Autenticación y Autorización con IAM

LECCIÓN 3

Presionar el ícono de cada tema para conocer ver su contenido

Roles de IAM características y casos prácticos

Credenciales de IAM para la autenticación

Autenticación multifactor (MFA)

Escenario de autenticación

Principio de mínimo privilegio

Políticas y permisos

Política basadas en recursos y en identidades

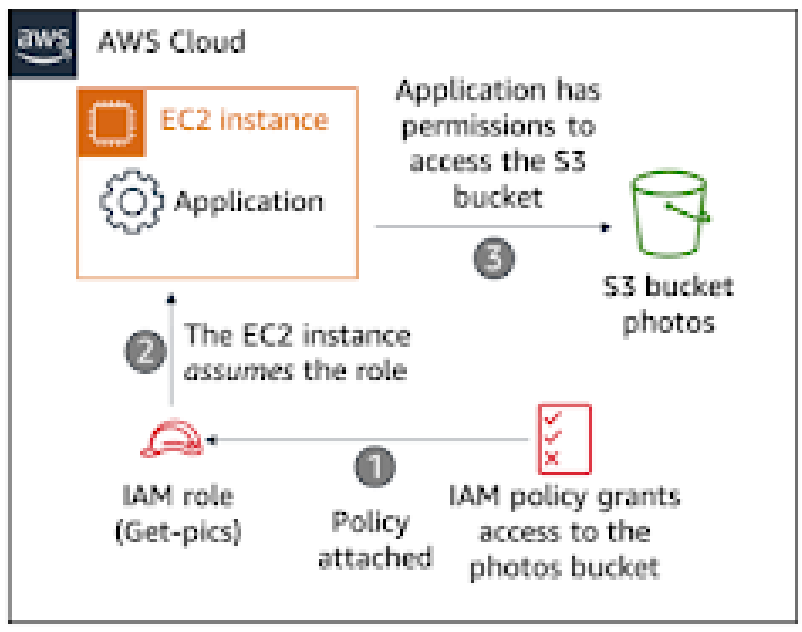
Políticas de IAM administradas e insertadas

Lógica de evaluación para políticas de IAM

Roles de IAM

características y casos prácticos

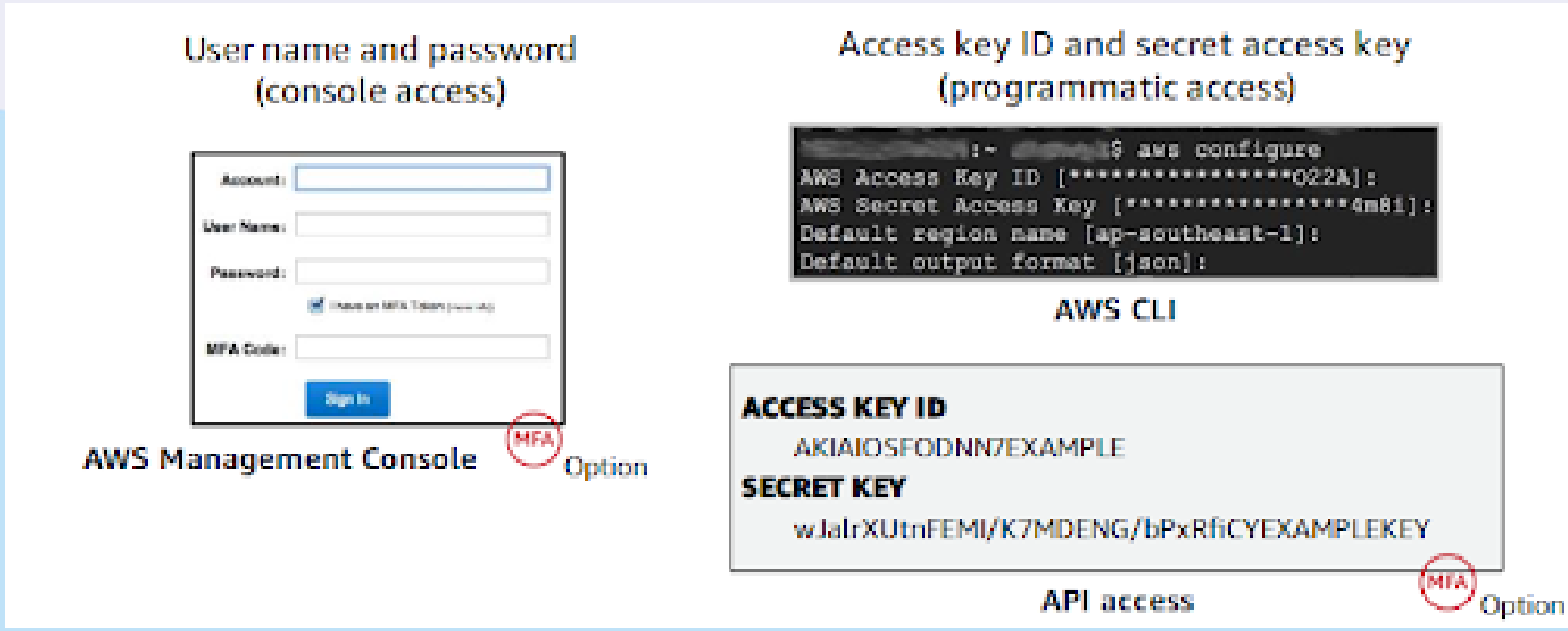
- Características del rol de IAM
  - Proporciona credenciales de seguridad *temporales*.
  - Un rol **no** se encuentra asociado únicamente con una persona.
  - Una *persona*, *aplicación* o *servicio de AWS* puede asumir un rol.
  - A menudo se utiliza un rol para delegar el acceso.
  - AWS Security Token Service (AWS STS) emite credenciales de seguridad temporales.
- Casos prácticos comunes
  - Aplicaciones que se ejecutan en Amazon Elastic Compute Cloud (Amazon EC2)
  - Acceso entre cuentas para un usuario de IAM
  - Aplicaciones móviles



