aws

Guía del usuario

Configuración de AWS

Configuración de AWS: Guía del usuario

Table of Contents

Información general

Esta guía proporciona instrucciones para crear una nueva Cuenta de AWS y configurar su primer usuario administrativo en AWS IAM Identity Center siguiendo las prácticas recomendadas de seguridad más recientes.

Una Cuenta de AWS es obligatoria para acceder a Servicios de AWS y cumple dos funciones básicas:

- Contenedor: una Cuenta de AWS es un contenedor para todos los recursos de AWS que puede crear como cliente de AWS. Cuando crea un bucket de Amazon Simple Storage Service (Amazon S3) o una base de datos de Amazon Relational Database Service (Amazon RDS) para almacenar sus datos, o una instancia de Amazon Elastic Compute Cloud (Amazon EC2) para procesar sus datos, está creando un recurso en su cuenta. Cada recurso se identifica de forma única mediante un nombre de recurso de Amazon (ARN) que incluye el ID de cuenta de la cuenta que contiene o es propietaria del recurso.
- Límite de seguridad: una Cuenta de AWS es el límite de seguridad básico de sus recursos de AWS. Los recursos que cree en su cuenta están disponibles solo para los usuarios que tengan credenciales para esa misma cuenta.

  Entre los recursos clave que puede crear en su cuenta están las identidades, como los usuarios y roles de IAM, y las identidades federadas, como los usuarios del directorio de usuarios de su empresa, un proveedor de identidades web, el directorio de IAM Identity Center o cualquier otro usuario que acceda a Servicios de AWS mediante el uso de credenciales proporcionadas a través de una fuente de identidad. Estas identidades tienen credenciales que alguien puede usar para iniciar sesión o autenticarse en AWS. Las identidades también tienen políticas de permisos que especifican lo que la persona que ha iniciado sesión está autorizada a hacer con los recursos de la cuenta.

Terminología

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

Administrador

También se denomina administrador de Cuenta de AWS o administrador de IAM. El administrador, normalmente personal de tecnología de la información (TI), es una persona que supervisa una Cuenta de AWS. Los administradores tienen un nivel de permisos superior al de la Cuenta de AWS que otros miembros de su organización. Los administradores establecen e implementan la configuración para la Cuenta de AWS. También crean usuarios de IAM o IAM Identity Center. El administrador proporciona a estos usuarios sus credenciales de acceso y una URL de inicio de sesión para iniciar sesión en AWS.

Cuenta

Una Cuenta de AWS estándar contiene tanto sus recursos de AWS 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. Las credenciales son la información que los usuarios proporcionan a AWS para iniciar sesión y acceder a los recursos de AWS. Las credenciales pueden incluir 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. En la autenticación y la autorización, un sistema utiliza las credenciales para identificar quién realiza una llamada y decidir si se permitirá el acceso solicitado. En AWS, estas credenciales son, por lo general, un ID de clave de acceso y una clave de acceso secreta.

Para obtener más información sobre las credenciales, consulte Descripción y obtención de las credenciales de AWS.

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

Credenciales corporativas

Las credenciales que proporcionan los usuarios al acceder a sus redes y recursos corporativos. El administrador corporativo puede configurar su Cuenta de AWS para que sea accesible con 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 se registra para obtener un Builder ID de AWS, crea un perfil. Su perfil incluye la información de contacto que ha proporcionado y la capacidad de administrar los dispositivos de autenticación multifactor (MFA) y las sesiones activas. También puede obtener más información sobre la privacidad y cómo gestionamos sus datos en su perfil. Para obtener más información sobre su perfil y cómo se relaciona con una Cuenta de AWS, consulte Builder ID de AWS y otras credenciales de AWS.

Usuario

Un usuario es una persona o aplicación en una cuenta que tiene que realizar llamadas a la API a productos de AWS. Cada usuario tiene un nombre único dentro de la Cuenta de AWS y un conjunto de credenciales de seguridad que no se comparten con otros usuarios. Estas credenciales son independientes de las credenciales de seguridad de la Cuenta de AWS. Cada usuario está asociado a una única Cuenta de AWS.

Credenciales del usuario raíz

Las credenciales del usuario raíz son las mismas que se utilizan para iniciar sesión en la AWS Management Console como usuario raíz. Para obtener más información sobre el usuario raíz, consulte Usuario raíz.

Código de verificación

Un código de verificación verifica su identidad durante el proceso de inicio de sesión con la autenticación multifactor (MFA). Los métodos de entrega de los códigos de verificación varían. Se pueden enviar por mensaje de texto o correo electrónico. Consulte con su administrador para obtener más información.

Usuarios y credenciales AWS

Al interactuar con AWS, debe especificar sus credenciales de seguridad de AWS con el fin de demostrar quién es usted y si tiene permiso para acceder a los recursos que solicita. AWS utiliza las credenciales de seguridad para autenticar y autorizar sus solicitudes.

