COLOMBIA POTENCIA DE LA VIDA

TIC

Lección 3
Protección de una cuenta nueva de AWS.

TALENTO TECH | AZ PROYECTOS EDUCATIVOS | UTP Universidad Tecnológica de Pereira

Acceso de usuario raíz de la cuenta de AWS frente al acceso de IAM

Práctica recomendada: no utilice el usuario raíz de la cuenta de AWS, excepto cuando sea necesario.

- Para acceder al usuario raíz de la cuenta, se requiere iniciar sesión con la dirección de email (y la contraseña) que utilizó para crear la cuenta.

Ejemplos de acciones que solo se puedes realizar con el usuario raíz de la cuenta:

- Actualizar la contraseña del usuario raíz de la cuenta
- Cambiar el plan de AWS Support
- Restaurar los permisos de un usuario de IAM
- Cambiar la configuración de la cuenta (por ejemplo, la información de contacto o las regiones permitidas)

Cuando se crea una cuenta de AWS por primera vez, se crea automáticamente una identidad de inicio de sesión conocida como usuario raíz de la cuenta. Esta identidad tiene acceso total a todos los servicios y recursos de AWS en esa cuenta. Para acceder a esta cuenta raíz, se utiliza la dirección de correo electrónico y la contraseña utilizadas durante la creación de la cuenta al iniciar sesión en la consola de administración de AWS.

Cuando se crea una cuenta de AWS por primera vez, se crea automáticamente una identidad de inicio de sesión conocida como usuario raíz de la cuenta. Esta identidad tiene acceso total a todos los servicios y recursos de AWS en esa cuenta. Para acceder a esta cuenta raíz, se utiliza la dirección de correo electrónico y la contraseña utilizadas durante la creación de la cuenta al iniciar sesión en la consola de administración de AWS.

Sin embargo, es importante destacar que AWS recomienda evitar el uso de las credenciales del usuario raíz para las actividades diarias de la cuenta. En su lugar, se aconseja utilizar AWS Identity and Access Management (IAM) para crear usuarios adicionales y asignar permisos específicos a cada usuario, siguiendo el principio de mínimo privilegio. Por ejemplo, si se requieren permisos de administrador, es preferible crear un usuario IAM, asignarle acceso total y utilizar esas credenciales para las interacciones con la cuenta. De esta manera, si es necesario modificar o revocar los permisos en el futuro, se pueden hacer cambios específicamente en las políticas asociadas a ese usuario IAM.

Además, si hay varios usuarios que necesitan acceso a la cuenta, se pueden crear credenciales únicas para cada uno de ellos y definir detalladamente qué recursos pueden acceder. Por ejemplo, se pueden crear usuarios IAM con permisos de solo lectura para ciertos recursos y distribuir esas credenciales solo a los usuarios que necesitan ese nivel de acceso. Es fundamental evitar compartir las mismas credenciales entre varios usuarios para mantener un control de acceso seguro y bien administrado.

Aunque el usuario raíz de la cuenta no debe utilizarse para tareas rutinarias, hay algunas tareas que solo se pueden cumplir iniciando sesión como usuario raíz de la cuenta. Puede encontrar una lista completa de estas tareas en la página de documentación de AWS.

Protección de una nueva cuenta de AWS: usuario raíz de la cuenta

Paso 1: Deje de utilizar el usuario raíz de la cuenta tan pronto sea posible.

- El usuario raíz de la cuenta tiene acceso ilimitado a todos sus recursos.

Pasos a seguir para dejar de utilizar el usuario raíz de la cuenta:

1. Inicie sesión como usuario raíz de la cuenta y cree un usuario de IAM para usted. Guarde las claves de acceso si es necesario.
2. Cree un grupo de IAM, otórguele permisos totales de administrador y agregue el usuario de IAM al grupo.
3. Deshabilite y elimine las claves de acceso de usuario raíz de la cuenta, en caso de que existan.
4. Habilite un apolítica de contraseñas para los usuarios.
5. Inicie sesión con sus nuevas credenciales de usuario de IAM.
6. guarde las credenciales de usuario raíz de la cuenta en un lugar seguro.

Para dejar de utilizar el usuario raíz de la cuenta, siga los siguientes pasos:

1. Cuando haya iniciado sesión en el usuario raíz de la cuenta, cree un usuario de IAM para usted con el acceso a la consola de administración de AWS habilitado (pero todavía no asocie ningún permiso al usuario). Guarde las claves de acceso de usuario de IAM si es necesario.
2. A continuación, cree un grupo de IAM, asígnele un nombre (como FullAccess) y asocie políticas de IAM al grupo que conceda acceso completo a al menos unos pocos de los servicios que utilizará. Luego, agregue al usuario de IAM al grupo.
3. Deshabilite y elimine las claves de acceso de usuario raíz de la cuenta, en caso de que existan.
4. Habilite una política de contraseñas para todos los usuarios. Copie el enlace de inicio de sesión de los usuarios de IAM desde la página del panel de IAM. A continuación, cierre la sesión como usuario raíz de la cuenta.
5. Vaya al enlace de inicio de sesión de los usuarios de IAM que copió e inicie sesión en la cuenta con las nuevas credenciales de usuario de IAM.
6. Guarde las credenciales de usuario raíz de la cuenta en un lugar seguro.

Para ver instrucciones detalladas sobre cómo configurar su primer usuario y grupo de IAM, consulte Creación del primer grupo y usuario administrador de IAM.

Protección de una nueva cuenta de AWS: MFA

Token de MFA

Paso 2: Habilite Multi-Factor Authentication (MFA).

- Exija MFA para su usuario raíz de la cuenta y para todos los usuarios de IAM.
- También puede usar MFA para controlar el acceso a las API de servicios de AWS.

Opciones para recuperar el token de MFA:

- Aplicaciones virtuales compatibles con MFA:
  - Google Authenticator
  - Authy Authenticator (aplicación de Windows Phone)
- Dispositivos de clave de seguridad U2F:
  - Por ejemplo, YubiKey
- Opciones de MFA de hardware:
  - Llavero o tarjeta de visualización ofrecida por Gemalto.

Otro paso importante para fortalecer la seguridad de una nueva cuenta de AWS es habilitar la Autenticación Multifactor (MFA), tanto para el usuario raíz de la cuenta como para todos los demás usuarios de IAM. La MFA requiere un segundo factor de autenticación además de la contraseña estándar, lo que añade una capa adicional de seguridad. Además, la MFA puede ser utilizada para controlar el acceso a través de métodos de autenticación programáticos. Para más detalles sobre cómo implementar la MFA. Consulte
Configuración del acceso a la API protegido por MFA.

Tiene algunas opciones para recuperar el token de MFA necesario para iniciar sesión cuando la MFA está habilitada. Las opciones incluyen aplicaciones virtuales compatibles con MFA (como Google Authenticator y Authy Authenticator), dispositivos con clave de seguridad U2F y opciones de MFA de hardware que proporcionan un llavero o una tarjeta de visualización.

Token de MFA

CloudTrail

Paso 3: Utilice AWS CloudTrail.

