**User Permission and Access**

**AWS Identity and Access Management (IAM)**

[**AWS Identity and Access Management (IAM)**](https://aws.amazon.com/iam/) enables you to manage access to AWS services and resources securely.

IAM gives you the flexibility to configure access based on your company’s specific operational and security needs. You do this by using a combination of IAM features, which are explored in detail in this lesson:

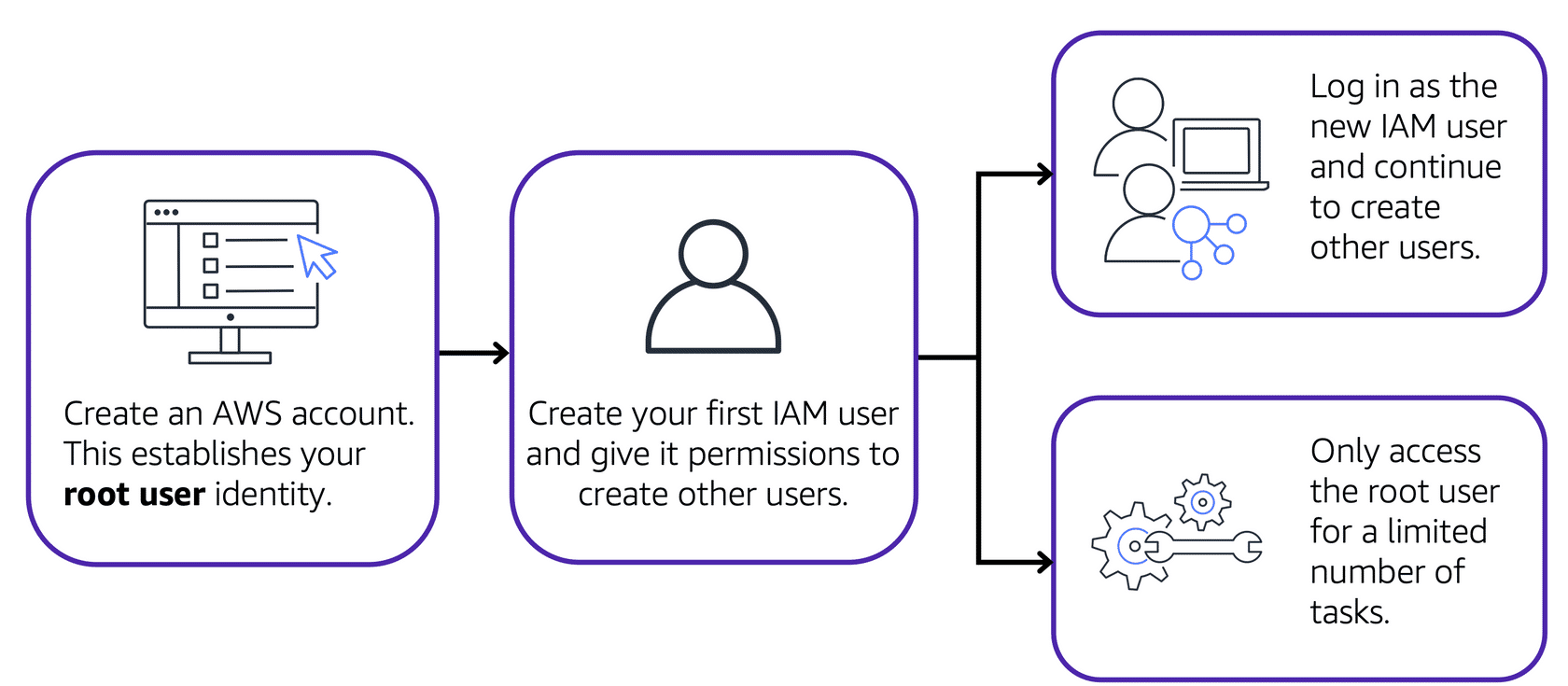
* IAM users, groups, and roles
* IAM policies
* Multi-factor authentication

You will also learn best practices for each of these features.