Por ejemplo, si desea descargar un archivo protegido de un bucket de Amazon Simple Storage Service (Amazon S3), sus credenciales deben permitir ese tipo de acceso. Si sus credenciales no muestran que está autorizado para descargar el archivo, AWS le denegará la solicitud. Sin embargo, sus credenciales de seguridad no son necesarias para descargar un archivo de un bucket de Amazon S3 que se comparte públicamente.

Usuario raíz

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

> **Important**
>
> Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el correo electrónico y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice 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 obtener la lista completa de las tareas que requieren que inicie sesión como 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 incluido el usuario raíz, consulte Identidades de IAM (usuarios, grupos de usuarios y roles).

Usuario del Identity Center IAM

Un usuario del IAM Identity Center inicia sesión a través del portal de acceso de AWS. El administrador o el empleado del servicio de asistencia proporcionan el portal de AWS de acceso o la URL de inicio de sesión específica. Si ha creado un usuario del IAM Identity Center para su Cuenta de AWS, se le ha enviado una invitación para unirse al usuario del IAM Identity Center a la dirección de correo electrónico deCuenta de AWS. La URL de inicio de sesión específica se incluye en la invitación por correo electrónico. Los usuarios del IAM Identity Center no pueden iniciar sesión a través de la AWS Management Console. Para obtener instrucciones paso a paso sobre cómo iniciar sesión, consulte Iniciar sesión en el portal de acceso de AWS.

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

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

Identidad federada

Una identidad federada es un usuario que puede iniciar sesión al utilizar un proveedor de identidades (IdP), 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 para entonces intercambiarlo por credenciales de seguridad temporales en AWS que tienen asignado un rol de IAM con permisos para utilizar los recursos en su Cuenta de AWS. No inicia sesión con la AWS Management Console o el portal de acceso de AWS. En su lugar, la identidad externa utilizada determina cómo se inicia sesión.

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

Usuario de IAM

Un usuario de IAM es una entidad que se crea en AWS. Este usuario es una identidad en su Cuenta de AWS que tiene permisos personalizados específicos. Sus credenciales de usuario de IAM

consisten en un nombre y una contraseña que se utilizan para iniciar sesión en la AWS Management Console. Para obtener instrucciones paso a paso sobre cómo iniciar sesión, consulte Iniciar sesión en la AWS Management Console como un usuario de IAM.

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

Usuario de Builder ID de AWS

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

Requisitos previos y consideraciones

Antes de comenzar el proceso de configuración, revise los requisitos de la cuenta, considere si necesitará más de una Cuenta de AWS y comprenda los requisitos para configurar su cuenta para el acceso administrativo en IAM Identity Center.

Requisitos de Cuenta de AWS

Para inscribirse en una Cuenta de AWS, debe proporcionar la siguiente información:

- Un nombre de cuenta: el nombre de la cuenta aparece en varios lugares, como en la factura, y en las consolas, como el panel de gestión de facturación y costos, y la consola de AWS Organizations.

  Le recomendamos que utilice un estándar de nomenclatura de cuentas para que el nombre de la cuenta pueda reconocerse y distinguirse fácilmente de otras cuentas que pueda tener. Si se trata de una cuenta de empresa, considere la posibilidad de utilizar un estándar de nomenclatura, como organización-propósito-entorno (por ejemplo, Empresa-auditoría-prod). Si se trata de una cuenta personal, considere la posibilidad de utilizar un estándar de nomenclatura, como nombre-apellido-propósito (por ejemplo, paulo-santos-cuentadeprueba).
- Una dirección de correo electrónico: esta dirección de correo electrónico se utiliza como nombre de inicio de sesión para el usuario raíz de la cuenta y es necesaria para la recuperación de la cuenta, por ejemplo, si olvida la contraseña. Debe poder recibir los mensajes enviados a esta dirección de correo electrónico. Antes de poder realizar determinadas tareas, debe comprobar que tiene acceso a la cuenta de correo electrónico.

> **Important**
>
> Si esta cuenta es para una empresa, le recomendamos que utilice una lista de distribución corporativa (por ejemplo, `it.admins@example.com`). Evite usar la dirección de correo electrónico corporativa de una persona (por ejemplo, `paulo.santos@example.com`). Esto ayuda a garantizar que su empresa pueda acceder a la Cuenta de AWS si un empleado cambia de puesto o deje la empresa. La dirección de correo electrónico se puede utilizar para restablecer las credenciales del usuario raíz de la cuenta. Asegúrese de proteger el acceso a esta lista o dirección de distribución.

- Un número de teléfono: este número se puede usar cuando se requiera la confirmación de la propiedad de la cuenta. Debe poder recibir llamadas a este número de teléfono.

> **Important**
>
> Si esta cuenta es para una empresa, le recomendamos que utilice un número de teléfono corporativo en lugar de un número de teléfono personal. Esto ayuda a garantizar que su empresa pueda acceder a la Cuenta de AWS si un empleado cambia de puesto o deje la empresa.

