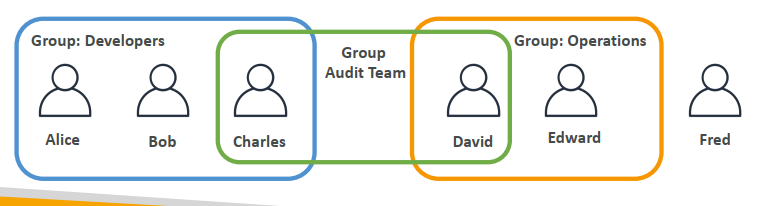
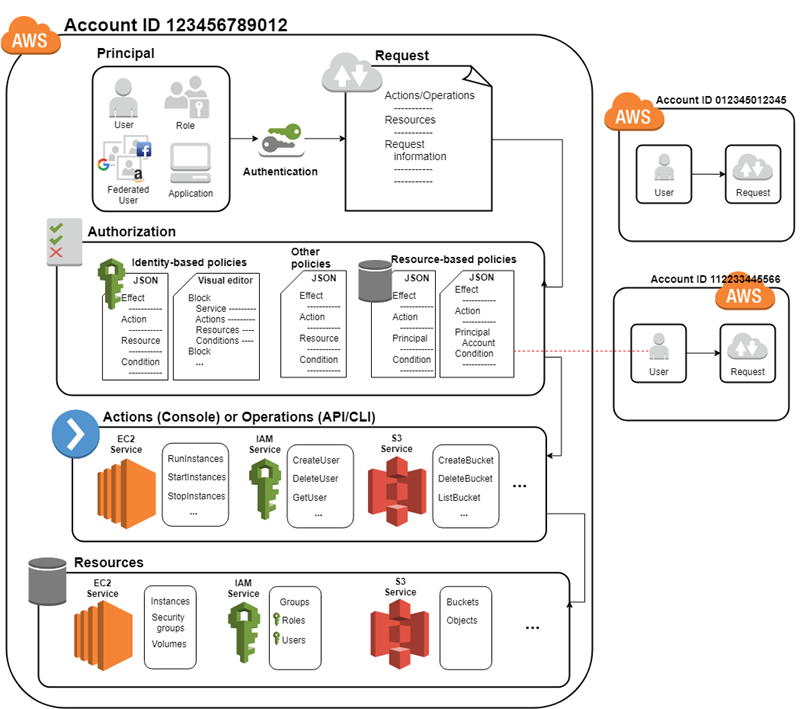
# IAM (Identification and Access Management)

Es un servicio Web que nos ayuda a controlar de forma segura, el acceso a los recursos de AWS. Se utiliza para verificar quien está **autenticado (quien puede iniciar sesión)** y quien tiene **autorización (tiene permisos)** para utilizar los recursos.

* **Servicio Global**
* **Características**
  + **Acceso compartido de la cuenta de AWS:** Varias personas pueden utilizar la misma cuenta sin tener que compartir las mismas credenciales entre todos.
  + **Permisos detallados:** Se pueden conceder distintos permisos a distintas personas para diferentes recursos.
  + **Acceso seguro a los recursos de AWS para aplicaciones que se ejecutan en EC2:** Se pueden asignar credenciales seguras a aplicaciones que se ejecutan en EC2, como si fueran personas que hacen uso de dichos servicios.
  + **Multi Factor Authentication:** Verificación de dos pasos
  + **Identidad Federada:** Se puede permitir a usuarios que tienen credenciales de otros lugares (por ej: La red corporativa o un proveedor de identidad de internet) obtengan acceso temporal a la cuenta de AWS
  + **Información de identidad para control:** CloudTrail recibe registros que incluye información sobre los usuarios que realizaron peticiones a los servicios de AWS dentro de una cuenta
  + **Consistencia Final:** IAM ofrece una alta disponibilidad, ya que replica los datos entre varios servidores distribuidos alrededor del mundo. Si una solicitud para cambiar algunos datos se realiza correctamente, el cambio se confirma y se almacena de forma segura.
* **Acceso a IAM**
  + AWS Management Console (Inicio de sesión en un navegador web)
  + Herramienta de Linea de Comandos (CLI)
  + SDK de AWS
  + API HTTPS de AWS
* **Términos**
  + **Recursos de IAM:** Objetos de usuario, grupo, función, política (policy) y proveedor de identidad almacenados en IAM
  + **Identidades de IAM:** Los objetos de recursos de IAM que se utilizan para identificar y agrupar **(usuarios, grupos y roles)**
  + **Entidades de IAM:** Los objetos de recursos de IAM que se utilizan para autenticación **(usuarios y roles)**
  + **Entidades principales:** Persona o aplicación que utiliza una cuenta raíz de AWS, un usuario de IAM o función IAM para iniciar sesión y realizar solicitudes, también se incluyen usuarios federados y roles asumidos.





