AWS IDENTITY AND ACCESS MANAGEMENT (IAM)

CONTENIDO

AWS IDENTITY AND ACCESS MANAGEMENT (IAM)

Para explicar el tema de identidades y accesos en AWS, vamos a poner como ejemplo una cafetería.

En esta cafetería cada empleado tiene una identidad. Entran a trabajar por la mañana e inician sesión en el sistema para registrar el horario, usar los registros y administrar los sistemas, lo cual pone en funcionamiento la cafetería, día a día.
Tienen las cajas registradoras y los equipos que ayudan a ejecutar toda la operación. Cada persona tiene acceso único a estos sistemas en función de quiénes son: Si Carlos está en la caja registradora tomando órdenes y Roberto está atrás, comprobando los niveles de inventario en el equipo, tienen dos inicios de sesión diferentes y dos conjuntos diferentes de permisos. Carlos puede manejar la caja registradora, pero si ingresara al sistema de inventario, no se le permitiría hacerlo.

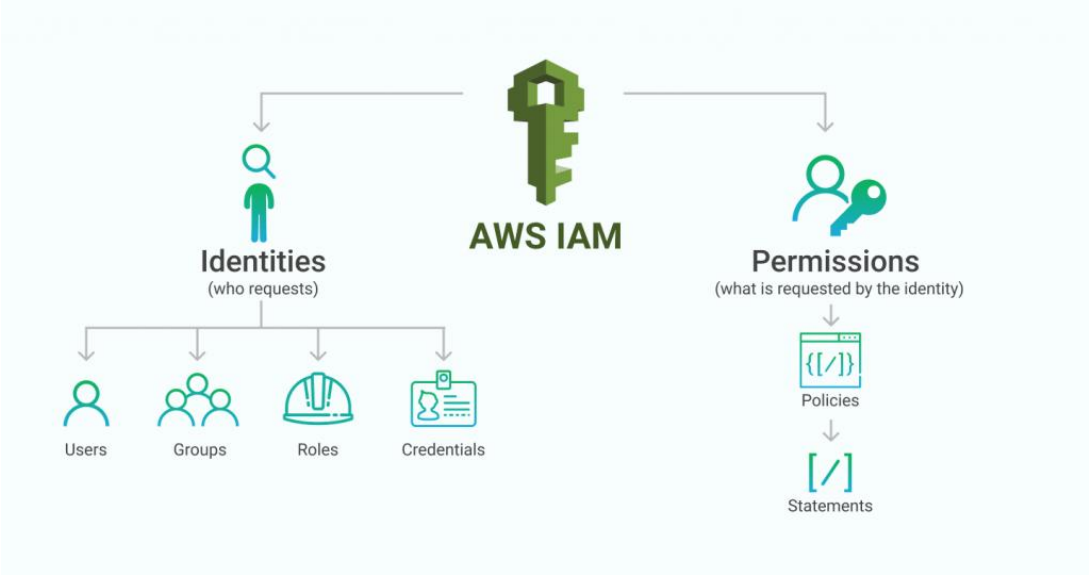
En AWS también se puede definir el alcance de los permisos de los usuarios, de forma similar a la cafetería. Cuando se crea una cuenta en AWS, se nos otorga lo que se llama el usuario de cuenta raíz. Este usuario raíz es el propietario de la cuenta de AWS y tiene permiso para hacer lo que quiera dentro de dicha cuenta. Esto es como ser propietario de la cafetería.
Ahora, supongamos que soy el propietario de la cafetería. Puedo entrar en la tienda, usar mis credenciales para trabajar en la caja registradora, trabajar en el sistema de inventario o cualquier otro sistema en la cafetería. No tengo restricciones.

Con el usuario raíz de AWS, se puede acceder y controlar cualquier recurso en la cuenta. Se puede poner en marcha bases de datos, instancias de EC2, servicios de blockchain o literalmente lo que se desee. Debido a que ese usuario es tan potente, se recomienda que en cuanto se cree una cuenta en AWS y se inicie sesión con el usuario raíz, se active la autenticación multifactor, o MFA (Multifactor Autentication en inglés), para asegurar de que no solo necesita el correo electrónico y la contraseña, sino también un token aleatorio para iniciar sesión.