Un rol de IAM es una identidad de IAM que proporciona la capacidad de definir un conjunto específico de permisos para acceder a los recursos que necesita un usuario o servicio. Un rol de IAM es similar a un usuario de IAM en cuanto a que puede adjuntarle políticas de permisos. Sin embargo, no adjunta los permisos a un usuario o grupo de IAM. En su lugar, los adjunta a un rol y el usuario o el servicio asume el rol según sea necesario.Cuando un usuario asume un rol, sus permisos anteriores se olvidan temporalmente. AWS devuelve credenciales de seguridad temporales que el usuario o la aplicación pueden utilizar para realizar solicitudes programáticas a AWS durante la sesión. AWS Security Token Service(AWS STS) emite las credenciales de seguridad temporales.Cuando utiliza roles de IAM, no necesita conceder credenciales de seguridad a largo plazo a cada entidad que requiere acceso a un recurso.En el caso de un servicio como Amazon EC2, las aplicaciones o los servicios de AWS pueden asumir un rol de manera programática en tiempo de ejecución. La entidad principal que asume el rol puede ser un usuario, grupo o rol de IAM de otra cuenta de AWS, incluidas las cuentas que no son de su propiedad. En el siguiente ejemplo se ilustra una situación en la que podría necesitar credenciales de seguridad temporales a fin de proporcionar un rol para una instancia de EC2:1.Un administrador crea el rol Get-pics en IAM, define una política que concede acceso a un bucket de Amazon Simple Storage Service(Amazon S3) denominado fotos y adjunta la política al rol.2.Una instancia de EC2 asume el rol Get-pics.3.A la instancia de EC2 se le conceden permisos temporales para acceder al bucket de S3 denominado fotos.

Página inicial

Credenciales de IAM
para la autenticación



Cuando interactúa con AWS mediante la consola, la AWS CLI o los SDK de AWS, debe proporcionar las credenciales de AWS. Se utilizan dos tipos principales de credenciales para la autenticación. El tipo de credencial que utilice depende de cómo acceda a AWS:

•Para autenticarse desde la consola, debe iniciar sesión con su nombre de usuario y contraseña.

•Para autenticarse de manera programática con la AWS CLI, los SDK y las API, debe proporcionar una clave de acceso de AWS. La clave de acceso de AWS es la combinación de un ID de clave de acceso y una clave de acceso secreta.

El método de autenticación dependerá de la situación. En la mayoría de las circunstancias, un usuario humano utilizará el método de la AWS CLI, mientras que un programa automatizado utilizará el método del SDK o la API.También es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS recomienda que utilice la MFA para aumentar la seguridad de su cuenta.

Para más información, consulte AWS Security Credentials (Credenciales de seguridad de AWS) en la Guía de referencia general de AWS

Página inicial

Autenticación multifactor
(MFA)

Agrega una capa adicional de protección además de su nombre de usuario y contraseña.

- Los usuarios solicitaron un código de autenticación.
- Puede basarse en hardware o en un dispositivo virtual.

