COLOMBIA POTENCIA DE LA VIDA

TIC

Lección 2
AWS Identity and Access Management (o IAM)

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

TIC

Presionar cada tema para ver si contenido

- Introducción
- Componentes esenciales
- Acceso
- MFA de IAM
- Acciones permitidas
- Autorización
- Políticas + Ejemplo
- Políticas basadas en recursos
- Permisos
- Grupos
- Roles + Ejemplo

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

AWS Identity and Access Management (o IAM)

Utilice IAM para administrar el acceso a los recursos de AWS:

- Un recurso es una entidad en una nueva cuenta de AWS con la que puede trabajar.
- Recurso de ejemplo: una instancia de Amazon EC2 o un bucket Amazon S3

Por ejemplo: controle quién puede terminar instancias de Amazon EC2

Defina los derechos de acceso detallados:

- Quién puede obtener acceso al recurso
- A qué recursos se puede obtener acceso y qué puede hacer el usuario con el recurso
- Cómo se puede obtener acceso a los recursos

IAM es una característica de cuenta de AWS

AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) es una herramienta que permite controlar quién tiene acceso a los diferentes servicios y recursos en la nube de AWS. Con IAM, puede gestionar la autenticación de usuarios y aplicar políticas de autorización para determinar qué acciones pueden realizar esos usuarios en cada servicio.

+INFO

IAM centraliza la gestión del acceso, lo que significa que puede controlar quién puede iniciar, configurar, administrar y finalizar recursos dentro de su cuenta de AWS. Ofrece un control detallado sobre qué recursos pueden ser accedidos y qué acciones pueden ser realizadas en ellos, incluso especificando qué llamadas a la API pueden ser realizadas por cada usuario.

Independientemente de si está utilizando la consola de administración de AWS, la CLI de AWS o los SDK de AWS, cada interacción con un servicio de AWS se realiza a través de la API. IAM le permite gestionar quién puede acceder a qué recursos y de qué manera pueden acceder a ellos.

Con IAM, puede otorgar diferentes niveles de permisos a diferentes usuarios para diferentes recursos. Por ejemplo, puede permitir que algunos usuarios tengan control total sobre una amplia gama de servicios de AWS, mientras que restringe a otros a solo lectura en determinados recursos, como buckets de Amazon S3. También puede conceder permisos para administrar instancias EC2 específicas o para acceder únicamente a la información de facturación de la cuenta.

Lo mejor de todo es que IAM es una característica incluida en su cuenta de AWS, sin costos adicionales.

IAM: componentes esenciales

Usuario de IAM

Persona o aplicación que se puede autenticar con una cuenta de AWS

Grupo de IAM

Colección de usuarios de IAM a los que se concede una autorización idéntica

Política de IAM

El documento que define a qué recursos se puede obtener acceso y el nivel de acceso a cada recurso

Rol de IAM

Mecanismo útil para conceder un conjunto de permisos a fin de realizar solicitudes de servicios de AWS

Para entender cómo emplear IAM para proteger su cuenta de AWS, es crucial comprender el propósito y la función de cada uno de los cuatro componentes de IAM.

Un usuario IAM representa una persona o aplicación identificada en una cuenta de AWS que necesita interactuar con los productos de AWS a través de llamadas a la API. Cada usuario debe tener un nombre único dentro de la cuenta de AWS y un conjunto exclusivo de credenciales de seguridad que no se comparten con otros usuarios. Estas credenciales son distintas de las credenciales de seguridad de la cuenta raíz de AWS. Cada usuario se define únicamente en una cuenta de AWS.

+INFO

Un grupo IAM es una colección de usuarios IAM. Los grupos de IAM se emplean para simplificar la gestión y definición de permisos para varios usuarios.

Una política IAM es un documento que establece los permisos necesarios para determinar las acciones que los usuarios pueden realizar en la cuenta de AWS. Por lo general, una política otorga acceso a recursos específicos y especifica las acciones permitidas sobre dichos recursos. También es posible que las políticas nieguen explícitamente ciertos accesos.

Un rol IAM es una herramienta utilizada para otorgar acceso temporal a recursos específicos de AWS dentro de una cuenta de AWS.

Autenticarse como usuario de IAM para obtener acceso

Cuando define un usuario de IAM, selecciona qué tipos de acceso puede utilizar el usuario.
Acceso mediante programación, se autentica lo siguiente:

- ID de clave de acceso
- Clave de acceso secreta
  - Proporciona acceso a la CLI de AWS y al SDK de AWS.

Acceso a la consola de administración de AWS, se autentica lo siguiente:

- ProporcionalD de cuenta o alias de 12 dígitos
- Nombre de usuario de IAM
- Contraseña de IAM
  - Si está habilitada, Multi-Factor Authentication (MFA) solicita un código de autenticación.

La autenticación es un principio fundamental en seguridad informática, donde un usuario o sistema debe validar su identidad antes de acceder a recursos protegidos. Puede compararse con el proceso de identificación que se realiza en un aeropuerto antes de pasar por el área de seguridad para abordar un vuelo. En ese caso, es necesario presentar una identificación al oficial de seguridad para demostrar quién es antes de ingresar a una zona restringida. De manera similar, se aplica un concepto análogo para acceder a los recursos de AWS en la nube.

