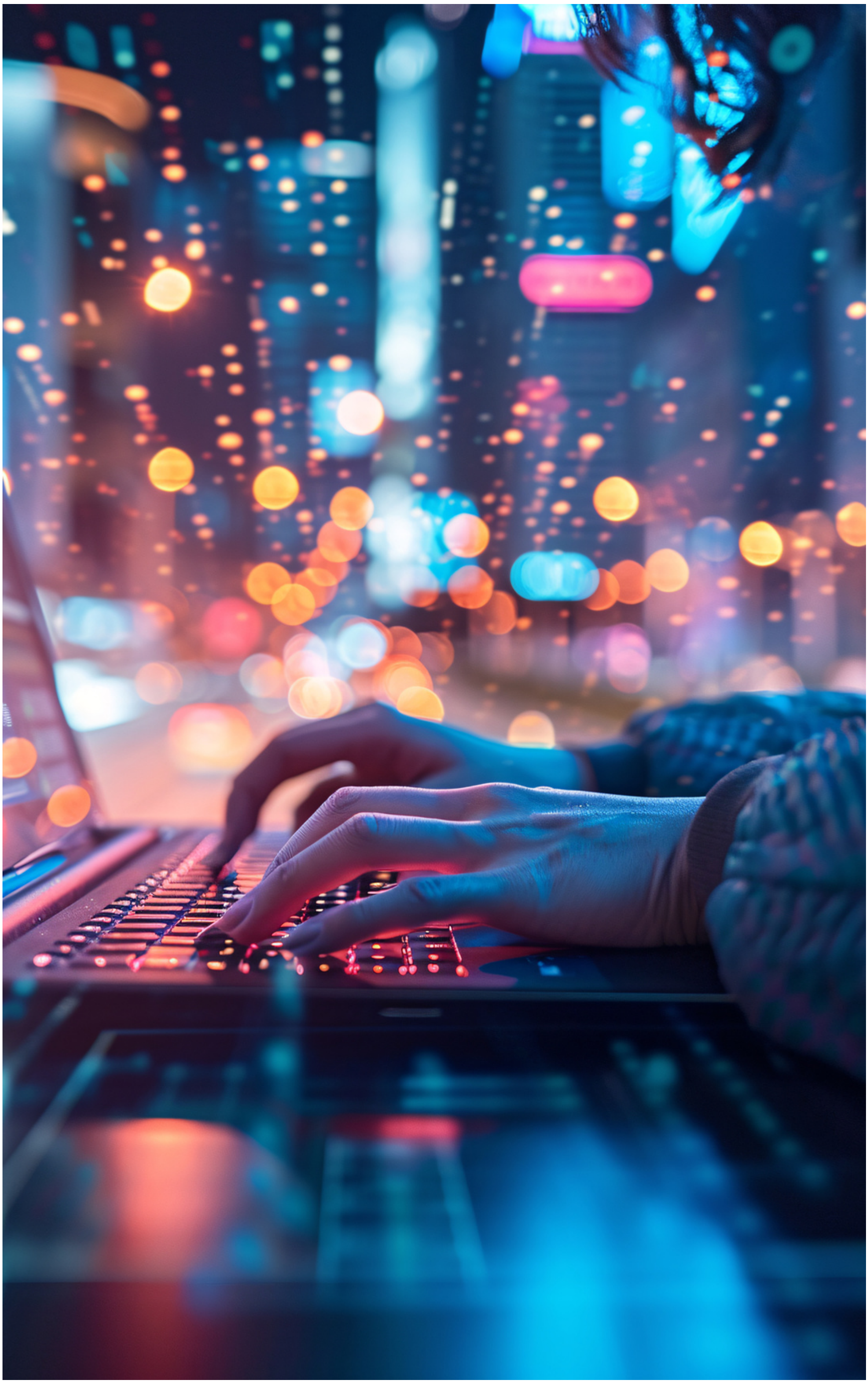
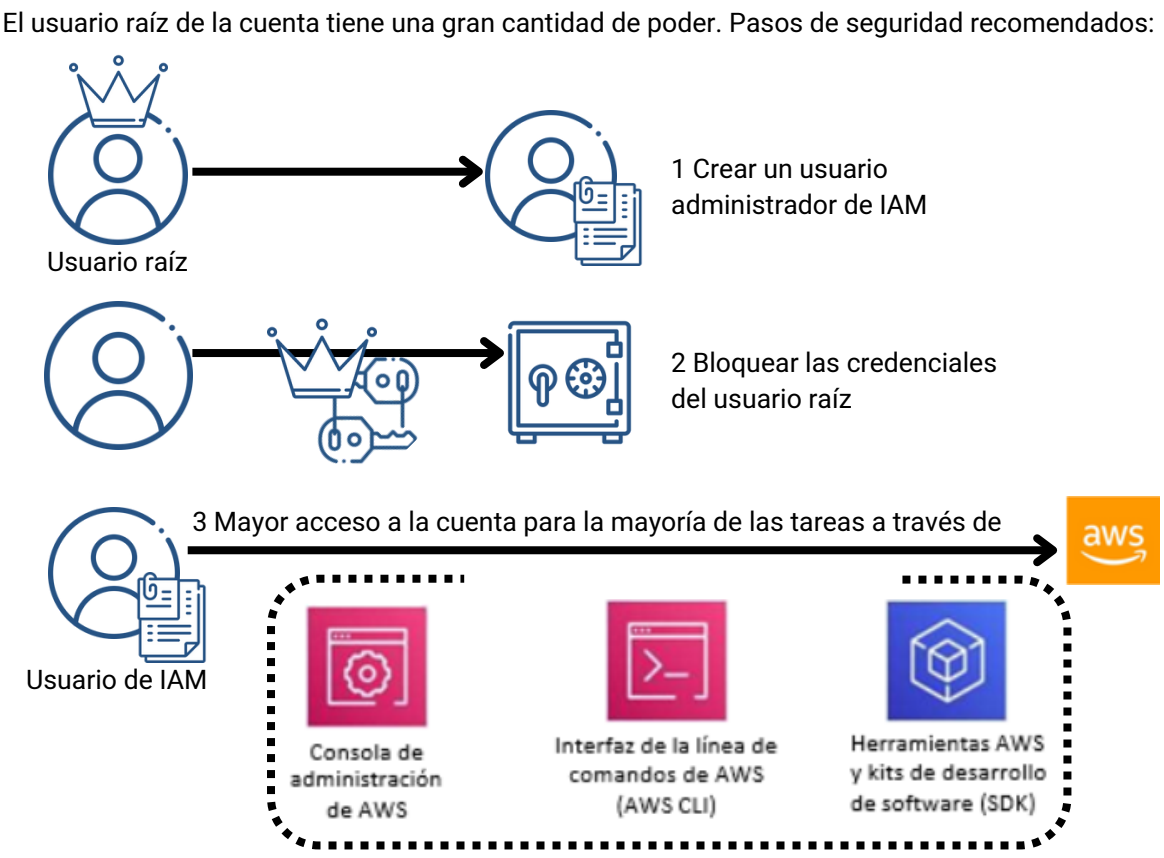
Lección 2

