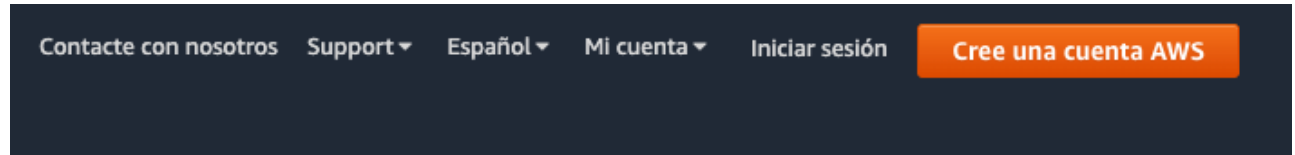


Tarea 2: Creación de una cuenta de AWS

Nombre: César Augusto Carchi Ludeña

1. Creación de la cuenta de AWS

- Accedemos a la página de [AWS](#) y pulsamos sobre **Cree una cuenta de AWS**.



- Completamos el formulario de registro. Asegúrate de elegir el tipo de **cuenta personal y el gratuito**.

Ofertas de la capa gratuita

Todas las cuentas de AWS pueden explorar 3 tipos diferentes de ofertas gratuitas, en función del producto utilizado.



Siempre gratis

Nunca vence



12 meses gratis

Inicio a partir de la fecha de registro inicial



Pruebas

Inicio a partir de la fecha de activación del servicio

Registrarse en AWS

Información de contacto

¿Cómo tiene previsto utilizar AWS?

- ☐ Empresarial: para su trabajo, escuela u organización
- ☒ Personal: para sus propios proyectos

¿A quién debemos contactar para consultar sobre esta cuenta?

Nombre completo

Número de teléfono

Introduzca el código de país y el número de teléfono.

+1 222-333-4444

País o región

Estados Unidos



Registrarse en AWS

Seleccionar un plan de soporte

Elija un plan de soporte para su cuenta personal o empresarial. [Compare planes y ejemplos de precio](#). Puede cambiar su plan en cualquier momento desde la consola de administración de AWS.

☒ Soporte de nivel Basic: gratis

- Recomendado para los usuarios nuevos que recién comienzan a utilizar AWS
- Acceso de autoservicio las 24 horas del día, los 7 días de la semana a los recursos de AWS
- Solo para problemas de facturación y cuentas
- Acceso a Personal Health Dashboard y Trusted Advisor



☐ Soporte Developer: a partir de 29 USD al mes

- Recomendado para desarrolladores que experimentan con AWS
- Acceso por correo electrónico a AWS Support durante el horario laboral
- Tiempos de respuesta de 12 horas (horario laboral)



☐ Soporte Business: a partir de 100 USD al mes

- Recomendado para ejecutar cargas de trabajo de producción en AWS
- Soporte técnico las 24 horas, los 7 días de la semana por correo electrónico, teléfono y chat
- Tiempos de respuesta de 1 hora
- Conjunto completo de recomendaciones de prácticas de Trusted Advisor



¿Necesita soporte de nivel Enterprise?

A partir de los 15 000 USD por mes, tendrá tiempos de respuesta de 15 minutos y una experiencia de conserje con un director técnico de cuenta asignado. [Más información](#)



¡Felicitaciones!

Gracias por registrarse en AWS.

Estamos activando la cuenta. Tardaremos solo unos minutos. Recibirá un correo electrónico cuando hayamos acabado.

[Ir a la consola de administración de AWS](#)

[Registrarse en otra cuenta](#) o [contacto de ventas](#)

- Iniciar sesión y acceder a los detalles de la cuenta AWS:



Iniciar sesión

☒ **Usuario raíz**

Propietario de la cuenta que realiza tareas que requieren acceso ilimitado. [Más información](#)

☐ **Usuario de IAM**

Usuario de una cuenta que realiza tareas diarias. [Más información](#)

Dirección de email del usuario raíz

Siguiente

Al continuar, acepta el [Contrato de cliente de AWS](#) u otro acuerdo para los servicios de AWS y el [Aviso de privacidad](#). Este sitio utiliza cookies esenciales. Consulte nuestro [Aviso de cookies](#) para obtener más información.

¿Es nuevo en AWS?