**AWS Account Root User**

When you first create an AWS account, you begin with an identity known as the [**root user**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html).

The root user is accessed by signing in with the email address and password that you used to create your AWS account. You can think of the root user as being similar to the owner of the coffee shop. It has complete access to all the AWS services and resources in the account.



**Best practice:**

Do **not** use the root user for everyday tasks.

Instead, use the root user to create your first IAM user and assign it permissions to create other users.

Then, continue to create other IAM users, and access those identities for performing regular tasks throughout AWS. Only use the root user when you need to perform a limited number of tasks that are only available to the root user. Examples of these tasks include changing your root user email address and changing your AWS support plan.

**IAM users**

An **IAM user** is an identity that you create in AWS. It represents the person or application that interacts with AWS services and resources. It consists of a name and credentials.

By default, when you create a new IAM user in AWS, it has no permissions associated with it. To allow the IAM user to perform specific actions in AWS, such as launching an Amazon EC2 instance or creating an Amazon S3 bucket, you must grant the IAM user the necessary permissions.

**Best practice:**

We recommend that you create individual IAM users for each person who needs to access AWS.

Even if you have multiple employees who require the same level of access, you should create individual IAM users for each of them. This provides additional security by allowing each IAM user to have a unique set of security credentials.

**IAM policies**

An **IAM policy** is a document that allows or denies permissions to AWS services and resources.

IAM policies enable you to customize users’ levels of access to resources. For example, you can allow users to access all of the Amazon S3 buckets within your AWS account, or only a specific bucket.

**Best practice:**

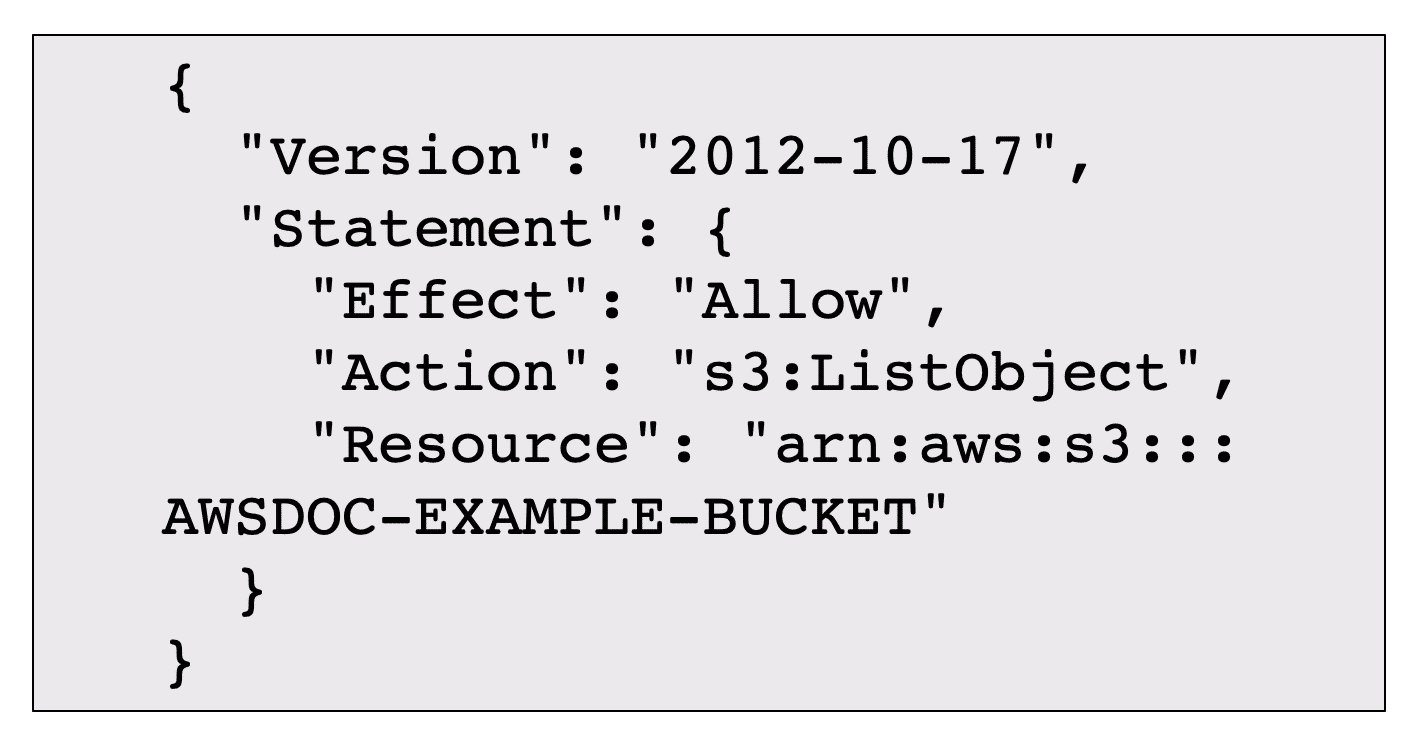
Follow the security principle of **least privilege** when granting permissions.