## Solicitud

Cuando una entidad principal intenta utilizar la AWS Management Console, la CLI o la API de AWS, la entidad principal envía una solicitud a AWS. La solicitud incluye la siguiente información:

* Acciones u operaciones que la entidad desea realizar
* Recurso de AWS sobre el que se quiere aplicar dichas acciones
* Persona o aplicación que utilizó una entidad (usuario o rol) que se utilizó para enviar la solicitud (incluye políticas asociadas a la entidad que el principal utilizó para iniciar sesión)
* Datos de entorno: Información sobre dirección IP, el agente de usuario, el estado de habilitación de SSL o la fecha y hora.
* Datos relacionados al recurso que se quiere utilizar.

## Autorización

Además de autenticarse (iniciar sesión), para completar una solicitud se debe estar autorizado. AWS utiliza las políticas (Documentos JSON) para determinar si se debe autorizar o denegar una solicitud. Estas políticas especifican los permisos otorgados a las entidades principales.

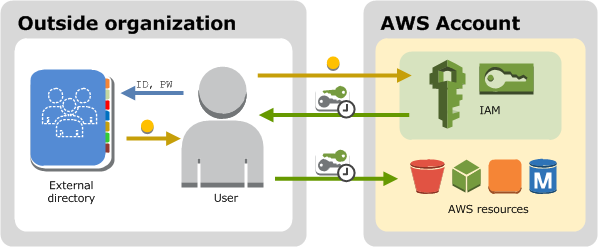
AWS comprueba cada política que se aplica al contexto de una solicitud**. Si una sola política de permisos, incluye una acción denegada, AWS deniega toda la solicitud y deja de evaluarla**. Esto se denomina **denegación explicita**. Dado que las solicitudes se deniegan de manera predeterminada, AWS autoriza una solicitud únicamente si las políticas de permisos aplicables permiten todas las partes de la solicitud

Normas generales de evaluación de una solicitud:

1. De forma predeterminada se deniegan todas las solicitudes (Por lo general, las solicitudes realizadas con credenciales de usuario root para los recursos de la cuenta siempre se autorizan) – Solo las políticas de control de servicios (SCP) de las organizaciones pueden restringir los permisos concedidos al usuario raíz.
2. Un permiso explicito en cualquier política de permisos (basada en identidad o recursos) anula esta opción predeterminada
3. Una denegación explicita en cualquier política, invalida cualquier permiso concedido.
4. La existencia de una SCP de Organizations, un límite de permisos de IAM o una política de sesión anula el permiso

## Federación de usuarios ya existentes

Si los usuarios de una organización ya tienen una forma de autenticarse, por ejemplo, iniciando sesión en la red de la empresa, no es necesario crear usuarios IAM independientes para ellos. En su lugar, se pueden federar esas identidades de usuario en AWS.



La federación es útil en los siguientes casos:

* **Mis usuarios ya poseen identidades en un directorio corporativo**

Si mi directorio corporativo es compatible con Security Assertion Markup Language 2.0 (SAML 2.0) se puede configurar dicho directorio para proporcionar acceso de inicio de sesión único (SSO) a la AWS Management Console

Si el directorio corporativo no es compatible con SAML 2.0, se puede crear una aplicación de agente de identidades para proporcionar acceso de inicio de sesión único (SSO) a la AWS Management Console.

Si el directorio corporativo es Microsoft Active Directory, se puede utilizar AWS Directory Service

* **Los usuarios ya poseen identidades de Internet**

Si está creando una aplicación móvil o una aplicación basada en web que permita que los usuarios se identifiquen mediante un proveedor de identidades de Internet como Login with Amazon, Facebook, Google o cualquier proveedor de identidades compatible con OpenID Connect (OIDC), la aplicación puede utilizar una federación para obtener acceso a AWS

NOTA: Utilizar Amazon Cognito para identidad federada con proveedores de identidad de Internet.

## Políticas y Usuarios

Los usuarios de IAM son identidades del servicio. Cuando se crean usuarios IAM, estos no pueden acceder a ningún elemento de la cuenta hasta que se les conceda el permiso.

De forma predeterminada, las acciones o los recursos que no se permiten de forma explícita se deniegan.

## Políticas y Grupos

Se pueden organizar a los usuarios IAM en grupos de IAM y asociar políticas al grupo. En ese caso, los usuarios individuales siguen teniendo sus propias credenciales, pero todos los usuarios de un grupo tienen los permisos que se asocian al grupo.

Los usuarios o los grupos pueden tener asociadas varias políticas que conceden permisos diferentes. **En ese caso, los permisos de los usuarios se calculan en base a la combinación de políticas**. No obstante, sigue aplicándose el principio básico: si no se ha concedido un permiso explícitamente para una acción y recurso, el usuario no tiene dichos permisos.

