Aspectos fundamentales de IAM

AWS Identity and Access Management (IAM)

- Comparte y controla de forma segura el acceso individual y grupal a sus recursos de AWS
- Se integra con muchos otros servicios de AWS
- Admite la administración de identidad federada
- Admite los permisos granulares
- Admite la autenticación multifactor (MFA)
- Proporciona información de identidad para brindar seguridad

IAM es un servicio web que ayuda a controlar de forma segura el acceso a los recursos de AWS. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) a fin de utilizar los recursos.

IAM se encuentra integrado en la mayoría de los servicios de AWS. Puede definir los controles de acceso desde un lugar en la consola de administración de AWS y surtirán efecto en todo su entorno de AWS.
Puede utilizar IAM para conceder a los usuarios, grupos y aplicaciones acceso granular a la consola y a las interfaces de programación de aplicaciones (API) de servicios de AWS mediante el uso de sistemas de identidad existentes. AWS admite la federación de sistemas corporativos como Microsoft Active Directory y proveedores de identidad basados en estándares. Esta capacidad es beneficiosa cuando se trata de integrar implementaciones en la nube nuevas con la infraestructura en las instalaciones existentes.

AWS IAM

IAM también admite la autenticación multifactor (MFA). Si MFA se encuentra activado y un usuario de IAM intenta iniciar sesión, se le solicita al usuario un código de autenticación. El código de autenticación se envía a un dispositivo de hardware de AWS MFA especialmente configurado o a un dispositivo de AWS MFA basado en software, como la aplicación Authenticator de Google.Mediante el uso de AWS CloudTrail, IAM también puede respaldar la seguridad de la información al proporcionar registros que incluyen la información de identidad de los usuarios que solicitan recursos en su cuenta.

Para más información, consulte ¿What Is IAM ? **(¿Qué es IAM?)** en la Guía del usuario de AWS Identity and Access Management

Para más información, consulte AWS Services that Work with IAM **(Servicios de AWS que funcionan con IAM)** en la Guía del usuario de AWS Identity and Access Management.

Lo que ofrece IAM

- Autenticación
- ¿**Quién** solicita acceso a la cuenta de AWS y los recursos que contiene?
  - Es importante establecer la identidad del solicitante con las credenciales.
  - El solicitante puede ser una *persona* o una *aplicación*; IAM los llama *entidades principales*.
- Autorización
  - Después de autenticar al solicitante, ¿**qué** deberían poder hacer?
  - IAM verifica las políticas que son relevantes para la solicitud con el fin de determinar si se debe permitir o rechazar la solicitud.

Con la autenticación de IAM , se puede utilizar la identidad de los solicitantes para controlar quién puede utilizar sus recursos de AWS. Con la autorización de IAM, también puede utilizar la administración de acceso para controlar qué recursos se pueden utilizar y de qué manera.

Para comprender los aspectos fundamentales de la autenticación y la autorización, considere una analogía bancaria. Piense en un banco que permita a sus clientes (usuarios) acceder a sus cuentas en línea. Supongamos que es un cliente del banco. Tiene dinero en una cuenta corriente en ese banco y quiere pagar una factura en línea. ¿Cualquier persona debería poder iniciar sesión en su cuenta bancaria y pagar sus facturas con el dinero de su cuenta? No, ninguna persona debería poder utilizar el dinero en su cuenta.

Antes de que el banco le permita acceder a su cuenta corriente, este debe asegurarse de que la persona que accede sea usted. El banco quiere autenticar que usted es quien dice ser. Por lo general, esta autenticación se logra al solicitarle que ingrese su nombre de usuario y una contraseña que supuestamente solo usted conoce.
Para mayor seguridad, es posible que haya configurado la autenticación de dos factores. Por lo tanto, además de escribir una contraseña, también debe recibir un código en su teléfono e ingresar ese código.

