CONCEPTOS DE IAM y S3
SEMANA 11- CDyR

Integrantes:

- Luque Mamani Magno Ricardo
- Quezada Marceliano Gian Carlos

Introducción al Servicio AWS IAM

1.- EXPLICA LA FUNCIONALIDAD PRINCIPAL DEL SERVICIO AWS IAM Y SU IMPORTANCIA EN LA ADMINISTRACIÓN DE ACCESOS EN LA NUBE DE AWS.

AWS Identity and Access Management (IAM) es un servicio que proporciona AWS para controlar y administrar de manera segura el acceso a los recursos de AWS mediante una cuenta raiz.

Funcionalidades principales:

Creacion de Usuarios

Al crear una cuenta en AWS, se nos crea un usuario raíz y contraseña (clave-valor) mediante el cual podemos crear múltiples usuarios. Un usuario se puede representar como una persona física a la que le asignamos distintos permisos (mediante las politicas) dentro de nuestra cuenta de AWS

Creacion de Grupos

Dentro de nuestra organización, es posible que múltiples usuarios necesiten acceder a los mismos servicios, por lo cual se crean grupos. Al realizarlo de esta manera, podemos administrar de manera centralizada los usuarios asignados a ese grupo simplemente aplicando politicas a nivel de grupo.

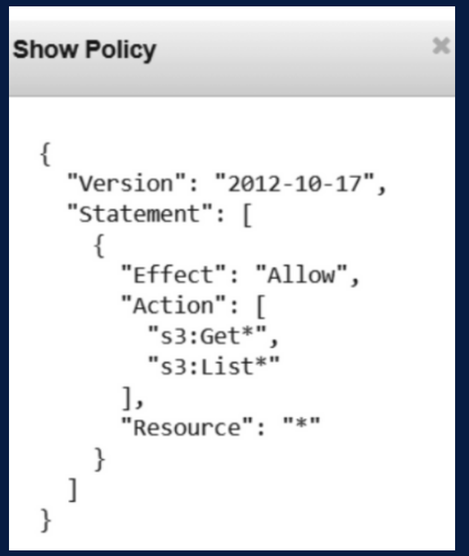
Políticas de Permisos

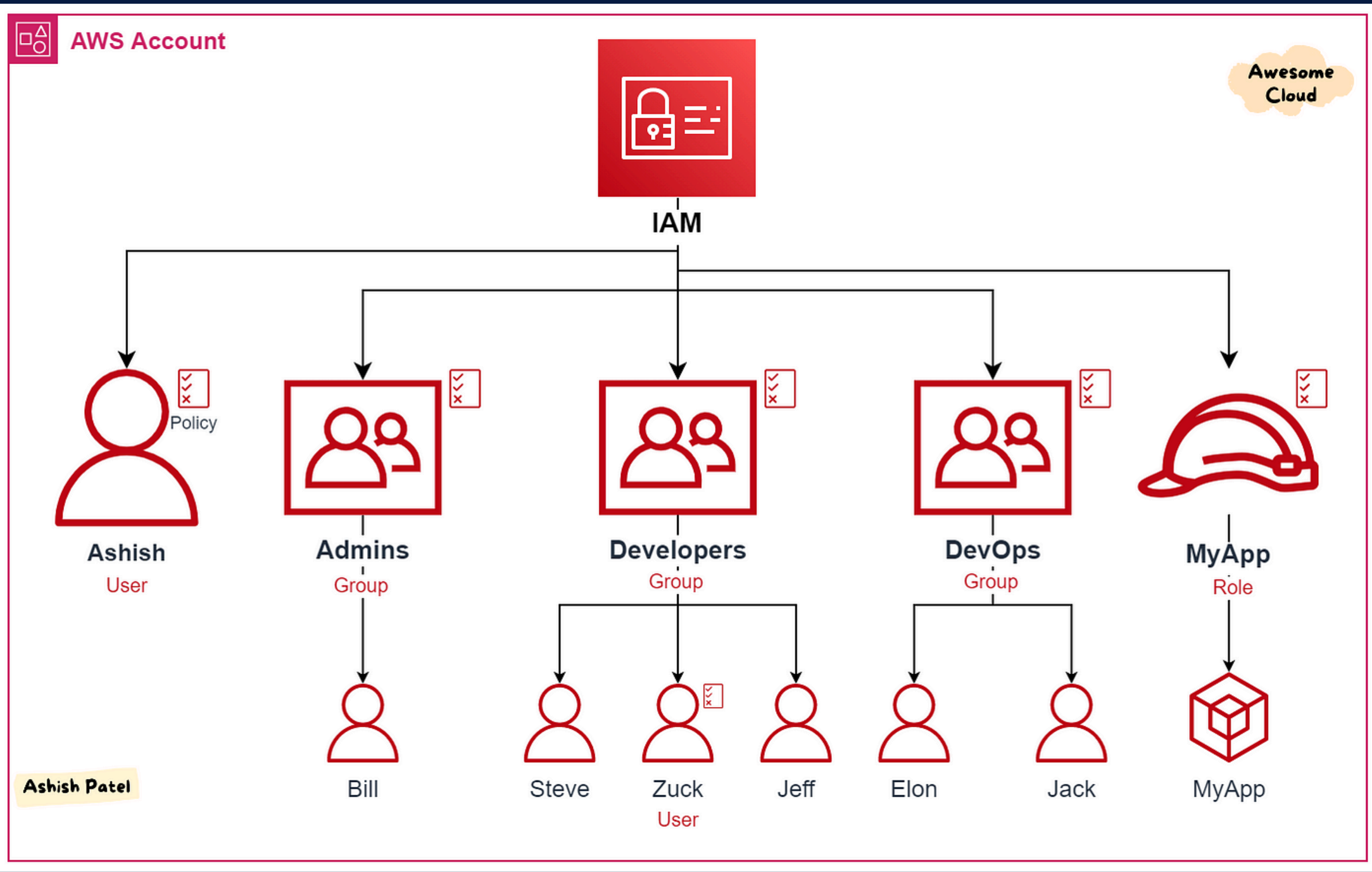
Son objetos adjuntados a una identidad, como un usuario, rol o grupo IAM. Estas políticas definen lo que una identidad pueden o no pueden hacer dentro de una cuenta de AWS, y se definen en documentos JSON.