By following this principle, you help to prevent users or roles from having more permissions than needed to perform their tasks.

For example, if an employee needs access to only a specific bucket, specify the bucket in the IAM policy. Do this instead of granting the employee access to all of the buckets in your AWS account.

**Example: IAM policy**

Here’s an example of how IAM policies work. Suppose that the coffee shop owner has to create an IAM user for a newly hired cashier. The cashier needs access to the receipts kept in an Amazon S3 bucket with the ID: AWSDOC-EXAMPLE-BUCKET.



In this example, the IAM policy is allowing a specific action within Amazon S3: ListObject. The policy also mentions a specific bucket ID: AWSDOC-EXAMPLE-BUCKET. When the owner attaches this policy to the cashier’s IAM user, it will allow the cashier to view all of the objects in the AWSDOC-EXAMPLE-BUCKET bucket.

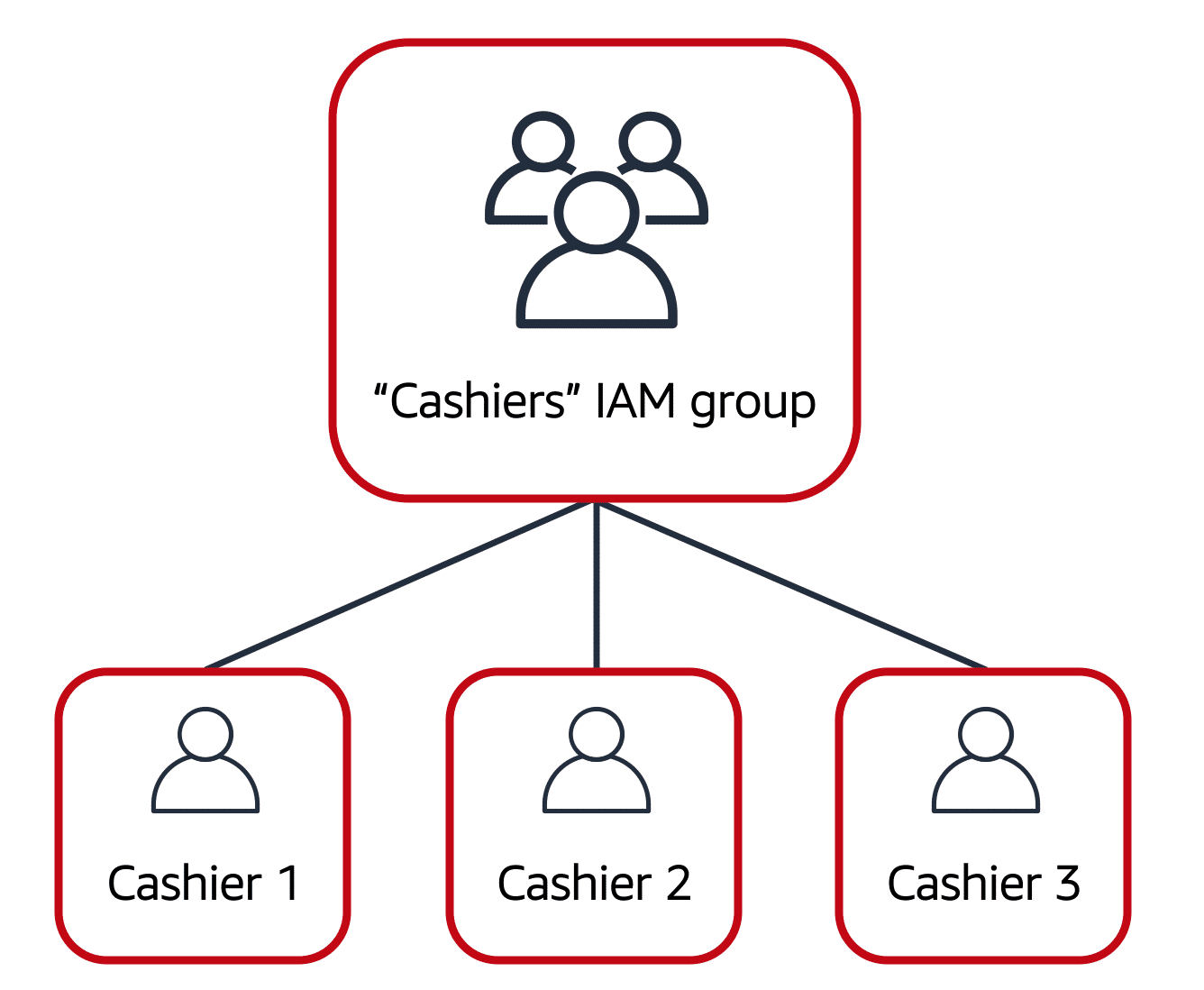
If the owner wants the cashier to be able to access other services and perform other actions in AWS, the owner must attach additional policies to specify these services and actions.

Now, suppose that the coffee shop has hired a few more cashiers. Instead of assigning permissions to each individual IAM user, the owner places the users into an [**IAM group**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html).

**IAM Groups**

An IAM group is a collection of IAM users. When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.

Here’s an example of how this might work in the coffee shop. Instead of assigning permissions to cashiers one at a time, the owner can create a “Cashiers” IAM group. The owner can then add IAM users to the group and then attach permissions at the group level.



Assigning IAM policies at the group level also makes it easier to adjust permissions when an employee transfers to a different job. For example, if a cashier becomes an inventory specialist, the coffee shop owner removes them from the “Cashiers” IAM group and adds them into the “Inventory Specialists” IAM group. This ensures that employees have only the permissions that are required for their current role.

What if a coffee shop employee hasn’t switched jobs permanently, but instead, rotates to different workstations throughout the day? This employee can get the access they need through [**IAM roles**](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html).

**IAM Roles**

In the coffee shop, an employee rotates to different workstations throughout the day. Depending on the staffing of the coffee shop, this employee might perform several duties: work at the cash register, update the inventory system, process online orders, and so on.

When the employee needs to switch to a different task, they give up their access to one workstation and gain access to the next workstation. The employee can easily switch between workstations, but at any given point in time, they can have access to only a single workstation. This same concept exists in AWS with IAM roles.

An IAM role is an identity that you can assume to gain temporary access to permissions.

Before an IAM user, application, or service can assume an IAM role, they must be granted permissions to switch to the role. When someone assumes an IAM role, they abandon all previous permissions that they had under a previous role and assume the permissions of the new role.

