Introducción a Cloud Computing

Identity Access Management

Mauricio Améndola / Sebastián Orrego – Profesor Adjunto
Escuela de Tecnología – Facultad de Ingeniería

UNIVERSIDAD ORT Uruguay

AGENDA

1. Qué es IAM?
2. Terminología
3. Cómo funciona IAM?
4. Características principales
5. Formas de interactuar con IAM
6. DEMO

Qué es Identity and Access Management (IAM)?

Qué es IAM?

Identity and Access Management

Es uno de los servicios principales y transversales en la nube de AWS, ya que es el que nos permite controlar y administrar de forma segura el acceso a los distintos recursos de AWS. Básicamente su rol es proveer:

- ➔ Autenticación (login)
- ➔ Autorización (tiene permisos)

Qué es IAM?

Identity and Access Management

Cuando se crea una cuenta de AWS por primera vez, se comienza con una identidad con acceso completo a todos los servicios y recursos. Esta identidad es denominada “root user”. Y es accedida mediante email y password utilizados para crear la cuenta.

Terminología

Terminología

➔ Resources

Objetos de usuario, grupo, rol, política y proveedor de identidad que se almacenan en IAM. Al igual que con otros servicios de AWS, se puede agregar, editar y eliminar recursos de IAM.

Terminología

➔ Identities

Los objetos de recursos de IAM que se utilizan para identificar y agrupar. Puede adjuntar una política a una “entity” de IAM. Esto incluye usuarios, grupos y roles.

Terminología

➔ Entities

Objetos de recursos de IAM que AWS usa para la autenticación. Estos incluyen usuarios de IAM, usuarios federados y roles de IAM asumidos.

Terminología

➔ Principals

Una persona o aplicación que utiliza el usuario root de la cuenta de AWS, un usuario de IAM o un rol de IAM para iniciar sesión y realizar solicitudes a AWS.

Terminología

➔ Request

Cuando un principal intenta utilizar la Consola de administración de AWS, la API de AWS o la AWS CLI, ese principal envía una solicitud a AWS. La solicitud incluye la siguiente información:

- ➔ Acciones u operaciones
- ➔ Recursos
- ➔ Principal
- ➔ Datos del entorno
- ➔ Datos de recursos

Terminología

➔ Autenticación

Un principal debe estar autenticado (iniciado sesión en AWS) con sus credenciales para enviar una solicitud a AWS. Algunos servicios, como Amazon S3 y AWS STS, permiten algunas solicitudes de usuarios anónimos. Sin embargo, son la excepción a la regla.
Para autenticarse desde la consola como usuario root, se debe iniciar sesión con su dirección de correo electrónico y contraseña. Como usuario de IAM, se ingresa con el ID de la cuenta o alias, y luego el nombre de usuario y contraseña. Para autenticarse desde la API o la AWS CLI, se debe proporcionar la access_key_id y secret_access_key_id. También es posible que sea necesario proporcionar información de seguridad adicional. Por ejemplo, AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta.

Terminología

➔ Autorización

También debe estar autorizado (permitido) para completar el request. Durante la autorización, AWS usa valores del contexto de la solicitud para verificar las políticas que se aplican a la solicitud. Luego usa las políticas para determinar si permite o rechaza la solicitud. La mayoría de las políticas se almacenan en AWS como documentos JSON y especifican los permisos para las entidades principales.

Terminología

➔ Autorización

AWS verifica cada política que se aplica al contexto de su solicitud. Si una única política de permisos incluye una acción denegada, AWS rechaza toda la solicitud y deja de evaluar. Esto se llama denegación explícita. La lógica de evaluación de una solicitud dentro de una sola cuenta sigue estas reglas generales:

- ➔ De forma predeterminada, se rechazan todas las solicitudes.
- ➔ Un permiso explícito en cualquier política de permisos (basada en identidad o basada en recursos) anula este valor predeterminado.
- ➔ La existencia de un SCP de organización, un límite de permisos de IAM o una política de sesión anula el permiso. Si existe uno o más de estos tipos de políticas, todos deben permitir la solicitud. De lo contrario, se niega implícitamente.
- ➔ Una denegación explícita en cualquier política anula cualquier permiso.