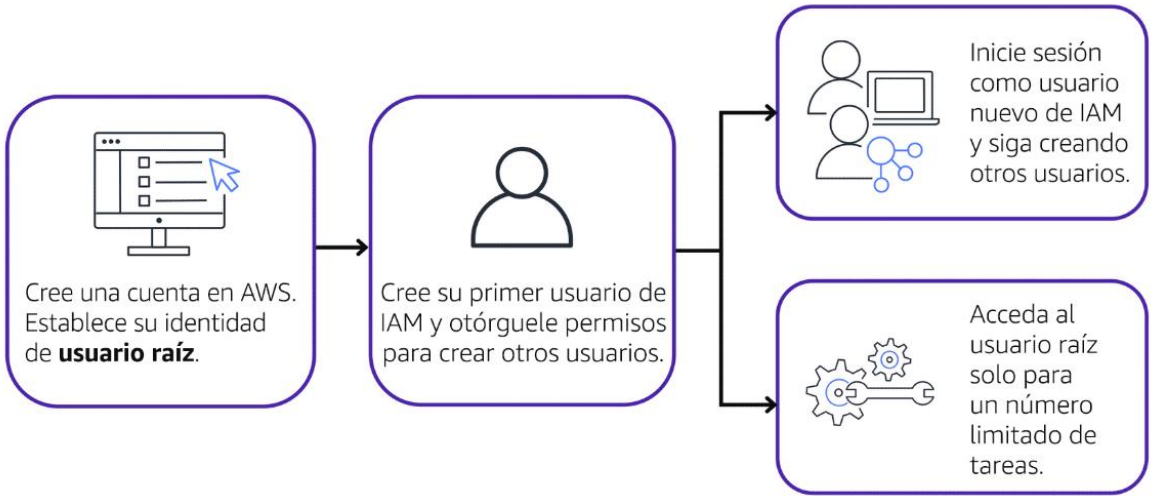
Eso es una buena medida de seguridad, pero incluso con el MFA activado, no se debe usar el usuario raíz para todo. Yo, como propietario de la cafetería, no doy mi nivel de acceso a todos los empleados. Si Carlos está en la caja registradora, no puede acceder al sistema de inventario. Se controla el acceso de forma granular mediante el servicio AWS Identity and Access Management o en ingles IAM.

AWS Identity and Access Management (IAM) permite administrar el acceso a los servicios y recursos de AWS de manera segura.

IAM ofrece la flexibilidad para configurar el acceso en función de las necesidades operativas y de seguridad específicas de su empresa. Para ello, utiliza una combinación de funciones de IAM: Usuarios, grupos y roles de IAM, políticas de IAM y autenticación multifactor.



USUARIO RAIZ (ROOT) DE LA CUENTA DE AWS: Cuando crea una cuenta de AWS por primera vez, comienza con una identidad conocida como el usuario raíz.
Para acceder al usuario raíz, tiene que iniciar sesión con la dirección de correo electrónico y la contraseña que utilizó para crear su cuenta de AWS. Puede considerar al usuario raíz como algo similar al propietario de la cafetería. Tiene acceso completo a todos los servicios y recursos de AWS de la cuenta.



PRÁCTICA RECOMENDADA: No utilice el usuario raíz para las tareas cotidianas, en su lugar, utilice el usuario raíz para crear el primer usuario de IAM y asignarle permisos para crear otros usuarios. A continuación, siga creando otros usuarios IAM y acceda a esas identidades para realizar tareas habituales en AWS.
Utilice el usuario raíz únicamente cuando necesite realizar un número limitado de tareas que solo están disponibles para el usuario raíz. Algunos ejemplos de estas tareas incluyen cambiar la dirección de correo electrónico del usuario raíz y cambiar el plan de soporte de AWS.

USUARIOS DE IAM: Cuando crea un usuario de IAM, de forma predeterminada, no tiene permisos, el usuario ni siquiera puede iniciar sesión en la cuenta de AWS al principio, tiene absolutamente cero permisos. No puede iniciar una instancia de EC2, no puede crear un bucket de S3, nada. Tiene que dar permiso explícitamente al usuario para realizar cualquier tipo de tarea en esa cuenta.

De forma predeterminada, todas las acciones están denegadas, tiene que permitir explícitamente cualquier acción realizada por el usuario. Esto les permite a las personas tener acceso solo a lo que necesitan y nada más. Esta idea se llama *principio de mínimo privilegio*.

PRÁCTICA RECOMENDADA: Se le recomienda que cree usuarios IAM individuales para cada persona que necesite acceder a AWS. Incluso si tiene varios empleados que requieran el mismo nivel de acceso, debe crear usuarios individuales de IAM para cada uno de ellos. Esto proporciona seguridad adicional al permitir que cada usuario de IAM disponga de un conjunto único de credenciales de seguridad.