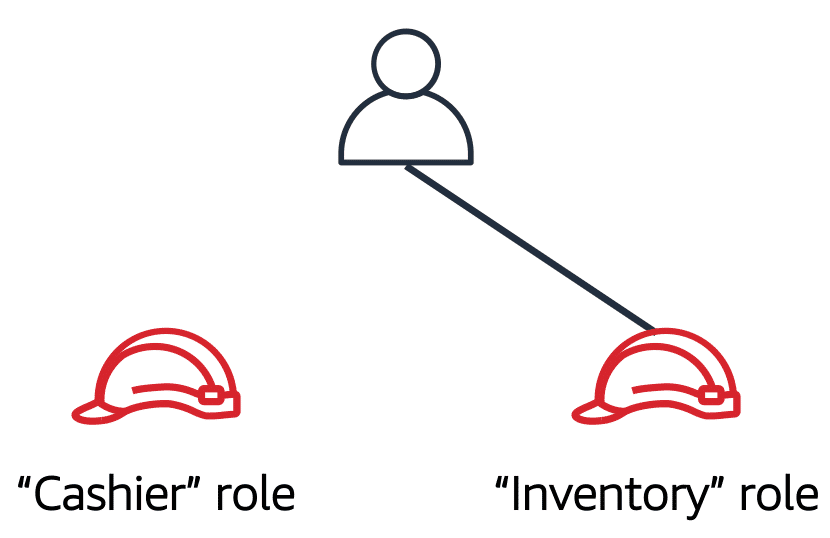
**Best practice:**

IAM roles are ideal for situations in which access to services or resources needs to be granted temporarily, instead of long-term.

**Example: IAM Roles**

Review an example of how IAM roles could be used in the coffee shop:

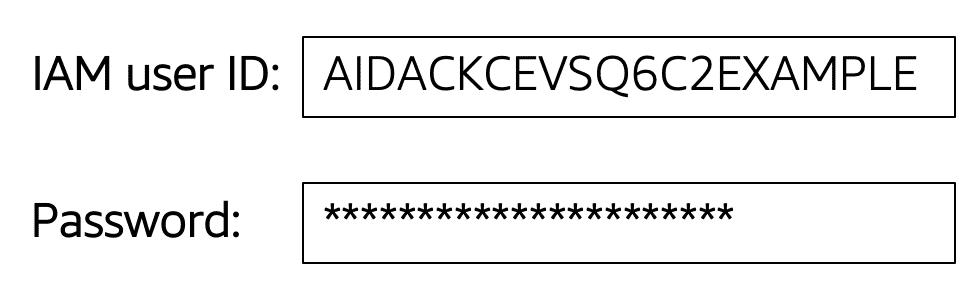
1. First, the owner grants the employee permissions to switch to a role for each workstation in the coffee shop.
2. Next, the employee begins their day by assuming the “Cashier” role. This grants them access to the cash register system.
3. Later in the day, the employee needs to update the inventory system. They assume the “Inventory” role. This grants the employee access to the inventory system and also revokes their access to the cash register system.



**Multi-factor Authentication**

Have you ever signed in to a website that required you to provide multiple pieces of information to verify your identity? You might have needed to provide your password and then a second form of authentication, such as a random code sent to your phone. This is an example of [**multi-factor authentication**](https://aws.amazon.com/iam/features/mfa/).

In IAM, multi-factor authentication (MFA) provides an extra layer of security for your AWS account.



1. First, when a user signs in to an AWS website, they enter their IAM user ID and password.
2. Next, the user is prompted for an authentication response from their AWS MFA device. This device could be a hardware security key, a hardware device, or an MFA application on a device such as a smartphone.
3. When the user has been successfully authenticated, they are able to access the requested AWS services or resources.