Usuarios de cuentas e IAM



Proteger la cuenta raíz

Cuando crea una cuenta de AWS, comienza con un usuario raíz. Este usuario puede iniciar sesión en la Consola de administración de AWS con la dirección de correo electrónico que se utilizó para crear la cuenta.



El usuario raíz de la cuenta de AWS tiene acceso completo a todos los recursos en la cuenta, incluida la información de facturación, los datos personales en el perfil del usuario y todos los recursos que fueron creados en cualquier servicio de AWS de la cuenta. No puede controlar los privilegios de las credenciales de usuario raíz de la cuenta de AWS.

AWS recomienda enfáticamente que no utilice las credenciales del usuario raíz para las interacciones diarias con AWS. En cambio, cree uno o más usuarios de IAM. Guarde las credenciales del usuario raíz en una ubicación segura. Para la mayoría de las tareas de administración y el acceso a cuentas en curso, puede usar las credenciales de usuario de IAM.

AWS Identity and Access Management (AWS IAM)

AWS Identity and Access Management también se conoce como IAM. Es un servicio que permite configurar control de acceso detallado a los recursos de AWS.

IAM habilita las prácticas recomendadas de seguridad al permitirle otorgar credenciales de seguridad únicas a los usuarios y grupos. Estas credenciales especifican a qué interfaces de programación de aplicaciones (API) de servicios de AWS y recursos pueden acceder. IAM es seguro según la configuración predeterminada.

Los usuarios no tienen acceso a los recursos de AWS hasta que se les otorguen permisos explícitamente.

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 otorgar a sus empleados y aplicaciones acceso a la Consola de administración de AWS y a las API de servicios de AWS, utilizando sus sistemas de identidad existentes. AWS admite la federación de sistemas corporativos como Microsoft Active Directory y proveedores de identidad basados en estándares. IAM también admite la autenticación multifactor (MFA).

Si MFA se encuentra habilitado y un usuario de IAM intenta iniciar sesión, se le solicitará un código de autenticación. El código de autenticación se entrega a un dispositivo MFA de AWS. El dispositivo MFA puede ser un dispositivo MFA de hardware. También puede ser un dispositivo MFA virtual al que accede el usuario a través de una aplicación que se ejecuta en el smartphone del usuario como Google Authenticator.

Puede crear cuentas que tengan privilegios similares a los del usuario raíz de la cuenta de AWS. Sin embargo, es mejor crear cuentas administrativas que otorguen solo los permisos necesarios. Siga el principio de mínimo privilegio. Por ejemplo, pregúntese si su administrador de base de datos (DBA) debería poder aprovisionar instancias de EC2. Si la respuesta es no, entonces aprovisione las cuentas en consecuencia.

Componentes de IAM: revisión

Usuario de IAM

Definido en su cuenta de AWS. Utilice las credenciales para autenticar mediante programación o a través de la Consola de administración de AWS.