+INFO

Al configurar un usuario IAM, se decide qué tipo de acceso tendrá ese usuario para interactuar con los recursos de AWS. Hay dos tipos de acceso que se pueden asignar: acceso mediante programación y acceso a la consola de administración de AWS. Puede otorgar sólo acceso mediante programación, solo acceso a la consola o ambos tipos de acceso a los usuarios.

Si se otorga acceso mediante programación, el usuario IAM debe proporcionar un ID de clave de acceso y una clave de acceso secreta al realizar llamadas a la API de AWS a través de la CLI de AWS, el SDK de AWS u otras herramientas de desarrollo.

Si se otorga acceso a la consola de administración de AWS, el usuario IAM debe completar los campos requeridos en la ventana de inicio de sesión del navegador. Se le pedirá al usuario que ingrese el ID de cuenta de 12 dígitos o el alias de cuenta correspondiente, junto con su nombre de usuario y contraseña de IAM. Si la autenticación multifactor (MFA) está habilitada para el usuario, también se le solicitará un código adicional de autenticación.

MFA de IAM

Consola de administración de AWS

- MFA proporciona más seguridad.
- Además del nombre de usuario y la contraseña, MFA requiere un código de autenticación único para acceder a los servicios de AWS

Los servicios y recursos de AWS pueden ser accesados a través de varias herramientas, como la consola de administración de AWS, la línea de comandos de AWS (CLI) o mediante los kits de desarrollo de software (SDK) y las interfaces de programación de aplicaciones (API). Como medida adicional de seguridad, se recomienda activar la autenticación multifactor (MFA).

+INFO

COLOMBIA POTENCIA DE LA VIDA

TIC

La autenticación multifactor (MFA) requiere que los usuarios y sistemas proporcionan un código adicional (junto con las credenciales de inicio de sesión regulares) para acceder a los servicios y recursos de AWS. Este código adicional, conocido como token de MFA, es generado por una aplicación de autenticación virtual (como Google Authenticator o Authy 2-Factor Authentication), dispositivos de clave de seguridad U2F o dispositivos físicos de MFA.

Habilitar MFA proporciona una capa adicional de seguridad al requerir un segundo factor de autenticación, lo que dificulta el acceso no autorizado a los recursos de AWS, incluso si las credenciales de inicio de sesión normales están comprometidas.

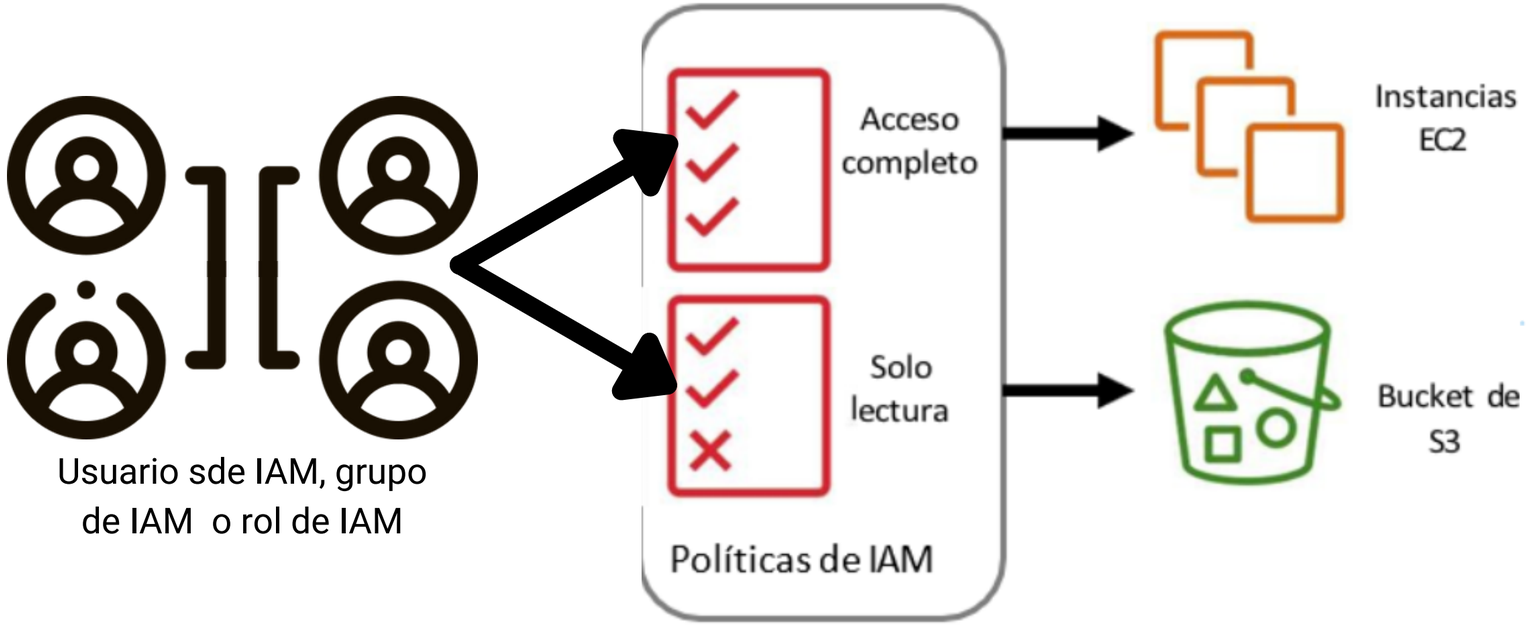
TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Autorización:
qué acciones están permitidas