- Un dispositivo de autenticación multifactor: para proteger sus recursos de AWS, habilite la autenticación multifactor (MFA) en la cuenta del usuario raíz. Además de las credenciales de inicio de sesión habituales, se requiere una autenticación secundaria cuando se activa la MFA, lo que proporciona una capa adicional de seguridad. Para obtener más información acerca de la MFA, consulte ¿Qué es la MFA? en la Guía del usuario de IAM.
- Plan de AWS Support: se le pedirá que elija uno de los planes disponibles durante el proceso de creación de la cuenta. Para obtener una descripción de los planes disponibles, consulte Comparar los planes de AWS Support.

Consideraciones sobre IAM Identity Center

Los siguientes temas proporcionan orientación para configurar IAM Identity Center para entornos específicos. Antes de continuar con Parte 2: cree un usuario administrativo en IAM Identity Center, comprenda las instrucciones que se aplican a su entorno.

Temas

- Active Directory o IdP externo
- AWS Organizations
- Roles de IAM
- Firewalls de última generación y puertas de enlace web seguras

Active Directory o IdP externo

Si ya administra usuarios y grupos en Active Directory o en un IdP externo, le recomendamos que considere la posibilidad de conectar esta fuente de identidad al habilitar IAM Identity Center y elegir

su fuente de identidad. Hacerlo antes de crear usuarios y grupos en el directorio predeterminado del Identity Centeres lo ayudará a evitar la configuración adicional que se requiere si cambia la fuente de identidad más adelante.

Si quiere utilizar Active Directory como fuente de identidad, la configuración debe cumplir los siguientes requisitos previos:

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

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

  - Conectar un directorio en AWS Managed Microsoft AD a IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.
  - Conectar un directorio autogestionado de Active Directory a IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.
- Utilice un Active Directory que resida en la cuenta de administrador delegada:

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

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

AWS Organizations

Su Cuenta de AWS debe ser gestionada por AWS Organizations. Si no ha creado una organización, no tiene que hacerlo. Cuando habilite IAM Identity Center, elegirá si desea que AWS cree una organización para usted.

Si ya ha configurado AWS Organizations, asegúrese de que todas las características estén habilitadas. Para obtener más información, consulte Habilitar todas las características de la organización en la Guía del usuario de AWS Organizations.

Para habilitar IAM Identity Center, debe iniciar sesión en la AWS Management Console utilizando las credenciales de su cuenta de administración de AWS Organizations. No puede habilitar IAM Identity Center si ha iniciado sesión con las credenciales de una cuenta de miembro de AWS Organizations. Para obtener más información, consulte Crear y gestionar una organización de AWS en la Guía del usuario de AWS Organizations.

Roles de IAM

Si ya ha configurado los roles de IAM en su Cuenta de AWS, le recomendamos que compruebe si su cuenta se acerca a la cuota de roles de IAM. Para obtener más información, consulte Cuotas de objetos de IAM.

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

Firewalls de última generación y puertas de enlace web seguras

Si filtra el acceso a dominios de AWS o puntos de conexión de URL específicos mediante una solución de filtrado de contenido web, como los NGFW o los SWG, debe añadir los siguientes dominios o puntos de conexión de URL a las listas de permitidos de su solución de filtrado de contenido web.

Dominios de DNS específicos

- *.awsapps.com (http://awsapps.com/)
- *.signin.aws

Puntos de conexión de URL específicos

- https://*[su directorio]*.awsapps.com/start
- https://*[su directorio]*.awsapps.com/login
- https://*[su región]*.signin.aws/platform/login

Uso de múltiples Cuentas de AWS

Las Cuentas de AWS sirven como límite de seguridad fundamental en AWS. Sirven como un contenedor de recursos que proporciona un nivel útil de aislamiento. La capacidad de aislar recursos y usuarios es un requisito clave para establecer un entorno seguro y bien gobernado.

Separar los recursos en Cuentas de AWS por separado lo ayuda a admitir los siguientes principios en su entorno de nube:

- Control de seguridad: las diferentes aplicaciones pueden tener diferentes perfiles de seguridad que requieren políticas y mecanismos de control diferentes. Por ejemplo, es más fácil hablar con un auditor y poder apuntar a una sola Cuenta de AWS que aloje todos los elementos de la carga de trabajo que estén sujetos a Normas de seguridad para la industria de tarjetas de pago (PCI).
- Aislamiento: una Cuenta de AWS es una unidad de protección de seguridad. Los posibles riesgos y amenazas a la seguridad deben estar contenidos dentro de una Cuenta de AWS sin afectar a otras. Puede haber diferentes necesidades de seguridad debido a los diferentes equipos o perfiles de seguridad.
- Muchos equipos: los diferentes equipos tienen diferentes responsabilidades y necesidades de recursos. Puede evitar que los equipos interfieran entre sí moviéndolos a Cuentas de AWS por separado.
- Aislamiento de datos: además de aislar a los equipos, es importante aislar los almacenes de datos en una cuenta. Esto puede ayudar a limitar la cantidad de personas que pueden acceder a ese almacén de datos y administrarlo. Esto ayuda a contener la exposición a datos altamente privados y, por lo tanto, puede ayudar a cumplir con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.
- Proceso de negocio: las distintas unidades de negocio o productos pueden tener propósitos y procesos completamente diferentes. Con varias Cuentas de AWS, puede satisfacer las necesidades específicas de una unidad de negocio.
- Facturación: una cuenta es la única forma verdadera de separar los elementos a nivel de facturación. Las cuentas múltiples ayudan a separar los elementos a nivel de facturación entre

unidades de negocio, equipos funcionales o usuarios individuales. Aún puede consolidar todas sus facturas en un único pagador (usando AWS Organizations y la facturación consolidada) y separar las partidas por Cuenta de AWS.