Grupo de IAM

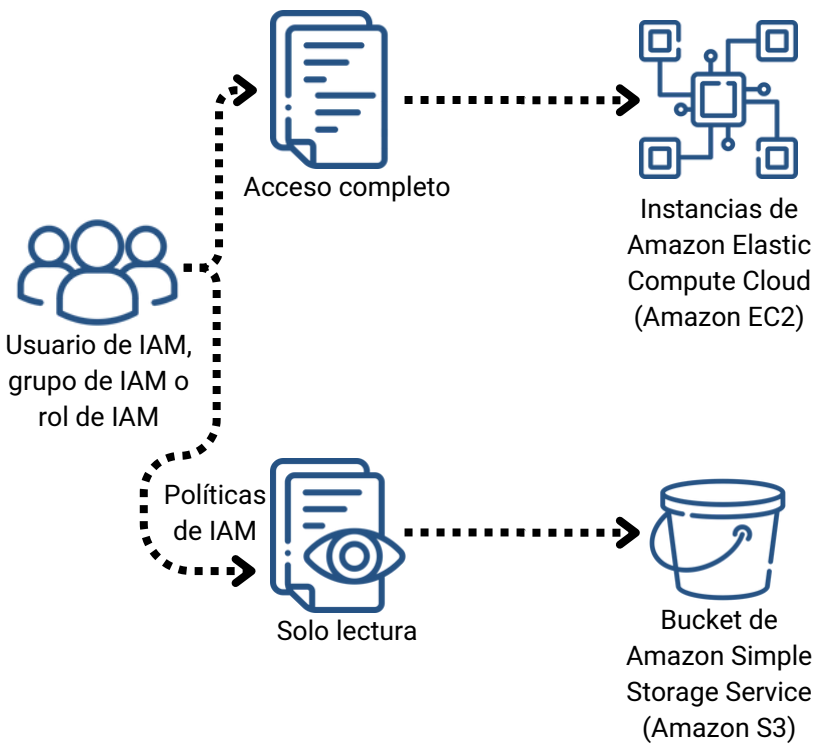
Un conjunto de usuarios de IAM a los que se les otorga una autorización idéntica.

Política de IAM

Define a qué recursos se puede acceder y el nivel de acceso a cada uno de estos recursos.

Rol de IAM

Mecanismos para otorgar acceso temporal para realizar solicitudes de servicios de AWS. Que puede ser asumido por una persona, aplicación o servicio.



Para comprender cómo utilizar IAM para proteger su cuenta de AWS, es importante entender el rol y la función de cada uno de los cuatro componentes de IAM.

Un usuario de IAM es una persona o aplicación que está definida en una cuenta de AWS y que debe realizar llamadas API a productos de AWS. Cada usuario debe tener un nombre único (sin espacios en el nombre) dentro de la cuenta de AWS y un conjunto de credenciales de seguridad que no se comparte con otros usuarios. Estas credenciales son diferentes de las credenciales de seguridad del usuario raíz de la cuenta de AWS. Cada usuario está definido en una y solo una cuenta de AWS.

Un grupo de IAM es un conjunto de usuarios de IAM. Puede utilizar grupos de IAM para simplificar la forma de especificar y administrar permisos para varios usuarios.

Una política de IAM es un documento que define permisos para determinar qué pueden y no pueden hacer los usuarios en la cuenta de AWS.

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

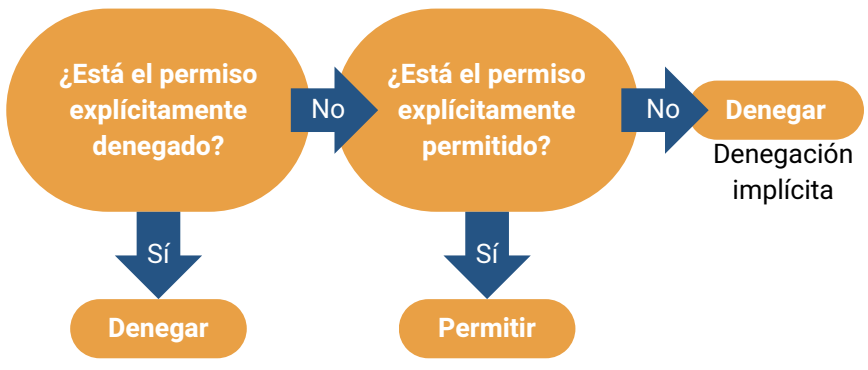
Premios de IAM

Los permisos se especifican en una política de IAM:

- Un documento tiene formato JavaScript Object Notation (JSON)
- Define qué recursos y operaciones están permitidas
- Práctica recomendada: siga el principio de mínimo privilegio
- Existen dos tipos de políticas:
  - Basada en la identidad: adjuntar a una entidad principal de IAM
  - Basada en recursos: adjuntar un recurso de AWS

Política de IAM

Cómo IAM determina los permisos en el momento de la solicitud:

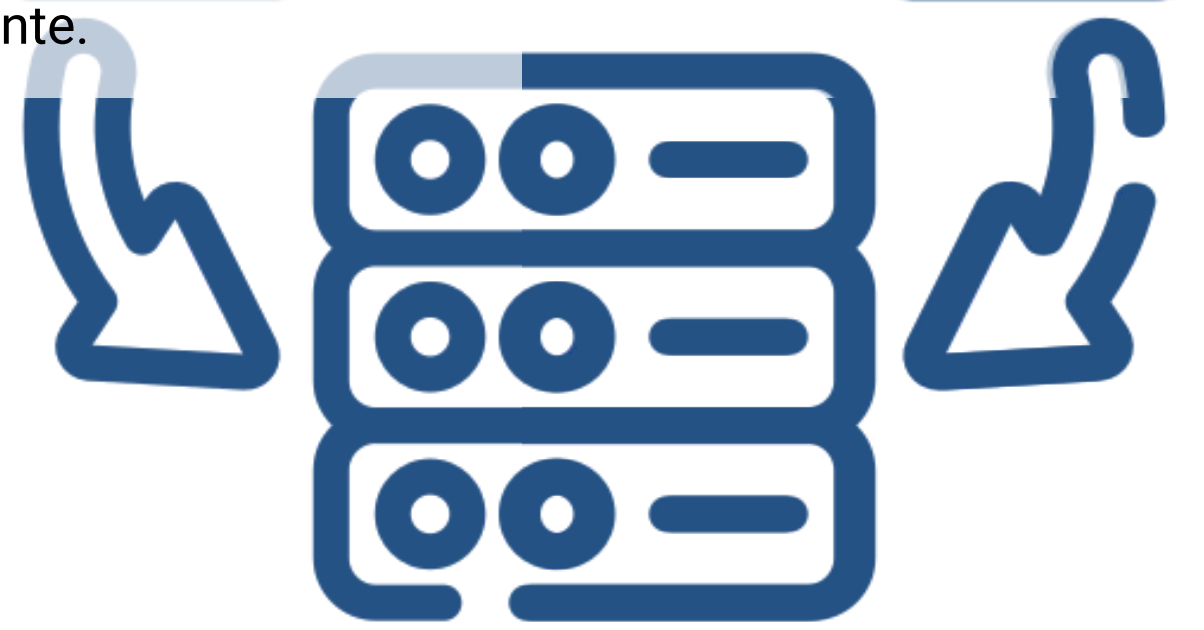


En IAM, los permisos se definen en los documentos de políticas de IAM. Las políticas le permiten ajustar los privilegios que se otorgan a las entidades principales. Las entidades principales de ejemplo son los usuarios de IAM, roles de IAM u otros servicios de AWS.

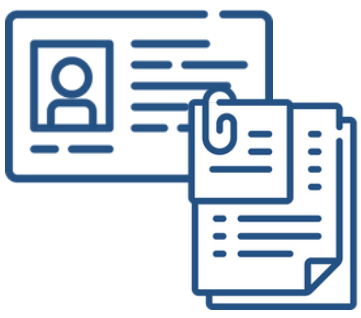
Cuando IAM determina si se autoriza un permiso, primero verifica la existencia de alguna política de denegación explícita aplicable. Si no existe una denegación explícita, comprueba si existe alguna política de permiso explícito. Si no existe una política de denegación explícita o de permiso explícito, IAM vuelve al valor predeterminado y deniega el acceso. Este proceso se denomina denegación implícita. Al usuario se le permitirá realizar la acción sólo si la acción solicitada no se deniega explícitamente y se permite explícitamente.

Cuando se desarrollan políticas de IAM, puede resultar difícil determinar si se otorgará acceso a un recurso a una entidad de IAM. El Simulador de políticas de IAM es una herramienta útil para probar y solucionar problemas de políticas de IAM.

Las políticas se almacenan como documentos con notación de objetos JavaScript (JSON). Se adjuntan a las entidades principales como políticas basadas en la identidad, o a recursos como políticas basadas en recursos.

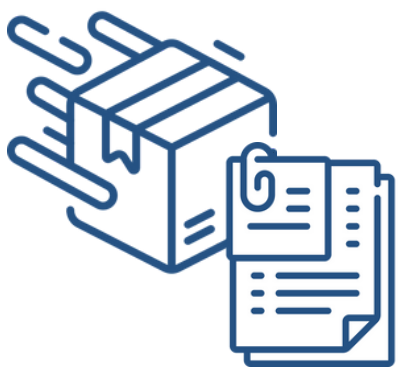


Políticas basadas en la identidad frente a políticas basadas en recursos



Políticas basadas en identidad

- Adjunta a un usuario, grupo o rol
- Tipos de política
  - Administradas por AWS
  - Administradas por el cliente
  - Insertadas