PRINCIPIO DE MÍNIMO PRIVILEGIO: El principio de mínimo privilegio en AWS IAM (Identity and Access Management) se refiere a la práctica de otorgar a los usuarios y recursos solo los privilegios y permisos necesarios para realizar sus tareas específicas. En otras palabras, se trata de limitar el acceso a lo esencial, equilibrando la facilidad de uso, la eficiencia y la seguridad.

PRÁCTICA RECOMENDADA: Siga el principio de seguridad de mínimo privilegio al momento de conceder permisos. Al seguir ese principio, puede evitar que los usuarios o roles tengan más permisos de los que necesitan para realizar sus tareas.
Por ejemplo, si un empleado necesita acceso a un bucket específico, indique el bucket en la *política de IAM*. Haga esto en lugar de conceder al empleado acceso a todos los buckets de la cuenta de AWS.

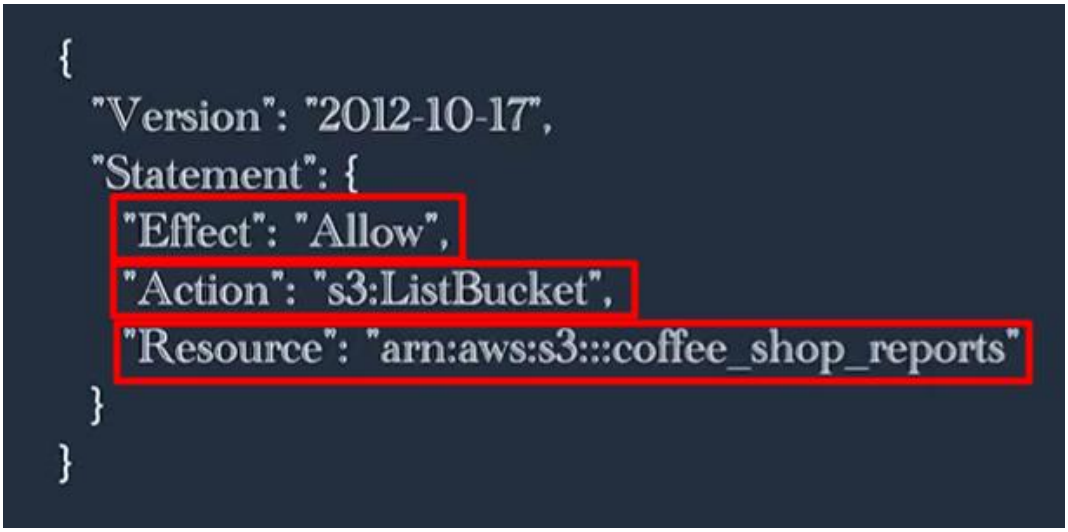
POLÍTICAS DE IAM: Una política de IAM en AWS es un objeto que, cuando se asocia a una identidad o recurso, define sus permisos. Estas políticas determinan si una solicitud realizada por una entidad principal de IAM (usuario o rol) se permite o se deniega.

La forma de conceder o denegar permisos es asociar lo que se denomina una política de IAM a un usuario de IAM. Una política de IAM es un documento que habilita o deniega los permisos a los servicios y recursos de AWS.

Las políticas de IAM le permiten personalizar los niveles de acceso de los usuarios a los recursos. Por ejemplo, puede permitir que los usuarios accedan a todos los buckets de Amazon S3 de la cuenta de AWS o solo a un bucket específico.

Solo hay dos opciones potenciales para el efecto en cualquier política: Ya sea Allow (permitir) o Deny (denegar).
Para la acción, puede enumerar cualquier llamada a la API de AWS y para el recurso, puede enumerar el recurso de AWS para el cual es esa llamada a la API específica.

En este ejemplo puede ver que tenemos un enunciado de permisos que tiene el efecto ***Allow***, permitir. La acción denominada ***s3: ListBucket*** y el recurso es un ID único para un bucket de s3. Así que, si adjunto a esta política a un usuario, ese usuario podría ver el bucket "coffee_shop_reports", pero no realizar ninguna otra acción en esta cuenta.



EJEMPLO POLÍTICA DE IAM: A continuación, se muestra un ejemplo de cómo funcionan las políticas de IAM.

Supongamos que el propietario de la cafetería tiene que crear un usuario de IAM para un cajero recién contratado. El cajero necesita acceder a los recibos guardados en un bucket de Amazon S3 con el ID: AWSDOC-EXAMPLE-BUCKET.