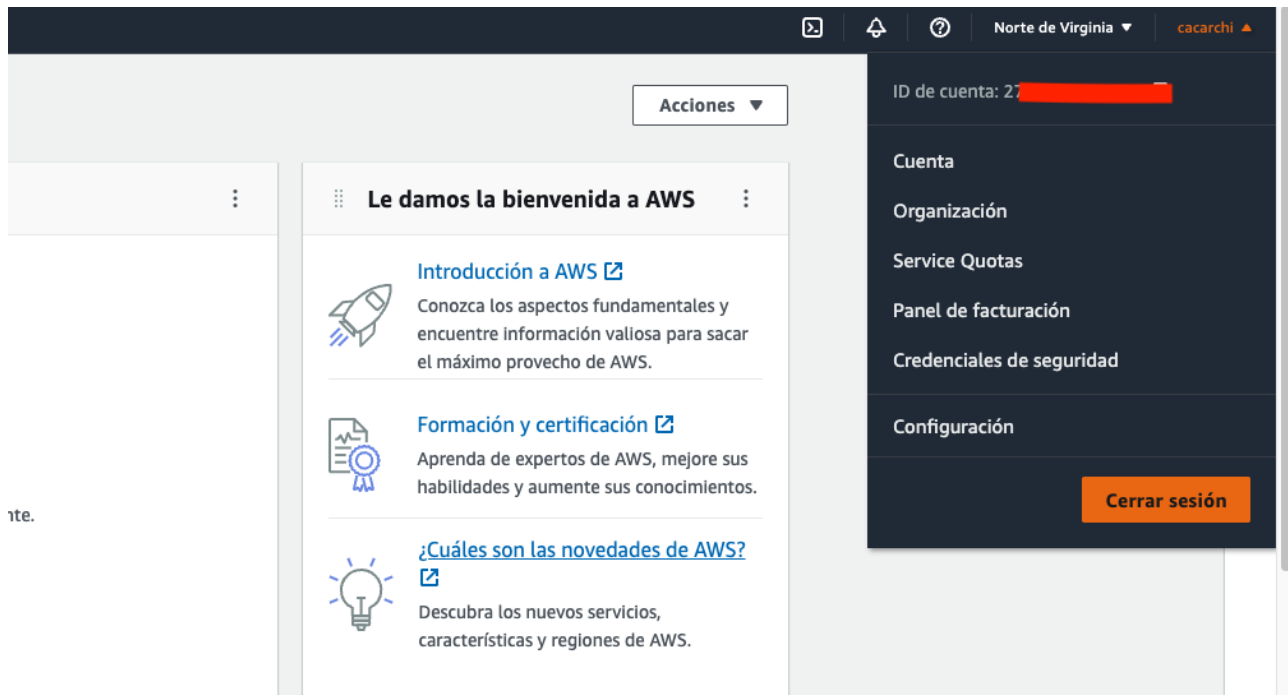
[Crear una cuenta de AWS](#)

Backup y restauración con AWS

Cree soluciones escalables, duraderas y seguras para la protección de datos con AWS.

[Más información »](#)





- Restringir uso de cuenta ROOT únicamente a operaciones críticas. Para ello accedemos a la opción "Cuenta" y nos ubicamos en la opción "Acceso de los usuarios y roles IAM a la información de facturación". Seguido hacemos clic en Editar y marcamos la casilla "Active el acceso de IAM" y pulsamos "Actualizar"

▼ Acceso de los usuarios y los roles de IAM a la información de facturación

[Editar](#)

Utilice la configuración de **Active el acceso de IAM** para permitir a los usuarios y roles de IAM obtener acceso a las páginas de la consola de administración de costos y facturación. Esta configuración por sí sola no otorga a los usuarios y roles de IAM los permisos necesarios para estas páginas de la consola. Además de activar el acceso de IAM, también debe asociar las políticas de IAM necesarias a esos usuarios o roles. Para obtener más información, consulte [Conceder acceso a las herramientas e información de facturación](#).

Si esta configuración está desactivada, los usuarios y roles IAM de esta cuenta no podrán acceder a las páginas de la consola de administración de costos y facturación, incluso si tienen acceso de administrador o las políticas IAM requeridas.