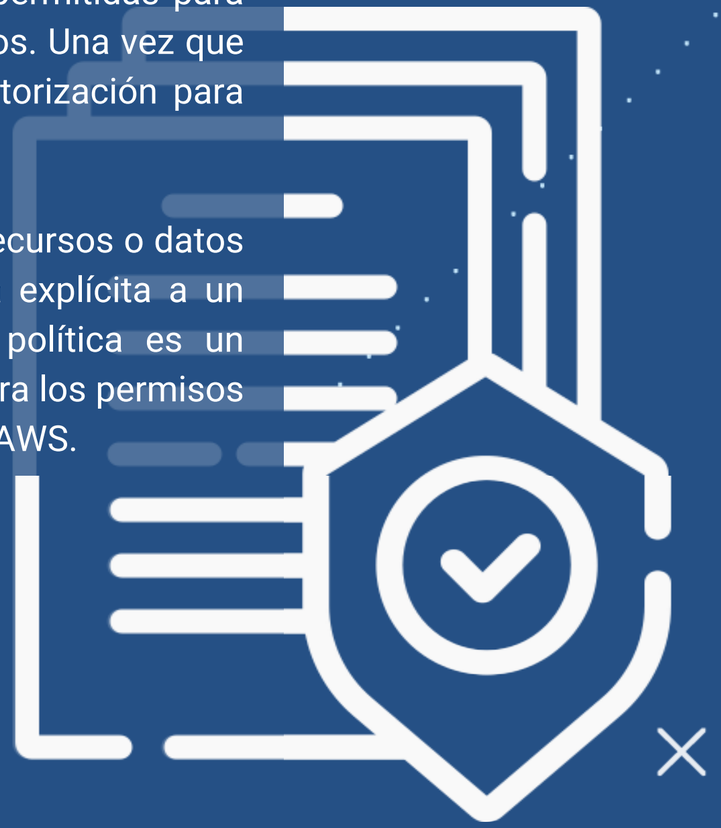
Una vez que el usuario o la aplicación se haya conectado a la cuenta de AWS, ¿qué pueden hacer?



+INFO

La autorización implica determinar qué acciones específicas están permitidas para un usuario, servicio o aplicación después de que han sido autenticados. Una vez que un usuario ha sido verificado como legítimo, se le debe otorgar autorización para acceder a los servicios de AWS.

Por defecto, los usuarios de IAM no tienen acceso automático a los recursos o datos en una cuenta de AWS. Es necesario otorgar permisos de manera explícita a un usuario, grupo o rol mediante la creación de una política. Una política es un documento en formato JavaScript Object Notation (JSON) que enumera los permisos concedidos o denegados para acceder a los recursos en la cuenta de AWS.



IAM: autorización

Permisos de IAM

Asigna permisos mediante la creación de una política de IAM.
Los permisos determinan qué recursos y operaciones están permitidas:

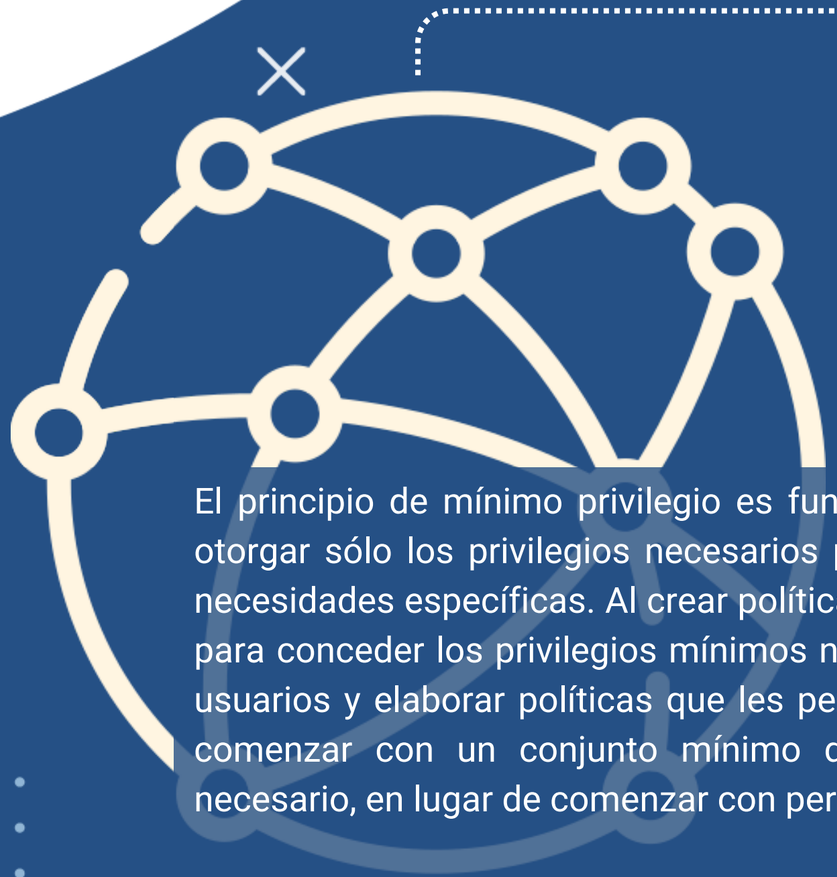
- De forma predeterminada, todos los permisos están denegados implícitamente.
- Si algo está denegado explícitamente, nunca se permite.