En este ejemplo de política de IAM se concede permiso para acceder a los objetos del bucket de Amazon S3 con el ID: AWSDOC-EJEMPLO-BUCKET:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListObject",
    "Resource": "arn:aws:s3:::
AWSDOC-EXAMPLE-BUCKET"
  }
}
```

En este ejemplo, la política de IAM permite una acción específica dentro de Amazon S3: ListObject. La política también menciona un ID de bucket específico: AWSDOC-EXAMPLE-BUCKET. Cuando el propietario adjunta esta política al usuario de IAM del cajero, le permitirá ver todos los objetos del depósito AWSDOC-EXAMPLE-BUCKET.

Si el propietario quiere que el cajero pueda acceder a otros servicios y realizar otras acciones en AWS, debe adjuntar las políticas adicionales para especificar esos servicios y acciones.

Ahora, supongamos que la cafetería ha contratado a unos cuantos cajeros más. En lugar de asignar permisos a cada usuario de IAM por separado, el propietario ubica los usuarios en un *grupo de IAM*.

TIPOS DE POLÍTICAS: A continuación, hablaremos de los tipos de políticas que están disponibles para nuestro uso en AWS y las veremos en orden desde las que se utilizan con más frecuencia hasta las que se utilizan con menos frecuencia:

- **Políticas basadas en identidad** (Identity-based policies): Las políticas basadas en identidad son documentos de políticas de permisos JSON que controlan qué acciones puede realizar una identidad (usuarios, grupos de usuarios y roles), en qué recursos y en qué condiciones. Las políticas basadas en la identidad pueden clasificarse así:

  - ***Políticas administradas***: Políticas independientes basadas en la identidad que puede adjuntar a varios usuarios, grupos y roles en su cuenta de AWS. Existen dos tipos de políticas administradas:

- ***Políticas administradas de AWS:*** Políticas administradas creadas y administradas por AWS.

- ***Políticas administradas por el cliente***: Políticas administradas que crea y administra en su cuenta de AWS. Las políticas administradas por el cliente ofrecen un control más preciso sobre las políticas que las políticas administradas por AWS.

- ***Políticas insertadas***: Políticas que agrega directamente a un único usuario, grupo o rol. Las políticas insertadas mantienen una relación estricta de uno a uno entre una política y una identidad. Se eliminan cuando se elimina la identidad.

- **Políticas basadas en recursos:** Las políticas basadas en recursos son documentos de política JSON que puede asociar a un recurso como, por ejemplo, un bucket de Amazon S3. Estas políticas conceden a la entidad principal especificada permiso para ejecutar acciones concretas en el recurso y definen en qué condiciones son aplicables. Las políticas basadas en recursos son políticas insertadas. No existen políticas basadas en recursos que sean administradas.

  Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en cuentas de cuentas de AWS distintas, también debe utilizar una política basada en identidades para conceder a la entidad principal el acceso al recurso. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional.

  El servicio de IAM solo admite un tipo de política basada en recursos, el llamado política de confianza de rol, que se asocia a un rol de IAM. Un rol de IAM es tanto una identidad como un recurso que admite políticas basadas en recursos. Por este motivo, debe asociar una política de confianza y una política basada en identidades al rol de IAM. Las políticas de confianza definen qué entidades principales (cuentas, usuarios, roles y usuarios federados) puede asumir el rol.