## Usuarios Federados y Roles

**Los usuarios federados y roles no tienen identidades permanentes en la cuenta de AWS como la tienen los usuarios IAM**. Para asignar permisos a un usuario federado, se puede crear una entidad a la que se hace referencia como rol y definir permisos para dicho rol. Cuando un usuario federado inicia sesión en AWS se asocia el usuario al rol y se le conceden los permisos que están definidos para el rol

## Políticas basadas en Identidad y Políticas basadas en Recursos

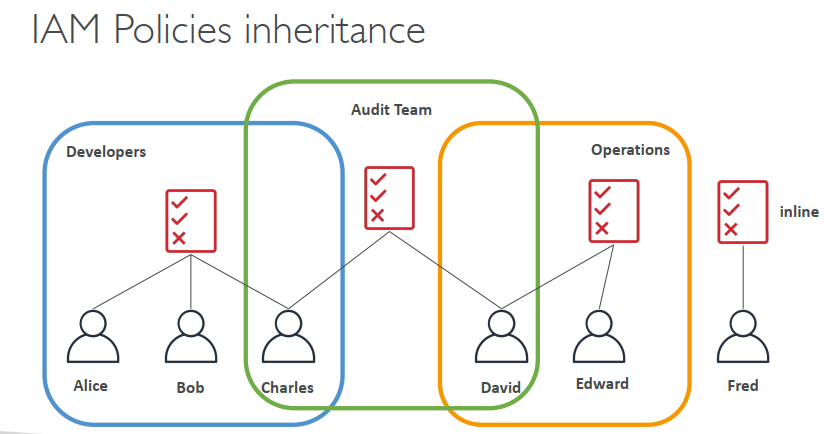
Las políticas basadas en identidad son políticas de permisos que se asocian a una identidad de IAM, como un usuario, grupo o rol. Las políticas basadas en recursos, son políticas de permisos asociadas a un recurso, como un bucket de S3

Las políticas basadas en identidad, controlan que acciones puede realizar una identidad, en que recursos y en qué condiciones. Se clasifican así:

* Políticas administradas
  1. Administradas por AWS: Administradas y creadas por AWS
  2. Administradas por el cliente: Administradas y creadas por el cliente. Ofrecen un control más preciso
  3. Políticas insertadas (inline): Administradas y creadas por el cliente y que están integradas en un único usuario, grupo o función (No recomendable)

**Las políticas basadas en recursos controlan que acciones puede realizar una entidad principal sobre ese recurso y en qué condiciones**. Las políticas basadas en recursos, son políticas inline y no hay políticas administradas basadas en recursos. Para hacer posible el acceso entre cuentas, se puede especificar toda una cuenta o entidades de IAM de otra cuenta como entidad principal en la política basada en recursos.

El servicio IAM solo admite un tipo de política de confianza basada en recursos, la llamada política de confianza de rol, que se asocia a un rol de IAM. Al ser un rol de IAM una entidad y un recurso que admite las políticas basadas en recursos, es necesario asociarle tanto una política de confianza como una política basada en identidad. **Las políticas de confianza definen que entidades principales (cuentas, usuarios, roles y usuarios federados) pueden asumir el rol.**

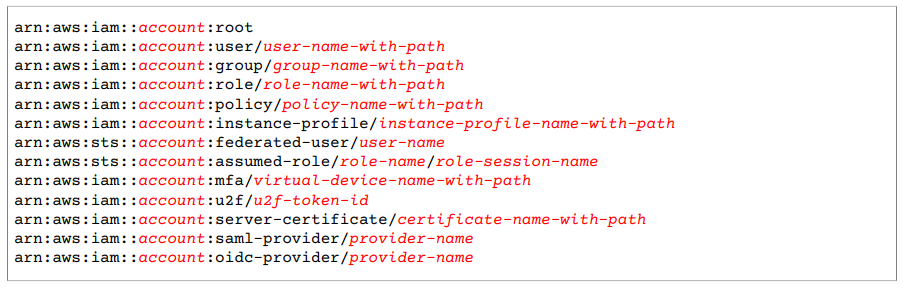


## ¿Cuándo crear un rol en vez de un usuario de IAM?

1. Cuando se cree una aplicación que se ejecuta en una instancia de EC2 y dicha aplicación realiza solicitudes a AWS
   1. Se crea un rol el cual será asumido por la/s instancias que ejecuten la aplicación
2. Cuando se crea una aplicación que se ejecutan en un móvil y realiza peticiones a AWS
   1. Lo conveniente es utilizar un proveedor de identidad como Login with Amazon, Facebook, Google, o Amazon Cognito para autenticar a los usuarios y asociarlos a un rol de IAM. La aplicación puede utilizar el rol para obtener credenciales temporales y realizar las acciones según el rol asumido.

## ARN de IAM

Donde:

* *Partition –* identifica la partición del recurso. Para las regiones estándar de aws, la partición es *aws*. Si se tienen recursos en otras particiones, la partición es *aws-partitionname.* Por ej, la partición de la región de china pekin es *aws-cn.* No se puede delegar el acceso entre cuentas en particiones diferentes
* *Service –* identifica el producto de aws. Los recursos de IAM siempre utilizan *iam.*
* *Región –* identifica la región del recurso. En el caso de IAM se deja siempre en blanco (recurso global).
* *Account –* especifica el ID de la cuenta de AWS sin guiones, o el alias de la cuenta.
* *Resource –* identifica el recurso especifico por su nombre (usuario, grupo, rol, política, etc)