Activar MFA para:

- Usuarios de la consola de administración de AWS.
- Usuarios de la API de AWS (requiere credenciales de seguridad temporales)

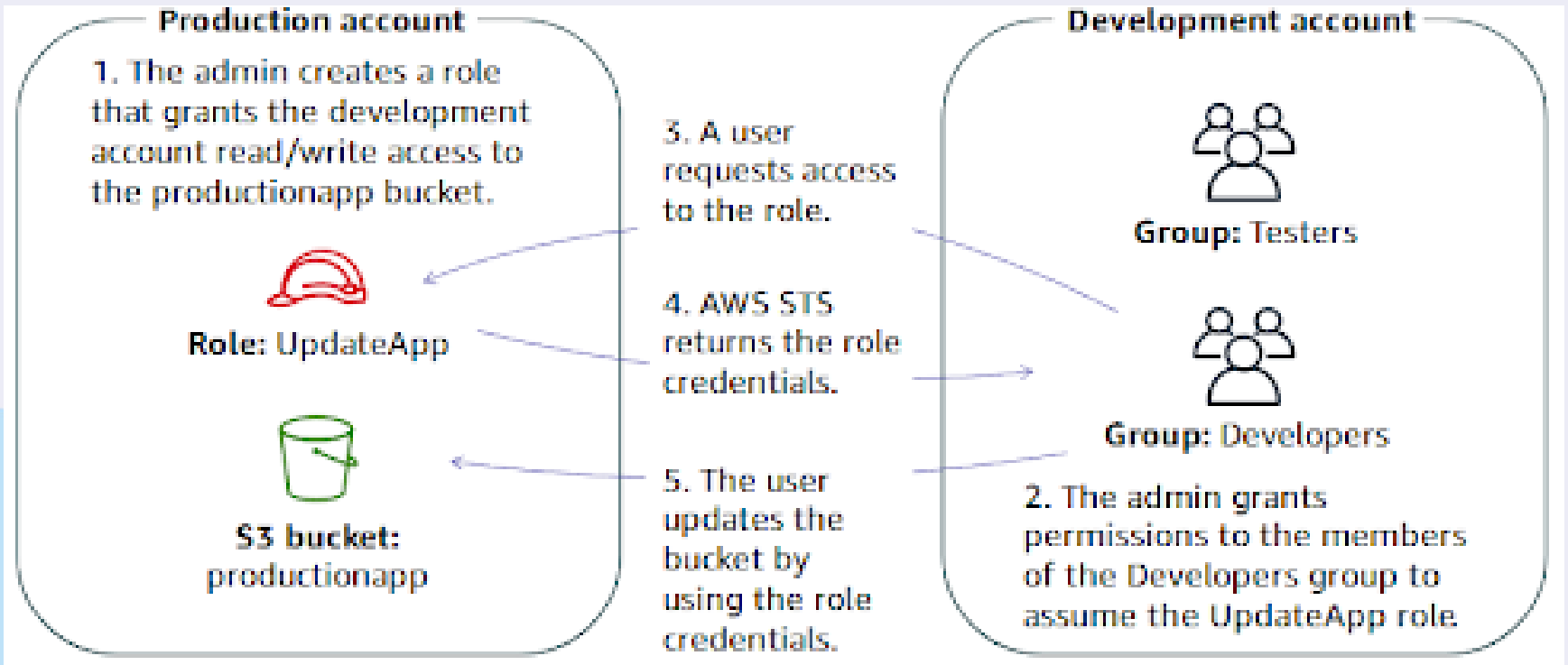
Ejemplos de dispositivos de MFA:

- Claves de seguridad (YubiKey, Gemalto)
- Aplicaciones (Google Authenticator, Authy)
- Dispositivos de hardware

La autenticación multifactor(MFA) es una práctica recomendada que agrega una capa adicional de protección, además de su nombre de usuario y contraseña. La MFA requiere dos o más factores para lograr la autenticación. Los factores incluyen lo siguiente:•algo que conozca, como una contraseña;•algo que tenga, como un token criptográfico;•algo que lo identifique, como su huella dactilar.La MFA no está activada de forma predeterminada. Cuando se encuentra habilitada la MFA y un usuario inicia sesión en la consola de administración de AWS, se le solicita su nombre de usuario y contraseña (el primer factor, lo que conoce). Luego, se les solicita una respuesta de autenticación de su dispositivo AWS MFA(el segundo factor: lo que tiene). Los ejemplos de dispositivos MFA incluyen dispositivos de clave de seguridad, como dispositivos YubiKey y Gemalto, y dispositivos virtuales, como Google Authenticatoro Authy.