- **Límites de permisos de IAM:** Un límite de permisos es una característica avanzada que le permite definir los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Al establecer un límite de permisos para una entidad, esta solo puede realizar las acciones que le permitan tanto sus políticas basadas en identidad como sus límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol como entidad principal no estarán

restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso.

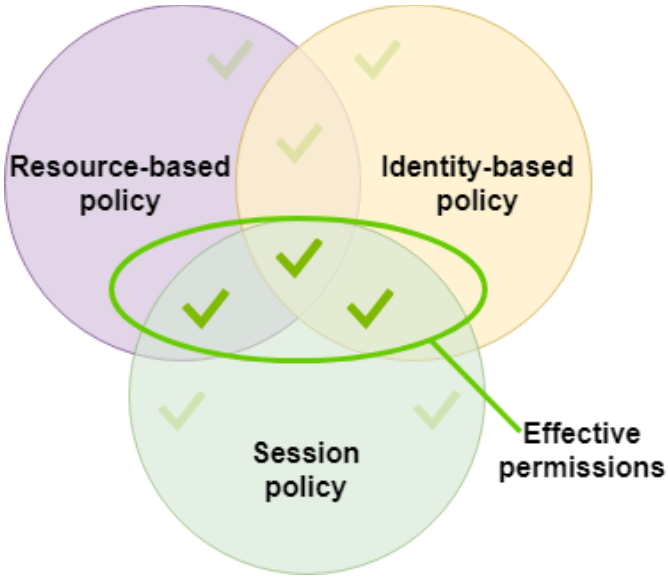
- **Políticas de control de servicios (SCP):** AWS Organizations es un servicio que le permite agrupar y administrar de forma centralizada las cuentas de Cuentas de AWS que posee su negocio. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. Las SCP son políticas JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada usuario raíz de la cuenta de AWS. Una denegación explícita en cualquiera de estas políticas anulará el permiso.

- **Listas de control de acceso (ACL):** Las listas de control de acceso (ACL) son políticas de servicio que le permiten controlar qué entidades principales de otra cuenta pueden obtener acceso a un recurso. Las ACL no se pueden utilizar para controlar el acceso de una entidad principal de la misma cuenta. Las ACL son similares a las políticas basadas en recursos, aunque son el único tipo de política que no utiliza el formato de documento de política JSON. Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL.

- **Políticas de sesión:** Las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de una sesión son la intersección de las políticas basadas en identidades aplicadas a la entidad de IAM (usuario o rol) utilizada para crear la sesión y las políticas de sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso.

  Puede crear una sesión de rol y pasar políticas de sesión mediante programación con las operaciones de API AssumeRole, AssumeRoleWithSAML o AssumeRoleWithWebIdentity. Puede transferir un único documento de política de sesión insertada JSON utilizando el parámetro Policy. Puede utilizar el parámetro PolicyArns para especificar hasta 10 políticas de sesión administrada.

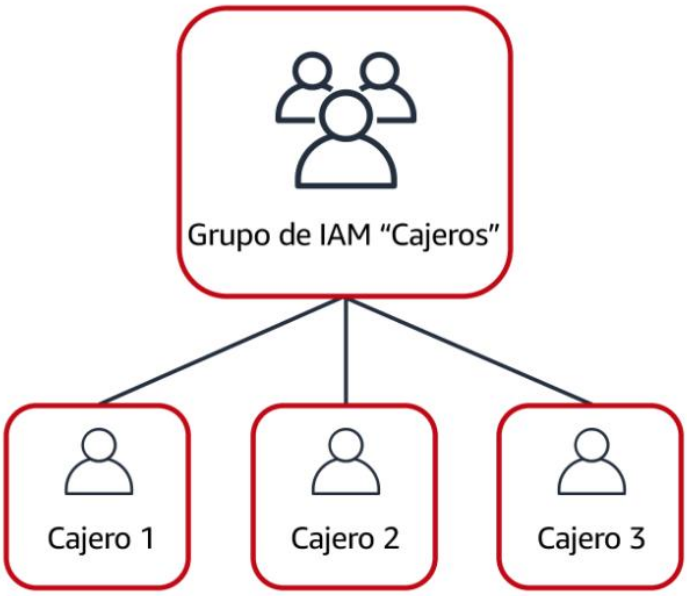
  Al crear una sesión de un usuario federado, se usan las claves de acceso del usuario de IAM para llamar de manera programática a la operación de API GetFederationToken. Asimismo, debe transferir las políticas de sesión. Los permisos de la sesión resultantes son la intersección de la política basada en identidades y la política de sesión.



GRUPOS DE IAM: Un grupo de IAM es un conjunto de usuarios de IAM. Cuando asigna una política de IAM a un grupo, a todos los usuarios del grupo se les conceden los permisos especificados por la política. Estos grupos permiten especificar permisos para varios usuarios, lo que facilita la administración de sus permisos. Por ejemplo, podrías crear un grupo llamado “Admin” y asignarle los permisos típicos que los administradores necesitan. Cualquier usuario en ese grupo automáticamente hereda los permisos del grupo “Admin”. Si un nuevo usuario se une a tu organización y necesita privilegios de administrador, simplemente lo agregas al grupo “Admin”. Además, puedes asociar políticas basadas en identidad a un grupo de usuarios para que todos los miembros reciban los permisos definidos en la política. Es una forma eficiente de gestionar el acceso en AWS.

