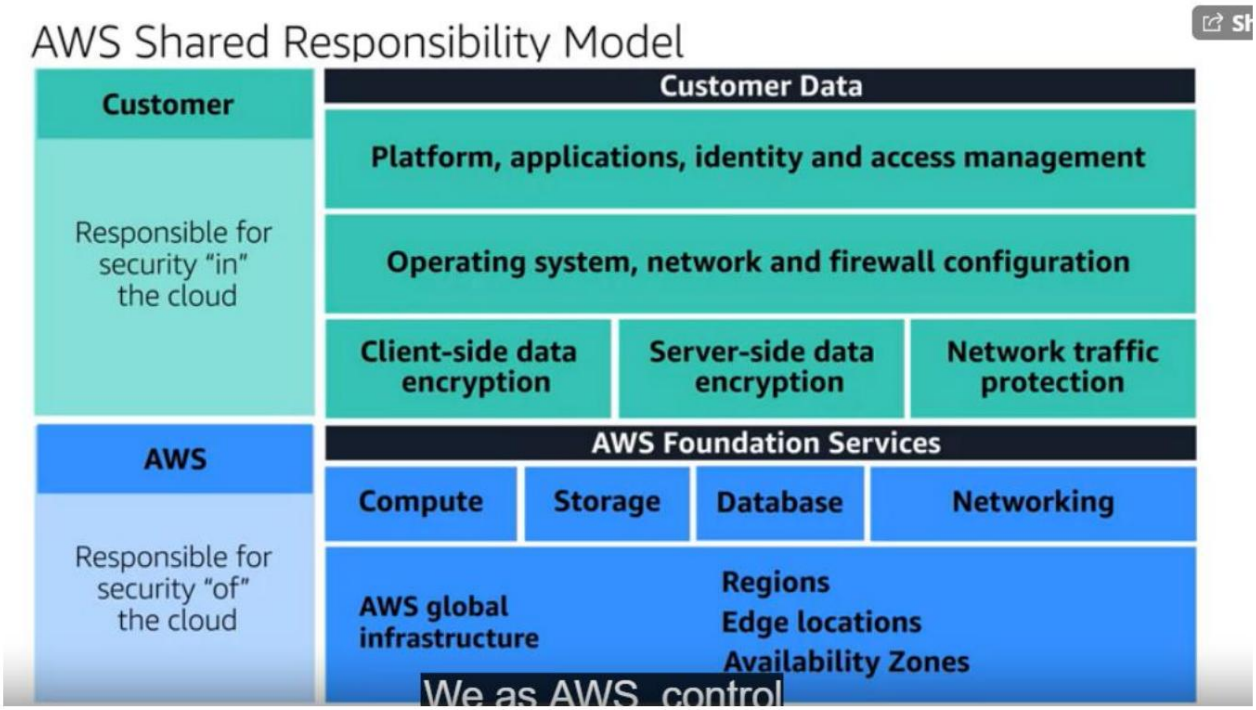
SEGURIDAD DE AWS

salman abdulkarim

https://www.linkedin.com/in/salmanabdulkarim/

Contenido

Modelo de Responsabilidad Compartida



El modelo de responsabilidad compartida de AWS

AWS es responsable de algunas partes de su entorno y usted (el cliente) es responsable de otras partes. Este concepto se conoce como el modelo de responsabilidad compartida.

El modelo de responsabilidad compartida se divide en responsabilidades del cliente (comúnmente denominadas "seguridad en la nube") y responsabilidades de AWS (comúnmente denominadas "seguridad en la nube").

CUSTOMERS			
	CUSTOMER DATA		
	PLATFORM, APPLICATIONS, IDENTITY AND ACCESS MANAGEMENT		
	OPERATING SYSTEMS, NETWORK AND FIREWALL CONFIGURATION		
	CLIENT-SIDE DATA ENCRYPTION	SERVER-SIDE ENCRYPTION	NETWORKING TRAFFIC PROTECTION

AWS				
	SOFTWARE			
	COMPUTE	STORAGE	DATABASE	NETWORKING
	HARDWARE/AWS GLOBAL INFRASTRUCTURE			
	REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS	

Puede pensar en este modelo como algo similar a la división de responsabilidades entre un propietario y un constructor de viviendas. El constructor (AWS) es responsable de construir su casa y asegurarse de que esté sólidamente construida. Como propietario (el cliente), es su responsabilidad asegurar todo en la casa asegurándose de que las puertas estén cerradas y bloqueadas.