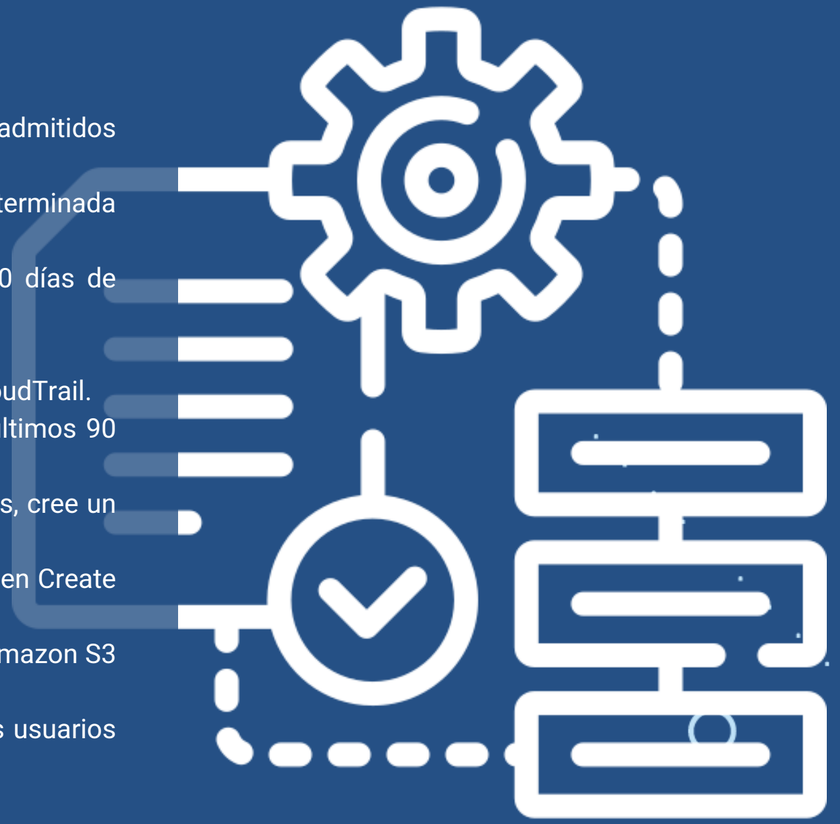
- CloudTrail realiza un seguimiento de la actividad de los usuarios en su cuenta.
  - Registra todas las solicitudes API para los recursos de todos los servicios admitidos de su cuenta.
- El historial básico de eventos de AWS CloudTrail está habilitado de forma predeterminada y es gratuito.
  - Contiene todos los datos de eventos de administración de los últimos 90 días de actividad de la cuenta.

Pasos a seguir para obtener acceso a CloudTrail:

1. Inicie sesión en la consola de administración de AWS y seleccione el servicio CloudTrail.
2. Haga clic en Event history (Historial de eventos) para ver, filtrar y buscar los últimos 90 días de eventos.

Para habilitar los registros de más de 90 días y las alertas de eventos especificados, cree un registro de seguimiento.

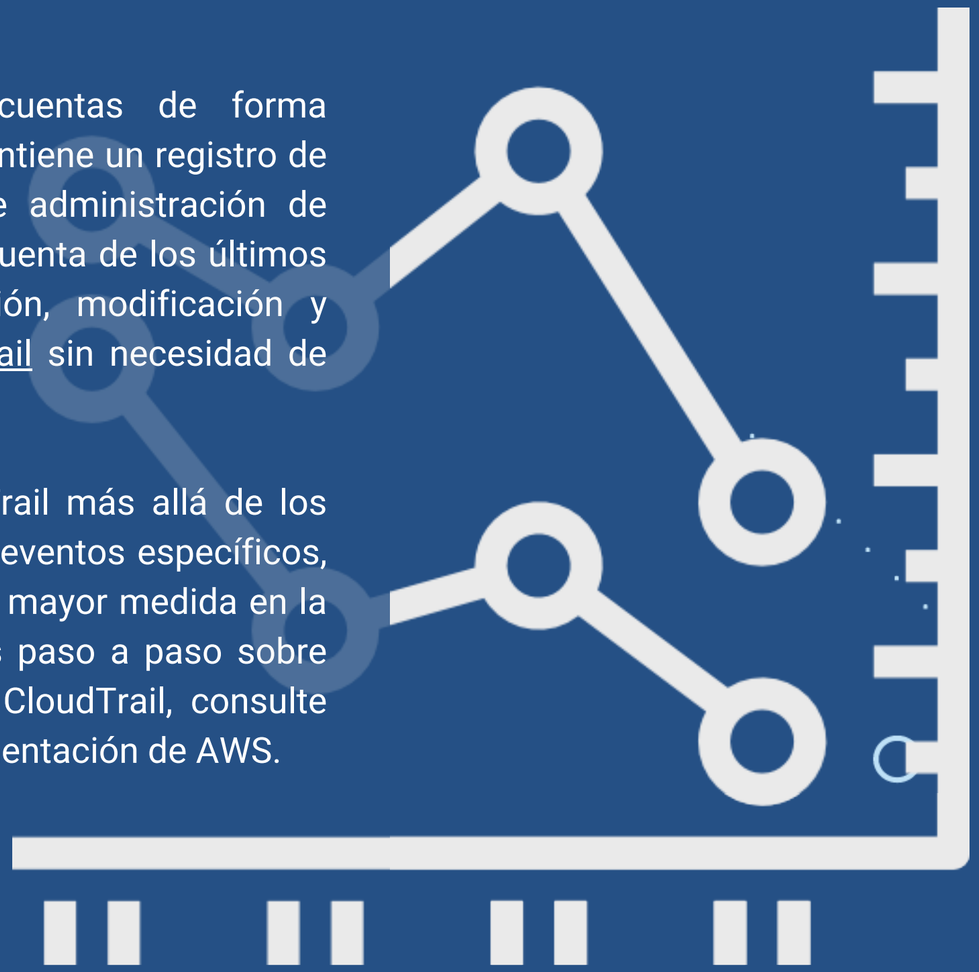
1. En la página de registros de seguimiento de la consola de CloudTrail, haga clic en Create trail (Crear registro de seguimiento).
2. Asígnele un nombre, aplíquelo a todas las regiones y cree un nuevo bucket de Amazon S3 para el almacenamiento de registros.
3. Configure las restricciones de acceso en el bucket de S3 (por ejemplo, solo los usuarios administradores deben tener acceso).



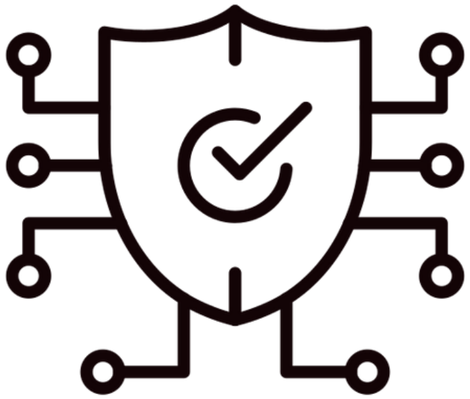
AWS CloudTrail es un servicio que registra todas las solicitudes de API a los recursos de su cuenta. De esta forma, permite realizar auditorías operativas en su cuenta.

AWS CloudTrail está habilitado para crear cuentas de forma predeterminada en todas las cuentas de AWS y mantiene un registro de los últimos 90 días de actividad de eventos de administración de cuentas. Puede ver y descargar la actividad de la cuenta de los últimos 90 días con relación a operaciones de creación, modificación y eliminación de servicios compatibles con CloudTrail sin necesidad de crear manualmente otro registro de seguimiento.

Para habilitar la retención de registros de CloudTrail más allá de los últimos 90 días y habilitar las alertas cuando haya eventos específicos, cree un nuevo registro de seguimiento (descrito en mayor medida en la diapositiva). Para obtener instrucciones detalladas paso a paso sobre cómo crear un registro de seguimiento en AWS CloudTrail, consulte Creación de un registro de seguimiento en la documentación de AWS.