Una forma de facilitar la administración de los usuarios y sus permisos es organizarlos en grupos de IAM. Los grupos son agrupaciones de usuarios y puede adjuntar una política a un grupo y a todos los usuarios de ese grupo, pues tendrán esos permisos. Si tiene un grupo de cajeros en la cafetería, en lugar de otorgarles acceso de forma individual a todos a la caja registradora, puede conceder acceso a todos los cajeros y luego simplemente agregar cada cajero individual al grupo. La misma idea con los grupos de IAM.

Este es un ejemplo de cómo podría funcionar esto en la cafetería: En lugar de asignar permisos a los cajeros de uno en uno, el propietario puede crear el grupo de IAM “Cajeros”. El propietario puede agregar usuarios de IAM al grupo y luego adjuntar permisos a nivel de grupo.



La asignación de políticas de IAM a nivel de grupo también facilita el ajuste de permisos cuando un empleado se transfiere a un puesto diferente. Por ejemplo, si un cajero se convierte en especialista en inventario, el propietario de la cafetería lo elimina del grupo de IAM “Cajeros” y lo añade al grupo de IAM “Especialistas en inventario”. Esto garantiza que los empleados solo tengan los permisos necesarios para su puesto actual.

Muy bien, hasta el momento con IAM tenemos: El usuario raíz, ellos pueden hacer cualquier cosa. Usuarios que se pueden organizar en grupos y también políticas que son documentos que describen los permisos que luego se pueden adjuntar a usuarios o grupos.

Ahora, ¿qué pasa si un empleado de una cafetería no ha cambiado de trabajo permanentemente, sino que rota a diferentes estaciones de trabajo a lo largo del día? Ese empleado puede obtener el acceso que necesita mediante los *roles de IAM*.

ROLES DE IAM: Un rol IAM en AWS es una entidad que define un conjunto de permisos para realizar solicitudes de servicios de AWS. A diferencia de los usuarios o grupos de IAM, los roles no están asociados con una persona específica, sino con quien necesite usar el rol.

Los roles de IAM son una parte esencial de la gestión de acceso y permisos en un entorno de AWS. Ofrecen una forma segura y eficiente de delegar permisos y acceso a los recursos de AWS sin tener que compartir credenciales a largo plazo. Utilice roles para conceder acceso temporal a los recursos de AWS, a usuarios, identidades externas, aplicaciones e incluso a otros servicios que normalmente no tendrían acceso a los recursos de AWS.

Además, los roles proporcionan credenciales de seguridad temporales para la sesión de rol, en lugar de credenciales a largo plazo como contraseñas o claves de acceso.

En la cafetería, un empleado rota a diferentes estaciones de trabajo a lo largo del día. Dependiendo del personal de la cafetería, este empleado puede realizar varias tareas: Trabajar en la caja registradora, actualizar el sistema de inventario, procesar pedidos en línea, etc. Cuando el empleado tiene que cambiar de tarea, pierde el acceso a una estación de trabajo y obtiene acceso a la siguiente. El empleado puede cambiar fácilmente de estación de trabajo, pero en cualquier momento dado, solo puede tener acceso a una única estación de trabajo. Este mismo concepto existe en AWS con roles de IAM.

Un rol de IAM es una identidad que puede asumir para obtener acceso temporal a los permisos. Para que una aplicación, un servicio o usuario de IAM pueda asumir un rol de IAM, se le deben conceder los permisos para cambiar a ese rol. Cuando alguien asume un rol de IAM, abandona todos los permisos anteriores que tenía en un rol anterior y asume los permisos del nuevo rol.

PRÁCTICA RECOMENDADA: Los roles de IAM son ideales para situaciones en las que el acceso a servicios o recursos debe concederse temporalmente, en lugar de a largo plazo.