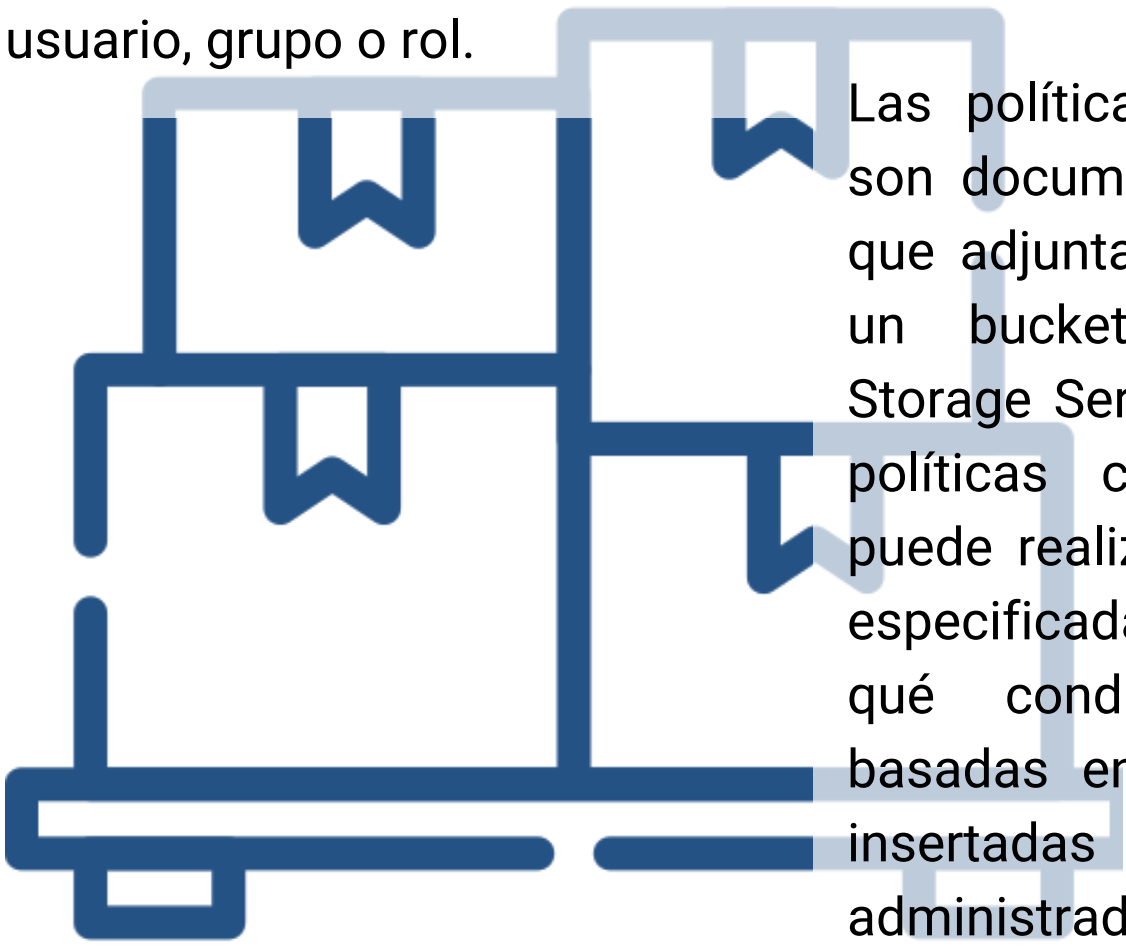


Políticas basadas en recursos

- Adjunta a recursos de AWS
  - Ejemplo: adjuntar a un bucket de Amazon S3
- Siempre una política insertada

Las políticas basadas en la identidad son políticas de permisos que puede adjuntar a una entidad principal (o identidad), tal como 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 la identidad pueden clasificarse a su vez como administradas por AWS, administradas por el cliente o insertadas. Las políticas administradas por AWS son creadas y administradas por AWS y puede adjuntarlas a varios usuarios, grupos y roles en su cuenta de AWS. Si es nuevo en el uso de las políticas, le recomendamos que comience utilizando las políticas administradas por AWS. Las políticas administradas por el cliente son aquellas que usted crea y administra en su cuenta de AWS. Las políticas administradas por el cliente proporcionan un control más preciso sobre sus políticas que las políticas administradas por AWS. Puede crear y editar una política de IAM en el editor visual o al crear un documento de política en formato JSON directamente. Las políticas insertadas son políticas que usted crea y administra, y que están insertadas directamente en un único usuario, grupo o rol.



Las políticas basadas en recursos son documentos de políticas JSON que adjunta a un recurso, tal como un bucket de Amazon Simple Storage Service (Amazon S3). Estas políticas controlan qué acciones puede realizar una entidad principal especificada en dicho recurso y en qué condiciones. Las políticas basadas en recursos son políticas insertadas y no hay políticas administradas basadas en recursos.

Estructura del documento de política de IAM

```
{
   "Version": "2012-10-17",
   "Statement":[{
      "Effect": "effect",
      "Action": "action",
      "Resource": "arn",
      "Condition":{
         "condition":{
            "key": "value"
         }
      }
   }]
}
```

- Efecto: el efecto puede ser permitir o denegar
- Acción: tipo de acceso que se permite o deniega
  "Action": "s3:GetObject"
- Recurso: recursos sobre los que actuará la acción
  "Resource": "arn:aws:sqs:us-west-2:123456789012:queue1"
- Condición: condiciones que deben cumplirse para que se aplique la regla
  "Condition" : {
    "StringEquals": {
      "aws:username" : "johndoe"
    }
  }

Las políticas de IAM se almacenan en AWS como documentos JSON. Las políticas basadas en la identidad son documentos de políticas que adjunta a un usuario o rol. Las políticas basadas en recursos son documentos de políticas que adjunta a un recurso. Un documento de política incluye uno o más enunciados individuales. Cada enunciado incluye información sobre un único permiso. Si una política incluye varios enunciados, AWS aplica un OR lógico entre enunciados cuando los evalúa.

Los siguientes son elementos comunes que se encuentran en un documento de políticas de IAM:

- Versión: especifique la versión del idioma de la política que desea utilizar. Como práctica recomendada, utilice la última versión del 17-10-2012.
- Enunciado: utilice este elemento de la política principal como un contenedor para los siguientes elementos. Puede incluir más de un enunciado en una política.
- Efecto: utilice Allow (Permitir) o Deny (Denegar) para indicar si la política permite o deniega el acceso.
- Entidad principal: si crea una política basada en recursos, debe indicar la cuenta, el usuario, el rol o el usuario federado al que desea permitir o denegar el acceso. Si va a crear una política de permisos de IAM para adjuntarla a un usuario o un rol, no puede incluir este elemento. La entidad principal está implícita como ese usuario o rol.
- Acción: incluye una lista de acciones que la política permite o deniega.
- Recurso: si crea una política de permisos de IAM, debe especificar una lista de recursos a los que se aplican las acciones. Si crea una política basada en recursos, este elemento es opcional.
- Condición (Opcional): especifica las circunstancias en las cuales la política otorga permisos.