Página inicial

Escenario de autenticación



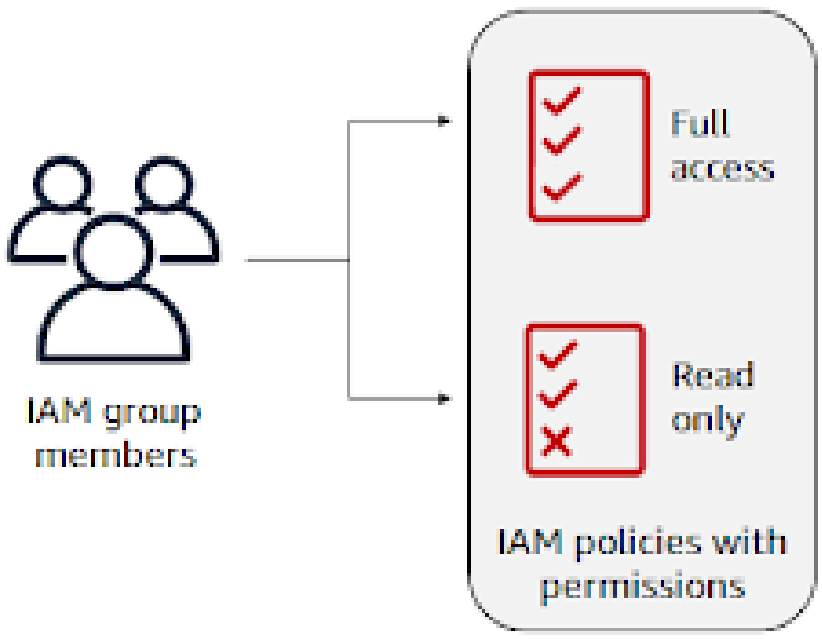
En este escenario, su organización ha creado varias cuentas de AWS para aislar el entorno de producción del entorno de desarrollo. Recuerde, una cuenta de AWS es un contenedor para sus recursos de AWS, por lo que la cuenta de producción y la cuenta de desarrollo son dos entornos completamente independientes. Después de probar una actualización dentro del entorno de desarrollo, debe conceder a los miembros del grupo de desarrolladores acceso temporal para actualizar el bucket de S3 de la aplicación de producción.

Siga los siguientes pasos para conceder este acceso temporal:

1. Un administrador en la cuenta de producción crea un rol que concede a la cuenta de desarrollo acceso de lectura o escritura a la cuenta de producción. Para hacer esto, debe definir una política de confianza que especifique la cuenta de desarrollo como principal. Esto autorizará a los usuarios de la cuenta de desarrollo a asumir el rol Update App (autenticación de cuenta de AWS).
2. En la cuenta de desarrollo, un administrador concede a los miembros del grupo de desarrolladores permisos para asumir el rol Update App. Debido a que este es un rol temporal, los desarrolladores recibirán permisos para llamar a AWS STS a fin de proporcionar un token de seguridad temporal. Cuando esto se complete, cualquier usuario de IAM que pertenezca al grupo de desarrolladores podrá asumir el rol Update App, según sea necesario.
3. El usuario solicita asumir el rol Update App mediante la consola, la API o la AWS CLI.
4. Al recibir la solicitud del rol, AWS STS devuelve las credenciales temporales al solicitante una vez que se completa la verificación.
5. Mediante el uso de las credenciales temporales que proporcionó AWS STS, el usuario del grupo de desarrolladores puede actualizar el bucket de la aplicación de producción en la cuenta de producción.

Página inicial

Principio de
mínimo privilegio



Prácticas recomendadas:

- Comience por conceder los permisos mínimos de cuenta de AWS que se necesitan para el puesto de trabajo.
- Conceda acceso adicional, según sea necesario.

Cuando conceda permisos a usuarios, grupos, roles y recursos, siga los consejos de seguridad estándar de autenticación sólida y el principio de mínimo privilegio. Esta práctica consiste en conceder sólo los permisos necesarios para realizar una tarea. Es más seguro comenzar con un conjunto mínimo de permisos y conceder permisos adicionales según sea necesario. Esto proporciona una mejor seguridad que comenzar con permisos que son demasiado permisivos e intentar restringirlos más adelante. Para definir el conjunto correcto de permisos, debe investigar un poco a fin de determinar el acceso que se necesita para realizar una tarea específica.Cuando cree políticas de IAM, determine lo que deben hacer sus usuarios y luego elabore políticas que les permitan realizar solo esas tareas. Del mismo modo, crea políticas para recursos individuales que identifiquen con precisión a quién se le permite acceder al recurso; solo permita los permisos mínimos para esos usuarios. Por ejemplo, quizá se debería permitir a los desarrolladores crear instancias de EC2 en los entornos de producción, pero no detenerlas ni terminarlas.