Ahora, suponga que ha iniciado sesión de forma correcta en el sitio web del banco (se ha autenticado). ¿Puede pagar su factura con el dinero en la cuenta de otrocliente ? No, no debería poder utilizar el dinero de otro cliente para pagar su factura. No tiene autorización para acceder a cuentas que no le pertenecen. Sin embargo,se encuentra autorizado a acceder al dinero de su cuenta y a pagar facturas con su dinero.¿Cómo se relaciona esta analogía con IAM? De manera similar a cómo un banco debe asegurar el acceso a los recursos (su dinero), usted, como propietario de una cuenta de AWS, debe asegurar el acceso a su cuenta de AWS.

Desea que todos los datos que almacena en su cuenta se encuentren seguros para que otros no puedan acceder a ellos. Del mismo modo, desea proteger la lógica de la aplicación de cualquier cosa que cree en AWS, para que otros no puedan modificarla.

IAM proporciona muchas funciones que pueden ayudarte a lograr estos objetivos de seguridad.

Información general sobre IAM

Usuario	Grupo	Rol	Política de IAM
Una persona o aplicación que puede autenticarse con una cuenta de AWS	Una colección de usuarios de IAM a los que se les concede una autorización idéntica	Una identidad que se utiliza para conceder un conjunto temporal de permisos con el fin de realizar solicitudes de servicio de AWS	El documento que define a qué recursos se puede acceder y el nivel de acceso a cada uno de estos

Puede utilizar IAM para controlar el acceso a sus recursos de AWS. Este control de acceso se logra al crear usuarios, grupos y roles. También puede aplicar el control de acceso al adjuntar políticas.

En el caso de IAM, estos términos se definen de la siguiente manera:

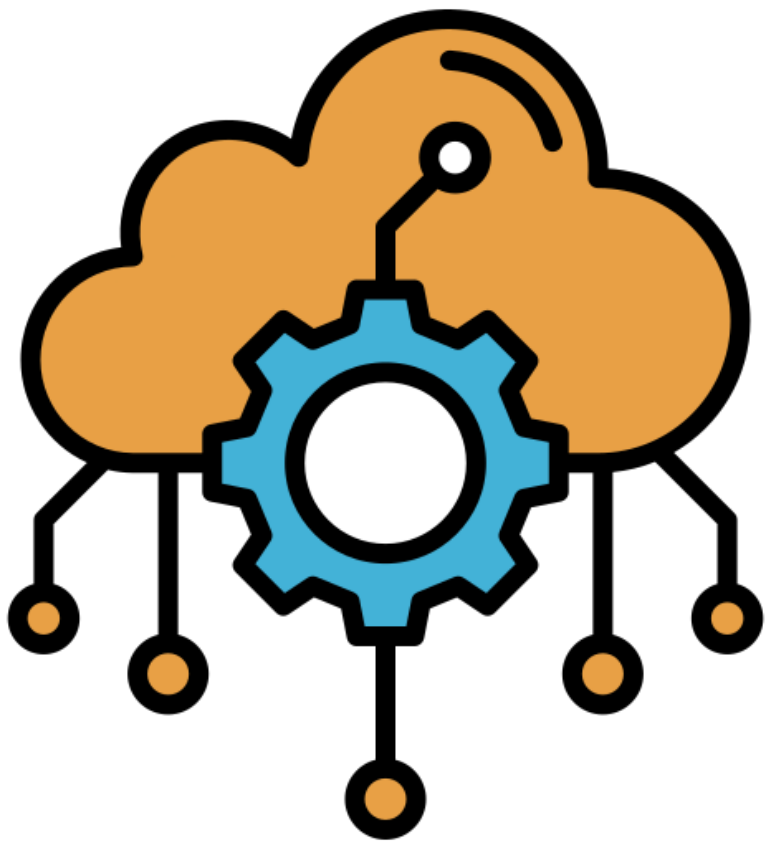
- Un usuario de IAM es una entidad que crea en AWS para representar a una persona o aplicación que interactúa con los servicios y recursos de la cuenta de AWS. Un usuario recibe un conjunto permanente de credenciales, que permanecen con el usuario hasta que se produce una rotación forzada. Con cuentas de AWS nuevas, la cuenta de usuario raíz es la primera cuenta de usuario de IAM que se establece.

