



Gestión de identidad y acceso en AWS (IAM)

</> Índice

- ¿Qué es IAM?
- Características de IAM
- Terminología básica en IAM
- Lab - IAM

</> ¿Qué es AWS Identity and Access Management (IAM)?

- IAM nos permite gestionar usuarios y su nivel de acceso a la consola de AWS
- Es muy importante que entendamos cómo funciona AWS para saber cómo administrar la cuenta de AWS de nuestra empresa en el mundo real





Características de IAM

IAM nos ofrece las siguientes características:

- Control centralizado de la cuenta de AWS
- Acceso compartido a la cuenta de AWS
- Gestión de permisos de forma granulada
- Federación de identidad (Active Directory, Facebook, LinkedIn, etc.)
- Autenticación multifactor
- Acceso temporal para usuarios o dispositivos cuando sea necesario
- Nos permite definir políticas para rotación de passwords
- Se integra con muchos servicios de AWS



Terminología básica de IAM

- **Usuarios**

Los usuarios finales que acceden a AWS tales como personas, empleados de una organización, etc.

- **Grupos**

Un grupo es una colección de usuarios. A cada usuario del grupo lleva implícitos los permisos del grupo al que pertenece

- **Políticas**

Las políticas viene definidas por unos documentos denominados *Policy documents*. Estos documentos están en formato JSON y definen permisos sobre lo que un Usuario, Grupo o Rol puede hacer

- **Roles**

Podemos crear roles y asignarlos a distintos recursos de AWS

</> ¿Cuál es la mejor manera de aprender sobre IAM?

"For the things we have to learn before we can do them, we learn by doing them"

Aristóteles



Lab - IAM

¿Qué hemos aprendido?

- IAM es universal. Aplica a todas las regiones
- La cuenta de root es simplemente la cuenta con la que nos hemos registrado. Tiene acceso de administración completo a AWS
- Los nuevos usuarios no tienen permisos asignados nada más crearlos
- Los nuevos usuarios tienen asignados una Access Key ID y una Secret Access Key nada más crearlos
- Estas claves no son lo mismo que el password. No podemos utilizarlas para logarnos en la consola, pero sí para hacer uso de las APIs de AWS
- Estas claves sólo se muestra una vez. Si las perdemos hay que regenerarla. Es buena idea guardarlas en algún sitio seguro
- Siempre hay que configurar a Autenticación Multifactor (MFA) en la cuenta de root
- Podemos crear y configurar las políticas de rotación de passwords
- Podemos crear alarmas de facturación



Consejos - IAM

- Crear cuentas de usuarios individuales y utilizar cuentas IAM desde el comienzo
- Habilitar MFA
- Restringir el uso de credenciales IAM lo más posible
- No usar la cuenta de usuario Root
- Habilitar CloudTrail
- Usar roles de IAM para EC2 delegando en la instancia la obtención de credenciales
- Asignar roles de IAM por realm (desarrollo, pre-producción, producción)



Importante - IAM

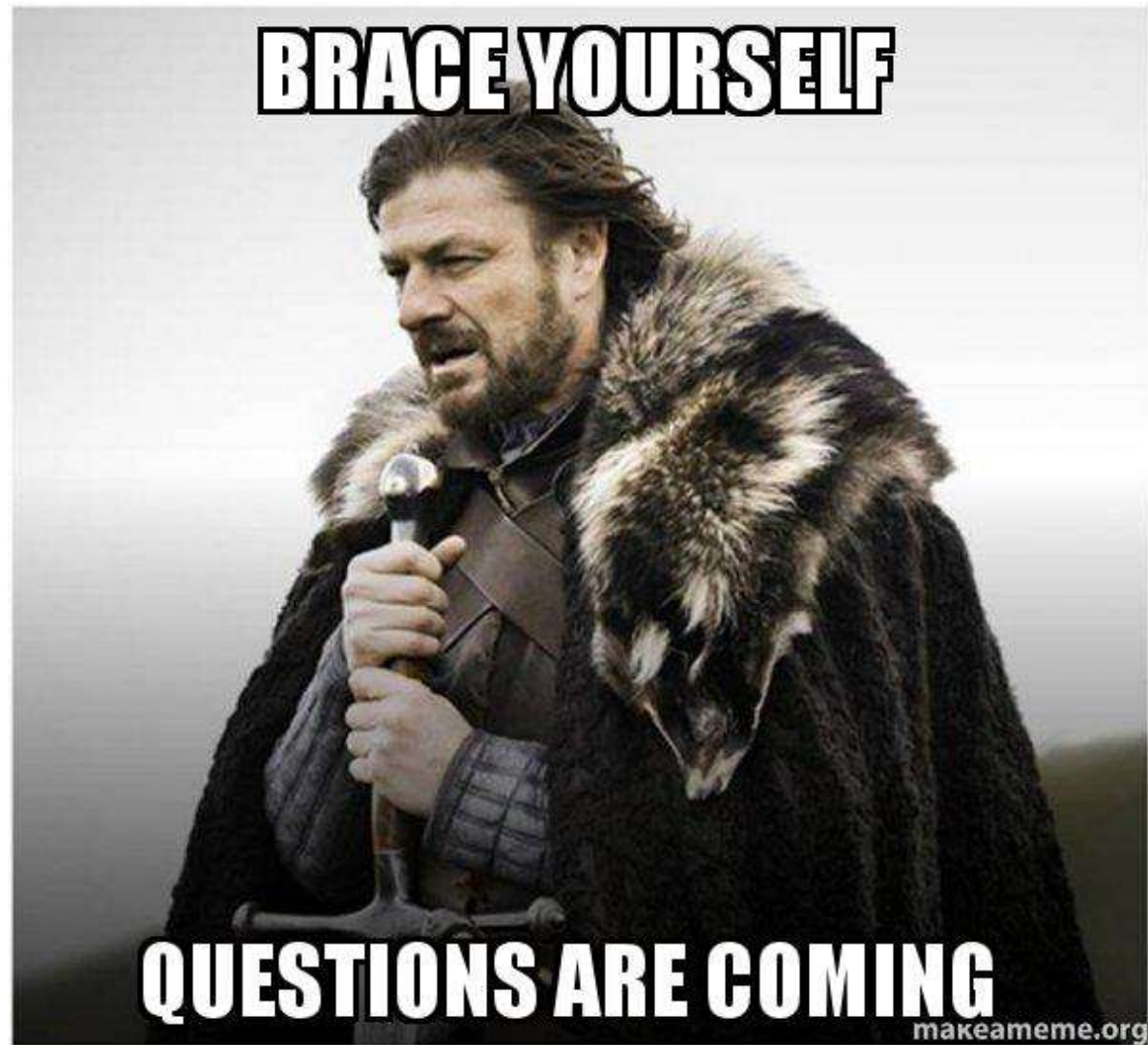
- NO compartir las credenciales
- Algunas peticiones a la API de IAM pueden tardar segundos
- SLA de IAM menor que el de otros servicios
- NO subir credenciales a los repositorios

</> Resumen

¿Qué hemos aprendido en este módulo?

- Conocer qué es IAM y para qué utilizarlo
- Conocer la terminología básica y saber diferenciar entre usuarios, grupos, políticas y roles
- Aprender a usar el servicio de IAM de AWS


</> Preguntas





- Unai Arríen
- Email de contacto: *unai.arrien@gmail.com*

info@devacademy.es 

687374918 

@DevAcademyES 