Página inicial

Políticas y permisos

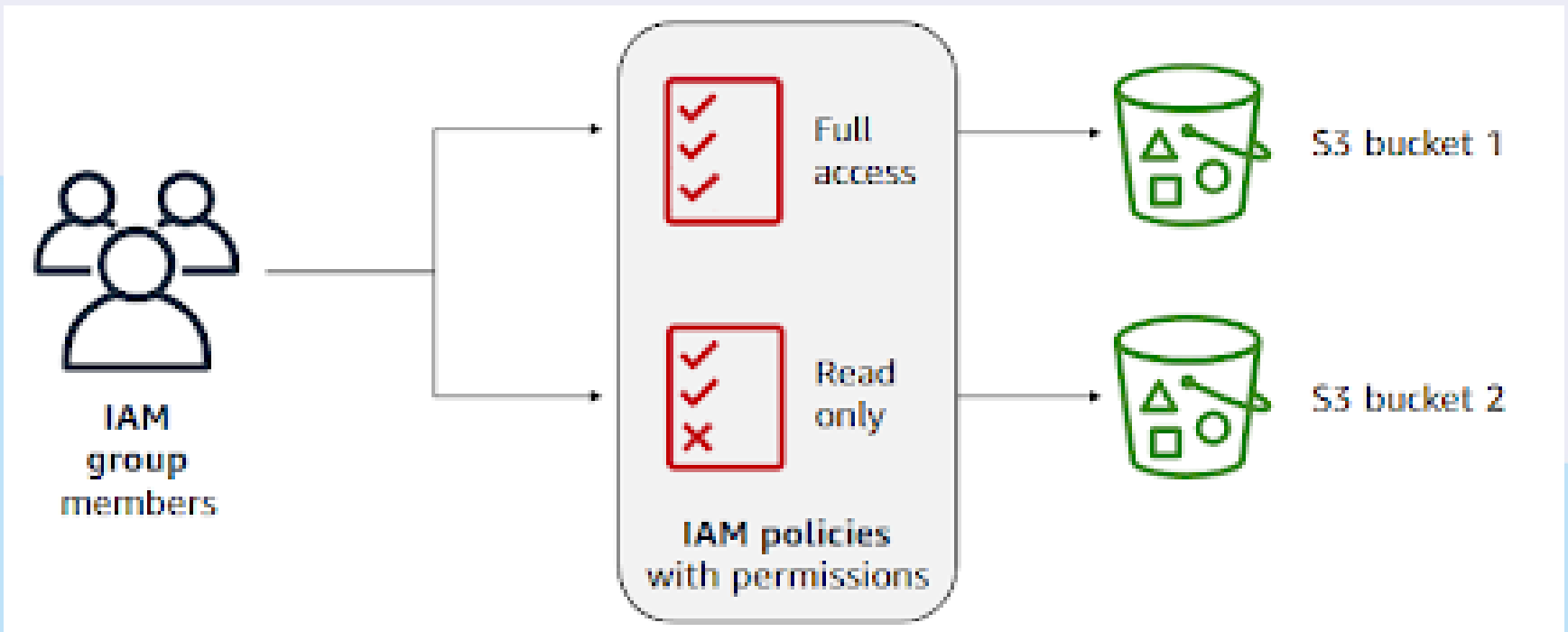


Diagrama del miembro del grupo de IAM que recibe acceso de las políticas y permisos de IAM. A los miembros del grupo de IAM se les asigna acceso completo al bucket de S3 1. También se les asigna acceso de sólo lectura al bucket de S3 2

Puede controlar el acceso a los recursos de AWS mediante políticas de IAM que conceden o deniegan permisos. En este ejemplo, los usuarios del grupo de IAM pueden leer, escribir y eliminar objetos en el bucket 1. Sin embargo, solo pueden leer los objetos en el bucket 2.
De forma predeterminada, un usuario, grupo o rol de IAM autenticado no puede acceder a nada en su cuenta hasta que le conceda permisos. Los permisos se conceden al crear una política. Las políticas son objetos que definen permisos para la identidad o el recurso al que se encuentran asociados. La mayoría de las políticas se definen y almacenan en un documento de notación de objetos JavaScript (JSON). Las políticas definen el efecto, las acciones, los recursos y las condiciones opcionales bajo las cuales una entidad puede invocar operaciones de API en la cuenta de AWS. De forma predeterminada, se deniegan todos los recursos y acciones que no se permiten de forma explícita. Cuando una entidad principal de IAM(usuario o rol) realiza una solicitud, AWS la evalúa en función de los permisos de estas políticas para determinar si se permitirá o denegará el acceso.