Clientes: seguridad en la nube Los clientes
son responsables de la seguridad de todo lo que crean y colocan en la nube de AWS.

Al utilizar los servicios de AWS, usted, el cliente, mantiene un control total sobre su contenido. Usted es responsable de administrar los requisitos de seguridad de su contenido, incluido qué contenido elige almacenar en AWS, qué servicios de AWS utiliza y quién tiene acceso a ese contenido. También controla cómo se otorgan, administran y revocan los derechos de acceso.

Los pasos de seguridad que tome dependerán de factores como los servicios que utilice, la complejidad de sus sistemas y las necesidades operativas y de seguridad específicas de su empresa. Los pasos incluyen seleccionar, configurar y parchear los sistemas operativos que se ejecutarán en las instancias de Amazon EC2, configurar grupos de seguridad y administrar cuentas de usuario.

AWS: Seguridad de la Nube AWS
es responsable de la seguridad de la nube.

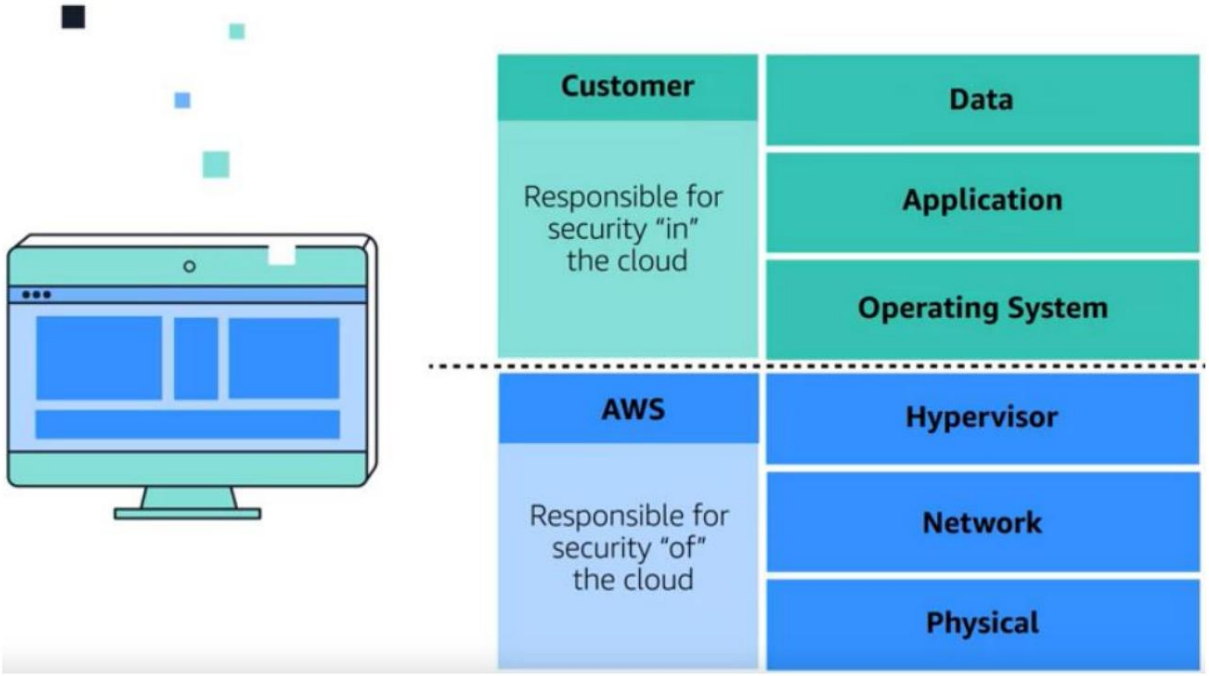
AWS opera, administra y controla los componentes en todas las capas de la infraestructura. Esto incluye áreas como el sistema operativo host, la capa de virtualización e incluso la seguridad física de los centros de datos desde los que operan los servicios.

