AWS Solutions Architect Associate

Capítulo 02

Sesión 01: IAM.

Al término de esta sesion, Ud. podrá:

- Conocer el servicio de IAM.
- Entender los diferentes conceptos que se encuentran dentro de IAM.
- Crear usuarios, grupos y roles.
- Asignar políticas a roles.
- Cambio de roles en instancias EC2.
- Prácticas de seguridad en IAM.
- Conocimiento detallado en el servicio de IAM.

RECURSOS

- FAQ: https://aws.amazon.com/es/iam/faqs/
- LIMITES:http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html#limits_iam

Identity Access Management

- AWS Identity and Access Management (IAM) permite controlar de forma segura el acceso de los usuarios a servicios y recursos de AWS.
- Con IAM puede crear y administrar usuarios y grupos de AWS, así como utilizar permisos para permitir o denegar el acceso de estos a los recursos de AWS.
- IAM es una característica de su cuenta de AWS que se ofrece sin cargos adicionales. Solo se le cobrará por la utilización de los demás servicios de AWS por parte de sus usuarios.

Identity Access Management

Acceso compartido a su cuenta de AWS

- Puede otorgar a otras personas permiso para administrar y usar recursos en su cuenta de AWS sin tener que compartir su contraseña o clave de acceso.

Permisos granulares

- Puede otorgar diferentes permisos a diferentes personas para diferentes recursos. Por ejemplo, puede permitir que algunos usuarios completen el acceso a Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift y otros servicios de AWS. Para otros usuarios, puede permitir el acceso de solo lectura a algunos contenedores S3.

Identity Access Management

Acceso seguro a los recursos de AWS para las aplicaciones que se ejecutan en Amazon EC2

- Puede usar las funciones de IAM para proporcionar de forma segura a las aplicaciones que se ejecutan en las instancias de EC2 las credenciales que necesitan para acceder a otros recursos de AWS.

Autenticación de múltiples factores (MFA)

- Puede agregar autenticación de dos factores a su cuenta y a usuarios individuales para mayor seguridad. Con MFA, usted o sus usuarios deben proporcionar no solo una contraseña o clave de acceso para trabajar con su cuenta, sino también un código de un dispositivo especialmente configurado.

Identity Access Management

Federación de identidad

- Puede permitir a los usuarios que ya tienen contraseñas en otro lugar, por ejemplo, en su red corporativa o con un proveedor de identidad de Internet, obtener acceso temporal a su cuenta de AWS.

Información de identidad para aseguramiento

- Si usa AWS CloudTrail, recibirá registros que incluyan información sobre aquellos que realizaron solicitudes de recursos en su cuenta. Esa información se basa en las identidades de IAM.

Identity Access Management

Cumplimiento de PCI DSS

- IAM admite el procesamiento, el almacenamiento y la transmisión de datos de tarjetas de crédito por parte de un comerciante o proveedor de servicios, y ha sido validado como compatible con el Estándar de seguridad de datos (DSS) de la Industria de tarjetas de pago (PCI).

Integrado con muchos servicios de AWS

- Funciona con gran cantidad de servicios de AWS.

Eventualmente consistente

- IAM, como muchos otros servicios de AWS, finalmente es consistente. IAM logra una alta disponibilidad al replicar datos en múltiples servidores dentro de los centros de datos de Amazon en todo el mundo.

Identity Access Management

Gratis

- La Administración de identidades y accesos de AWS es una característica de su cuenta de AWS que se ofrece sin costo adicional. Los usuarios de IAM solo te cobrarán por el uso de otros productos de AWS.
- El servicio de token de seguridad de AWS es una función incluida de su cuenta de AWS que se ofrece sin costo adicional.
- Se le cobrará únicamente por el uso de otros servicios de AWS a los que acceden sus credenciales temporales de seguridad de AWS STS.

Identity Access Management

- Permite la centralización de nuestras cuentas de AWS.
- Permisos granulares a diferentes servicios dentro de la plataforma de AWS.
- Federación, conexión a través de Facebook, LDAP, AD, Google, Linkedin y otros.
- Autenticación Multifactor.
- Acceso temporal para usuarios y dispositivos.
- Política de rotación de password.
- Soporta PCI DSS Compliance.
- Se integra con gran cantidad de servicios de la plataforma de aws.

Términos Clave - IAM

- **Usuario**: Usuarios Finales.
- **Grupo**: Colección de usuarios que se pueden agrupar por un set de permisos establecidos.
- **Rol**: Pueden ser agregados a recursos de AWS con permisos especiales.
- **Políticas**: Es un documento que define uno o más permisos.