Tipos de políticas

Página inicial

6 tipos de políticas

En la actualidad, AWS admite seis tipos de políticas:

- Políticas basadas en identidades:estas políticas se adjuntan a las identidades de IAM y conceden permisos a la identidad.
- Políticas basadas en recursos: se adjuntan a los recursos y conceden permisos a la entidad principal que se especifica en la política.
- Límites de permisos: estos definen los permisos máximos que las políticas basadas en identidades pueden conceder a una entidad. Los límites de permisos no conceden permisos.
- Política de control de servicios (SCP) de AWS Organizations:define los permisos máximos para los miembros de la cuenta de una organización o unidad organizativa (OU). Puede utilizar las SCP para limitar los permisos de las políticas basadas en identidades o en recursos, pero no se pueden utilizar con el fin de conceder permisos.
- Listas de control de acceso (ACL):puede utilizar una ACL para controlar qué entidades principales en otras cuentas pueden acceder al recurso al que se ha adjuntado la ACL. No se puede utilizar una ACL para conceder permisos a entidades que se encuentran en la misma cuenta. Las ACL son el único tipo de política que no utiliza el formato de documento JSON.
- Políticas de sesión:se utilizan con la AWS CLI o la API de AWS a fin de crear una sesión temporal para un rol o usuario federado. Puede utilizar políticas de sesión para limitar los permisos que un rol o las políticas basadas en identidades de un usuario concede a una sesión. Las políticas de sesión limitan los permisos pero no pueden concederlos.

Volver

Página inicial

Política basadas en recursos y en identidades

Políticas basadas en *identidades*

¿A qué tiene acceso una identidad en particular?

Carlos

Recurso	Read	Write	List
Recurso X	Permitir	Permitir	Permitir

Richard

Recurso	Read	Write	List
Recurso Y	Permitir	N/A	N/A
Recurso Z	Permitir	N/A	N/A

Gerentes

Recurso	Read	Write	List
Recurso X	N/A	N/A	Permitir
Recurso Y	N/A	N/A	Permitir
Recurso Z	N/A	N/A	Permitir

Políticas basadas en *recursos*

¿Quién tiene acceso a un recurso en particular?

Recurso X

Usuario	Read	Write	List
Ana	Permitir	Permitir	Permitir
Akua	Permitir	Permitir	Permitir
Mary	Permitir	N/A	Permitir
Mateo	N/A	N/A	Permitir

Recurso Y

Usuario	Read	Write	List
Paulo	Permitir	Permitir	Permitir
Nikki	Permitir	N/A	N/A
Mateo	N/A	Permitir	Permitir

Nota: En las tablas, N/A significa que no se aplica porque la política no especifica permisos para esa acción en particular.Para reiterar, dos tipos de políticas de IAM pueden conceder permisos: políticas basadas en identidades y políticas basadas en recursos. La diferencia entre los dos tipos de políticas es el resultado de dónde se aplican, que depende del tipo de acceso que autorice o restrinja.Las políticas basadas en identidades se asocian a un usuario, grupo o rol de IAM. Indican lo que esa identidad puede hacer. Por ejemplo, podría conceder a un usuario la capacidad de acceder a una tabla de Amazon DynamoDB.Las políticas basadas en recursos se asocian a un recurso. Indican lo que un usuario específico (o grupo de usuarios) puede hacer con el recurso. Por ejemplo, puede utilizar políticas basadas en recursos para conceder acceso a un bucket de S3 o conceder acceso entre cuentas entre dos cuentas de AWS de confianza.

Para más información, consulte Identity-Based Policies and Resource-Based Policies (Políticas basadas en identidades y Políticas basadas en recursos) en la Guía del usuario de AWS Identity and Access Management