ARN y comodines

- Los recursos se identifican usando el formato Amazon Resource Name (ARN)
  - Sintaxis: arn:partition:service:region:account:resource
  - Ejemplo: “Resource”: “arn:aws:iam: :123456789012:user/mmajor”
- Puede utilizar un comodín (*) para brindar acceso a todas las acciones para un servicio específico de AWS.
  - Ejemplos:
    - “Action”: “s3:*”
    - “Action”: “iam:*AccessKey*”

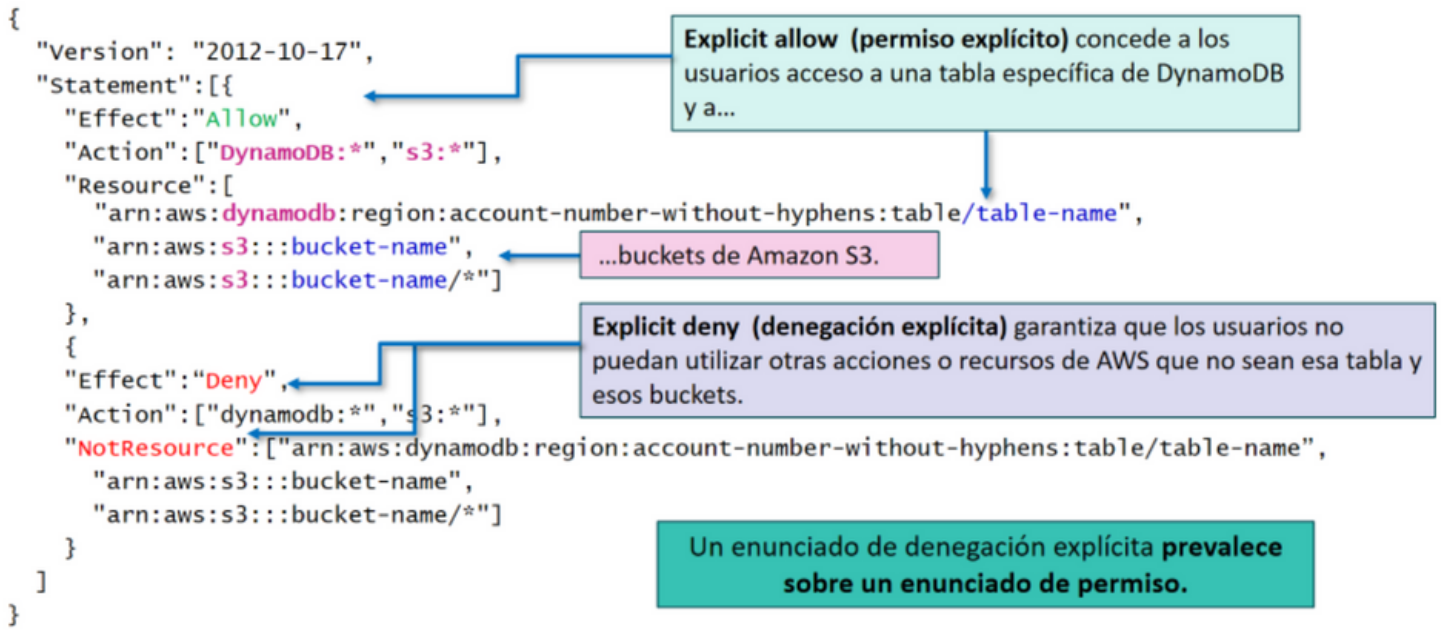
Para las políticas basadas en la identidad (permisos de IAM), debe especificar una lista de recursos a los que se aplican las acciones. El elemento Resource especifica el objeto o los objetos que cubre el enunciado. Los enunciados deben incluir un elemento Resource o NotResource.

La mayoría de los recursos tienen un nombre descriptivo (por ejemplo un usuario llamado Bobo un grupo llamadoDesarrolladores). Sin embargo, el lenguaje de la política de permisos requiere que especifique el recurso o recursos a través del siguiente formato de Amazon Resource Name (ARN).

Cada servicio tiene su propio conjunto de recursos. Aunque siempre utiliza un ARN para especificar un recurso, los detalles del ARN de un recurso dependen del servicio y del recurso. Para obtener información sobre cómo especificar un recurso, consulte la documentación del servicio para cuyos recursos está escribiendo un enunciado.

También puede utilizar comodines en documentos de políticas de IAM, como en ARN o en Acciones. Puede utilizar el carácter comodín (*). Un asterisco (*) representa cualquier combinación de cero o más caracteres. Por ejemplo, un valor de “Acción” de "s3:*" se aplica a todas las acciones S3. También puede utilizar comodines (*) como parte del nombre de la acción. Por ejemplo, el valor de la ”Acción” de "iam:*AccessKey*" se aplica a todas las acciones de IAM que incluyen la cadena AccessKey, incluidas CreateAccessKey, DeleteAccessKey, ListAccessKeys, y UpdateAccessKey.

Ejemplo de política de IAM



Como se mencionó previamente, los documentos de políticas de IAM están escritos en JSON.

Esta política de IAM de ejemplo otorga acceso de usuario solo a los siguientes recursos:

- La tabla de Amazon DynamoDB cuyo nombre está representado por table-name.

El bucket de S3 de la cuenta de AWS, cuyo nombre está representado porbucket-namey todos los objetos que contiene.

La política de IAM también incluye un elemento de denegación explícita ("Effect":"Deny"). El elemento NotResource ayuda a garantizar que los usuarios no puedan usar ninguna acción o recurso de DynamoDB o S3, salvo los especificados en la política. Este es el caso aunque se hayan concedido permisos en otra política. Un enunciado de denegación explícita prevalece sobre un enunciado de permiso.

Actividad: análisis de las políticas de IAM

En esta actividad dirigida por el instructor, se presentarán ejemplos de políticas de IAM. Para cada política, se le harán preguntas acerca de si la política permite o deniega acciones particulares. El instructor lo dirigirá a un análisis de cada pregunta y revelará las respuestas correctas una a la vez.