La configuración de **Active el acceso de IAM** no controla el acceso a:

- Las páginas de la consola correspondientes a la detección de anomalías en los costos de AWS, la información general de los Savings Plans, el inventario de Savings Plans, la compra de Savings Plans y el carrito de Savings Plans
- La visualización de la administración de costos en la AWS Console Mobile Application
- Las API del SDK de administración de costos y facturación (API de AWS Cost Explorer, AWS Budgets y AWS Cost and Usage Report)

El acceso de los usuarios o los roles de IAM a la información de facturación está desactivado.

▼ Acceso de los usuarios y los roles de IAM a la información de facturación

Utilice la configuración de **Active el acceso de IAM** para permitir a los usuarios y roles de IAM obtener acceso a las páginas de la consola de administración de costos y facturación. Esta configuración por sí sola no otorga a los usuarios y roles de IAM los permisos necesarios para estas páginas de la consola. Además de activar el acceso de IAM, también debe asociar las políticas de IAM necesarias a esos usuarios o roles. Para obtener más información, consulte [Conceder acceso a las herramientas e información de facturación](#).

Si esta configuración está desactivada, los usuarios y roles IAM de esta cuenta no podrán acceder a las páginas de la consola de administración de costos y facturación, incluso si tienen acceso de administrador o las políticas IAM requeridas.

La configuración de **Active el acceso de IAM** no controla el acceso a:

- Las páginas de la consola correspondientes a la detección de anomalías en los costos de AWS, la información general de los Savings Plans, el inventario de Savings Plans, la compra de Savings Plans y el carrito de Savings Plans
- La visualización de la administración de costos en la AWS Console Mobile Application
- Las API del SDK de administración de costos y facturación (API de AWS Cost Explorer, AWS Budgets y AWS Cost and Usage Report)
- Herramienta de la huella de carbono del cliente de la página Informes de coste y uso

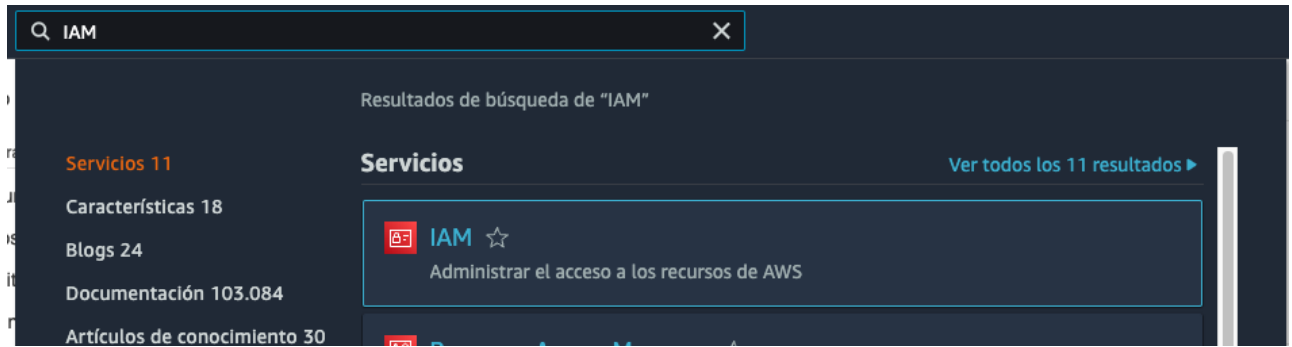
☒ **Active el acceso de IAM**

Actualizar

Cancelar

Seguridad de la cuenta de AWS

- **Acceder a IAM:** Para ello en la barra de búsqueda escribimos IAM y pulsamos sobre el servicio sugerido.



- Lo primero que vemos al acceder al panel de IAM es una alerta de seguridad que nos indica que no tenemos activado el múltiple factor de autenticación (MFA). Pulsamos sobre “Agregar MFA”

Panel de IAM

Recomendaciones de seguridad 1

!