Página inicial

Políticas de IAM
administradas e insertadas

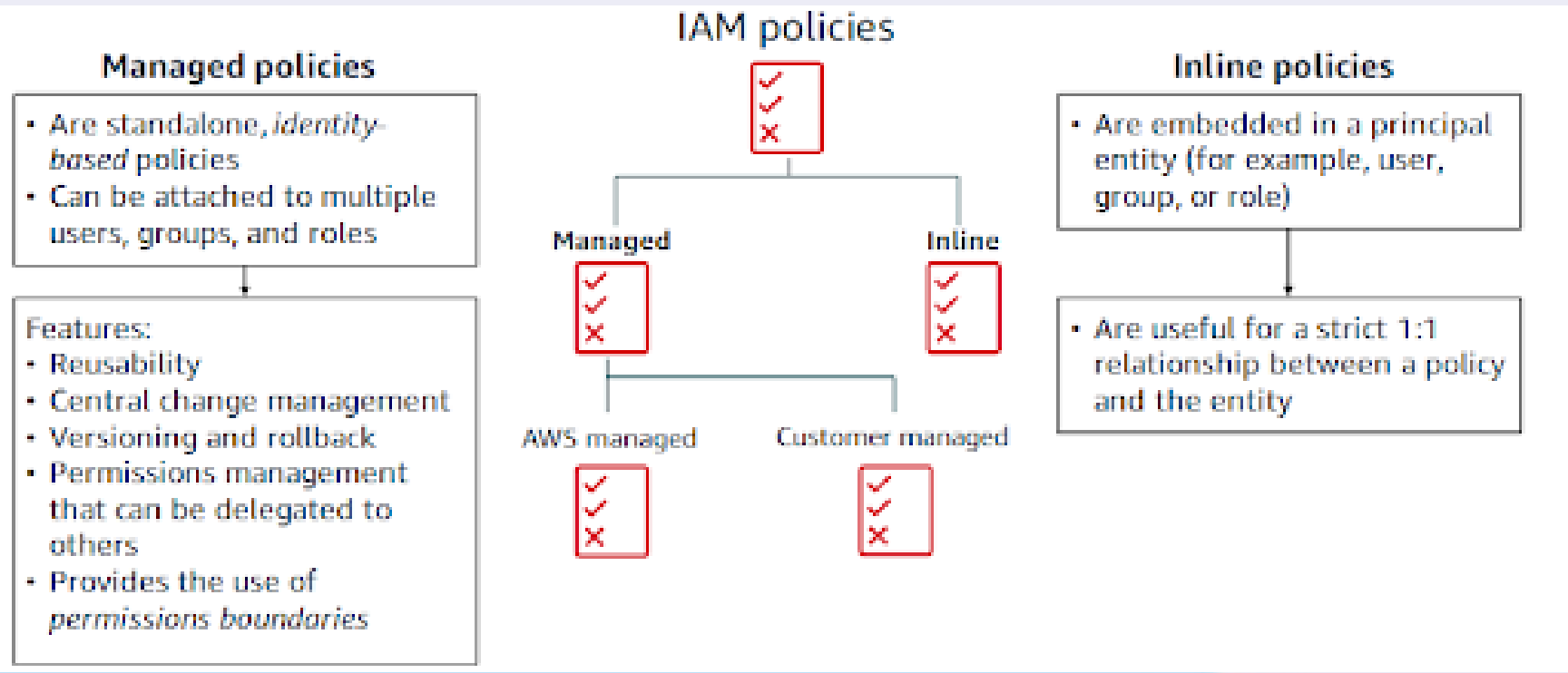


Diagrama que muestra que las políticas de IAM se dividen en dos categorías, administradas e insertadas. Las políticas administradas luego se dividen en políticas administradas por AWS y políticas administradas por el cliente.

Las políticas de IAM pueden ser administradas o insertadas.

Políticas administradas

- Las políticas administradas son políticas independientes basadas en identidades que pueden adjuntar a varios usuarios, grupos y roles.
- Las políticas administradas por AWS las crea y administra AWS.Las políticas administradas por el cliente las crea y administra usted.
- Las políticas administradas proporcionan varias funciones, incluidas las siguientes:
- Capacidad de reutilización.
- Se pueden administrar los cambios de forma centralizada.
- Se permiten el control de versiones y la restauración.
- La capacidad de delegar la administración de permisos a otros usuarios.
- Las políticas administradas también proporcionan el uso de límites de permisos. Esta es una función avanzada que permite que una política administrada establezca los permisos máximos que una política basada en identidades puede conceder a una entidad de IAM.

Políticas insertadas

- Las políticas insertadas se incrustan en una entidad principal, como un usuario, Puede utilizar la misma política para varias entidades, pero esas entidades no comparten la política. En un grupo o un rol. Es decir, la política es parte inherente de la entidad.
- Las políticas insertadas son útiles cuando se quiere mantener una relación estricta de uno a uno entre una política y la entidad principal a la que se aplica. Esto se debe a que las políticas insertadas no se pueden adjuntar de manera inadvertida a la entidad incorrecta.

Los casos de uso variarán y se deben seleccionar las políticas en función de la situación. En la mayoría de los casos, AWS recomienda el uso de políticas administradas en lugar de políticas insertadas.