Considere esta política de IAM y luego responda las preguntas.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:Get*",
            "iam:List*"
        ],
        "Resource": "*"
    }
}
```

1. ¿A qué servicio de AWS le otorga acceso esta política?
2. ¿Le permite crear un usuario, grupo, política o rol de IAM?
3. Vaya a https://docs.aws.amazon.com/IAM/latest/UserGuide/ y en el panel de navegación izquierdo expanda Reference > Policy Reference > Actions, Resources, and Condition Keys. Seleccione Identity and Access Management. Desplácese hasta la lista Actions Defined by Identity And Access Management.

Nombre al menos tres acciones específicas que permite la acción iam:Get*

1. El servicio de IAM.
2. No. El acceso está limitado a solicitudes get y list. Otorga efectivamente permisos de solo lectura.
3. iam:Get* permite muchas acciones específicas, incluidas GetGroup, GetPolicy, GetRole, y otras.

Mire el documento de política de IAM de ejemplo. El instructor ahora le hará una serie de preguntas para evaluar si comprende qué acciones permitirá y denegará esta política.

Considere esta política de IAM y luego responda las preguntas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ec2:TerminateInstances"],
            "Resource": ["*"]
        },
        {
            "Effect": "Deny",
            "Action": ["ec2:TerminateInstances"],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            },
            "Resource": ["*"]
        }
    ]
}
```

1. ¿Le permite la política terminar cualquier instancia de EC2 en cualquier momento sin condiciones?
2. ¿Se le permite hacer la llamada de terminación desde cualquier lugar?
3. ¿Puede terminar instancias si realiza la llamada desde un servidor que tiene asignada una dirección IP de 192.0.2.243?

1. No. El primer objeto del enunciado lo permite. Sin embargo, el segundo objeto del enunciado aplica una condición.
2. No. Solo puede realizar la solicitud desde uno de los dos rangos de direcciones IP que se especifican en aws:SourceIp
3. Sí, porque el rango de direcciones IP de enrutamiento entre dominios sin clase (CIDR) 192.0.2.0/24 incluye las direcciones IP 192.0.2.0 a 192.0.2.255. Se puede utilizar un recurso como la herramienta CIDR to IP Range para calcular el rango de un bloque de CIDR.

Analice el segundo ejemplo de archivo de política de IAM. La primera parte muestra Effect: Allow and Action ec2:TerminateInstance for resource. La segunda parte muestra Effect Deny for action ec2:TerminateInstances with condition NotIpAddress aws:SourceIp 192.0.2.0/24 and 203.0.113.0/24 for resource. El instructor ahora le volverá a hacer una serie de preguntas para evaluar si comprende qué acciones permitirá y denegará esta política.

Para accesibilidad: documento de política de ejemplo en formato JSON. Muestra una sección del enunciado con dos partes. La primera parte muestra Effect:Allow and Action EC2:TerminateInstance for resource *. La segunda parte muestra effect Deny for action EC2:TerminateInstances with condition NotIpAddress aws:SourceIp 192.0.2.0/24 and 203.0.113.0/24 for resource *. **Fin de la descripción de accesibilidad.**

Considere esta política de IAM
y luego responda las preguntas.

```
{
   "Version": "2012-10-17",
   "Statement":[{
      "Condition": {
        "StringNotEquals": {
           "ec2:InstanceType": [
              "t2.micro",
              "t2.small"
           ]
        }
      },
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Action": [
         "ec2:RunInstances",
         "ec2:StartInstances"
      ],
     "Effect": "Deny"
   }
]
```

1 ¿Qué acciones permite la política?
2 Supongamos que la política incluye un objeto de enunciado adicional, como este ejemplo:

"Effect": "Allow",
"Action": "ec2:*",
"Resource": "*"
}

¿Cómo restringiría la política el acceso que le otorga este enunciado adicional?
3 Si la política incluyera tanto el enunciado de la izquierda como el enunciado de la pregunta 2, ¿podría terminar una instancia m3.xlarge que existía en la cuenta?

1. No le permite hacer nada (el efecto es Denegar)
2. Tendría acceso completo al servicio Amazon EC2. Sin embargo, solo se le permitiría lanzar o iniciar instancias EC2 del tipo de instancia t2.micro o t2.small
3. Sí.

Observe el tercer y último ejemplo de documento de política de IAM. El instructor ahora le volverá a hacer una serie de preguntas para evaluar si comprende qué acciones permitirá y denegará esta política.

AWS CloudTrail

Registra y supervisa la actividad del usuario
Proporciona un historial de eventos de la cuenta de AWS

- Acciones realizadas a través de la Consola de administración de AWS, SDK, AWS CLI
- Aumenta la visibilidad de la actividad de sus usuarios y recursos
- Historial de eventos de 90 días proporcionado de forma predeterminada, sin costo