Práctica recomendada: seguir el principio de mínimo privilegio.

Nota: El alcance de las configuraciones de servicios de IAM es global. Las configuraciones se aplican a todas las regiones de AWS.

Para otorgar permisos a un usuario, grupo o rol en AWS, es necesario crear una política de IAM o utilizar una política existente en la cuenta. No hay permisos predefinidos, por lo que todas las acciones en la cuenta se consideran denegadas por defecto (denegación implícita), a menos que se permita explícitamente. Cualquier acción que no esté permitida explícitamente será denegada automáticamente. Además, cualquier acción que se niegue explícitamente siempre será rechazada.

+INFO



El principio de mínimo privilegio es fundamental en seguridad informática. Este principio sugiere otorgar sólo los privilegios necesarios para que un usuario realice sus tareas, basándose en sus necesidades específicas. Al crear políticas de IAM, se recomienda seguir este enfoque de seguridad para conceder los privilegios mínimos necesarios. Se debe identificar las tareas requeridas por los usuarios y elaborar políticas que les permitan llevar a cabo únicamente esas tareas. Es preferible comenzar con un conjunto mínimo de permisos y otorgar permisos adicionales según sea necesario, en lugar de comenzar con permisos demasiado amplios y luego intentar restringirlos.

Es importante tener en cuenta que las configuraciones de IAM tienen un alcance global, lo que significa que se aplican en todas las regiones de AWS y no se limitan a una región específica.

Políticas de IAM

Una política de IAM es un documento que define permisos.

- Habilita el control de acceso detallado.

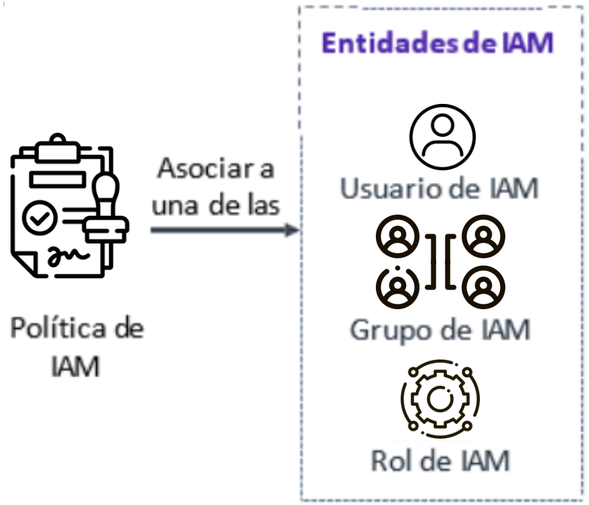
Existen dos tipos de políticas: basadas en identidad y basadas en recursos

Políticas basadas en identidad :

- Asocian una política a cualquier entidad de IAM.
  - Un usuario de IAM, un grupo de IAM, o una rol IAM
- Las políticas especifican lo siguiente:
  - Acciones que puede realizar la entidad
  - Acciones que la entidad no puede realizar
- Una sola política se puede asociar a varias entidades.
- Una sola entidad puede tener varias políticas asociadas a ella.

Políticas basadas en recursos

- Están asociadas a un recurso (como un bucket de S3)



Una política de IAM es una instrucción formal de permisos que se concederá a una entidad. Las políticas se pueden asociar a cualquier entidad de IAM. Las entidades incluyen usuarios, grupos, roles o recursos. Por ejemplo, puede asociar una política a sus recursos de AWS para bloquear todas las solicitudes que no provengan de un rango de direcciones de protocolo de Internet (IP) aprobado.