AWS es responsable de proteger la infraestructura global que ejecuta todos los servicios que se ofrecen en la nube de AWS. Esta infraestructura incluye regiones de AWS, zonas de disponibilidad y ubicaciones de borde.

AWS administra la seguridad de la nube, específicamente la infraestructura física que aloja sus recursos, que incluyen:

- Seguridad física de los centros de datos
- Infraestructura de hardware y software
- Infraestructura de red
- Infraestructura de virtualización

Aunque no puede visitar los centros de datos de AWS para ver esta protección de primera mano, AWS proporciona varios informes de auditores externos. Estos auditores han verificado su cumplimiento con una variedad de estándares y regulaciones de seguridad informática.



Permiso de usuario y acceso

Administración de acceso e identidad de AWS (IAM)

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

IAM le brinda la flexibilidad de configurar el acceso en función de las necesidades operativas y de seguridad específicas de su empresa. Para ello, utilice una combinación de funciones de IAM, que se exploran en detalle en esta lección:

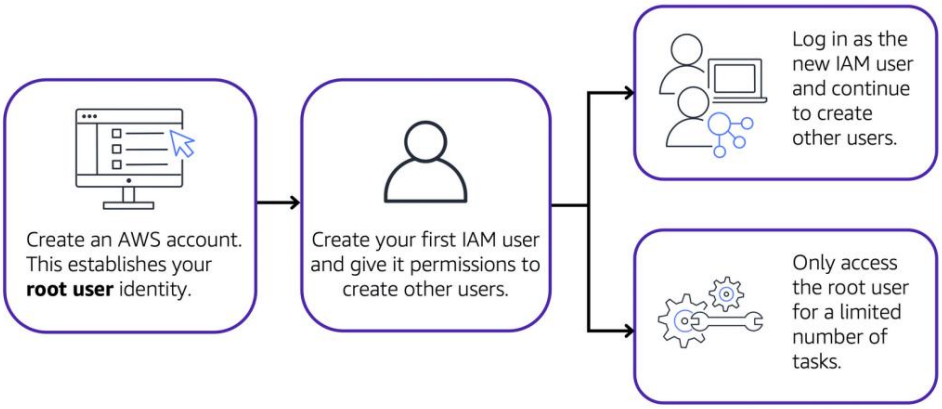
- Usuarios, grupos y roles de IAM
- Políticas de gestión de identidades y accesos
- Autenticación multifactor

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

Usuario raíz de la cuenta de AWS

Cuando crea una cuenta de AWS por primera vez, comienza con una identidad conocida como usuario raíz.

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



Mejores prácticas:

No utilice el usuario root para las tareas cotidianas.

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

Luego, continúe creando otros usuarios de IAM y acceda a esas identidades para realizar tareas regulares en AWS. Solo use el usuario raíz cuando necesite realizar un número limitado de tareas que solo están disponibles para el usuario raíz. Ejemplos de estas tareas incluyen cambiar su dirección de correo electrónico de usuario raíz y cambiar su plan de soporte de AWS.

Usuarios de gestión de identidades y accesos

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. Consiste en 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 lanzar una instancia de Amazon EC2 o crear un depósito de Amazon S3, debe otorgar al usuario de IAM los permisos necesarios.

Mejores prácticas:

Le 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 gestión de identidades y accesos

Una política de IAM es un documento que otorga o deniega 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 depósitos de Amazon S3 dentro de su cuenta de AWS, o solo a un depósito específico.

Práctica recomendada: siga el principio de seguridad de privilegios mínimos 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. Haga esto en lugar de otorgar acceso al empleado a todos los depósitos en su cuenta de AWS.