You can enable MFA for the root user and IAM users. As a best practice, enable MFA for the root user and all IAM users in your account. By doing this, you can keep your AWS account safe from unauthorized access.

====================== ESPAÑOL ======================

**Permiso y acceso de usuario**

AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM)

le permite administrar el acceso a los servicios y recursos de AWS de manera segura.

IAM le brinda la flexibilidad de configurar el acceso en función de las necesidades operativas y de seguridad específicas de su empresa. Esto se hace mediante una combinación de características de IAM, que se exploran en detalle en esta lección:

Usuarios, grupos y roles de IAM

Políticas de IAM

Autenticación de múltiples factores

También aprenderá las mejores prácticas para cada una de estas características.

Usuario raíz de la cuenta de AWS

Cuando crea por primera vez una cuenta de AWS, comienza con una identidad conocida como el

usuario raíz

.

El usuario raíz se accede iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear su cuenta de AWS. Puede pensar en el usuario raíz como similar al propietario de la cafetería. Tiene acceso completo a todos los servicios y recursos de AWS en la cuenta.

Mejor práctica:

No use el usuario raíz para tareas cotidianas.

En su lugar, utilice el usuario raíz para crear su primer usuario de IAM y asignarle permisos para crear otros usuarios.

Luego, continúe creando otros usuarios de IAM y acceda con esas identidades para realizar tareas regulares en toda AWS. Utilice el usuario raíz solo cuando necesite realizar un número limitado de tareas disponibles solo para el usuario raíz. Ejemplos de estas tareas incluyen cambiar la dirección de correo electrónico del usuario raíz y cambiar su plan de soporte de AWS.

Usuarios de IAM

Un usuario de IAM es una identidad que crea en AWS. Representa a la persona o aplicación que interactúa con los servicios y recursos de AWS. Consta de un nombre y credenciales.

De forma predeterminada, cuando crea un nuevo usuario de IAM en AWS, no tiene permisos asociados. Para permitir que el usuario de IAM realice acciones específicas en AWS, como iniciar una instancia de Amazon EC2 o crear un depósito de Amazon S3, debe otorgarle los permisos necesarios.

Mejor práctica:

Recomendamos que cree usuarios de IAM individuales para cada persona que necesite acceder a AWS.

Incluso si tiene varios empleados que requieren el mismo nivel de acceso, debe crear usuarios de IAM individuales para cada uno de ellos. Esto proporciona seguridad adicional al permitir que cada usuario de IAM tenga un conjunto único de credenciales de seguridad.

Políticas de IAM

Una política de IAM es un documento que permite o deniega permisos a 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 depósitos de Amazon S3 en su cuenta de AWS o solo a un depósito específico.

Mejor práctica:

Siga el principio de seguridad del privilegio mínimo al otorgar permisos.

Al seguir este principio, ayuda a evitar que los usuarios o roles tengan más permisos de los necesarios para realizar sus tareas.

Por ejemplo, si un empleado necesita acceso solo a un depósito específico, especifique el depósito en la política de IAM en lugar de otorgar acceso a todos los depósitos en su cuenta de AWS.

Ejemplo: Política de IAM

Aquí tiene un ejemplo de cómo funcionan las políticas de IAM. Suponga que el propietario de la cafetería debe crear un usuario de IAM para un cajero recién contratado. El cajero necesita acceso a los recibos almacenados en un depósito de Amazon S3 con la ID: AWSDOC-EXAMPLE-BUCKET.

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

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

Ahora, suponga que la cafetería ha contratado a algunos cajeros más. En lugar de asignar permisos a cada usuario de IAM individualmente, el propietario coloca a los usuarios en un

grupo de IAM

.

Grupos de IAM

Un grupo de IAM es una colección de usuarios de IAM. Cuando asigna una política de IAM a un grupo, todos los usuarios del grupo obtienen los permisos especificados en la política.