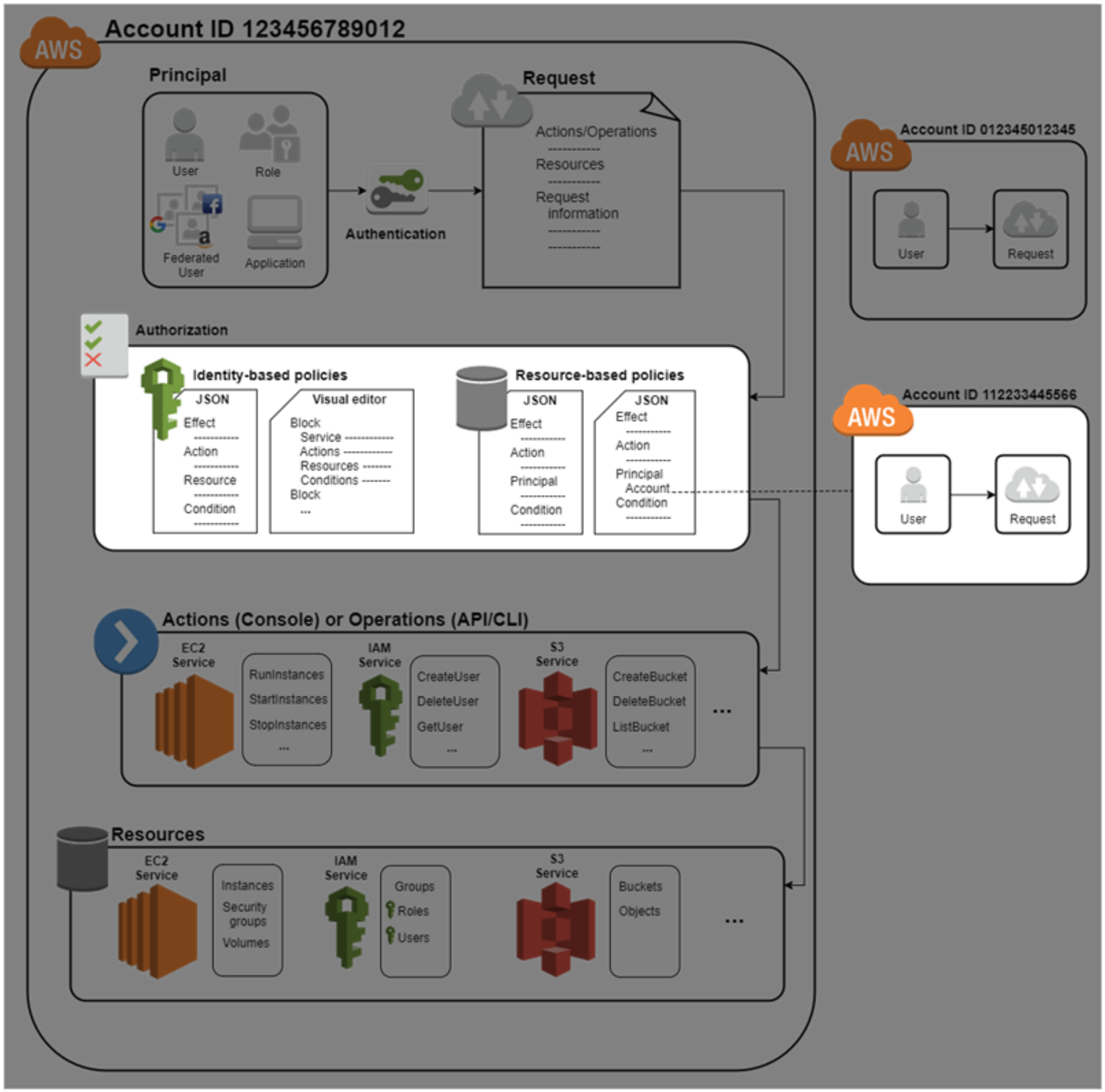
Conceptos - IAM

- IAM es global, no aplica por regiones.
- La cuenta root es la cuenta creada cuando se configuro por primera vez la cuenta de AWS.
- Los nuevos usuarios tendrán una Access Key ID y una Secret Access Key cuando se crean por primera vez.
- Estas claves no son las mismas que el password, estas se utilizan para acceder a la CLI y para interactuar con algunas API y otros servicios.
- Solamente se pueden descargar una vez, si se pierden se deben volver a generar unas nuevas desde la consola de AWS.