Protección de una nueva cuenta de AWS: informes de facturación



Paso 2: Habilite Multi-Factor Authentication (MFA).

- Exija MFA para su usuario raíz de la cuenta y para todos los usuarios de IAM.
- También puede usar MFA para controlar el acceso a las API de servicios de AWS.

Opciones para recuperar el token de MFA:

- Aplicaciones virtuales compatibles con MFA:
  - Google Authenticator
  - Authy Authenticator (aplicación de Windows Phone)
- Dispositivos de clave de seguridad U2F:
  - Por ejemplo, YubiKey
- Opciones de MFA de hardware:
  - Llavero o tarjeta de visualización ofrecida por Gemalto.

Otro paso recomendado para proteger una nueva cuenta de AWS consiste en habilitar los informes de facturación, como el informe de uso y costo de AWS. Los informes de facturación proporcionan información sobre el uso de los recursos de AWS y los costos estimados de dicho uso. AWS envía los informes a un bucket de Amazon S3 que usted especifique y AWS los actualiza al menos una vez al día.

El informe de uso y costo de AWS realiza un seguimiento del uso en la cuenta de AWS y proporciona los cargos estimados, ya sea por hora o por día.

Consulte la documentación de AWS para obtener más información acerca de cómo crear un informe de uso y costo de AWS.

El mentor puede optar por mostrar una explicación completa de los dos primeros pasos principales que debe completar para proteger una nueva cuenta de AWS. (Estos pasos se han descrito en las diapositivas anteriores). En las diapositivas de esta lección, se muestran capturas de pantalla de cómo es realizar el proceso en detalle.

COLOMBIA POTENCIA DE LA VIDA

TIC

Presionar cada tema para ver si contenido

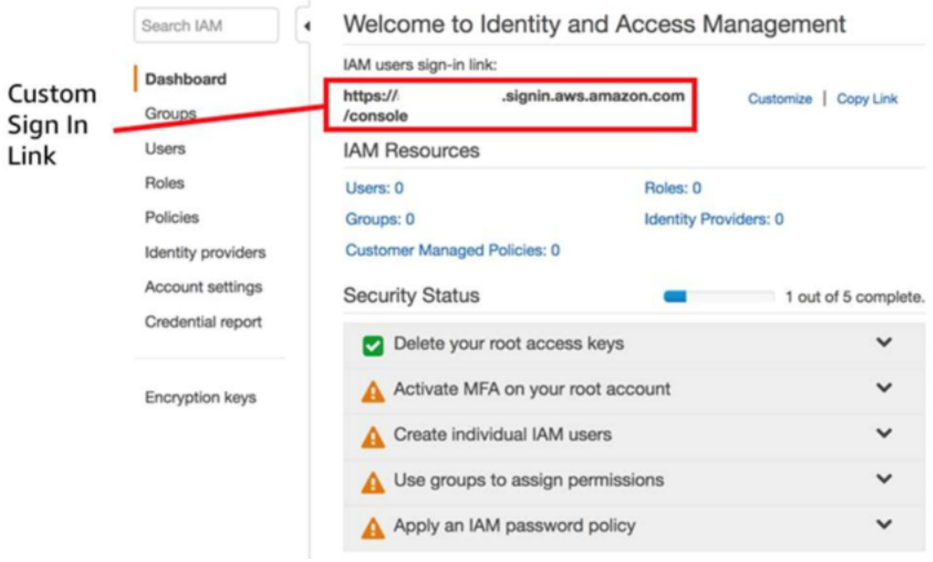
- Estado de seguridad
- Activar MFA
- Usuario individual
- Creación de usuario
- Seguridad del panel
- Política de contraseñas
- Comprobaciones

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Revisión del estado de seguridad de IAM



La captura de pantalla muestra un ejemplo del aspecto del panel de la consola de IAM cuando ha iniciado sesión como usuario raíz de la cuenta de AWS. Pasos a seguir para obtener acceso a esta pantalla en una cuenta:

1. Inicie sesión en la consola de administración de AWS como usuario raíz de la cuenta de AWS.
2. Vaya a la página de servicio de IAM y haga clic en el enlace Dashboard (Panel).

Revise la información en el panel Security Status (Estado de seguridad).

+INFO

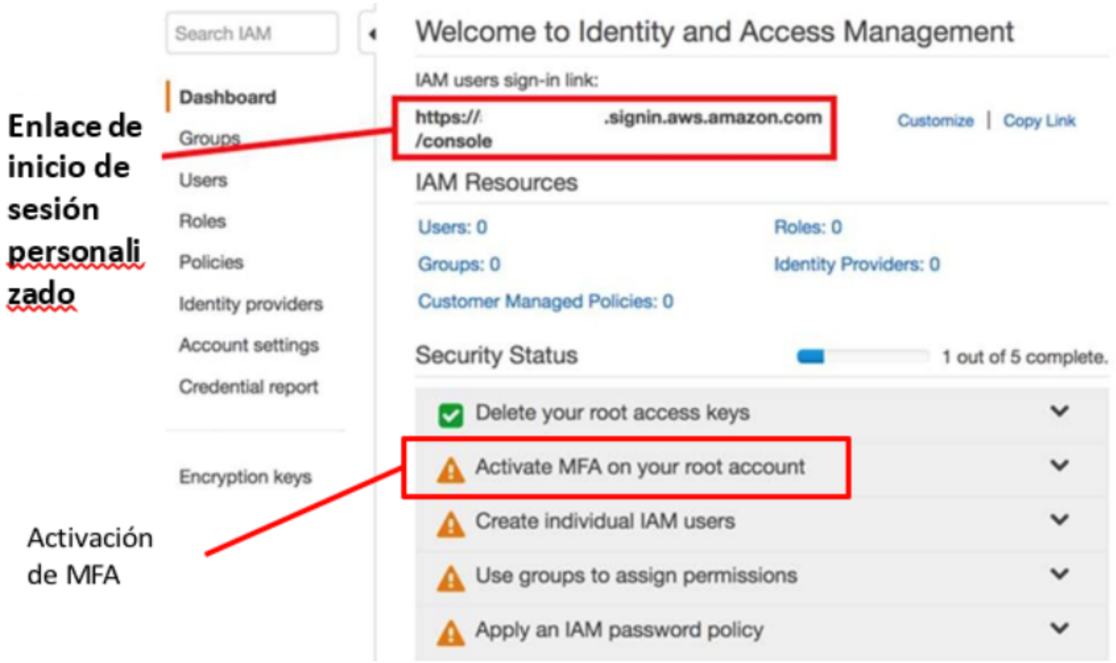
En la captura de pantalla, solo se ha completado una de las cinco comprobaciones de estado de seguridad (Elimine las claves de acceso raíz). El objetivo de una persona que completa los pasos para proteger la cuenta es recibir marcas verdes junto a cada elemento de estado de seguridad.

Una revisión de la lista de estado de seguridad actual indica lo siguiente:

- La MFA no se ha activado en el usuario raíz de la cuenta de AWS.
- No se crearon usuarios de IAM individuales.
- No se asignan permisos a grupos.
- No se aplicó una política de contraseñas de IAM.