+INFO

EJEMPLO

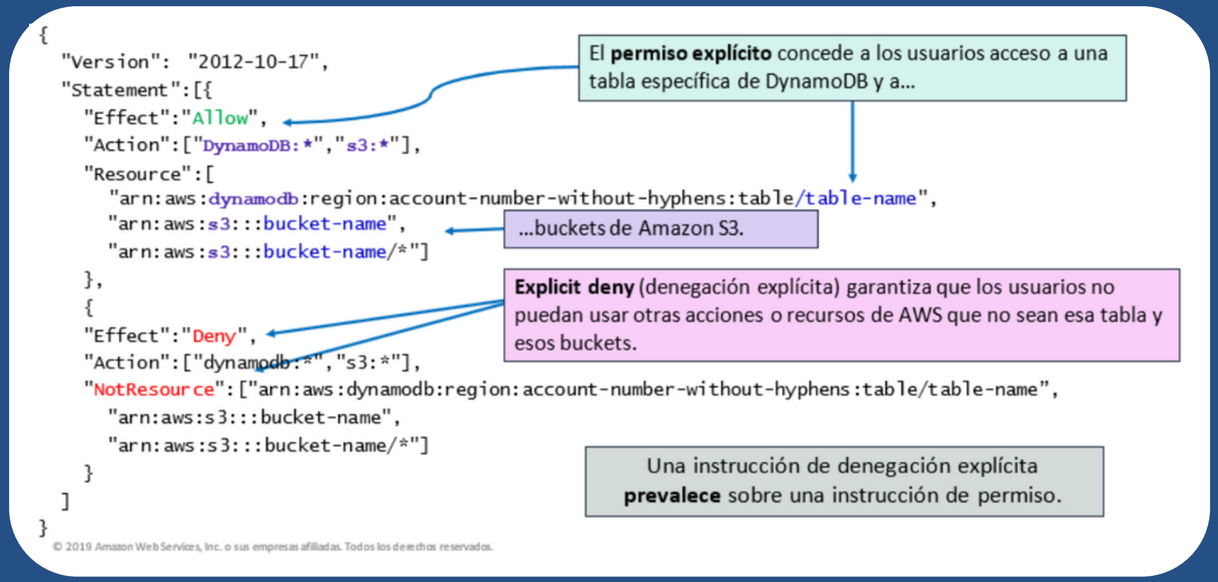
Las políticas especifican cuáles son las acciones permitidas, cuáles son los recursos a los que estas tienen permiso y cuál será el efecto cuando el usuario solicite acceso a los recursos.

El orden en que se evalúan las políticas no modifica el resultado de la evaluación. Se evalúan todas las políticas y el resultado es siempre el permiso o la denegación de la solicitud. Cuando hay un conflicto, se aplica la política más restrictiva.
Hay dos tipos de políticas de IAM. Las políticas basadas en identidad son políticas de permisos que puede asociar a una entidad principal (o identidad), como por ejemplo un usuario, rol o grupo de IAM. Estas políticas controlan qué acciones puede realizar dicha identidad, en qué recursos y en qué condiciones. Las políticas basadas en identidad se pueden clasificar del siguiente modo:

- Políticas administradas: políticas independientes basadas en identidad que puede asociar a varios usuarios, grupos y roles en su cuenta de AWS.
- Políticas insertadas: políticas que crea y administra y que están insertadas directamente en un único usuario, grupo o rol.

Las políticas basadas en recursos son documentos de política JSON que se pueden asociar a un recurso como, por ejemplo, un bucket de S3. Estas políticas controlan qué acciones puede realizar una entidad principal especificada en dicho recurso y en qué condiciones.

Ejemplo de política de IAM



Como mencionamos anteriormente, las políticas de IAM se redactan utilizando el formato JSON. El ejemplo de política de IAM que se proporciona otorga a los usuarios acceso restringido a los siguientes recursos específicos:

- Una tabla en DynamoDB, cuyo nombre está representado por "table-name".
- Un bucket de S3 en la cuenta de AWS, cuyo nombre está representado por "bucket-name", y todos los objetos contenidos en él.

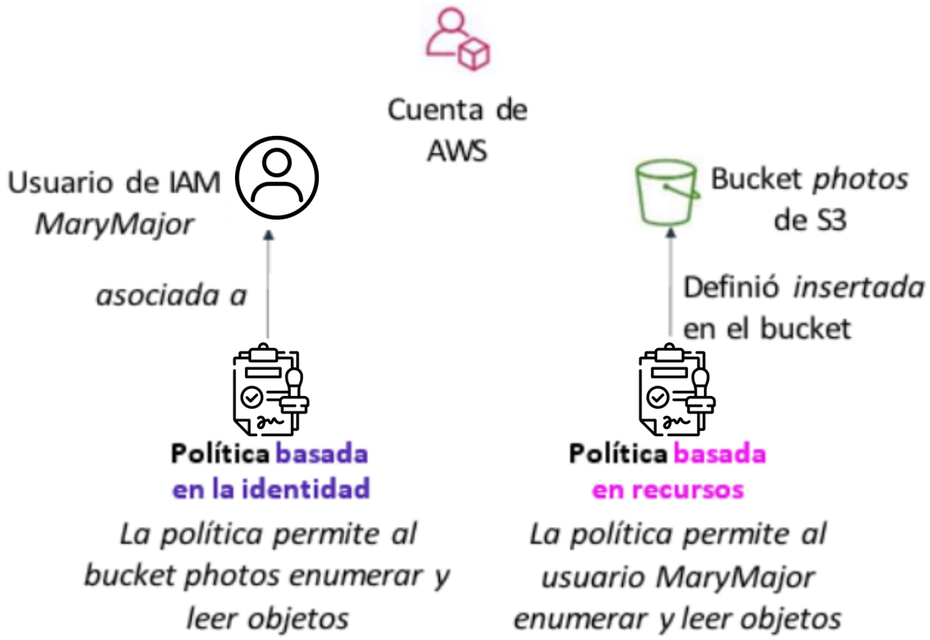
Además, esta política de IAM incluye una declaración de denegación explícita con el efecto "Deny". La inclusión del elemento "NotResource" garantiza que los usuarios no puedan acceder a ninguna otra acción o recurso en DynamoDB o S3 que no esté especificado en la política, incluso si se les conceden permisos mediante otra política. En el sistema de IAM, una instrucción de denegación explícita siempre tiene prioridad sobre una instrucción de permiso.