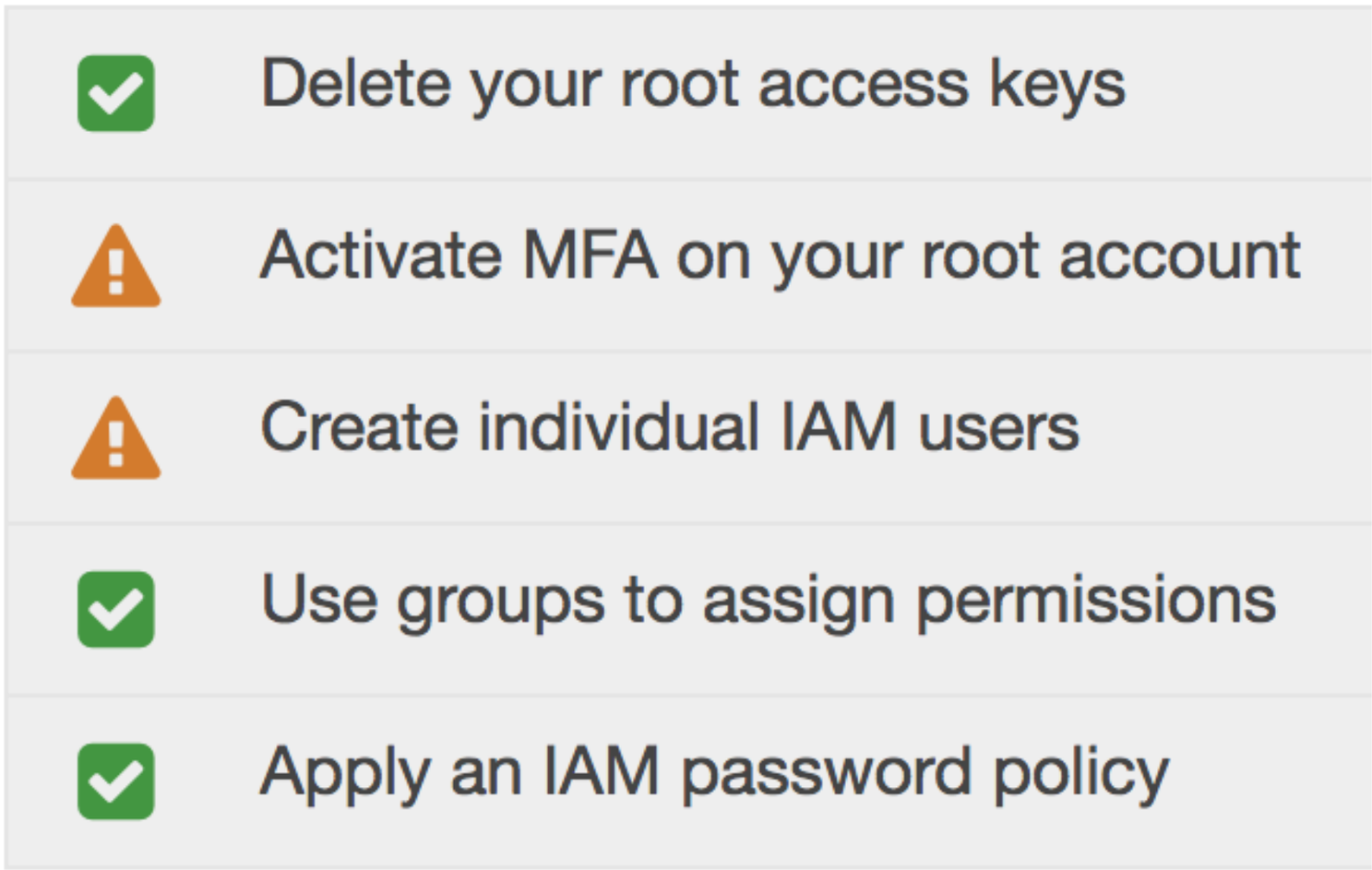
Gestión de Acceso

- AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS.
- Cuando un principal realiza una solicitud en AWS, el servicio IAM comprueba si el principal está autenticado (firmado) y autorizado (tiene permisos).
- Usted administra el acceso creando políticas y adjuntándolas a identidades de IAM o recursos de AWS.
- Esas políticas especifican los permisos permitidos o denegados. Para obtener detalles sobre el resto del proceso de autenticación y autorización, consulte Descripción de cómo funciona IAM.