Para entender la idea de los roles, pensemos en la cafetería. Como sabemos, Roberto trabaja en la tienda y dependiendo del personal de la tienda día a día, podría trabajar en la caja registradora o en el sistema de inventario, o podría ser quien limpie al final del día sin acceso a ningún sistema.

Yo, como propietario, tengo la autoridad para asignar estos roles diferentes a Roberto. Sus responsabilidades y el acceso son variables y cambian día a día. Solo porque trabajó en el seguimiento de inventario en el sistema ayer, no significa que deba estar en cualquier momento. Su rol en el trabajo cambia y es de naturaleza temporal. El mismo tipo de idea existe en AWS.

Puede crear identidades en AWS que se denominan roles. Los roles tienen permisos asociados que permiten o deniegan acciones específicas. Y estos roles pueden asumirse por una cantidad de tiempo determinado. Es similar a un usuario, pero no tiene nombre de usuario ni contraseña. En cambio, es una identidad que puede asumir para obtener acceso a permisos temporales.

Vamos analizar un ejemplo de cómo se puede utilizar un rol de IAM en el ejemplo de la cafetería:

1

Primero, el dueño de la cafetería le otorga acceso al empleado a los roles de “Caja” y de “Inventario” para que pueda cambiar entre estas dos estaciones de trabajo.

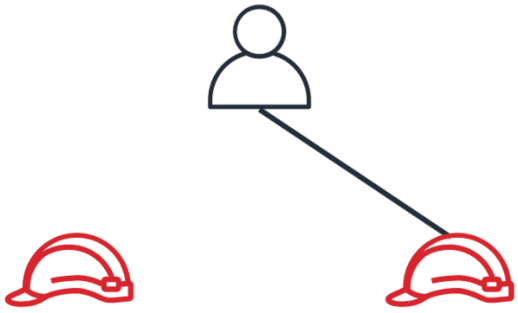
El empleado comienza su día asumiendo el rol de “Cajero”. Esto le da acceso al sistema de la caja registradora.

2

Rol de “cajero”

3

Más tarde en el día, el empleado necesita actualizar el sistema de inventario. Asume el rol de “Inventario”. De esa manera, se concede al empleado acceso al sistema del inventario y se le revoca el acceso al sistema de la caja registradora.



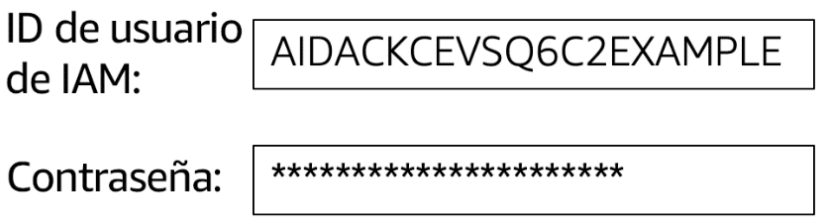
Rol de “cajero” Rol de “inventario”

Los roles de IAM son una herramienta flexible y poderosa para administrar el acceso a los recursos de AWS de manera segura y eficiente. Puedes crear, administrar y asignar roles según tus necesidades específicas dentro de tu cuenta de AWS.

AUTENTICACIÓN MULTIFACTOR: ¿Alguna vez ha iniciado sesión en un sitio web que requiere que proporcione varios datos para verificar su identidad? Es posible que haya tenido que proporcionar su contraseña y una segunda forma de autenticación, como un código aleatorio enviado a su teléfono. Este es un ejemplo de la autenticación multifactor.

En IAM, la autenticación multifactor (MFA) suministra otra capa de seguridad para su cuenta de AWS. Veamos cómo funciona MFA:

Primero, para iniciar sesión en un sitio web de AWS, el usuario introduce su ID de usuario y contraseña de IAM:



Luego, se solicita al usuario una respuesta de autenticación desde su dispositivo MFA de AWS. Este dispositivo puede ser una clave de seguridad de hardware, un dispositivo de hardware o una aplicación de MFA en un dispositivo como un smartphone:

Cuando el usuario se autenticó de forma correcta, podrá acceder a los servicios o recursos de AWS solicitados:

Puede habilitar la MFA para el usuario raíz y los usuarios de IAM.

PRÁCTICA RECOMENDADA: Habilite la MFA para el usuario raíz y para todos los usuarios de IAM de su cuenta. De este modo, puede mantener su cuenta de AWS a salvo del acceso no autorizado.

BENEFICIOS DE IAM

Establezca permisos de barreras de protección y acceso detallado: Establezca y administre barreras de protección con permisos amplios y avance hacia los privilegios mínimos mediante el uso de controles de acceso detallados para sus cargas de trabajo.

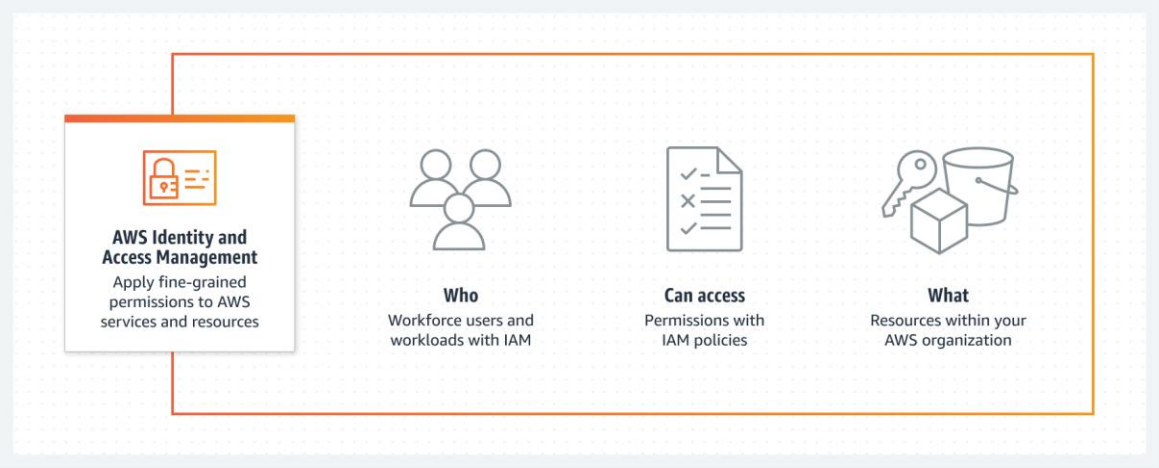