Terminología

➔ Acciones u Operaciones

Una vez que su solicitud ha sido autenticada y autorizada, AWS aprueba las acciones u operaciones en su solicitud. Las operaciones las define un servicio e incluyen cosas que puede hacer con un recurso, como ver, crear, editar y eliminar ese recurso. Por ejemplo, IAM admite aproximadamente 40 acciones para un recurso de usuario, incluidas las siguientes acciones:

- ➔ CreateUser
- ➔ DeleteUser
- ➔ GetUser
- ➔ UpdateUser

Para permitir que un principal realice una operación, se debe incluir las acciones necesarias en una política que se aplique al principal o al recurso afectado.

Terminología

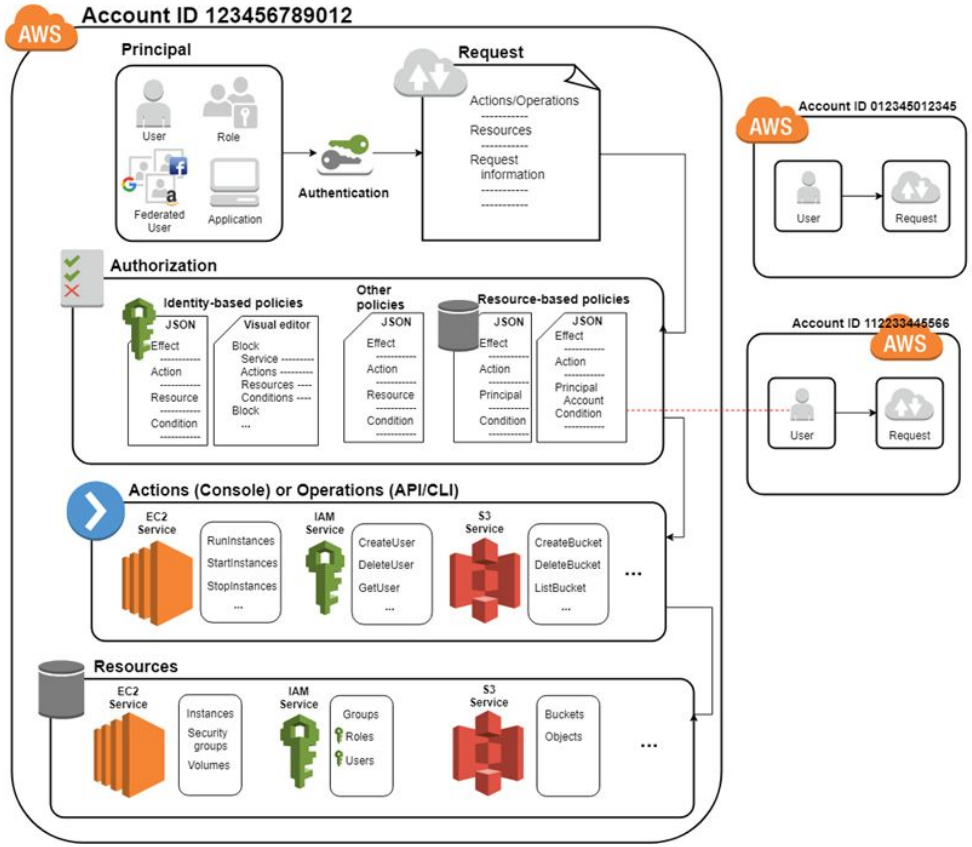
➔ Resources

Una vez que su solicitud ha sido autenticada y autorizada, AWS aprueba las acciones u operaciones en su solicitud. Las operaciones las define un servicio e incluyen cosas que puede hacer con un recurso, como ver, crear, editar y eliminar ese recurso. Por ejemplo, IAM admite aproximadamente 40 acciones para un recurso de usuario, incluidas las siguientes acciones:

- ➔ CreateUser
- ➔ DeleteUser
- ➔ GetUser
- ➔ UpdateUser

Para permitir que un principal realice una operación, se debe incluir las acciones necesarias en una política que se aplique al principal o al recurso afectado.

Cómo funciona IAM?


Account ID 123456789012
AWS
Principal
User
Role
Federated User
Application
Authentication
Request
Actions/Operations
Resources
Request information
Authorization
Identity-based policies
JSON
Effect
Action
Resource
Condition
Visual editor
Block
Service
Actions
Resources
Conditions
Block
...
Other policies
JSON
Effect
Action
Resource
Condition
Resource-based policies
JSON
Effect
Action
Principal
Condition
JSON
Effect
Action
Principal
Account
Condition
Actions (Console) or Operations (API/CLI)
EC2 Service
RunInstances
StartInstances
StopInstances
...
IAM Service
CreateUser
DeleteUser
GetUser
...
S3 Service
CreateBucket
DeleteBucket
ListBucket
...
Resources
EC2 Service
Instances
Security groups
Volumes
IAM Service
Groups
Roles
Users
S3 Service
Buckets
Objects
...
Account ID 012345012345
AWS
User
Request
Account ID 112233445566
AWS
User
Request

Principales características

Principales características

- ➔ Acceso compartido a la cuenta de AWS
- ➔ Permisos granulares
- ➔ Acceso seguro a los recursos utilizados para las aplicaciones que corren en EC2
- ➔ Autenticación multi-factor (MFA)
- ➔ Identity Federation
- ➔ PCI-DSS compliance
- ➔ Integrado con muchos servicios de AWS
- ➔ Es gratis

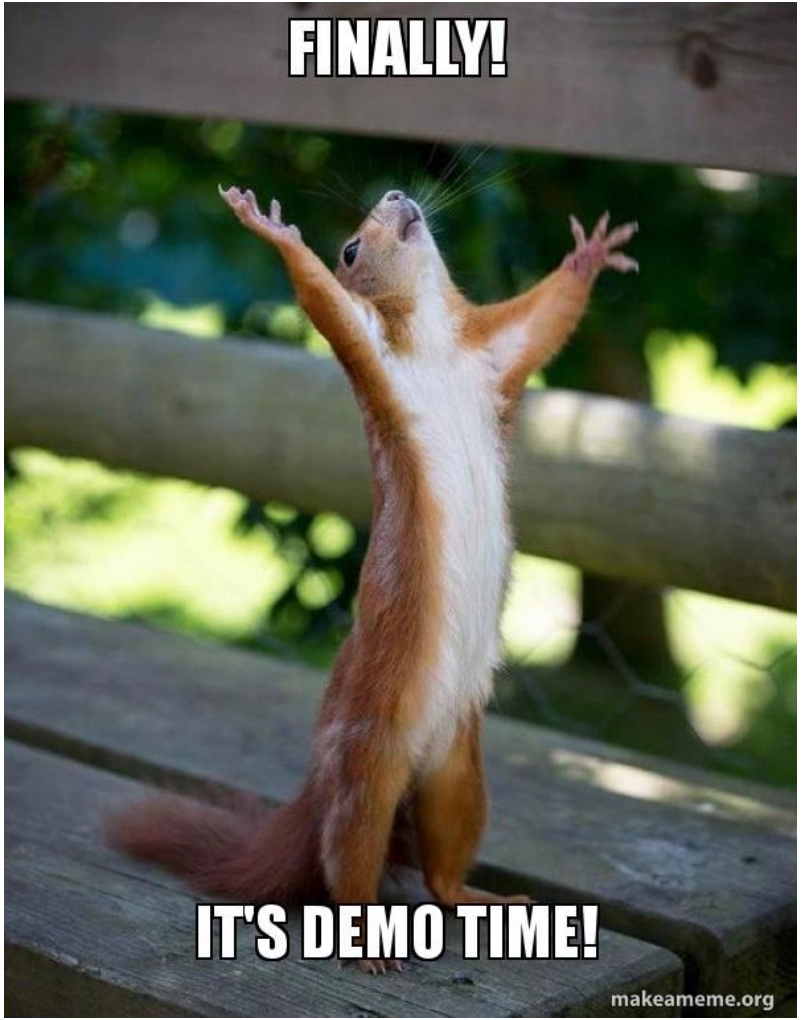
Formas de interactuar con IAM

Formas de interactuar con IAM

- ➔ Mediante la interfaz web
- ➔ Utilizando la línea de comando aws-cli
- ➔ Request a la API

Material adicional

➔ AWS Documentation


FINALLY!
IT'S DEMO TIME!
makeameme.org