Página inicial

Lógica de evaluación
para políticas de IAM

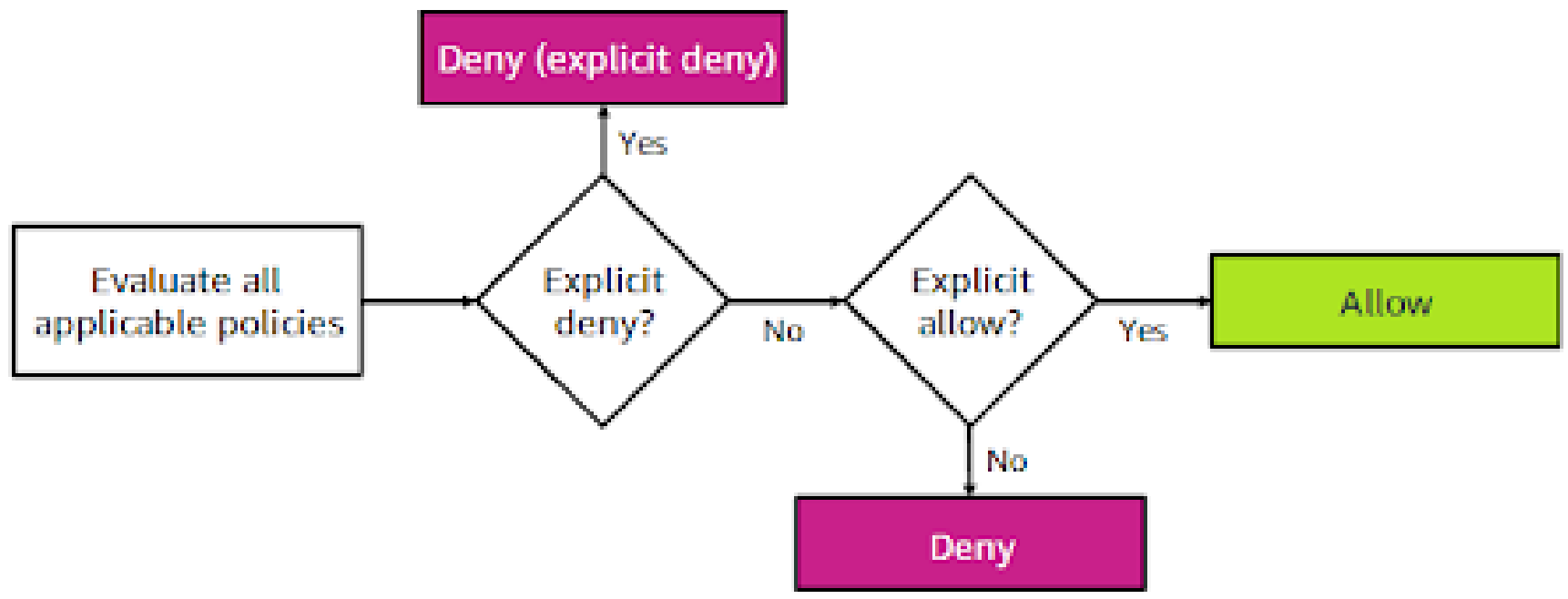


Diagrama de lógica de evaluación para políticas de IAM. En primer lugar, las políticas se evalúan para una denegación explícita. Si existe una denegación explícita, se deniega el acceso. Si no existe una denegación explícita, la política se evalúa para un permiso explícito. Si existe un permiso explícito, se otorga el acceso, pero si no existe, se deniega el acceso.

En este diagrama, se muestra la lógica que utiliza AWS al evaluar las políticas de IAM. AWS evalúa todas las políticas aplicables y pasa por esta lógica de evaluación:

- De forma predeterminada, se deniegan todas las solicitudes.
- Un permiso explícito anula la denegación predeterminada.
- Una denegación explícita anula cualquier permiso explícito.

El orden en que se evalúan las políticas no modifica el resultado de la evaluación. Todas las políticas se evalúan, y el resultado es siempre que la solicitud se permite o deniega. Supongamos que se genera un conflicto (una política permite una acción y otra política deniega una acción). Luego, la política más restrictiva (es decir, la política que rechaza la acción) se aplica.

Estos son algunos aprendizajes clave de esta lección del módulo:

- Los permisos para acceder a los servicios y recursos de la cuenta de AWS se definen en los documentos de la política de IAM.
- Adjunte políticas de IAM a usuarios, grupos o roles de IAM.
- Siga el principio de mínimo privilegio cuando conceda acceso a la cuenta.
- Cuando IAM determina los permisos, una denegación explícita siempre anulará cualquier enunciado de permiso.

Página inicial