Ejemplo: política de IAM Este es un ejemplo de cómo funcionan las políticas de IAM. Suponga que el propietario de la cafetería tiene que crear un usuario de IAM para un cajero recién contratado. El cajero necesita acceso a los recibos guardados en un depósito de Amazon S3 con el ID: AWSDOC-EXAMPLE-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 depósito específico: AWSDOC-EXAMPLE-BUCKET. Cuando el propietario adjunte esta póliza a la

usuario de IAM del cajero, permitirá que el cajero vea todos los objetos en el depósito AWSDOC-EXAMPLE-BUCKET.

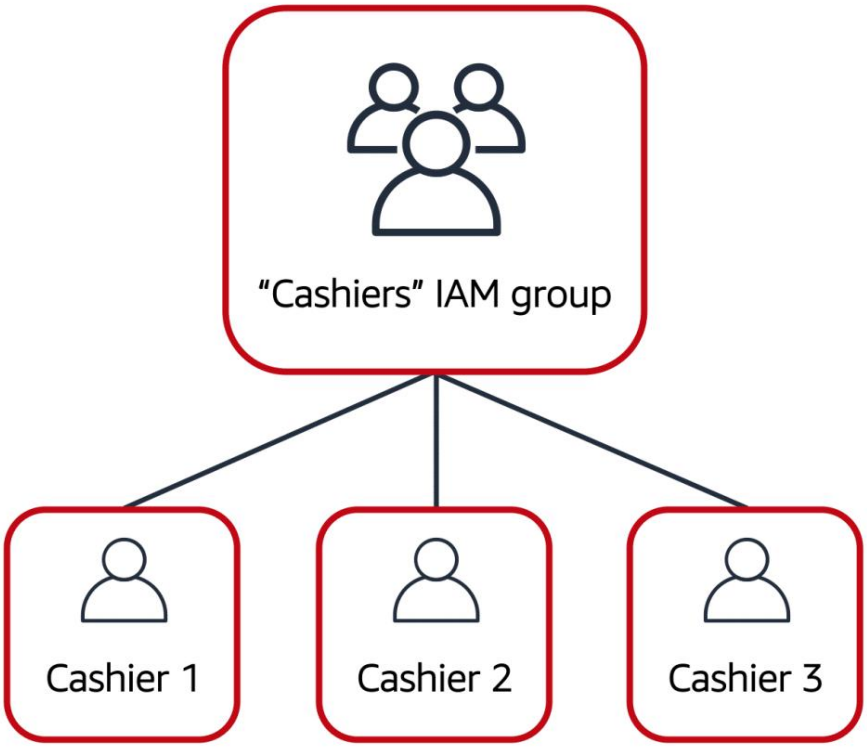
Si el propietario desea que el cajero pueda acceder a otros servicios y realizar otras acciones en AWS, el propietario debe adjuntar políticas adicionales para especificar estos servicios y acciones.

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

Grupos de gestión de identidades y accesos

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 por la política.

He aquí 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 un grupo de IAM de "Cajeros". Luego, 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 trabajo 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 agrega al grupo de IAM "Especialistas en inventario". Esto garantiza que los empleados solo tengan los permisos necesarios para su rol actual.

¿Qué pasa si un empleado de una cafetería no ha cambiado de trabajo de forma permanente, sino que rota a diferentes estaciones de trabajo a lo largo del día? Este empleado puede obtener el acceso que necesita a través de los roles de IAM.

Funciones de gestión de identidades y accesos

En la cafetería, un empleado rota en diferentes estaciones de trabajo a lo largo del día. Dependiendo de la dotación de 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 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, puede tener acceso a una sola 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.

Antes de que un usuario, aplicación o servicio de IAM 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.