Agregar MFA para el usuario raíz

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Agregar MFA

↻

✓

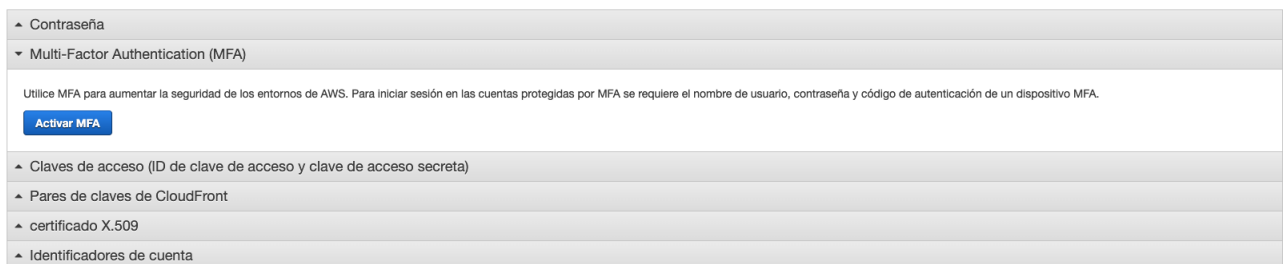
El usuario raíz no tiene claves de acceso activas

El uso de claves de acceso asociadas a un usuario de IAM en lugar del usuario raíz mejora la seguridad.

Recursos de IAM

Grupos de usuarios	Usuarios	Roles	Políticas	Proveedores de identidad
0	0	2	0	0

- Activamos MFA:



- Como podemos observar, AWS soporta diferentes tipos de autenticación de múltiple factor, en nuestro caso seleccionamos “Dispositivo MFA virtual” y pulsamos en “continuar”

Administrar el dispositivo MFA

Elija el tipo de dispositivo MFA para asignar:

☒ **Dispositivo MFA virtual**
Aplicación "Authenticator" instalada en el equipo o dispositivo móvil

☐ **Llave de seguridad U2F**
YubiKey o cualquier otro dispositivo compatible con U2F

☐ **Otro dispositivo MFA de hardware**
Token Gemalto

Para obtener más información acerca de los dispositivos MFA admitidos, consulte [AWS Multi-Factor Authentication](#)

Cancelar

Continuar

También puede escribir la clave secreta. [Mostrar la clave secreta](#)

3. Escriba dos códigos de MFA consecutivos a continuación

Código de MFA 1

Código de MFA 2

Configurar un dispositivo MFA virtual

☒ **Ha asignado un tipo de MFA virtual correctamente**
Esta MFA virtual se requerirá durante el inicio de sesión.

Cerrar

Se va a crear un nuevo usuario para realizar acciones específicas en AWS. Con este usuario accederemos normalmente y root solo utilizaremos para acciones de seguridad de la cuenta y facturación.

- **Agregar nuevo usuario:** Dentro del panel de IAM seleccionamos "Usuarios" y "Agregar usuarios"



- **Configuración nuevo usuario:** Introducimos un nombre para el usuario, por ejemplo "TESTUSER" y activamos la opción "Contraseña: acceso a la consola de administración de AWS" y "Contraseña personalizada"

Introducimos una contraseña robusta y desactivamos la opción "Requerir el restablecimiento de contraseña". Pulsamos en "Siguiente: Permisos".

Añadir usuario(s)



Establecer los detalles del usuario

Puede añadir varios usuarios a la vez con los mismos permisos y el mismo tipo de acceso. [Más información](#)

Nombre de usuario*

TESTUSER

[+ Añadir otro usuario](#)

Seleccionar el tipo de acceso de AWS

Seleccione cómo estos usuarios accederán principalmente a AWS. Si elige únicamente el acceso mediante programación, NO evitará que los usuarios accedan a la consola por medio de un rol asumido. Las claves de acceso y las contraseñas generadas automáticamente se proporcionan en el último paso. [Más información](#)

Seleccione el tipo de credenciales de AWS*

☐

Clave de acceso: acceso mediante programación

Habilita una **ID de clave de acceso** y una **clave de acceso secreta** para el SDK, la CLI y la API de AWS, además de otras herramientas de desarrollo.

☒

Contraseña: acceso a la consola de administración de AWS

Habilita una **contraseña** que permite a los usuarios iniciar sesión en la consola de administración de AWS.

Contraseña de la consola*

☐

Contraseña generada automáticamente

☒

Contraseña personalizada

.....

☐

Mostrar contraseña

Requerir el restablecimiento de contraseña

☒

El usuario debe crear una contraseña nueva en el próximo inicio de sesión

Los usuarios obtienen automáticamente la política [IAMUserChangePassword](#) que les permite cambiar su propia contraseña.