La cuenta tiene un enlace de inicio de sesión de usuario personalizado. Tenga en cuenta que el número de cuenta se ocultó en esta captura de pantalla. Si lo desea, puede utilizar el enlace Customize (Personalizar) ubicado a la derecha del enlace de inicio de sesión de usuario de IAM para cambiar el nombre de la cuenta de forma que no muestre el número de cuenta. Este enlace se utiliza para iniciar sesión en la cuenta y se puede enviar a los usuarios después de crear sus cuentas.

Activar MFA en el usuario raíz de la cuenta



Antes de crear usuarios de IAM en la cuenta, active MFA en el usuario raíz de la cuenta. Para iniciar sesión como usuario raíz de la cuenta, utilice la dirección de email con la que creó la cuenta. El usuario raíz de la cuenta tiene acceso a todo, por lo que es importante proteger esta cuenta con restricciones.

+INFO

COLOMBIA POTENCIA DE LA VIDA

TIC

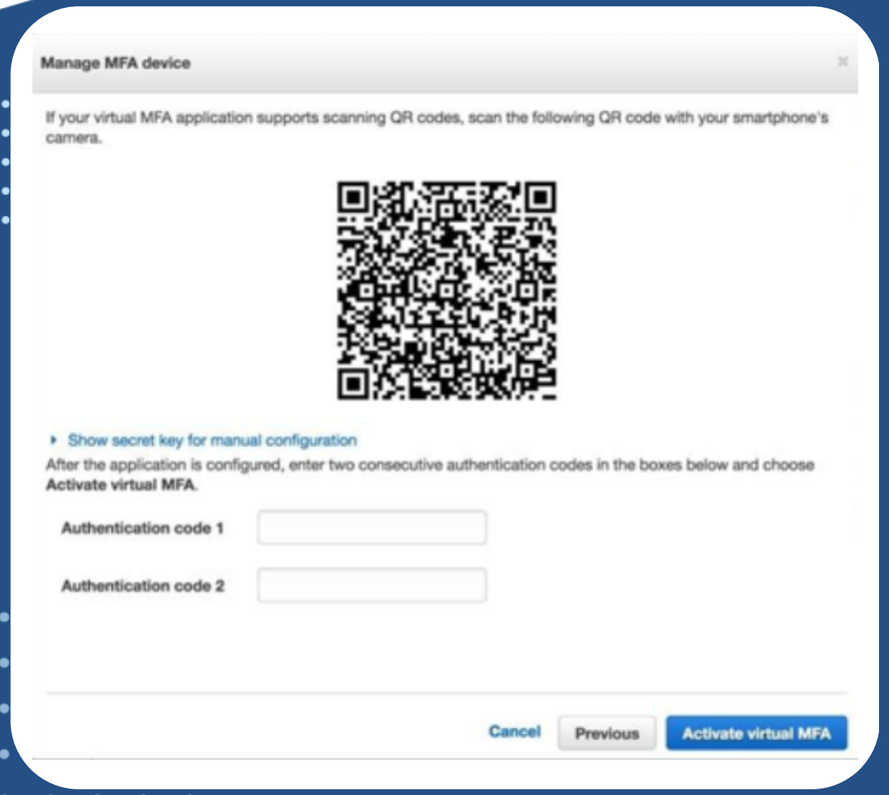
Pasos a seguir para configurar MFA:

1. Haga clic en el enlace Activate MFA on your root account (Activar MFA en su cuenta raíz).
2. Haga clic en Manage MFA (Administrar FMA).
3. Haga clic en Assign MFA device (Asignar dispositivo MFA). Tiene tres opciones: dispositivo MFA virtual, clave de seguridad U2F y otro dispositivo MFA físico. Un dispositivo de hardware es un dispositivo de hardware real.
4. Para esta demostración, seleccione Virtual MFA device (Dispositivo MFA virtual) y, a continuación, haga clic en Continue (Continuar).
5. Aparece un nuevo cuadro de diálogo que pide configurar un dispositivo MFA virtual. Debe descargarse una aplicación (como Google Authenticator) para esta tarea. Una vez completa la descarga, haga clic en Show QR code (Mostrar código QR).