Administre la carga de trabajo y las identidades del personal en todas sus cuentas de AWS: Administre las identidades en una sola cuenta de AWS o conecte de forma centralizada las identidades a varias cuentas de AWS.

Utilice conjuntos de permisos y credenciales de seguridad temporales para acceder a sus recursos de AWS: Otorgue credenciales de seguridad temporales para las cargas de trabajo que accedan a sus recursos de AWS mediante IAM y conceda acceso a su personal con AWS IAM Identity Center.

Analice el acceso y valide las políticas de IAM a medida que avanza hacia el nivel de privilegios mínimos: Genere políticas de privilegios mínimos, verifique el acceso externo y no utilizado a los recursos y analice continuamente los permisos para dimensionarlos correctamente.

FUNCIONAMIENTO

Con AWS Identity and Access Management (IAM), puede especificar quién o qué puede acceder a los servicios y recursos en AWS, administrar de forma centralizada los permisos específicos y analizar el acceso para perfeccionar los permisos en todo AWS.



CASOS DE USO

Aplicar permisos específicos y escalar con el control de acceso basado en atributos: Cree permisos detallados en función de los atributos del usuario, como el departamento, el cargo y el nombre del equipo, mediante el control de acceso basado en atributos.

Administrar el acceso por cuenta o escalar el acceso en todas las cuentas y aplicaciones de AWS: Administre identidades por cuenta con IAM o utilice el centro de identidades de AWS IAM para proporcionar acceso a varias cuentas y asignaciones de aplicaciones en todo AWS.

Establecer barreras de protección preventivas y para toda la organización en AWS: Utilice las políticas de control de servicios a fin de establecer barreras de protección de permisos para los roles y usuarios de IAM e implemente un perímetro de datos alrededor de sus cuentas en AWS Organizations.

Establecer, verificar y adaptar los permisos hasta llegar al privilegio mínimo: Agilice la administración de permisos y utilice los resultados de las cuentas cruzadas mientras establece, verifica y perfecciona las políticas en su recorrido hacia el privilegio mínimo.

CONCLUSIONES

- Los usuarios de IAM representan a personas o aplicaciones específicas, tienen credenciales de inicio de sesión (como contraseñas o claves de acceso), se les asignan permisos específicos para acceder a recursos de AWS y se recomienda usar credenciales temporales siempre que sea posible.

- Los grupos de usuarios de IAM son colecciones de usuarios de IAM administrados como una unidad, facilitan la gestión y el seguimiento de permisos de seguridad. Los usuarios se agregan a grupos y heredan los permisos del grupo.

- Los roles de IAM no están asociados a usuarios específicos, se utilizan para asignar permisos a entidades que no son usuarios o grupos, como servicios de AWS o aplicaciones externas y son esenciales para otorgar acceso temporal y seguro a recursos específicos sin compartir credenciales.

- Los usuarios son para acceso externo, los grupos simplifican la administración y los roles son útiles para acceso temporal y seguro.

- Una política de IAM es un documento JSON que describe qué llamadas a la API puede o no puede realizar un usuario.

- AWS Identity and Access Management (IAM) es una característica de la cuenta de AWS que está disponible sin costo adicional y permite administrar el acceso a los servicios y recursos de AWS de manera segura.

- IAM brinda un control preciso sobre quién puede acceder a los recursos en AWS y cómo lo hacen, lo que contribuye a la seguridad y eficiencia de la infraestructura en la nube.