- Un grupo de IAM es un conjunto de usuarios de IAM. Puede utilizar grupos para conceder el mismo conjunto de permisos a varios usuarios.

- Un rol de IAM es similar a un usuario en cuanto a que es una identidad de AWS a la que puede adjuntar políticas de permisos. Estos determinarán lo que la identidad puede y no puede hacer en AWS.
- Sin embargo, un rol no tiene credenciales a largo plazo (como una contraseña o claves de acceso) asociadas. En cambio, cuando una persona o una aplicación asume un rol, se le proporcionan credenciales de seguridad temporales para la sesión del rol. Los roles de IAM se tratarán más adelante en este módulo.

- Una política de IAM es un documento en el que se enumeran los permisos de forma explícita. La política se puede adjuntar a un usuario de IAM , un grupo de IAM, un rol de IAM o cualquier combinación de estos recursos. Las políticas de IAM se analizarán con más profundidad más adelante en este módulo.

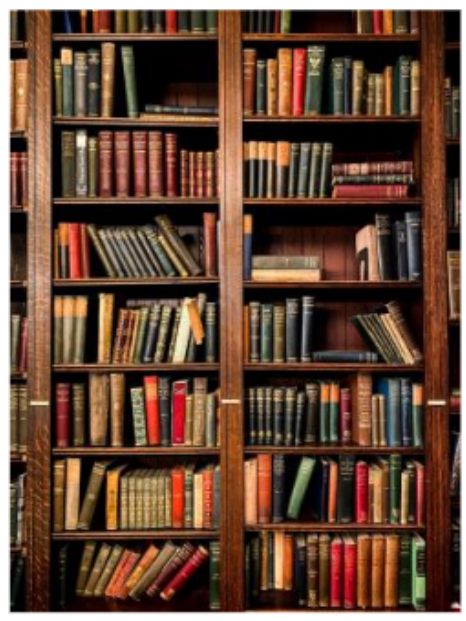
Para configurar el acceso a largo plazo, una práctica recomendada es adjuntar políticas de IAM a grupos de IAM y luego asignar usuarios de IAM a esos grupos de IAM. Un usuario de IAM que es miembro de un grupo de IAM hereda los permisos asociados a ese grupo. También puede adjuntar políticas de IAM directamente a un usuario de IAM para personalizar aún más el acceso que se concede mediante el grupo



Para más información, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de AWS Identity and Access Management

Terminología de IAM

- *Entidad de IAM:* AWS la utiliza para la autenticación (usuarios y roles)
- *Identidad de IAM:* se utiliza para identificar y agrupar
  - Puede adjuntar una política a una identidad de IAM (usuario, grupo o rol).
- *Recurso de IAM:* los objetos del usuario, grupo, rol, política y proveedor de identidad que se almacenan en IAM
  - Puede agregar, editar y eliminar recursos de IAM.
- *Entidad principal:* una persona o aplicación que utiliza el usuario raíz de la cuenta de AWS, el usuario de IAM o el rol de IAM para iniciar sesión y realizar solicitudes a AWS



LOS SIGUIENTES TÉRMINOS SON ESPECÍFICOS DE IAM Y LOS UTILIZARÁ A LO LARGO DE ESTE CURSO

Las entidades de IAM son los objetos de los recursos de IAM que utiliza AWS para la autenticación. Estas incluyen usuarios y roles de IAM. Las entidades de usuario de IAM le permiten iniciar sesión en la consola. Esto puede ser para tareas interactivas y para realizar solicitudes programáticas a los servicios de AWS mediante la API o la AWS Command Line Interface (AWS CLI).

Las identidades de IAM son los objetos de los recursos de IAMque se utilizan para identificar y agrupar. Puede adjuntar una política a una identidad de IAM. Estas incluyen usuarios, grupos y roles.

Los recursos de IAM son los objetos de los usuarios, grupos, roles, políticas y proveedores de identidad que se almacenan en IAM. Al igual que con otros servicios de AWS, puede agregar, editar y eliminar recursos de IAM.