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

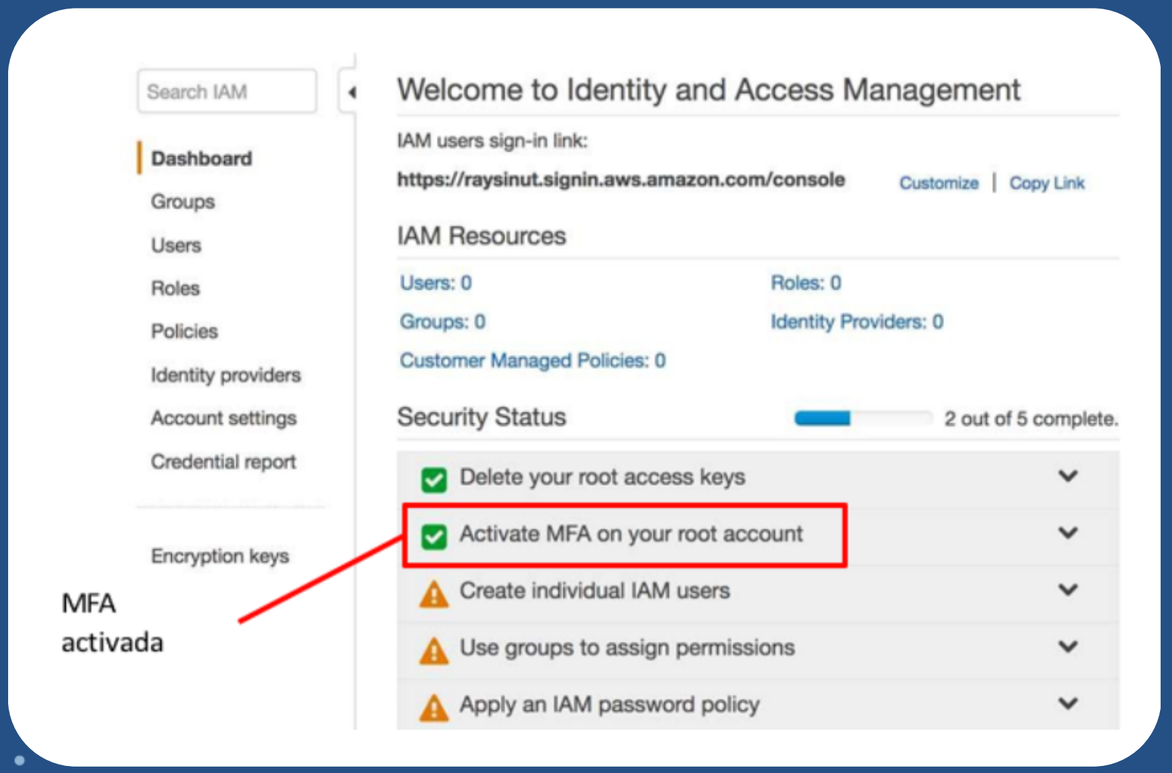


6 En la aplicación de autenticación, seleccione el signo más (+).

7 Escanee el código de barras y escriba el primer código de autenticación.

8 Espere un momento para que se muestre el segundo código y escríbalo.

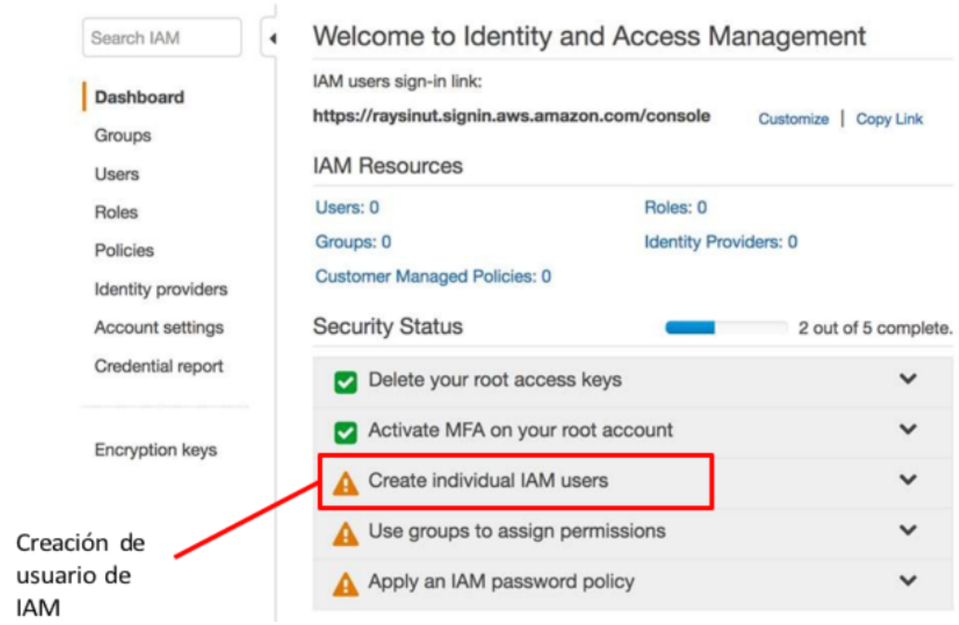
9 Haga clic en el botón Assign MFA (Asignar MFA).



10 Haga clic en Finish (Terminar) y actualice el navegador.

En el panel Security Status (Estado de seguridad), ahora debería aparecer un icono de marca de verificación verde que indica que la MFA está activada en el usuario raíz de la cuenta.

Crear un usuario individual de IAM



Creación de usuario de IAM

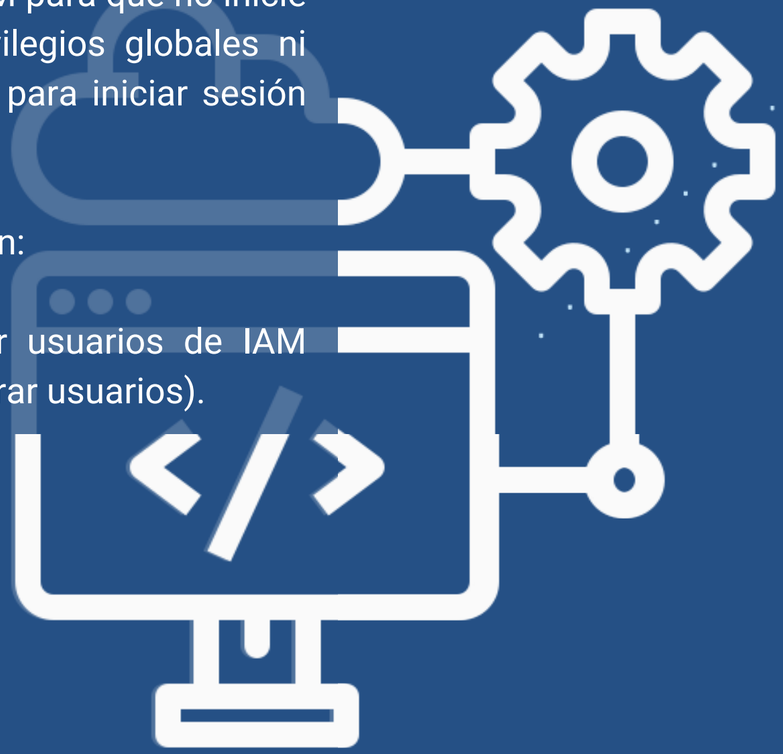
La mayoría de las cuentas de AWS se comparten entre varios usuarios de una organización. Para admitir esta práctica, puede configurar cada usuario con permisos asignados individualmente o puede agregar usuarios al grupo de IAM adecuado que les conceda permisos específicos.

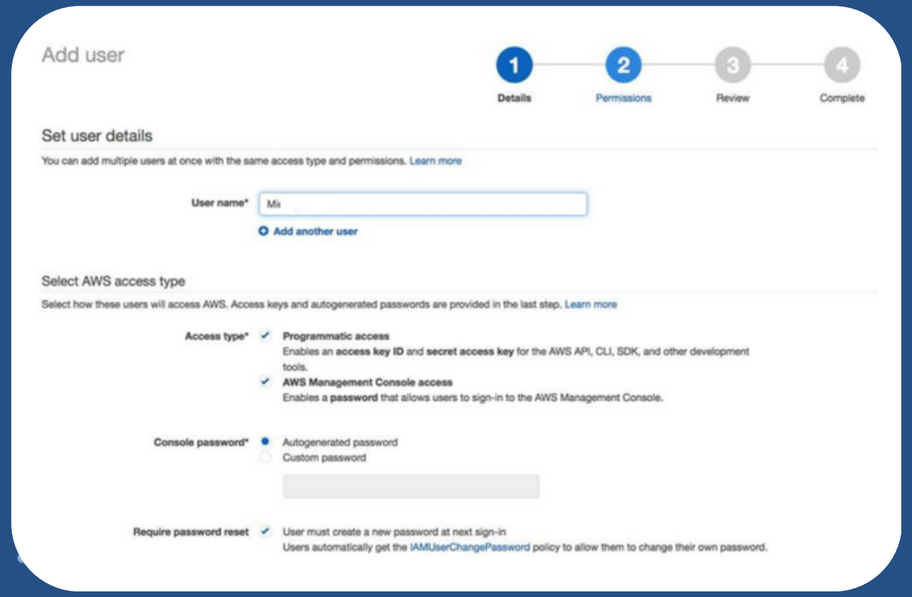
+INFO

Una práctica recomendada de AWS consiste en proporcionar a cada usuario su propio inicio de sesión de usuario de IAM para que no inicie sesión como usuario raíz de la cuenta con privilegios globales ni utilice las mismas credenciales que otra persona para iniciar sesión en la cuenta.

Pasos a seguir para implementar esta configuración:

1 Haga clic en Create individual IAM users (Crear usuarios de IAM individuales) y seleccione Manage Users (Administrar usuarios).





