAM a otros servicios.
- IAM Identity Center: permite administrar las instancias, las aplicaciones, las asignaciones, las concesiones y los métodos de autenticación del IAM Identity Center.
- Identity Store: permite leer la información de usuarios y grupos del almacén de identidades.
- IAM Identity Center OAuth: permite autenticar las sesiones de IAM a través del IAM Identity Center OAuthh.
- Perfil de usuario y directorio: permite administrar los conectores, los perfiles de usuario y las configuraciones de directorios del IAM Identity Center, incluida la configuración de un proveedor de identidad externo.
- Suscripciones de usuarios: permite enumerar las suscripciones de los usuarios.

Para ver más detalles sobre la política, incluyendo la última versión del documento de política JSON, consulte ApplicationProvisioningPolicy en la Guía de referencia de políticas administradas de AWS .

AWS política gestionada: SignInLocalDevelopmentAccess

La `SignInLocalDevelopmentAccess` política concede permisos de acceso programático para AWS utilizar las credenciales de la consola.

Puede asociar `SignInLocalDevelopmentAccess` a los usuarios, grupos y roles.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- Autorizar el acceso a OAuth2: otorga permiso para autenticarse a través de un navegador y obtener un código de autorización de OAuth 2.0 para el intercambio de credenciales
- Creación de un token OAuth2: otorga permiso para intercambiar un código de autorización por un token de acceso y un token de actualización de OAuth 2.0, que se puede usar para acceder a los servicios desde las herramientas y aplicaciones para desarrolladores AWS

> **Note**
>
> Añadir esta política AWS gestionada te da permiso tanto para la autenticación en el mismo dispositivo como para la autenticación multidispositivo. Esta política autoriza acciones en los siguientes recursos:
>
> - `arn:aws:signin:`*`region`*`:`*`account-id`*`:oauth2/public-client/localhost`— Se utiliza para la autenticación en el mismo dispositivo con. `aws login`
> - `arn:aws:signin:`*`region`*`:`*`account-id`*`:oauth2/public-client/remote`— Se utiliza para la autenticación multidispositivo con. `aws login --remote`
>
> Para controlar el acceso a cualquiera de los métodos de autenticación, puede crear su propia política gestionada o política de control de servicios (SCP). Utilice estos ARN de recursos para permitir o denegar el acceso programático a AWS con las credenciales de la consola.

Para obtener más información, consulte Inicie sesión con las credenciales de la consola (recomendado). Para ver más detalles sobre la política, incluyendo la última versión del documento de política JSON, consulte SignInLocalDevelopmentAccess en la Guía de referencia de políticas administradas de AWS .

AWS política gestionada: AWSSignInResourcePolicyManagement

La `AWSSignInResourcePolicyManagement` política otorga permisos para administrar la configuración de autorizaciones de la consola y las declaraciones de permisos de los recursos para AWS Sign-In.

Puede asociar `AWSSignInResourcePolicyManagement` a los usuarios, grupos y roles.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `signin:PutConsoleAuthorizationConfiguration`— Crear o actualizar la configuración de autorización de la consola.
- `signin:GetConsoleAuthorizationConfiguration`— Recupera la configuración de autorización de la consola actual.
- `signin:DeleteConsoleAuthorizationConfiguration`— Eliminar la configuración de autorización de la consola.
- `signin:PutResourcePermissionStatement`— Crear o actualizar las declaraciones de permisos de los recursos.
- `signin:DeleteResourcePermissionStatement`— Eliminar las declaraciones de permiso de los recursos.
- `signin:ListResourcePermissionStatements`— Listar las declaraciones de permisos de recursos de la cuenta.
- `signin:GetResourcePolicy`— Recuperar la política consolidada basada en los recursos.

La siguiente es la política JSON:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "signin:PutConsoleAuthorizationConfiguration",
                "signin:GetConsoleAuthorizationConfiguration",
                "signin:DeleteConsoleAuthorizationConfiguration",
                "signin:PutResourcePermissionStatement",
```

```
                "signin:DeleteResourcePermissionStatement",
                "signin:ListResourcePermissionStatements",
                "signin:GetResourcePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Adjunte esta política a los directores de IAM (usuarios o roles) que gestionan las políticas basadas en recursos. AWS Sign-In Esto incluye a los administradores de seguridad responsables de configurar los controles de acceso basados en la red, a los responsables de cumplimiento que deben auditar las políticas de acceso a las consolas y a los equipos de operaciones que gestionan las configuraciones de los accesos de recuperación de emergencia.

> **Important**
>
> Esta política otorga acceso administrativo a los controles de autorización de la consola. Aplique el principio del privilegio mínimo al asignar esta política. Considere la posibilidad de utilizar las condiciones de IAM para restringir aún más cuándo y cómo se pueden utilizar estos permisos.

Para ver más detalles sobre la política, incluyendo la última versión del documento de política JSON, consulte AWSSignInResourcePolicyManagement en la Guía de referencia de políticas administradas de AWS .

AWS Sign-In actualizaciones de AWS políticas administradas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas AWS Sign-In desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS Sign-In documento.