- Asignación de cuotas: las cuotas de servicio de AWS se aplican por separado para cada Cuenta de AWS. Separar las cargas de trabajo en diferentes Cuentas de AWS les impide consumir cuotas entre sí.

Todas las recomendaciones y procedimientos descritos en esta guía cumplen con el Marco de Well-Architected de AWS. Este marco está diseñado para ayudarlo a diseñar una infraestructura en la nube flexible, resiliente y escalable. Incluso cuando empieza de a poco, le recomendamos que proceda de acuerdo con las directrices en el marco. Hacerlo puede ayudarlo a escalar su entorno de forma segura y sin afectar sus operaciones en curso a medida que crece.

Antes de empezar a agregar varias cuentas, querrá desarrollar un plan para administrarlas. Para ello, le recomendamos que utilice AWS Organizations, que es un servicio de AWS gratuito, para gestionar todas las Cuentas de AWS en su organización.

AWS también ofrece AWS Control Tower, que añade capas de automatización de AWS administrada a las organizaciones y la integra automáticamente con otros servicios de AWS, como AWS CloudTrail, AWS Config, Amazon CloudWatch, AWS Service Catalog y otros. Estos servicios pueden generar costos adicionales. Para obtener más información, consulte Precios de AWS Control Tower.

Parte 1: configure una Cuenta de AWS nueva

Estas instrucciones lo ayudarán a crear una Cuenta de AWS y proteger las credenciales del usuario raíz. Complete todos los pasos antes de continuar con Parte 2: cree un usuario administrativo en IAM Identity Center.

Temas

Paso 1: regístrese en una cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Seleccione Crear una Cuenta de AWS.

   > **Note**
   >
   > Si ha iniciado sesión en AWS recientemente, seleccione Iniciar sesión en la consola. Si la opción Crear una Cuenta de AWS nueva no está visible, primero seleccione Iniciar sesión en otra cuenta y, a continuación, seleccione Crear una Cuenta de AWS nueva.

3. Introduzca la información de su cuenta y, a continuación, elija Continuar.

   Asegúrese de introducir la información de su cuenta correctamente, especialmente su dirección de correo electrónico. Si ingresa su dirección de correo electrónico de forma incorrecta, no podrá acceder a su cuenta.
4. Elija Personal o Profesional.

   La diferencia entre estas opciones radica únicamente en la información que le solicitamos. Ambos tipos de cuentas tienen las mismas características y funciones.
5. Introduzca la información de su empresa o su información personal según las instrucciones que se proporcionan en Requisitos de Cuenta de AWS.
6. Lea y acepte el Acuerdo con el cliente de AWS.
7. Seleccione Crear una cuenta y continuar.

En este momento, recibirá un mensaje de correo electrónico para confirmar que su Cuenta de AWS está lista para usar. Puede iniciar sesión en su cuenta nueva con la dirección de correo electrónico y contraseña que proporcionó al registrarse. Sin embargo, no puede utilizar ningún servicio de AWS hasta que termine de activar su cuenta.

8. En la página de Información de pago, introduzca la información sobre su método de pago. Si quiere usar una dirección diferente a la que usó para crear la cuenta, seleccione Usar una dirección nueva e introduzca la dirección que desea usar para la facturación.
9. Elija Verifica y añadir.

> **Note**
>
> Si su dirección de contacto está en la India, el acuerdo de usuario de su cuenta es con AISPL, un vendedor local de AWS en la India. Debe proporcionar su CVV como parte del proceso de verificación. Es posible que también tenga que introducir una contraseña de un solo uso, según su banco. AISPL cobra a su método de pago 2 INR como parte del proceso de verificación. AISPL reembolsa los 2 INR después de completar la verificación.

10. Para verificar su número de teléfono, elija el código de país o región de la lista e introduzca un número de teléfono al que se lo pueda llamar en los próximos minutos. Introduzca el código CAPTCHA y envíelo.
11. El sistema de verificación automática de AWS lo llama y le proporciona un PIN. Introduzca el PIN con su teléfono y, a continuación, seleccione Continuar.
12. Seleccione un plan de AWS Support.

    Para obtener una descripción de los planes disponibles, consulte Comparar los planes de AWS Support.

    Aparece una página de confirmación que indica que su cuenta se está activando. Esto suele hacerse en unos minutos, pero puede tardar hasta 24 horas. Durante la activación, puede iniciar sesión en su Cuenta de AWS nueva. Hasta que se complete la activación, es posible que vea el botón de Inscripción completa. Puede omitirlo.