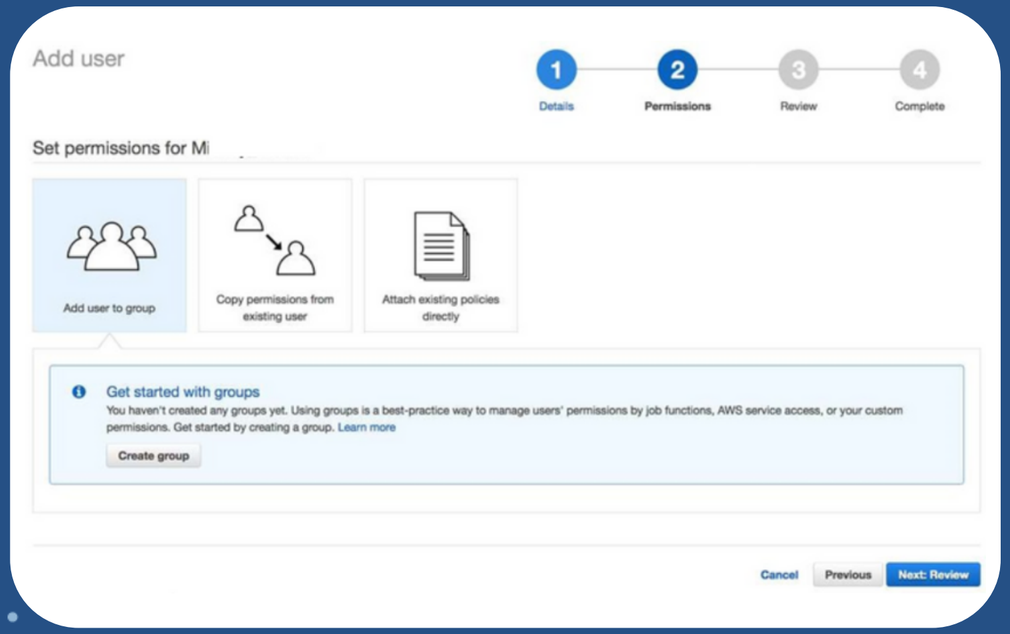
2 Seleccione Add user (Agregar usuario) y especifique un nuevo nombre de usuario. Tenga en cuenta que los nombres de usuario no pueden tener espacios.

3 Seleccione Access type (Tipo de acceso). Existen dos tipos de acceso (puede conceder uno o ambos tipos al usuario, pero para esta demostración, conceda ambos tipos):

- El acceso mediante programación permite al usuario tener acceso a la CLI de AWS para aprovisionar recursos. Esta opción generará una clave de acceso por única vez. Se la debe guardar ya que será necesaria para todos los accesos futuros.
- El acceso a la consola de administración de AWS permite al usuario iniciar sesión en la consola de AWS.

4 Si decide conceder acceso a la consola, seleccione Autogenerate password (Generar contraseña automática) o seleccione Custom password (Contraseña personalizada) y escriba una.

5 Haga clic en Next: Permissions(Siguiente: permisos).

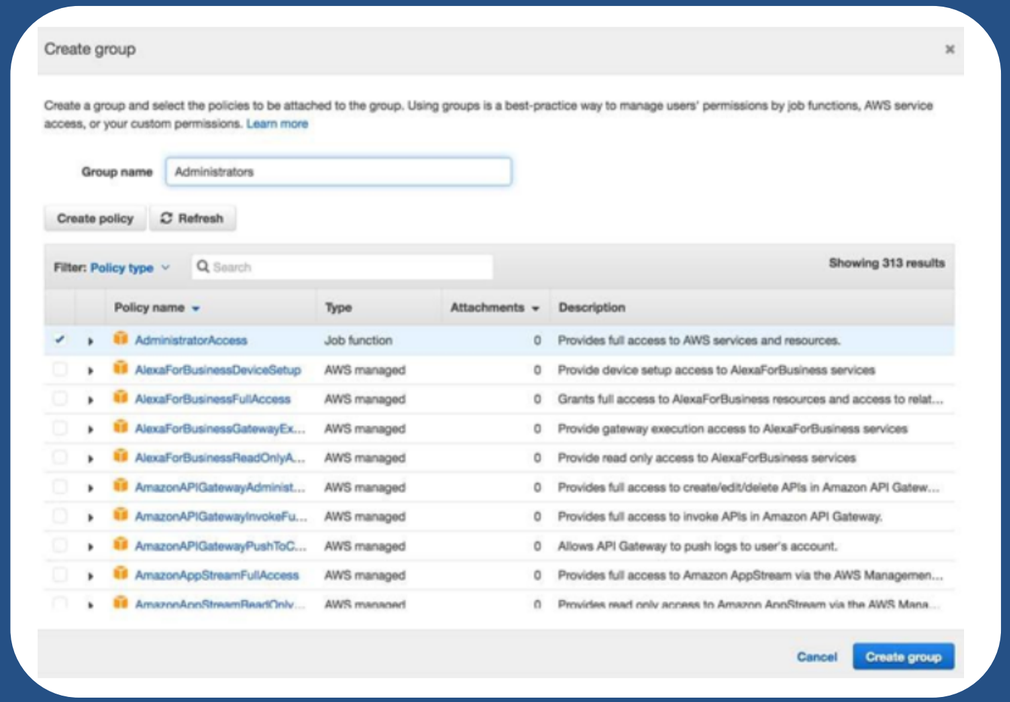


A continuación, asignará los permisos. Tiene tres opciones para asignar permisos:

- Agregar un usuario al grupo
- Copiar permisos de un usuario existente
- Asociar directamente las políticas existentes

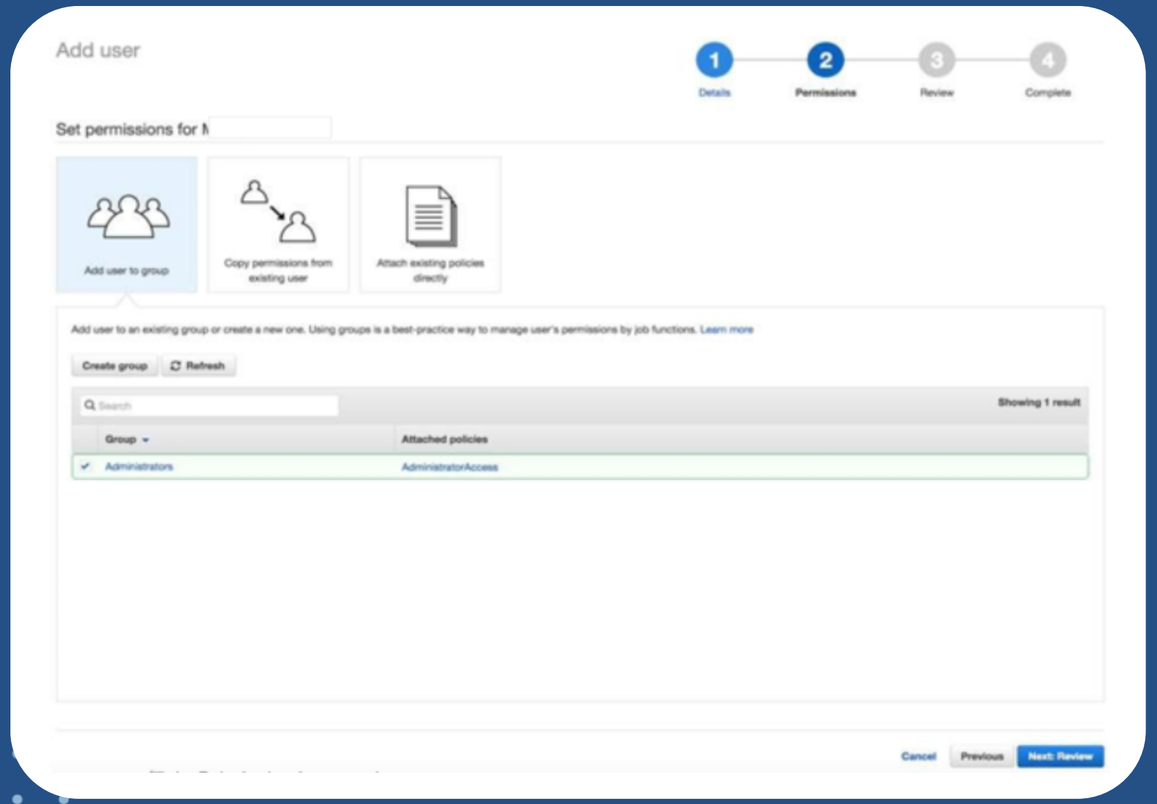
6 Quiere agregar el usuario a un grupo, entonces seleccione Add user to group (Agregar usuario a grupo) y, luego, Create group (Crear grupo).