Políticas basadas en recursos

Las políticas basadas en identidad se asocian a un usuario, grupo o rol.
Las políticas basadas en recursos se asocian a un recurso (no a un usuario, grupo o rol)
Características de las políticas basadas en recursos:

- Especifican quién tiene acceso al recurso y que acciones se pueden realizar en él.
- Las políticas son insertadas solamente, no se administran.

Las políticas basadas en recursos solo se admiten en algunos servicios de AWS



Aunque las políticas basadas en identidad están asociadas a un usuario, grupo o rol, las políticas basadas en recursos se asocian a un recurso, como un bucket de S3. Estas políticas especifican quién puede obtener acceso al recurso y qué acciones pueden realizar en él.

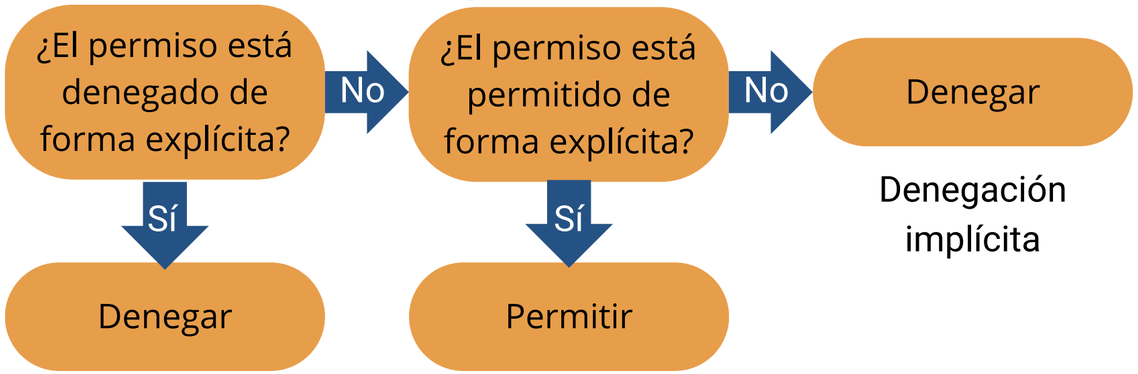
+INFO

Las políticas basadas en recursos se definen únicamente de forma directa, lo que significa que usted define la política en el propio recurso, en lugar de crear un documento de política de IAM independiente. Por ejemplo, para crear una política de bucket de S3 (un tipo de política basada en recurso) en un bucket de S3, vaya al bucket, haga clic en la pestaña Permissions (Permisos), haga clic en el botón Bucket Policy (Política de bucket) y defina allí el documento de política con formato JSON. Una lista de control de acceso (ACL) de Amazon S3 es otro ejemplo de una política basada en recursos.

El diagrama muestra dos formas diferentes en las que se podría conceder acceso al usuario MaryMajor a objetos en el bucket de S3 denominado photos. A la izquierda, puede ver un ejemplo de una política basada en identidad. Una política de IAM que concede acceso al bucket de S3 se asocia al usuario MaryMajor. A la derecha, puede ver un ejemplo de una política basada en recursos. La política de bucket de S3 para el bucket photos especifica que el usuario MaryMajor tiene permiso para enumerar y leer los objetos del bucket.

Permisos de IAM

Modo en que IAM determina permisos:



Las políticas de IAM le permiten ajustar los privilegios que se conceden a los usuarios, grupos y funciones de IAM.

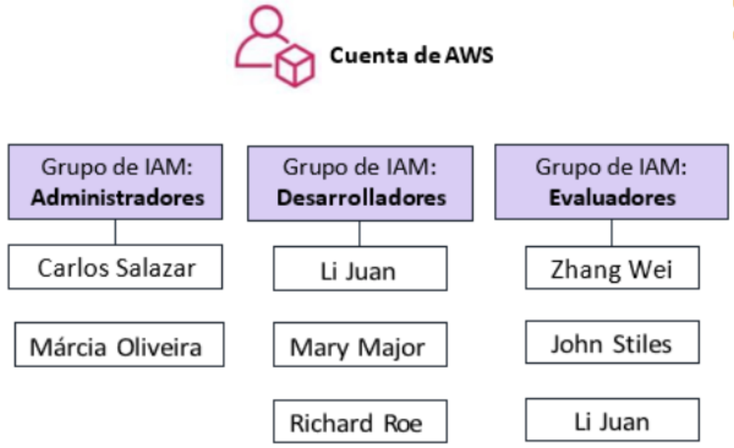
Cuando IAM determina si se concede un permiso, IAM comprueba primero la existencia de cualquier política de denegación explícita aplicable.

Si no existe ninguna denegación explícita, comprueba si existe alguna política de permisos explícitos aplicable. Si no existe una política de denegación explícita ni de permiso explícito, IAM vuelve a la forma predeterminada, que consiste en negar el acceso. Este proceso se denomina denegación implícita. El usuario solo podrá realizar la acción si la acción solicitada no está denegada de forma explícita y está permitida de forma explícita.