Cambio	Descripción	Fecha
AWSSignInResourcePolicyManagement: política nueva	Se agregó una nueva política AWS administrada que otorga permisos para administrar la	10 de junio de 2026

Cambio	Descripción	Fecha
	configuración de autorizaciones de la consola y las declaraciones de permisos de los recursos para AWS Sign-In.	
SignInLocalDevelopmentAccess: política nueva	Se agregó una nueva política AWS administrada que otorga permisos de acceso programático para AWS usar las credenciales de consola existentes.	19 de noviembre de 2025
ApplicationProvisioningPolicy: política nueva	Se agregó una nueva política AWS administrada que otorga permisos integrales para las operaciones de aprovisionamiento de aplicaciones y administración de identidades, incluida la administración de roles y políticas de IAM, la configuración del centro de identidad de IAM y las operaciones del almacén de identidades.	30 de septiembre de 2025
AmazonManagedSignUpServicePolicy: política nueva	Se agregó una nueva política AWS administrada que otorga los permisos necesarios para los procesos de registro de AWS cuentas, incluidas las operaciones de verificación de clientes y configuración de pagos.	30 de septiembre de 2025

Cambio	Descripción	Fecha
AWS Sign-In comenzó a rastrear los cambios	AWS Sign-In comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	30 de septiembre de 2025

Historial del documento

En la siguiente tabla se describen las adiciones importantes a la AWS Sign-In documentación. Actualizamos la documentación con frecuencia para dar respuesta a los comentarios que se nos envía.

- Última actualización importante de la documentación: 10 de junio de 2026

Cambio	Descripción	Fecha
Support for Sign-in resource-based policies and resources control policies	Se agregó documentación para controlar el Consola de administración de AWS acceso mediante políticas Sign-in basadas en recursos y políticas de control de recursos (RCP), una nueva referencia sobre las claves de condición, la política `AWSSignInResourcePolicyManagement` administrada y la solución de problemas relacionada.	10 de junio de 2026
Support para Sign in with GitHub y Amazon	AWS Sign-In ahora es compatible con Iniciar sesión con GitHub e Iniciar sesión con Amazon para que puedas crear una ID de creador de AWS con tu cuenta GitHub o con Amazon.	10 de marzo de 2026
Support for Sign in with Apple	AWS Sign-In ahora es compatible con Iniciar sesión con Apple para que puedas crear una ID de creador de	5 de febrero de 2026

	AWS con tu cuenta de Apple. ID de creador de AWS temas actualizados y nuevos temas de solución de problemas añadidos a la sección Solución de ID de creador de AWS problemas.	
Nueva política gestionada	AWS Sign-In ha publicado una nueva política gestionada. `SignInLocalDevelopmentAccess` concede permisos de acceso programático para poder AWS utilizar las credenciales de consola existentes. Para obtener más información, consulte AWS Sign-In las actualizaciones de las políticas AWS administradas.	19 de noviembre de 2025
Soporte para iniciar sesión con Google	AWS Sign-In ahora es compatible con el inicio de sesión con Google para que puedas crear una ID de creador de AWS con tu cuenta de Google. ID de creador de AWS se han actualizado los temas y se han añadido nuevos temas de solución de problemas a la sección Solución de ID de creador de AWS problemas.	30 de septiembre de 2025

Nuevas políticas administradas	AWS Sign-In ha publicado dos nuevas políticas gestionadas. `AmazonManagedSignUpServicePolicy` concede los permisos necesarios para completar los procesos de registro de AWS cuentas. `ApplicationProvisioningPolicy` otorga permisos integrales para las operaciones de aprovisionamiento de aplicaciones y administración de identidades. Para obtener más información, consulte AWS Sign-In las actualizaciones de las políticas AWS gestionadas.	30 de septiembre de 2025
Temas de solución de problemas actualizados	Se agregaron nuevos temas de solución de problemas para iniciar sesión en ID de creador de AWS y en Consola de administración de AWS.	27 de febrero de 2024
Se han actualizado varios temas para que aparezcan mejor organizados.	Tipos de usuario actualizados, eliminados Determine el tipo de usuario e incorpore su contenido a los tipos de usuario, Cómo iniciar sesión en AWS	15 de mayo de 2023

Se han actualizado varios temas y el banner superior	Tipos de usuario actualizados, determinar el tipo de usuario, cómo iniciar sesión AWS, ¿qué es AWS Sign-in? . También se han actualizado los procedimientos de inicio de sesión de usuario raíz y de usuario de IAM.	3 de marzo de 2023
Párrafo de introducción actualizado para Consola de administración de AWS iniciar sesión	Se ha desplazado Determinar tipo de usuario a la parte superior de la página y se ha eliminado la nota que había en Usuario raíz de la cuenta.	27 de febrero de 2023
Añadido ID de creador de AWS	Se agregaron ID de creador de AWS temas a la Guía del AWS Sign-In usuario y se integró contenido en los temas existentes.	31 de enero de 2023
Actualización organizativa	Basándonos en los comentarios de los clientes, se ha actualizado la tabla de contenido para que los métodos de inicio de sesión fueran más claros. Se han actualizado los tutoriales de inicio de sesión. Se han actualizado Terminología y Determinar tipo de usuario. Se ha mejorado la interconexión para definir términos como usuario de IAM y usuario raíz.	22 de diciembre de 2022

Nueva guía	Esta es la primera versión de la Guía AWS Sign-In del usuario.	31 de agosto de 2022

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