Nota: Un grupo es donde coloca a los usuarios para que hereden las políticas asignadas al grupo.



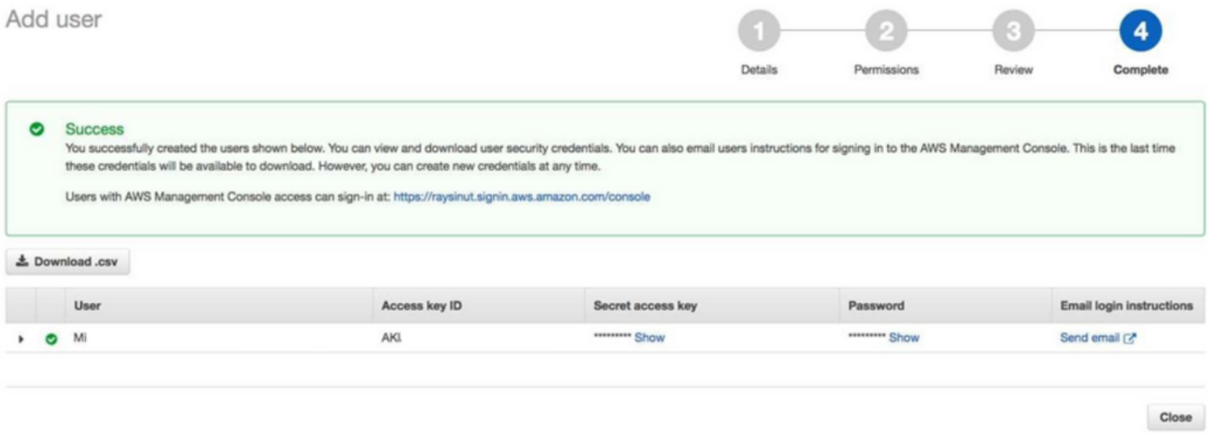
7

Asigne un nombre al grupo. En este ejemplo, conceda acceso administrativo al desarrollador principal y, a continuación, seleccione Create group (Crear grupo).



8 Seleccione Next Review (Siguiente revisión) para revisar lo que se creará y, a continuación, seleccione Create user (Crear usuario).

Creación exitosa de usuario de IAM



Cuando se crea un usuario (suponiendo que habilitó el acceso mediante programación y la consola cuando definió la configuración Access type [Tipo de acceso] y creó el usuario), se generan varios artefactos:

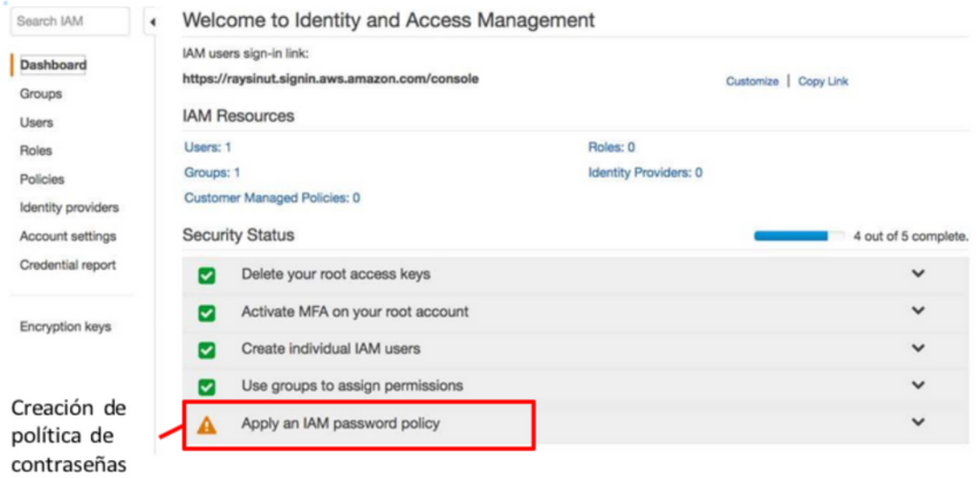
1. Un ID de clave de acceso que se puede utilizar para firmar las llamadas a la API de AWS cuando el usuario utiliza la CLI de AWS o los SDK de AWS.
2. Una clave de acceso secreta que también se utiliza para firmar llamadas a la API de AWS cuando el usuario utiliza la CLI de AWS o los SDK de AWS.
3. Una contraseña que se puede utilizar para iniciar sesión en la consola de administración de AWS.

+INFO

Seleccione Show (Mostrar) para mostrar los valores de cada campo. Las credenciales también se pueden descargar seleccionando Download .csv (Descargar.csv). Esta será la única vez que tendrá la opción de descargar estas credenciales. No tendrá la oportunidad de recuperar la clave de acceso secreta después de esta pantalla. Por lo tanto, debe descargar las credenciales o, como mínimo, copiar la clave de acceso secreta y pegarla en un lugar seguro.

Importante: Nunca almacene estas credenciales en un lugar público (por ejemplo, nunca incruste estas credenciales en el código que cargue en GitHub o en otro lugar). Puede usar esta información para acceder a su cuenta. Si alguna vez le preocupa que sus credenciales se hayan visto comprometidas, inicie sesión como usuario con permisos de acceso de administrador de IAM y elimine la clave de acceso existente. Si lo desea, puede crear una nueva clave de acceso.

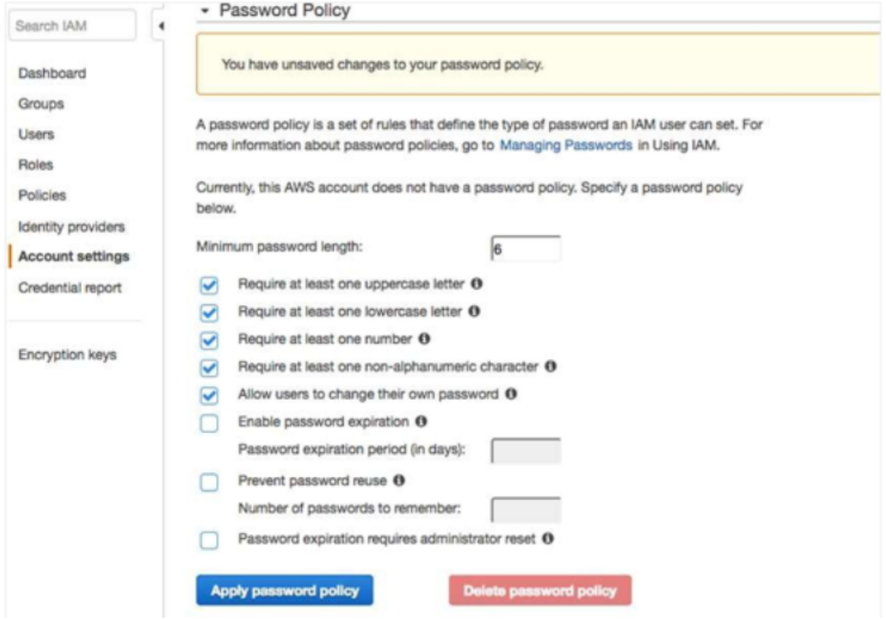
Estado de seguridad del panel



Cuando vuelva al panel de IAM, los puntos relacionados con el estado de seguridad Create individual IAM users (Crear usuarios de IAM individuales) y Use groups to assign permissions (Usar grupos para asignar permisos) deberían mostrar que se han tratado.