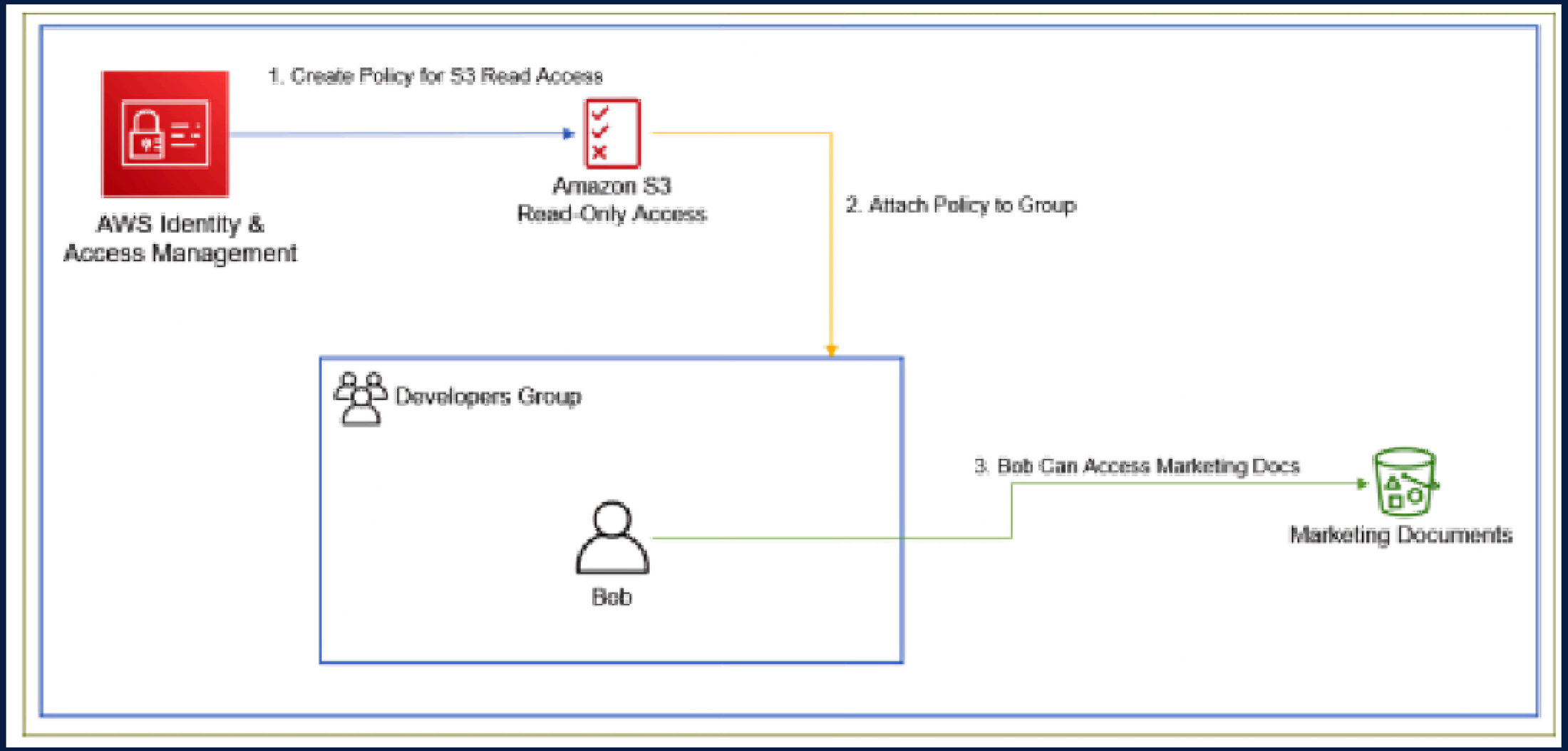
Tipos de Políticas de Permisos

- Basadas en identidad: Definen lo que una entidad puede hacer.
- Basadas en recursos: Adjuntadas al recursos de cada cuenta.
- Limites de permisos: Definimos el conjunto máximo de permisos para las políticas basadas en identidad.
- Políticas de control de acceso,

Ejemplo de Políticas de Permisos




AWS Account
Awesome Cloud
IAM
Policy
Ashish
User
Admins
Group
Developers
Group
DevOps
Group
MyApp
Role
Bill
Steve
Zuck
User
Jeff
Elon
Jack
MyApp
Ashish Patel


1. Create Policy for S3 Read Access
AWS Identity &
Access Management
Amazon S3
Read-Only Access
2. Attach Policy to Group
Developers Group
Bob
3. Bob Can Access Marketing Docs
Marketing Documents

Asignación de credenciales temporales con roles IAM

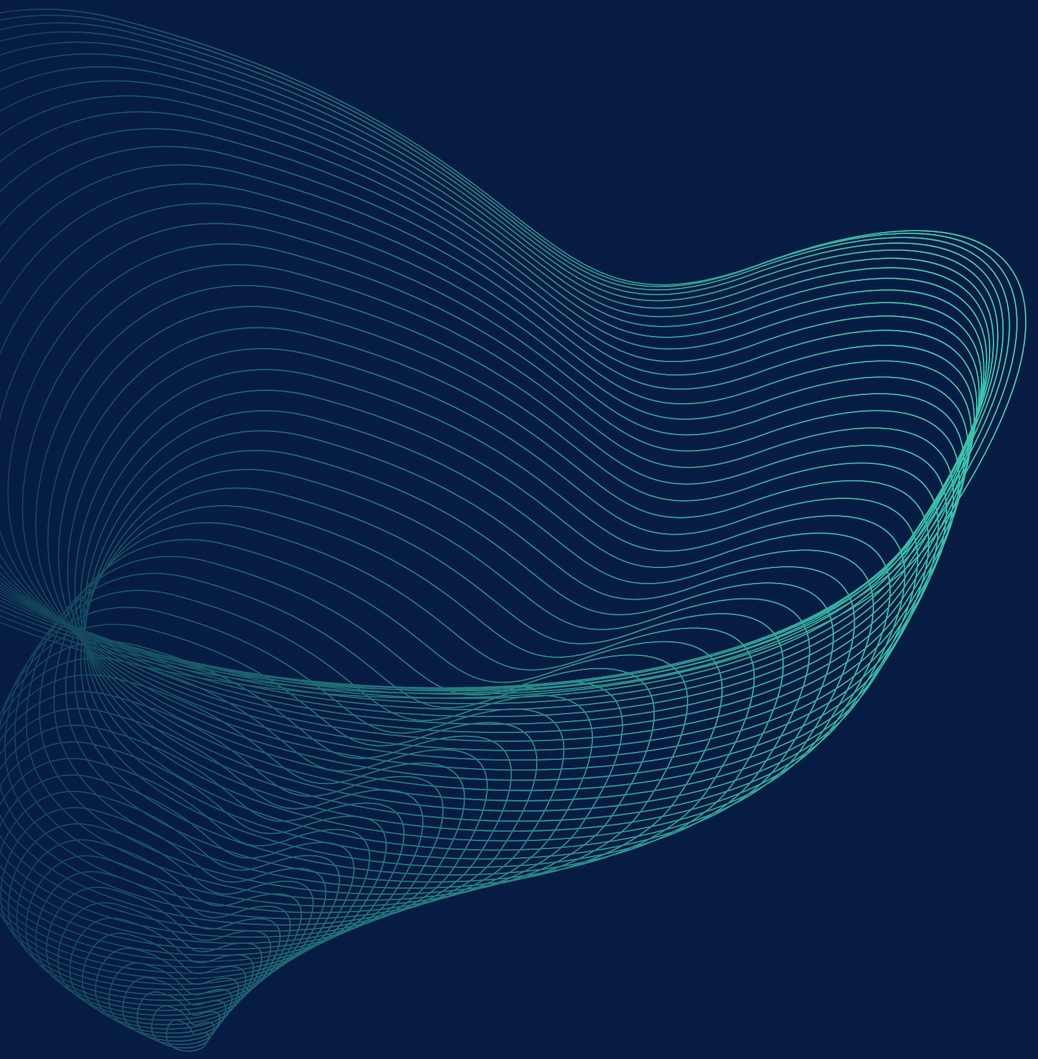
2.- EXPLICA QUÉ SON LOS ROLES IAM Y CÓMO SE UTILIZAN PARA ASIGNAR CREDENCIALES TEMPORALES. PROPORCIONA UN CASO DE USO COMÚN.

Los roles de IAM en AWS son una forma de control de acceso seguro, entidades confiables como usuarios, aplicaciones o servicios de AWS (como EC2) pueden asumir roles para obtener credenciales de seguridad temporales para realizar solicitudes a los distintos recursos o servicios que ofrece AWS. La estructura de roles le permite delegar el acceso con permisos definidos, lo que ayuda a mantener un entorno seguro.

Laboratorio de AWS Lab Learner

Ejercicio 1: Creación y gestión de usuarios IAM

Crea tres usuarios IAM con diferentes niveles de permisos. Asigna políticas específicas a cada uno y documenta los pasos realizados.



¡GRACIAS!