Identificar

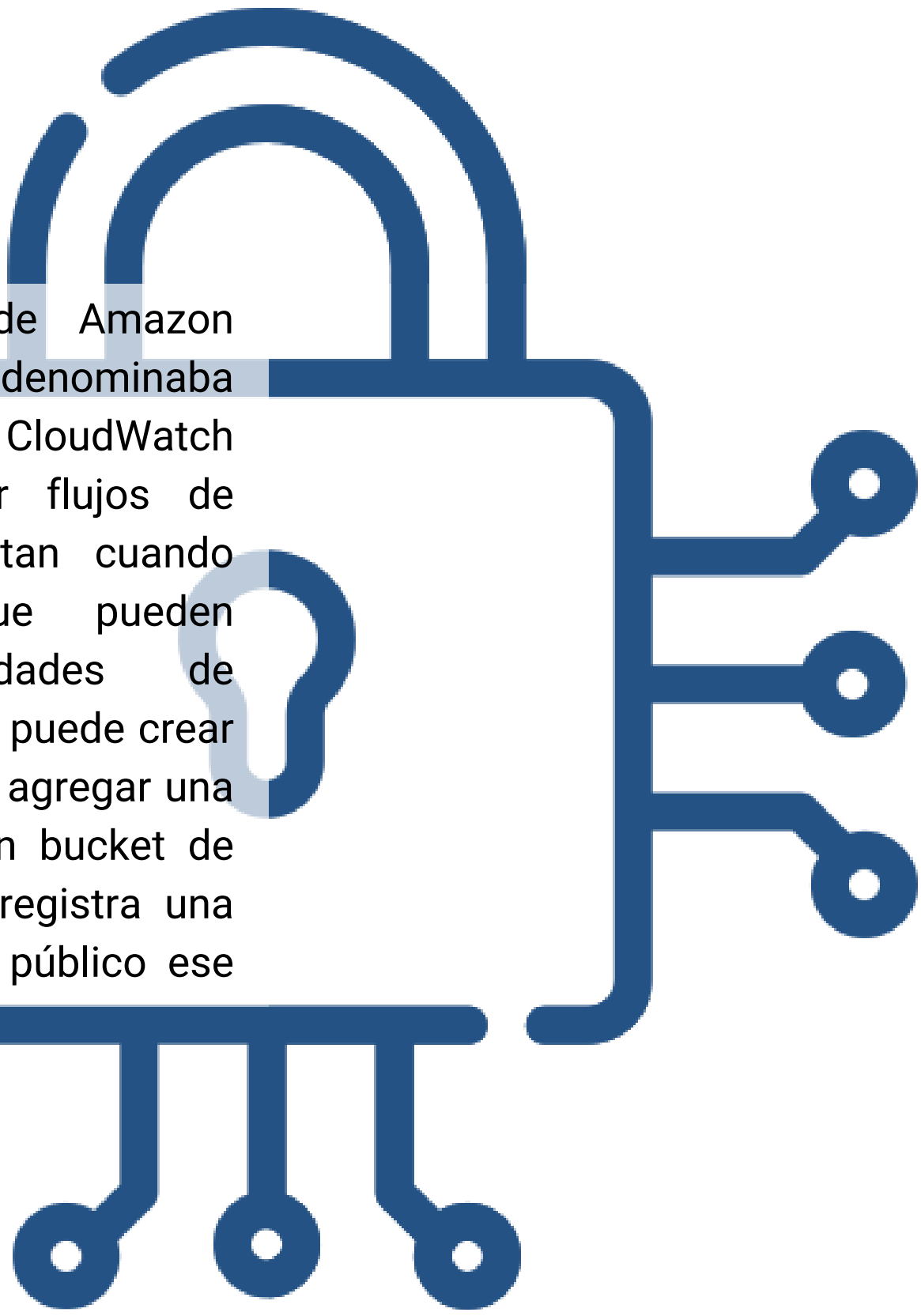
- Quién accedió a su cuenta
- Cuándo y desde dónde
- Qué acción tomaron en un servicio de AWS

Herramienta útil para

- Realizar análisis de la seguridad
- Descubrir qué llamadas fueron bloqueadas (por ejemplo, por políticas de IAM)

AWS CloudTrail es un servicio que permite la gobernanza, el cumplimiento y la auditoría de su cuenta de AWS. Con CloudTrail, puede monitorear de manera continua y retener la actividad de la cuenta que está relacionada con acciones en toda su infraestructura de AWS. Proporciona un historial de eventos de la actividad de la cuenta, incluidas las acciones realizadas a través de la Consola de administración de AWS, los SDK de AWS y las herramientas de línea de comandos. Con este historial de eventos se simplifican el análisis de seguridad, el seguimiento de cambios de recursos y la solución de problemas.

Puede descubrir y solucionar problemas operativos y de seguridad mediante la captura de un historial completo de los cambios que tuvieron lugar en su cuenta de AWS durante un período específico. Puede identificar qué usuarios y cuentas realizaron llamadas a AWS, cuándo se hicieron y cuáles fueron las direcciones IP de origen. CloudTrail le permite rastrear y responder automáticamente a la actividad de la cuenta que amenaza la seguridad de sus recursos de AWS.



Con la integración de Amazon EventBridge (se denominaba anteriormente Amazon CloudWatch Events), puede definir flujos de trabajo que se ejecutan cuando detecta eventos que pueden provocar vulnerabilidades de seguridad. Por ejemplo, puede crear un flujo de trabajo para agregar una política específica a un bucket de S3 cuando CloudTrail registra una llamada API que hace público ese bucket.

CloudTrail registra información importante sobre cada acción, incluido quién realizó la solicitud, los servicios utilizados, las acciones realizadas, los parámetros de las acciones y los elementos de respuesta que devolvió el servicio de AWS. El servicio también ayuda a las organizaciones a cumplir con los requisitos de cumplimiento y auditoría que deben respetar.

Entre los aprendizajes clave de esta lección de esta unidad, se incluyen los siguientes:

- Evite usar el usuario raíz de la cuenta para tareas comunes. En cambio, cree y utilice las credenciales de usuario de IAM.
- Los permisos para acceder a los recursos de la cuenta de AWS se definen en uno o más documentos de la política de IAM.
- Adjuntar políticas de IAM a usuarios, grupos o roles de IAM.
- Cuando IAM determina los permisos, una denegación explícita siempre anulará cualquier enunciado de permiso.
- Es una práctica recomendada seguir el principio de mínimo privilegio cuando conceda acceso a la cuenta.