El punto de seguridad restante que se debe tratar es aplicar una política de contraseñas de IAM.

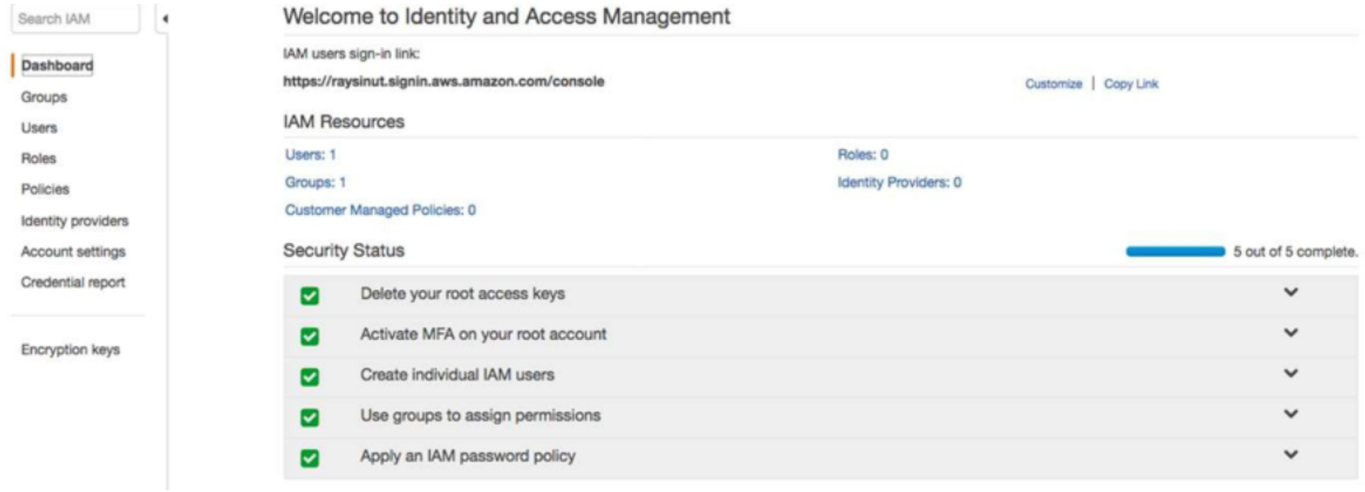
Establecer una política de contraseña



La política de contraseñas de IAM es un conjunto de reglas que define el tipo de contraseña que puede configurar un usuario de IAM.

Seleccione las reglas que deben cumplir las contraseñas y, a continuación, seleccione Apply password policy (Aplicar política de contraseñas).

Comprobaciones de estado de seguridad completadas



Ahora, todas las señales de verificación en el estado de seguridad deben ser de color verde. Esto significa que su cuenta ahora satisface todas las verificaciones de seguridad de IAM que se muestran. ¡Felicitaciones por haber completado esta tarea!

Los aprendizajes clave de esta lección están relacionados con las prácticas recomendadas para proteger una cuenta de AWS. Estas prácticas recomendadas son las siguientes:

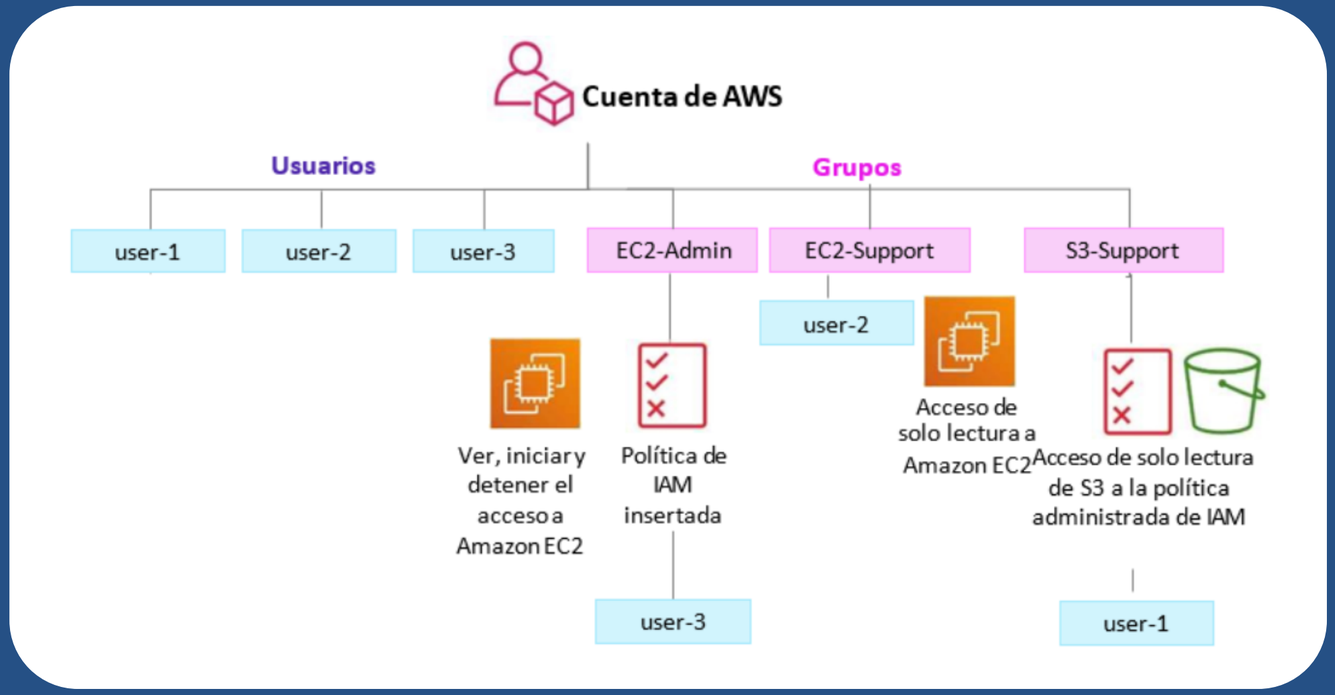
- Proteja los inicios de sesión con Multi-Factor Authentication (MFA).
- Elimine las claves de acceso de usuario raíz de la cuenta.
- Cree usuarios de IAM individuales y otorgue permisos de acuerdo con el principio de mínimo privilegio.
- Utilice grupos para asignar permisos a usuarios de IAM.
- Configure una política de contraseñas sólida.
- Delegue el uso de roles en lugar del uso compartido de credenciales.
- Monitoree la actividad de la cuenta con AWS CloudTrail.

Laboratorio 1: Introducción a IAM de AWS

Tarea 1: analizar los usuarios y los grupos
Tarea 2: agregar usuarios a los grupos
Tarea 3: iniciar sesión y probar los usuarios

En este laboratorio práctico, podrá hacer lo siguiente:

- Analizar usuarios y grupos de IAM creados previamente
- Inspeccionar políticas de IAM a medida que se apliquen a los grupos creados previamente
- Seguir una situación real y agregar usuarios a grupos que tengan capacidades específicas habilitadas
- Ubicar y usar la URL de inicio de sesión de la IAM
- Experimentar con los efectos de las políticas de IAM en el acceso a los recursos de AWS



En el diagrama, se muestran los recursos que tendrá su cuenta de AWS después de completar los pasos del laboratorio. También, se describe cómo se configurarán los recursos.

INICIO