    AWS envía un mensaje de correo electrónico de confirmación cuando se completa la activación de la cuenta. Busque el mensaje de correo electrónico de confirmación en su carpeta de correo

electrónico y correo no deseado. Tras recibir este mensaje, tendrá acceso completo a todos los servicios de AWS.

Paso 2: inicie sesión como usuario raíz

Cuando crea por primera vez una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todas las Servicios de AWS y recursos de la cuenta. Esta identidad recibe el nombre de usuario raíz de Cuenta de AWS, y se accede a ella iniciando sesión con el correo electrónico y la contraseña que utilizó para crear la cuenta.

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

Para iniciar sesión como usuario raíz

1. Abra la AWS Management Console en https://console.aws.amazon.com/.

   > **Note**
   >
   > Si ha iniciado sesión anteriormente como usuario raíz en este navegador, es posible que el navegador recuerde la dirección de correo electrónico para Cuenta de AWS.
   > 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. Para volver a la página principal de inicio de sesión, elija Iniciar sesión con dirección de correo electrónico de usuario raíz.

2. Si no ha iniciado sesión anteriormente en este navegador, aparecerá la página principal de inicio de sesión. Si es el propietario de la cuenta, elija Usuario raíz. Introduzca su dirección de correo electrónico de Cuenta de AWS asociada a su cuenta y elija Siguiente.

3. Es posible que se le pida que complete un control de seguridad. Complete esto para continuar con el siguiente paso. Si no puede completar el control de seguridad, intente escuchar el audio o actualizar el control de seguridad para ver si hay un nuevo conjunto de caracteres.
4. Escriba la contraseña y elija Iniciar sesión.

Paso 3: active la MFA para su usuario raíz de Cuenta de AWS

Para mejorar la seguridad de sus credenciales de usuario raíz, le recomendamos que siga la práctica recomendada de seguridad para activar la autenticación multifactor (MFA) para su Cuenta de AWS. Como el usuario raíz puede realizar operaciones confidenciales en su cuenta, añadir esta capa adicional de autenticación lo ayuda a protegerla mejor. Hay diversos tipos de MFA disponibles.

Para obtener instrucciones sobre cómo activar la MFA para el usuario raíz, consulte Habilitar dispositivos de MFA para usuarios en AWS en la Guía del usuario de IAM.

Parte 2: cree un usuario administrativo en IAM Identity Center

Después de completar Parte 1: configure una Cuenta de AWS nueva, los siguientes pasos lo ayudarán a configurar el acceso a la Cuenta de AWS para un usuario administrativo, que se utilizará para realizar las tareas diarias.

> **Note**
>
> En este tema se proporcionan los pasos mínimos necesarios para configurar correctamente el acceso de administrador para una Cuenta de AWS y crear un usuario administrativo en IAM Identity Center. Para obtener más información, consulte la Introducción de la Guía del usuario de AWS IAM Identity Center.

Temas

Paso 1: activar el IAM Identity Center

> **Note**
>
> Si no activó la autenticación multifactor (MFA) para el usuario raíz, complete Paso 3: active la MFA para su usuario raíz de Cuenta de AWS antes de continuar.

Activar el IAM Identity Center

1. Inicie sesión en la AWS Management Console como propietario de cuenta al elegir Usuario raíz e ingresar el correo electrónico de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

2. Abra la consola del IAM Identity Center
3. En Activar el IAM Identity Center, seleccione Activar.
4. El IAM Identity Center requiere AWS Organizations. Si no ha creado una organización, debe elegir si desea que AWS cree una para usted. Elija Crear una organización AWS para completar este proceso.

   AWS Organizations envía automáticamente un correo electrónico de verificación a la dirección asociada a su cuenta de administración. Puede pasar algún tiempo hasta que reciba el correo electrónico de verificación. Verifique la dirección de correo electrónico en un plazo de 24 horas.

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

Paso 2: elija su fuente de identidad

Su fuente de identidad en IAM Identity Center define dónde se administran sus usuarios y grupos. Puede elegir una de las siguientes opciones como fuente de identidad:

- Directorio de IAM Identity Center: cuando habilita IAM Identity Center por primera vez, se configura automáticamente con un directorio de IAM Identity Center como fuente de identidad predeterminada. Aquí es donde crea sus usuarios y grupos, y asigna su nivel de acceso a sus cuentas y aplicaciones de AWS.
- Active Directory: elija esta opción si quiere seguir administrando los usuarios en su directorio de Microsoft AD administrado por AWS mediante AWS Directory Service o en su directorio autogestionado en Active Directory (AD).
- Proveedor de identidades externo: elija esta opción si desea administrar los usuarios en un proveedor de identidades (IdP) externo, como Okta o Azure Active Directory.

Después de habilitar IAM Identity Center, debe elegir su fuente de identidad. La fuente de identidad que elija determina dónde busca IAM Identity Center los usuarios y grupos que necesitan acceso

con inicio de sesión único. Tras elegir la fuente de identidad, creará o especificará un usuario y le asignará permisos administrativos a su Cuenta de AWS.

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

Temas

Conectar Active Directory u otro IdP y especificar un usuario

Si ya utiliza Active Directory o un proveedor de identidades (IdP) externo, los siguientes temas lo ayudarán a conectar su directorio a IAM Identity Center.

Puede conectar un directorio de AWS Managed Microsoft AD, un directorio autogestionado en Active Directory o un IdP externo con IAM Identity Center. Si planea conectar un directorio de AWS Managed Microsoft AD o un directorio autogestionado en Active Directory, asegúrese de que la configuración de Active Directory cumpla con los requisitos previos de Active Directory o IdP externo.

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

configuración de la MFA. Los IDP externos no admiten el uso de la MFA en IAM Identity Center. Para obtener más información, consulte Habilitar la MFA en la Guía del usuario de AWS IAM Identity Center.

AWS Managed Microsoft AD

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

Directorio autogestionado en Active Directory

1. Revise la guía en Conectarse a un Active Directory de Microsoft.
2. Siga los pasos que se indican en Conectar un directorio autogestionado de Active Directory a IAM Identity Center.
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en IAM Identity Center. Para obtener más información, consulte Sincronizar un usuario administrativo en IAM Identity Center.

IdP externo

1. Revise la guía en Conectarse a un proveedor de identidades externo.
2. Siga las instrucciones de Conectarse a un proveedor de identidad externo.
3. Configure su IdP para aprovisionar usuarios al IAM Identity Center.

> **Note**
>
> Antes de configurar el aprovisionamiento automático y basado en grupos de todas las identidades de sus empleados desde su IdP al IAM Identity Center, le recomendamos que sincronice el único usuario al que quiere conceder permisos administrativos en el IAM Identity Center.

Sincronice un usuario administrativo en el IAM Identity Center

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

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

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

Siguiente paso: Paso 3: crear un conjunto de permisos administrativos

Utilice el directorio predeterminado y cree un usuario en el IAM Identity Center

Cuando se activa el IAM Identity Center por primera vez, se configura de manera automática con un directorio del IAM Identity Center como fuente de identidad predeterminada. Complete los siguientes pasos para crear un usuario en el IAM Identity Center.

1. Inicie sesión en AWS Management Console como propietario de cuenta al elegir Usuario raíz e ingresar su correo electrónico de Cuenta de AWS. En la siguiente página, escriba su contraseña.
2. Abra la Consola del IAM Identity Center.
3. Siga los pasos que se indican en Añadir usuarios para crear un usuario.

   Al especificar los detalles del usuario, puede enviar un correo electrónico con las instrucciones de configuración de la contraseña (esta es la opción predeterminada) o generar una contraseña de un solo uso. Si envía un correo electrónico, asegúrese de especificar una dirección de correo electrónico a la que pueda acceder.
4. Cuando haya agregado el usuario, regrese a este procedimiento. Si ha mantenido la opción predeterminada de enviar un correo electrónico con las instrucciones de configuración de la contraseña, haga lo siguiente:

   a. Recibirá un correo electrónico con el asunto Invitación para unirse a AWS Single Sign-On. Abra ese correo electrónico de invitación y elija Aceptar invitación.

   b. En la página de Registro de usuarios nuevos, introduzca y confirme una contraseña y, a continuación, seleccione Establecer nueva contraseña.

      > **Note**
      >
      > Asegúrese de guardar la contraseña. Lo necesitará más adelante para Paso 5: inicie sesión en el portal de acceso de AWS con sus credenciales administrativas.

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

Siguiente paso: Paso 3: crear un conjunto de permisos administrativos

Paso 3: crear un conjunto de permisos administrativos

Los conjuntos de permisos se guardan en el IAM Identity Center y definen el nivel de acceso que tienen los usuarios y grupos en una cuenta Cuenta de AWS. Realice los siguientes pasos para crear un conjunto de permisos que conceda permisos administrativos.

1. Inicie sesión en AWS Management Console como propietario de cuenta al elegir Usuario raíz e ingresar el correo electrónico de Cuenta de AWS. En la siguiente página, escriba su contraseña.
2. Abra la consola del IAM Identity Center.
3. En el panel de navegación del IAM Identity Center, en Permisos multicuenta, seleccione Conjuntos de permisos.
4. Elija Crear conjunto de permisos.
5. Para el Paso 1: seleccione el tipo de conjunto de permisos, en la página Seleccione el tipo de conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente. La configuración predeterminada otorga acceso total a los servicios y recursos AWS mediante el conjunto de permisos predefinidos de AdministratorAccess.

   > **Note**
   >
   > El conjunto de permisos predefinidos de AdministratorAccess utiliza la política gestionada AdministratorAccess de AWS.

6. Para el Paso 2: especificar los detalles del conjunto de permisos, en la página Especificar detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente. La configuración predeterminada limita la sesión a una hora.
7. Para el Paso 3: revisar y crear, en la página Revisar y crear, haga lo siguiente:
   1. Revise el tipo de conjunto de permisos y confirme que es AdministratorAccess.
   2. Revise la política administrada AWS y confirme que es AdministratorAccess.
   3. Seleccione Crear.

Paso 4: configurar el acceso Cuenta de AWS para un usuario administrativo

Para configurar el acceso a Cuenta de AWS de un usuario administrativo en el IAM Identity Center, debe asignar el usuario al conjunto de permisos AdministratorAccess.

1. Inicie sesión en AWS Management Console como propietario de cuenta al elegir Usuario raíz e ingresar su correo electrónico de Cuenta de AWS. En la siguiente página, escriba su contraseña.
2. Abra la Consola del IAM Identity Center.
3. En el panel de navegación, en Permisos para varias cuentas, elijaCuentas de AWS.
4. En la página Cuentas de AWS, aparece una lista de su organización en forma de árbol. Seleccione la casilla de verificación situada junto a la Cuenta de AWS a la que desea asignar el acceso administrativo. Si tiene varias cuentas en su organización, active la casilla de verificación situada junto a la cuenta de administración.
5. Seleccione Asignar usuarios o grupos.
6. Para el Paso 1: seleccionar usuarios y grupos, en la página Asignar usuarios y grupos a "***AWSnombre-de-cuenta***", haga lo siguiente:

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

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

    2. Tras confirmar que se haya seleccionado el usuario correcto, seleccione Siguiente.
7. Para el Paso 2: seleccionar conjuntos de permisos, en la página Asignar conjuntos de permisos a "***AWS-nombre-de-cuenta***", en Conjuntos de permisos, seleccione el conjunto de permisos AdministratorAccess.
8. Elija Siguiente
9. Para el Paso 3: Revisar y enviar, en la página Revisar y enviar las tareas a "***AWS-nombre-de-cuenta***", haga lo siguiente:

    1. Revise el usuario y el conjunto de permisos seleccionados.
    2. Tras confirmar que el usuario correcto está asignado al conjunto de permisos de AdministratorAccess, elija Enviar.

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

10. Si aplican alguna de las siguientes condiciones, siga los pasos de Habilitar MFA para habilitar MFA para el IAM Identity Center:

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

> **Note**
>
> Si utiliza un proveedor de identidad externo, tenga en cuenta que el IdP externo, no el IAM Identity Center, administra la configuración de MFA. Los IDP externos no admiten el uso de MFA en el IAM Identity Center.

Al configurar el acceso a la cuenta para el usuario administrativo, del IAM Identity Center crea el rol de IAM correspondiente. Este rol, controlado por el IAM Identity Center, se crea en la Cuenta de AWS correspondiente y se le adjuntan al rol las políticas especificadas en el conjunto de permisos.

Paso 5: inicie sesión en el portal de acceso de AWS con sus credenciales administrativas

Complete los siguientes pasos para confirmar que puede iniciar sesión en el portal de acceso de AWS con las credenciales del usuario administrativo y que puede acceder a la Cuenta de AWS.

1. Inicie sesión en la AWS Management Console como propietario de cuenta eligiendo Usuario raíz e ingresando el correo electrónico de su Cuenta de AWS. En la siguiente página, escriba su contraseña.
2. Abra la consola de AWS IAM Identity Center en https://console.aws.amazon.com/singlesignon/.
3. En el panel de navegación, elija Panel.

4. En la página del Panel, en Resumen de ajustes, copie la URL del portal de acceso de AWS.
5. Abra otro navegador, pegue la URL del portal de acceso de AWS que copió y presione Entrar.
6. Inicie sesión mediante cualquiera de las siguientes opciones:

   - Si utiliza Active Directory o un proveedor de identidades (IdP) externo como fuente de identidad, inicie sesión con las credenciales del usuario de Active Directory o IdP que asignó al conjunto de permisos de AdministratorAccess en IAM Identity Center.
   - Si utiliza el directorio predeterminado de IAM Identity Center como fuente de identidad, inicie sesión con el nombre de usuario que especificó al crear el usuario y la nueva contraseña que especificó para el usuario.
7. Después de iniciar sesión, un icono de Cuenta de AWS aparece en el portal.
8. Al seleccionar el icono de Cuenta de AWS, aparecen el nombre de la cuenta, el ID de la cuenta y la dirección de correo electrónico asociados a la cuenta.
9. Elija el nombre de la cuenta para mostrar el conjunto de permisos de AdministratorAccess y seleccione el enlace de la Consola de administración a la derecha de AdministratorAccess.

   Al iniciar sesión, el nombre del conjunto de permisos al que está asignado el usuario aparece como un rol disponible en el portal de acceso de AWS. Porque ha asignado este usuario al conjunto de permisos de `AdministratorAccess`, el rol aparecerá en el portal de acceso de AWS como: `AdministratorAccess/`*`nombre de usuario`*
10. Si se lo redirige a la Consola de administración de AWS, ha terminado correctamente de configurar el acceso administrativo a la Cuenta de AWS. Continúe con el paso 10.
11. Cambie al navegador que utilizó para iniciar sesión en la AWS Management Console y configure IAM Identity Center y cierre la sesión del usuario raíz de su Cuenta de AWS.

    > **Important**
    >
    > Le recomendamos encarecidamente que siga la práctica recomendada de utilizar las credenciales del usuario administrativo al iniciar sesión en el portal de acceso de AWS y que no utilice las credenciales del usuario raíz para sus tareas diarias.

Para permitir que otros usuarios accedan a sus cuentas y aplicaciones, y para administrar IAM Identity Center, cree y asigne conjuntos de permisos únicamente a través de IAM Identity Center.

Solución para problemas de conexión de Cuenta de AWS

Utilice la información que aquí se incluye para solucionar problemas relacionados para crear una Cuenta de AWS.

Problemas

- No he recibido la llamada de AWS para verificar mi cuenta nueva
- Cuando intento verificarlo mi Cuenta de AWS por teléfono, aparece un error sobre el "número máximo de intentos fallidos"
- Han pasado más de 24 horas y mi cuenta no está activada

No he recibido la llamada de AWS para verificar mi cuenta nueva

Al crear una Cuenta de AWS, debe proporcionar un número de teléfono en el que pueda recibir un mensaje de texto SMS o una llamada de voz. Debe especificar qué método utilizar para verificar el número.

Si no recibe el mensaje o la llamada, compruebe lo siguiente:

- Que ingresó el número de teléfono correcto y seleccionó el código de país correcto durante el proceso de registro.
- Si utiliza un teléfono móvil, asegúrese de tener señal de móvil para recibir llamadas o mensajes de texto SMS.
- La información que haya introducido para el método de pago es correcta.

Si no recibió un mensaje de texto SMS o una llamada para completar el proceso de verificación de identidad, AWS Support podemos ayudarlo a activar su Cuenta de AWS manualmente. Utilice los siguientes pasos:

1. Asegúrese de que lo puedan contactar al número de teléfono que proporcionó para su Cuenta de AWS.
2. Abra la AWS Supportconsola y elija Crear caso.
   a. Elija Soporte de cuentas y facturación
   b. En Tipo, seleccione Cuenta.
   c. En Categoría, seleccione Activación.

d. En la sección de Descripción del caso, indique la fecha y la hora en las que podamos contactarlo.

e. En la sección Opciones de contacto, seleccione Chat para ver los Métodos de contacto.

f. Elija Enviar.

> **Note**
>
> Puede crear un caso con AWS Support incluso si su Cuenta de AWS no está activada.

Cuando intento verificarlo mi Cuenta de AWS por teléfono, aparece un error sobre el "número máximo de intentos fallidos"

AWS Support puede ayudarlo a activar su cuenta manualmente. Siga estos pasos:

1. Inicie sesión en su Cuenta de AWS con la dirección de correo electrónico y la contraseña que especificó al crear su cuenta.
2. Abra la consola AWS Support y elija Crear caso.
3. Elija Soporte de cuentas y facturación
4. En Tipo, seleccione Cuenta.
5. En Categoría, seleccione Activación.
6. En la sección de Descripción del caso, indique la fecha y la hora en las que podamos contactarlo.
7. En la sección Opciones de contacto, seleccione Chat para ver los Métodos de contacto.
8. Elija Enviar.

AWS Support lo contactará y intentará activar manualmente su Cuenta de AWS.

Han pasado más de 24 horas y mi cuenta no está activada

En ocasiones, la activación de la cuenta puede retrasarse. Si el proceso tarda más de 24 horas, compruebe lo siguiente:

- Finalice el proceso de activación de la cuenta.

Si ha cerrado la ventana del proceso de registro antes de añadir toda la información necesaria, abra la página de registro. Seleccione Iniciar sesión en una cuenta existente Cuenta de AWS e inicie sesión con la dirección de correo electrónico y la contraseña que eligió para la cuenta.

- Compruebe la información asociada a su método de pago.

  En la consola AWS Billing and Cost Management, consulte los Métodos de pago para ver si hay errores.
- Póngase en contacto con su institución financiera.

  En ocasiones, las instituciones financieras rechazan las solicitudes de autorización de AWS. Póngase en contacto con la institución asociada a su método de pago y pídale que apruebe las solicitudes de autorización de AWS. AWScancela la solicitud de autorización tan pronto como la apruebe su institución financiera, por lo que no se le cobrará por la solicitud de autorización. Es posible que las solicitudes de autorización sigan figurando como un pequeño cargo (normalmente 1 USD) en los estados de cuenta de su institución financiera.
- Revise su correo electrónico y su carpeta de correo no deseado para ver si hay solicitudes de información adicional.
- Pruebe con otro navegador.
- Póngase en contacto con AWS Support.

  Póngase en contacto con AWS Support para obtener ayuda. Mencione cualquier paso de solución de problemas que ya haya probado.

> **Note**
>
> No proporcione información confidencial, como números de tarjetas de crédito, en ninguna correspondencia con AWS.