Aquí tiene un ejemplo de cómo podría funcionar esto en la cafetería. En lugar de asignar permisos a los cajeros uno por uno, el propietario puede crear un grupo de "Cajeros" de IAM. Luego, el propietario puede agregar usuarios de IAM al grupo y adjuntar permisos a nivel de grupo.

Asignar políticas de IAM a nivel de grupo también facilita ajustar los permisos cuando un empleado se traslada a otro trabajo. Por ejemplo, si un cajero se convierte en especialista en inventario, el propietario de la cafetería lo elimina del grupo de "Cajeros" y lo agrega al grupo de "Especialistas en inventario". Esto garantiza que los empleados solo tengan los permisos necesarios para su rol actual.

¿Qué sucede si un empleado de la cafetería no cambia de trabajo permanentemente, sino que rota entre diferentes estaciones de trabajo durante el día? Este empleado puede obtener el acceso que necesita a través de

roles de IAM

.

Roles de IAM

En la cafetería, un empleado rota entre diferentes estaciones de trabajo durante el día. Dependiendo de la dotación de personal de la cafetería, este empleado podría realizar varias tareas: trabajar en la caja registradora, actualizar el sistema de inventario, procesar pedidos en línea, y así sucesivamente.

Cuando el empleado necesita cambiar a una tarea diferente, renuncia a su acceso a una estación de trabajo y obtiene acceso a la siguiente estación de trabajo. El empleado puede cambiar fácilmente entre estaciones de trabajo, pero en un momento dado, solo puede tener acceso a una estación de trabajo. Este mismo concepto existe en AWS con los roles de IAM.

Un rol de IAM es una identidad que puede asumir para obtener acceso temporal a permisos.

Antes de que un usuario de IAM, aplicación o servicio pueda asumir un rol de IAM, se le deben otorgar

permisos para cambiar al rol. Cuando alguien asume un rol de IAM, abandona todos los permisos anteriores que tenía bajo un rol anterior y asume los permisos del nuevo rol.

Mejor práctica:

Los roles de IAM son ideales para situaciones en las que se necesita otorgar acceso a servicios o recursos temporalmente, en lugar de a largo plazo.

Ejemplo: Roles de IAM

Revise un ejemplo de cómo podrían utilizarse roles de IAM en la cafetería:

Primero, el propietario otorga permisos al empleado para cambiar a un rol para cada estación de trabajo en la cafetería.

Luego, el empleado comienza su día asumiendo el rol de "Cajero". Esto le otorga acceso al sistema de caja registradora.

Más tarde en el día, el empleado necesita actualizar el sistema de inventario. Asume el rol de "Inventario". Esto le otorga acceso al sistema de inventario y también revoca su acceso al sistema de caja registradora.

Autenticación de múltiples factores

¿Alguna vez ha iniciado sesión en un sitio web que le ha pedido que proporcione múltiples piezas de información para verificar su identidad? Es posible que haya necesitado proporcionar su contraseña y luego una segunda forma de autenticación, como un código aleatorio enviado a su teléfono. Este es un ejemplo de la

autenticación de múltiples factores

.

En IAM, la autenticación de múltiples factores (MFA) proporciona una capa adicional de seguridad para su cuenta de AWS.

Primero, cuando un usuario inicia sesión en un sitio web de AWS, ingresa su ID de usuario de IAM y su contraseña.

A continuación, se le solicita al usuario una respuesta de autenticación de su dispositivo AWS MFA. Este dispositivo puede ser una clave de seguridad de hardware, un dispositivo de hardware o una aplicación MFA en un dispositivo como un teléfono inteligente.

Cuando el usuario se autentica con éxito, puede acceder a los servicios o recursos de AWS solicitados.

Puede habilitar MFA para el usuario raíz y los usuarios de IAM. Como mejor práctica, habilite MFA para el usuario raíz y todos los usuarios de IAM en su cuenta. Al hacerlo, puede mantener segura su cuenta de AWS contra el acceso no autorizado.