SIMULADOR

Puede ser difícil descubrir si el acceso a un recurso se concederá a una entidad de IAM cuando desarrolle políticas de IAM. El simulador de políticas de IAM es una herramienta útil para probar y solucionar problemas de políticas de IAM.

Grupos de IAM



Un grupo de IAM es un conjunto de usuarios de IAM.
Un grupo se utiliza para conceder los mismos permisos a varios usuarios.

- Se conceden los permisos cuando se asocia la política o las políticas de IAM al grupo.

Un usuario puede pertenecer a varios grupos.
No hay grupo predeterminado.
Los grupos no pueden estar anidados.

Un grupo de IAM consiste en un conjunto de usuarios de IAM. Estos grupos proporcionan una manera práctica de asignar permisos a varios usuarios, simplificando así la gestión de los permisos para este conjunto de usuarios.

Por ejemplo, podrías establecer un grupo de IAM llamado "Desarrolladores" y asociar una o varias políticas de IAM a este grupo para conceder los permisos necesarios para acceder a los recursos de AWS que normalmente requieren los desarrolladores.

+INFO

Cuando añades un usuario al grupo "Desarrolladores", automáticamente heredará los permisos asignados al grupo. Esto significa que no es necesario asignar directamente políticas de IAM a cada usuario individualmente. Si un nuevo empleado se une a tu organización y necesita permisos de desarrollador, simplemente lo agregas al grupo "Desarrolladores". De manera similar, si un empleado cambia de función dentro de tu organización, en lugar de editar los permisos de ese usuario, solo necesitas eliminarlo del grupo correspondiente.

Algunas características importantes de los grupos de IAM son:

- Un grupo puede contener múltiples usuarios, y un usuario puede pertenecer a varios grupos.
- Los grupos no pueden ser anidados. Esto significa que un grupo solo puede contener usuarios y no puede incluir otros grupos dentro de él.
- No existe un grupo predefinido que incluya automáticamente a todos los usuarios de la cuenta de AWS. Si deseas crear un grupo que incluya a todos los usuarios de la cuenta, debes crearlo tú mismo y agregar a cada usuario nuevo manualmente.

Roles de IAM

Rol de IAM

Un rol de IAM es una identidad de IAM con permisos específicos.
Es similar a un usuario de IAM
- Asocia políticas de permisos a él.

Es diferente a un usuario de IAM.
- No está asociado de forma exclusiva a una persona.
- Está diseñado para que lo pueda asumir una persona, una aplicación o un servicio.

El rol proporciona credenciales de seguridad temporales.
Ejemplos de cómo se utilizan los roles de IAM para delegar el acceso:
- Utilizado por un usuario de IAM en la misma cuenta de AWS que utiliza el rol
- Utilizado por un servicio de AWS, como Amazon EC2, en la misma cuenta que utiliza el rol
- Utilizado por un usuario de IAM en una cuenta de AWS diferente a la que utiliza el rol

Un rol de IAM es una identidad de IAM que se puede crear en su cuenta y que tiene permisos específicos. Un rol de IAM es similar a un usuario de IAM porque también es una identidad de AWS a la que puede asociar políticas de permisos y esos permisos determinan lo que la identidad puede hacer y lo que no en AWS.

Sin embargo, en lugar de estar asociada únicamente a una persona, el objetivo es que pueda asignarse un rol a cualquier persona que lo necesite. Además, un rol no tiene asociadas credenciales estándar a largo plazo, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este le proporciona credenciales de seguridad temporales para la sesión de rol.

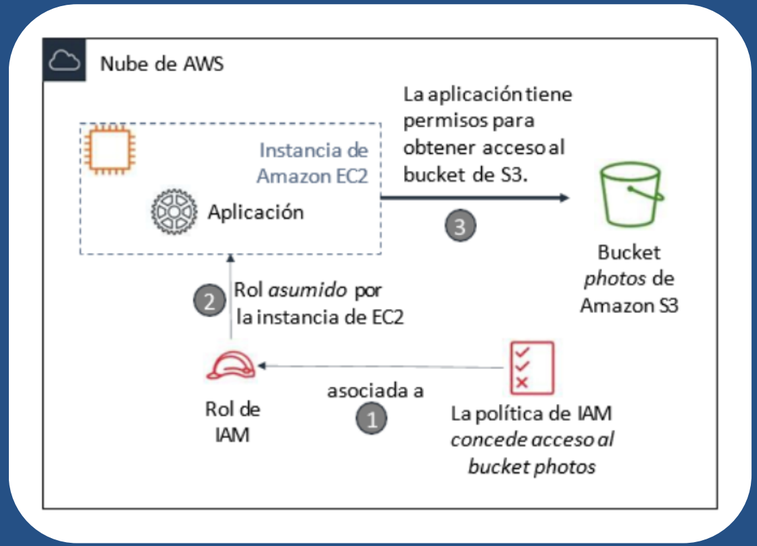
+INFO

EJEMPLO

Puede utilizar roles para delegar el acceso a usuarios, aplicaciones o servicios que normalmente no tendrían acceso a los recursos de AWS. Por ejemplo, es posible que desee conceder acceso a los usuarios de su cuenta de AWS a los recursos que no suelen tener o conceder acceder a los usuarios de una cuenta de AWS a los recursos de otra cuenta. También puede que quiera permitir que una aplicación móvil utilice los recursos de AWS, pero no desea integrar las claves de AWS en la aplicación (donde serían difíciles de rotar y donde los usuarios pueden potencialmente extraerlas y usarlas de forma incorrecta). Además, a veces es posible que desee conceder acceso a AWS a los usuarios que ya tienen identidades definidas fuera de AWS, como en su directorio corporativo. O bien, es posible que quiera conceder acceso a su cuenta a terceros para que puedan realizar una auditoría en los recursos.