* Obligatorio


[Cancelar](#)


[Siguiente: Permisos](#)

- **Seguido, creamos un nuevo grupo:**

▼ Establecer permisos

 Añadir un usuario al grupo

 Copiar permisos de un usuario existente

 Asociar directamente las políticas existentes



Introducción a los grupos

Aún no ha creado ningún grupo. El uso de grupos es una práctica recomendada para administrar los permisos de los usuarios por funciones de trabajo, el acceso a los servicios de AWS o sus permisos personalizados. Empezar por crear un grupo. [Más información](#)

Crear un grupo

► Establecer un límite de permisos

Ingresamos el nombre del grupo "Console-Admin" y seleccionamos el permiso "AdministratorAccess", finalmente, clic en "Crear grupo" y continuamos con la configuración del usuario "Etiquetas".

Crear un grupo

Cree un grupo y seleccione las políticas que desea asociar a este. El uso de grupos es una práctica recomendada para administrar los permisos de los usuarios por funciones de trabajo, el acceso a los servicios de AWS o sus permisos personalizados. [Más información](#)

Nombre de grupo

Console-Admin

Crear una política

Actualizar

Filtrar políticas

Buscar

Mostrando 753 resultados

	Nombre de la política	Tipo	Utilizado como	Descripción
<input checked="" type="checkbox"/>	AdministratorAccess	Función de trabajo	Ninguna	Provides full access to AWS services and resources.
<input type="checkbox"/>	AdministratorAccess-Amplify	Administrado por AWS	Ninguna	Grants account administrative permissions while explicitly allowing direct access to resources needed by Amplify a...
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	Administrado por AWS	Ninguna	Grants account administrative permissions. Explicitly allows developers and administrators to gain direct access to...
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	Administrado por AWS	Ninguna	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	Administrado por AWS	Ninguna	Grants full access to AlexaForBusiness resources and access to related AWS Services
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	Administrado por AWS	Ninguna	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessLifesizeDelegatedAccessPolicy	Administrado por AWS	Ninguna	Provide access to Lifesize AVS devices
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	Administrado por AWS	Ninguna	Provide access to Poly AVS devices
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	Administrado por AWS	Ninguna	Provide read only access to AlexaForBusiness services
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	Administrado por AWS	Ninguna	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.

Cancelar

Crear un grupo

Añadir un usuario al grupo

Crear un grupo

Actualizar

Buscar

Mostrando 1 resultado

Grupo	Políticas asociadas
<input checked="" type="checkbox"/> Console-Admin	AdministratorAccess

- Seleccionamos "console-Admin" y clic en "Siguiente: Etiquetas"

Añadir un usuario al grupo

Crear un grupo Actualizar

Mostrando 1 resultado

Grupo ▾	Políticas asociadas
<input checked="" type="checkbox"/> Console-Admin	AdministratorAccess

► Establecer un límite de permisos

[Cancelar](#)[Anterior](#)[Siguiente: Etiquetas](#)

Pulsamos "Siguiente: Revisar" sin añadir ninguna etiqueta. Finalmente, revisamos que todos los datos son correctos y pulsamos sobre "Crear un usuario".

Añadir usuario(s)

1

2

3

4

5

Añadir etiquetas (opcional)

Las etiquetas de IAM son pares de clave-valor que puede añadir a su usuario. Las etiquetas pueden incluir información del usuario, como una dirección de correo electrónico, o información descriptiva, como un puesto de trabajo. Utilice las etiquetas para organizar, hacer un seguimiento o controlar el acceso para este usuario. [Más información](#)

Clave	Valor (opcional)	Quitar
<input type="text" value="Añadir una clave nueva"/>	<input type="text"/>	

Puede añadir 50 etiquetas más.

[Cancelar](#)[Anterior](#)[Siguiente: Revisar](#)

- Validar información:

Añadir usuario(s)



Revisar

Revise las opciones que ha elegido. Después de crear el usuario, puede ver y descargar la contraseña y la clave de acceso generadas automáticamente.

Detalles del usuario

Nombre de usuario	TESTUSER
Tipo de acceso de AWS	Acceso a la consola de administración de AWS: con contraseña
Tipo de contraseña de la consola	Personalizado
Requerir el restablecimiento de contraseña	No
Límite de permisos	No se ha establecido un límite de permisos

Resumen de permisos

El usuario que se muestra más arriba se añadirá a los grupos siguientes.