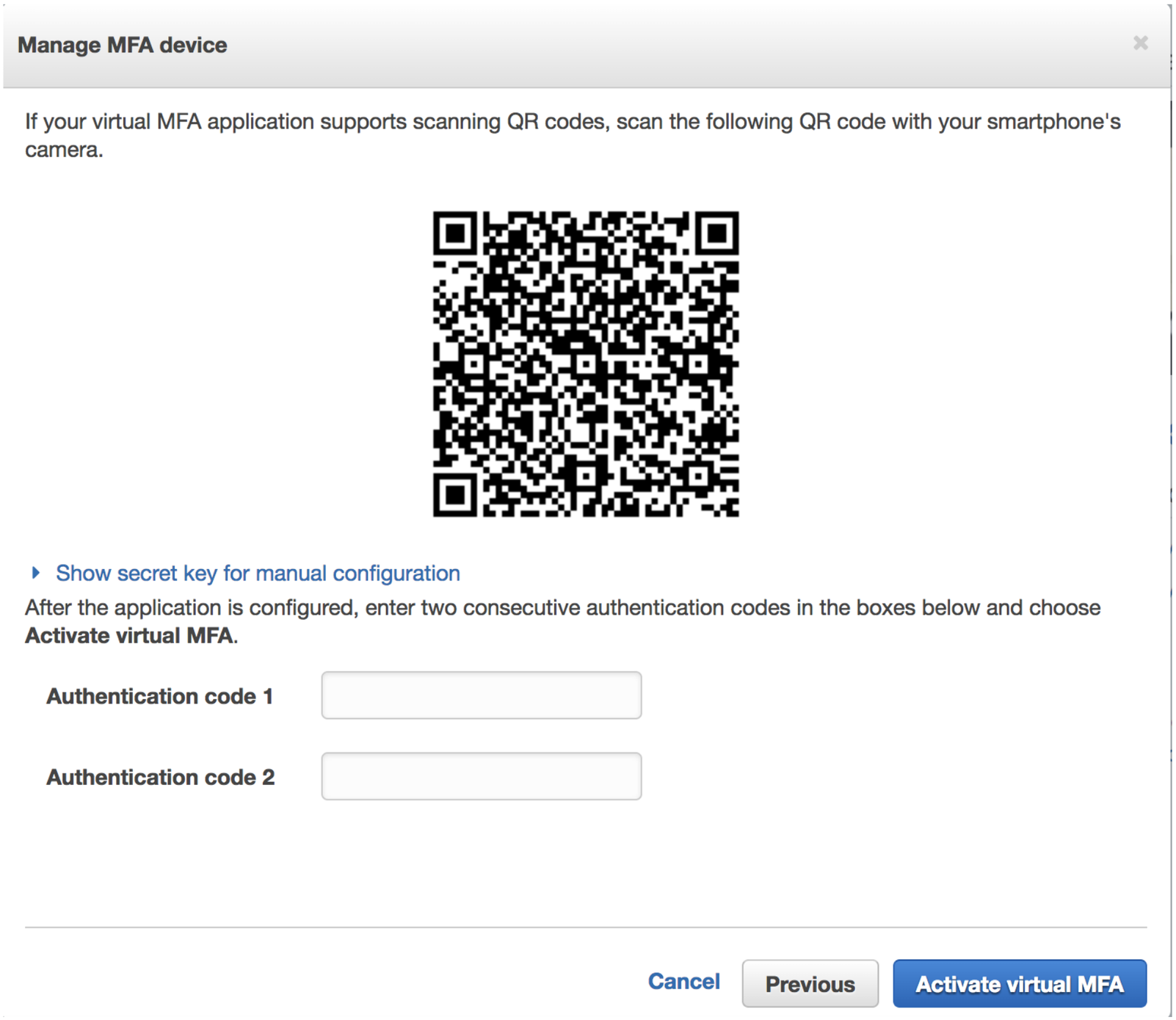
Gestion de Acceso



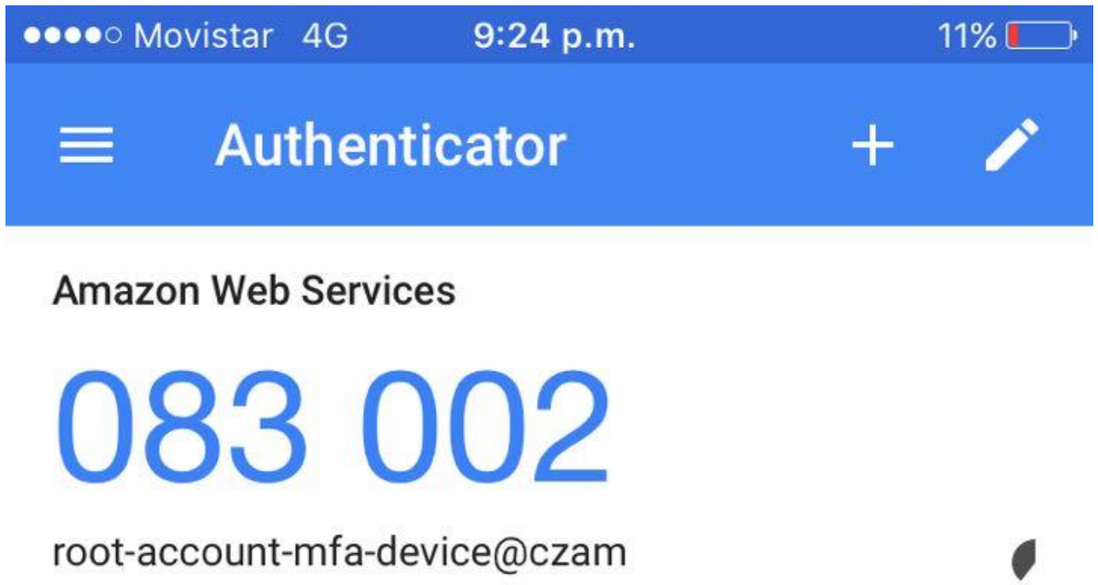
Seguridad - IAM

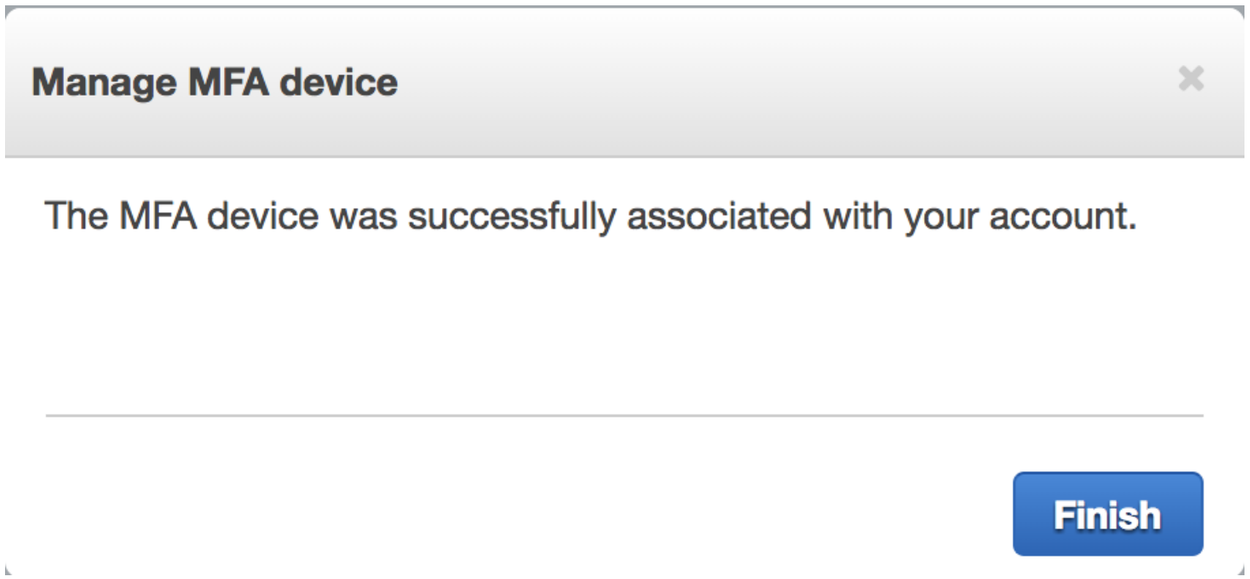


Seguridad MFA - IAM



Seguridad MFA - IAM





LABORATORIO

1. Cambiar dirección de conexión a la consola de AWS.
2. Creación de un usuario IAM.
3. Creación de un Role IAM.
4. Creación de un Grupo IAM.
5. Verificación de Políticas.
    1. Policy Generator.
    2. Inline Policy.
6. Activar MFA.
7. Políticas de rotación de Password.
8. Creación de una EC2 con IAM Usuario y con IAM Role.