Una entidad principal es una persona o aplicación que utiliza el usuario raíz de la cuenta de AWS, un usuario de IAM o un rol de IAM para iniciar sesión y realizar solicitudes a AWS. Las entidades principales incluyen roles asumidos y usuarios federados, es decir, identidad externa que no tiene una cuenta de AWS. La entidad principal se autentica como el usuario raíz de la cuenta de AWS o una entidad de IAM para realizar solicitudes a AWS.

SOLICITUDES EN IAM

Se realiza una solicitud cada vez que una entidad principal intenta utilizar la consola de administración de AWS, la interfaz de programación de aplicaciones (API) o la AWS Command Line Interface (AWS CLI).

La solicitud contiene la siguiente información:

- Acciones u operaciones: lo que la entidad principal desea realizar
- Recursos: el objeto en el que se realizan las acciones u operaciones
- Entidad principal: la persona o aplicación que envía una solicitud mediante un usuario o rol
- Datos del entorno: la dirección IP, el agente de usuario, el estado habilitado de
- Secure Sockets Layer (SSL) o la hora del día
- Datos del recurso: datos relacionados con el recurso que se solicita

Se realiza una solicitud cada vez que una entidad principal intenta utilizar la consola, la API o la AWS CLI. La solicitud contiene la siguiente información: Las acciones u operaciones son lo que desea realizar la entidad principal. Los recursos son el objeto u objetos sobre los que se realizan las acciones u operaciones.•La entidad principales la persona o aplicación que utiliza un usuario o rol para enviar la solicitud.Los datos del entorno consisten en la dirección IP, el agente de usuario, el estado habilitado de Secure Sockets Layer(SSL) o la hora del día.Los datos de recursos son los datos relacionados con el recurso que se solicita. AWS recopila toda la información sobre la solicitud en un contexto de solicitud, que luego se utiliza para evaluar y autorizar (o prevenir) la solicitud.

Puntos de enlace de servicio

- Si desea conectarse a un servicio de AWS, debe utilizar la URL del punto de entrada para ese servicio, conocido como *punto de enlace*.
- Los kits de desarrollo de software (SDK) de AWS y la AWS CLI utilizan el punto de enlace predeterminado para cada servicio en una región de AWS.
- Puede especificar puntos de enlace alternativos para solicitudes de API en función de los requisitos de configuración.

Si desea conectarse a un servicio de AWS, debe utilizar la URL del punto de entrada para ese servicio, conocido como punto de enlace. Los kits de desarrollo de software (SDK) de AWS y la AWS CLI utilizan el punto de enlace predeterminado para cada servicio en una región de AWS. Un ejemplo de punto de enlace de Amazon Elastic Compute Cloud (Amazon EC2) es ec2.us-east-1.amazonaws.com, que es el punto de enlace de servicio de EE.UU. Este (Norte de Virginia) para Amazon EC2. El uso de puntos de enlace regionales es extremadamente útil cuando se realizan llamadas API directas para servicios de AWS individuales dentro de la misma región.

Puede crear políticas de puntos de enlace y adjuntarlas a los puntos de enlace, pero las políticas de puntos de enlace no anularán ni reemplazarán las políticas de usuario de IAM ni las políticas específicas del servicio. Una política de punto de enlace es una política independiente que sirve para controlar solo el acceso al servicio especificado desde el punto de enlace. Solo puede adjuntar una política de punto de enlace a un punto de enlace, pero puede modificar la política en cualquier momento. Estas políticas son similares a las políticas de IAM pero difieren en que deben contener un elemento principal y el tamaño de la política de punto de enlace no puede exceder los 20480 caracteres

ESTOS SON ALGUNOS APRENDIZAJES CLAVE DE ESTA LECCIÓN DEL MÓDULO 1:

•IAM es un servicio web que ayuda a controlar de forma segura el acceso a los recursos de AWS.

•La autenticación se ocupa de quién solicita el acceso. La autorización determina a qué se tiene acceso.

•IAM utiliza usuarios, grupos, roles y políticas para proporcionar autenticación y autorización a los recursos de AWS.