AWS IAM

Definición

AWS Identity and Access Management (IAM) es un **servicio web** de Amazon que permite controlar de forma segura el acceso a los recursos de AWS. Con IAM, se pueden crear y gestionar usuarios y grupos, y utilizar permisos para permitir o denegar su acceso a los recursos de AWS.

Componentes

Usuarios

- **Definición**: Un usuario en IAM es una identidad que puede representar a una persona, una aplicación o un servicio que utiliza los recursos de AWS.
- **Usos**: Los usuarios se crean para conceder acceso a individuos u aplicaciones a los recursos de AWS. Cada usuario tiene un conjunto de credenciales de seguridad únicas, como contraseñas y claves de acceso.

Grupos

- **Definición**: Un grupo es una colección de usuarios en IAM. Permite asignar permisos de manera colectiva a un conjunto de usuarios.
- **Usos**: Los grupos facilitan la gestión de permisos al agrupar usuarios que necesitan permisos similares. Por ejemplo, puede haber un grupo de "Desarrolladores" con permisos específicos para recursos de desarrollo.

Políticas

- **Definición**: Una política es un documento en formato JSON que, cuando está asociado a una identidad (usuario, grupo, rol), define sus permisos.

Tipos de Políticas:

- **Políticas Administradas por AWS (AWS Managed Policies)**:
  - **Descripción**: Políticas predefinidas y mantenidas por AWS.
  - **Ejemplos**: `AmazonEC2ReadOnlyAccess`, `AmazonS3FullAccess`.
  - **Ventajas**: No requieren creación desde cero y son actualizadas automáticamente por AWS.
- **Políticas Administradas por el Cliente (Customer Managed Policies)**:
  - **Descripción**: Políticas creadas y gestionadas por el usuario.
  - **Usos**: Para definir permisos específicos no cubiertos por políticas administradas por AWS.
  - **Ventajas**: Flexibilidad para definir permisos detallados y específicos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "a4b:Search*",
                "a4b:List*",
                "a4b:Get*"
            ],
            "Resource": "*"
        }
    ]
}
```

- **Políticas en Línea (Inline Policies)**:
  - **Descripción**: Políticas asociadas directamente a un solo usuario, grupo o rol.
  - **Usos**: Definir permisos específicos para una identidad particular.
  - **Ventajas**: Permite una definición precisa de permisos para una identidad sin afectar a otras.
- **Políticas de Sesión (Session Policies)**:
  - **Descripción**: Políticas temporales adjuntadas a una sesión cuando se asume un rol o se utilizan credenciales temporales.
  - **Usos**: Otorgar permisos adicionales o restrictivos durante una sesión específica.
  - **Ventajas**: Flexibilidad para definir permisos temporales sin modificar las políticas permanentes.
- **Políticas de Control de Servicio (Service Control Policies - SCPs)**:
  - **Descripción**: Políticas aplicadas a nivel de la Organización de AWS.
  - **Usos**: Gestionar el acceso a los recursos de AWS en todas las cuentas de la organización.
  - **Ventajas**: Gestión centralizada de permisos en una organización multi-cuenta.
- **Políticas Basadas en Recursos (Resource-Based Policies)**:
  - **Descripción**: Políticas adjuntadas directamente a recursos de AWS.
  - **Usos**: Definen qué identidades pueden acceder y qué acciones pueden realizar sobre un recurso específico.
  - **Ventajas**: Control de acceso granular a nivel de recurso.

Roles

- **Definición**: Un rol es una identidad en IAM con permisos específicos que pueden ser asumidos por usuarios, aplicaciones o servicios.
- **Usos**: Los roles son útiles para delegar permisos temporalmente. Por ejemplo, un rol puede ser asumido por una instancia de EC2 para acceder a otros recursos sin necesidad de almacenar claves de acceso en la instancia.

Identidades Federadas

- **Definición**: Permiten a usuarios fuera de AWS (como los de Microsoft Active Directory, Facebook, Google, etc.) obtener acceso temporal a los recursos de AWS.
- **Usos**: Facilitan la integración con sistemas de autenticación externos para proporcionar acceso temporal a los recursos de AWS sin necesidad de crear usuarios IAM para cada entidad externa.

Usos de AWS IAM

1. **Control Granular de Acceso**:
   - Definir permisos detallados para recursos específicos mediante políticas personalizadas.
   - Utilizar políticas administradas por AWS para configuraciones comunes.
2. **Gestión de Usuarios y Grupos**:
   - Creación y gestión de usuarios individuales con credenciales únicas.
   - Agrupación de usuarios con permisos similares para facilitar la administración.
3. **Delegación de Acceso con Roles**:
   - Asignar roles a servicios de AWS como EC2, Lambda, etc., para que puedan interactuar con otros servicios de AWS.
   - Permitir a entidades externas asumir roles con permisos específicos para acceder a recursos de AWS.
4. **Acceso Temporal y Seguro**:
   - Utilización de identidades federadas para proporcionar acceso temporal a recursos sin comprometer la seguridad.
   - Implementación de roles de sesión temporal con permisos específicos.

5. **Cumplimiento y Auditoría**:
    - Registro de actividades mediante AWS CloudTrail para auditoría y cumplimiento de normativas.
    - Monitoreo y revisión de políticas y permisos para garantizar la adherencia a las mejores prácticas de seguridad.