En todos estos casos de uso de ejemplo, los roles de IAM son un componente esencial en la implementación en la nube.

Ejemplo de uso de un rol de IAM



Situación:
Una aplicación que se ejecuta en una instancia de EC2 necesita acceso a un bucket de S3
Solución:

- Definir una política de IAM que conceda acceso al bucket de S3
- Asociar la política a un rol
- Permitir que la instancia EC2 asuma el rol

En el diagrama, un desarrollador ejecuta una aplicación en una instancia EC2 que requiere acceso al bucket de S3 denominado photos. Un administrador crea el rol de IAM y lo asocia a la instancia EC2. El rol incluye una política de permisos que otorga acceso de solo lectura al bucket de S3 especificado. También incluye una política de confianza que permite a la instancia EC2 asumir el rol y obtener las credenciales temporales.

Cuando la aplicación se ejecuta en la instancia, puede utilizar las credenciales temporales del rol para obtener acceso al bucket photos. El administrador no necesita conceder permiso al desarrollador de la aplicación para obtener acceso al bucket photos y el desarrollador nunca necesita compartir ni administrar las credenciales.

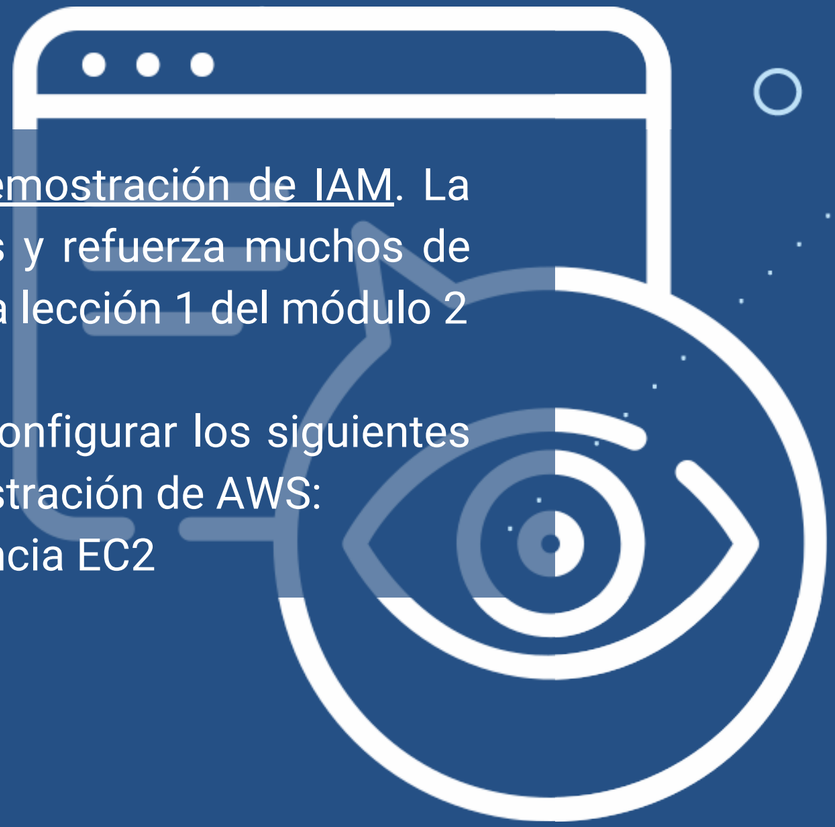
Para obtener más información acerca de este ejemplo, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2.

Estos son algunos de los aprendizajes clave de esta lección:

- Las políticas de IAM se crean con la notación de objetos JavaScript (JSON) y definen permisos.
- Las políticas de IAM se pueden asociar a cualquier entidad de IAM.
- Las entidades son usuarios de IAM, grupos de IAM y roles de IAM.
- Un usuario de IAM permite que una persona, aplicación o servicio pueda autenticarse en AWS.
- Un grupo de IAM permite asociar las mismas políticas a varios usuarios de una manera sencilla.
- Un rol de IAM puede tener asociadas políticas de permisos y se puede utilizar para delegar acceso temporal a usuarios o aplicaciones.

COLOMBIA POTENCIA DE LA VIDA

TIC



Ahora, dedique un momento a ver la demostración de IAM. La grabación dura poco más de 4 minutos y refuerza muchos de los conceptos que se han tratado en esta lección 1 del módulo 2

En la demostración, se muestra cómo configurar los siguientes recursos mediante la consola de administración de AWS:

- Un rol de IAM que utilizará una instancia EC2
- Un grupo de IAM
- Un usuario de IAM

INICIO

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira