Roles vs Grupos en AWS IAM

En AWS IAM, tanto los roles como los grupos son componentes esenciales para la gestión de permisos y acceso a recursos, pero tienen diferentes usos y características. A continuación, se comparan los roles y los grupos para clarificar sus diferencias y aplicaciones.

Roles

Definición

Un rol es una **identidad en IAM** con permisos específicos que pueden ser asumidos por usuarios, aplicaciones o servicios. Los roles no tienen credenciales permanentes asociadas; en su lugar, las identidades que asumen el rol obtienen credenciales temporales.

Características

- **Permisos Temporales**: Los roles otorgan permisos temporales mediante la asunción del rol, lo que proporciona credenciales temporales a la entidad que asume el rol.
- **Sin Credenciales Directas**: A diferencia de los usuarios, los roles no tienen credenciales directas (como contraseñas o claves de acceso).
- **Delegación de Acceso**: Los roles se utilizan para permitir que las entidades asuman permisos específicos temporalmente, ideal para aplicaciones y servicios que necesitan interactuar con otros recursos de AWS sin almacenar credenciales.
- **Cross-Account Access**: Los roles permiten acceder a recursos en otras cuentas de AWS de manera segura.
- **Roles de Servicio**: Los roles pueden ser utilizados por servicios de AWS (como EC2, Lambda) para realizar acciones en nombre del usuario sin necesitar claves de acceso.

Usos

- **Aplicaciones y Servicios**: Permitir que instancias de EC2, funciones Lambda y otros servicios de AWS realicen acciones en otros recursos sin requerir claves de acceso.
- **Acceso Externo**: Proveer acceso temporal a usuarios externos mediante la asunción de roles.
- **Seguridad Mejorada**: Minimizar el riesgo al evitar el almacenamiento de claves de acceso en aplicaciones y servicios.

Grupos

Definición

Un grupo es una **colección de usuarios en IAM**. Los grupos permiten asignar permisos de manera colectiva a un conjunto de usuarios, facilitando la administración de permisos.

Características

- **Agrupación de Usuarios**: Los grupos permiten la agrupación de usuarios con permisos similares, simplificando la gestión de permisos.
- **Permisos Colectivos**: Los permisos se asignan a los grupos y los usuarios heredan estos permisos al ser miembros del grupo.
- **Facilidad de Administración**: La gestión de permisos se simplifica al permitir asignar, modificar o revocar permisos a múltiples usuarios a través del grupo.

Usos

- **Administración Centralizada**: Facilitar la administración de permisos para grandes conjuntos de usuarios con necesidades de acceso similares.
- **Roles Departamentales**: Crear grupos basados en departamentos o funciones (por ejemplo, desarrolladores, administradores, equipo de soporte) y asignar permisos específicos a cada grupo.
- **Simplificación de Políticas**: Reducir la complejidad de la gestión de políticas al asociar permisos a grupos en lugar de usuarios individuales.

Comparación

Característica	Roles	Grupos
Identidad	Asumida temporalmente por usuarios/servicios	Colección de usuarios
Credenciales	Temporales, proporcionadas al asumir el rol	Permanentes, asociadas a usuarios
Usos Principales	Acceso temporal, delegación de permisos, aplicaciones y servicios	Administración de permisos de usuarios
Asignación de Permisos	Directamente al rol	Al grupo, heredado por usuarios
Cross-Account Access	Sí	No
Roles de Servicio	Sí (para servicios de AWS)	No

Ejemplos de Uso

Roles

- **Instancia de EC2**: Una instancia de EC2 necesita acceder a un bucket de S3. Se crea un rol con permisos para S3 y se asigna a la instancia de EC2.
- **Acceso Externo**: Un proveedor necesita acceso temporal a ciertos recursos de AWS. Se crea un rol con los permisos necesarios y se permite que el proveedor asuma el rol temporalmente.

Grupos

- **Desarrolladores**: Se crea un grupo "Desarrolladores" con permisos para recursos de desarrollo (por ejemplo, acceso a EC2 y RDS). Todos los usuarios desarrolladores se añaden a este grupo.
- **Administradores**: Se crea un grupo "Administradores" con permisos de administración completa en la cuenta de AWS. Los administradores de sistemas se añaden a este grupo.