Tipo	Nombre
Grupo	Console-Admin

Etiquetas

No se han añadido etiquetas.

[Cancelar](#)[Anterior](#)[Crear un usuario](#)

Configurar Alias para la cuenta de AWS

- En el panel de IAM, pulsamos sobre "Crear" en la esquina superior derecha.



Cuenta de AWS

ID de cuenta

 27 [redacted]

Alias de cuenta

27 [redacted] [Crear](#)

URL de inicio de sesión para los usuarios de IAM de esta cuenta

 [https://\[redacted\]signin.aws.amazon.com/console](https://[redacted]signin.aws.amazon.com/console)

entidad

- Ingresamos el nuevo alias y una vez creado cerramos la sesión.

Crear alias para la cuenta de AWS 275474348402 ✕

Alias preferido

testuser-[REDACTED]

No debe tener más de 63 caracteres. Los caracteres válidos son a-z, 0-9 y - (guión).

Nueva URL de inicio de sesión

https://[REDACTED]

i Los usuarios de IAM todavía podrán utilizar la URL predeterminada que contiene el ID de la cuenta de AWS.

Cancelar Guardar los cambios

- Ahora ingresamos con la cuenta "Alias". Para ello seleccionamos "Usuario de IAM" e introducimos el alias de la cuenta y pulsamos sobre "Iniciar sesión".



Iniciar sesión

☐ Usuario raíz

Propietario de la cuenta que realiza tareas que requieren acceso ilimitado. [Más información](#)

☒ Usuario de IAM

Usuario de una cuenta que realiza tareas diarias. [Más información](#)

ID de cuenta (12 dígitos) o alias de cuenta

testuse[REDACTED]

Siguiente

Al continuar, acepta el [Contrato de cliente de AWS](#) u otro acuerdo para los servicios de AWS y el [Aviso de privacidad](#). Este sitio utiliza cookies esenciales. Consulte nuestro [Aviso de cookies](#) para obtener más información.

¿Es nuevo en AWS?

Crear una cuenta de AWS

- Adicionalmente, se puede agregar a este usuario MFA.

Panel de IAM

Recomendaciones de seguridad

- ✓ El usuario raíz tiene MFA. Al contar con la autenticación multifactor (MFA) para el usuario raíz se mejora la seguridad de esta cuenta.
- ✓ Cuenta con MFA. Al contar con la autenticación multifactor (MFA) para el usuario raíz se mejora la seguridad de esta cuenta.
- ✓ El usuario TESTUSER no tiene claves de acceso activas que no hayan sido utilizadas durante más de un año. La desactivación o la eliminación de claves de acceso no utilizadas mejora la seguridad.

Recursos de IAM

Grupos de usuarios	Usuarios	Roles	Políticas	Proveedores de identidad
1	1	2	0	0

Novedades

- Amazon GuardDuty ahora detecta las credenciales de instancia de EC2 utilizadas desde otra cuenta de AWS. Hace 4 meses
- Amazon S3 Object Ownership ahora puede deshabilitar las listas de control de acceso para simplificar la administración de acceso a los datos en S3. Hace 6 meses
- Amazon Redshift simplifica el uso de otros servicios de AWS al incorporar el rol de IAM predeterminado. Hace 6 meses
- IAM Access Analyzer le ayuda a generar políticas detalladas que especifican las acciones requeridas para más de 50 servicios. Hace 9 meses

[Ver todo](#)

Cuenta de AWS

ID de cuenta: [REDACTED]

Alias de cuenta: [REDACTED] [Editar](#) | [Eliminar](#)

URL de inicio de sesión para los usuarios de IAM de esta cuenta: [REDACTED].signin.aws.amazon.com/console

Enlaces rápidos

- [Mis credenciales de seguridad](#)
Administre las claves de acceso, la autenticación multifactor (MFA) y otras credenciales.

Herramientas

- [Simulador de políticas](#)
El simulador evalúa las políticas que elija y determina los permisos efectivos para cada una de las acciones que especifique.
- [Web Identity Federation Playground](#)
Realice la autenticación en cualquiera de los