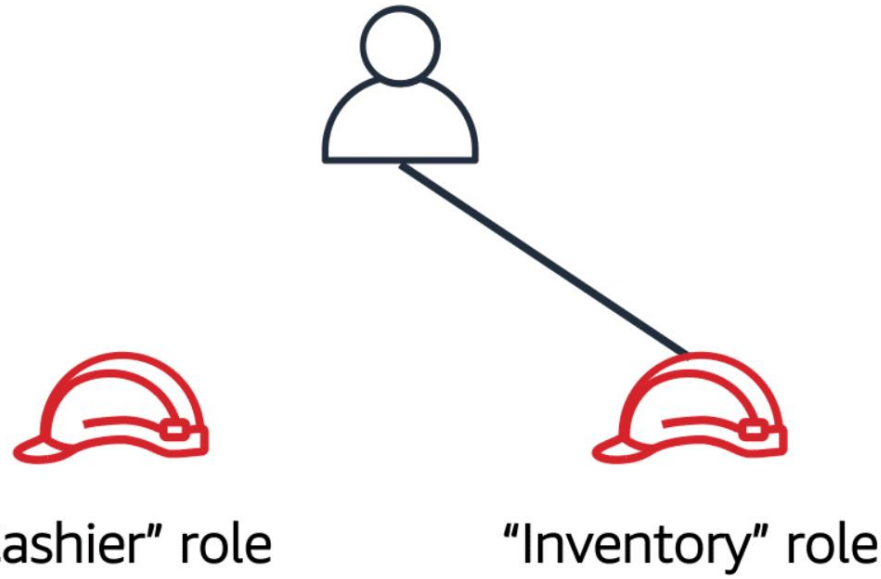
Mejores prácticas:

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

Ejemplo: roles de IAM

Revise un ejemplo de cómo se podrían usar los roles de IAM en la cafetería:

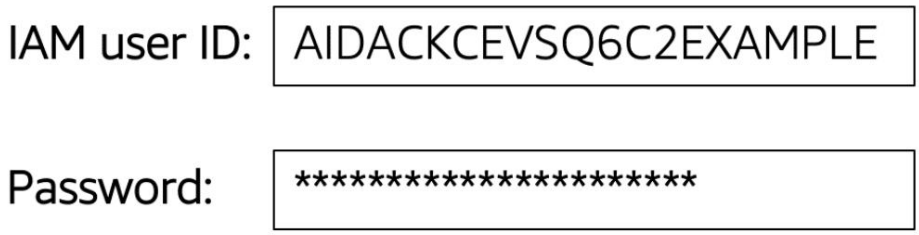
1. Primero, el propietario otorga permisos al empleado para cambiar a un rol para cada estación de trabajo en la cafetería.
2. A continuación, el empleado comienza su día asumiendo el rol de “Cajero”. Esto les otorga acceso al sistema de caja registradora.
3. Más tarde en el día, el empleado necesita actualizar el sistema de inventario. Asumen el rol de "Inventario". Esto otorga al empleado acceso al sistema de inventario y también revoca su acceso al sistema de caja registradora.



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 luego una segunda forma de autenticación, como un código aleatorio enviado a su teléfono. Este es un ejemplo de autenticación multifactor.

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



1. Primero, cuando un usuario inicia sesión en un sitio web de AWS, ingresa su ID de usuario y contraseña de IAM.
2. A continuación, se solicita al usuario una respuesta de autenticación de su dispositivo AWS MFA.
   Este dispositivo podría ser una clave de seguridad de hardware, un dispositivo de hardware o una aplicación MFA en un dispositivo como un teléfono inteligente.
3. Cuando el usuario se ha autenticado con éxito, puede acceder a la solicitud
   Servicios o recursos de AWS.

Puede habilitar MFA para el usuario raíz y los usuarios de IAM. Como práctica recomendada, habilite MFA para el usuario raíz y todos los usuarios de IAM en su cuenta. Al hacer esto, puede mantener su cuenta de AWS a salvo de accesos no autorizados.
acceso.

Organizaciones de AWS

Organizaciones de AWS

Suponga que su empresa tiene varias cuentas de AWS. Puede utilizar AWS Organizations para consolidar y administrar varias cuentas de AWS dentro de una ubicación central.

Cuando crea una organización, AWS Organizations crea automáticamente una raíz, que es el contenedor principal para todas las cuentas de su organización.

En AWS Organizations, puede controlar de forma centralizada los permisos para las cuentas de su organización mediante políticas de control de servicios (SCP). Las SCP le permiten imponer restricciones a los servicios, recursos y acciones de API individuales de AWS a los que pueden acceder los usuarios y las funciones de cada cuenta.

La facturación consolidada es otra característica de AWS Organizations. Aprenderá sobre la facturación consolidada en un módulo posterior.

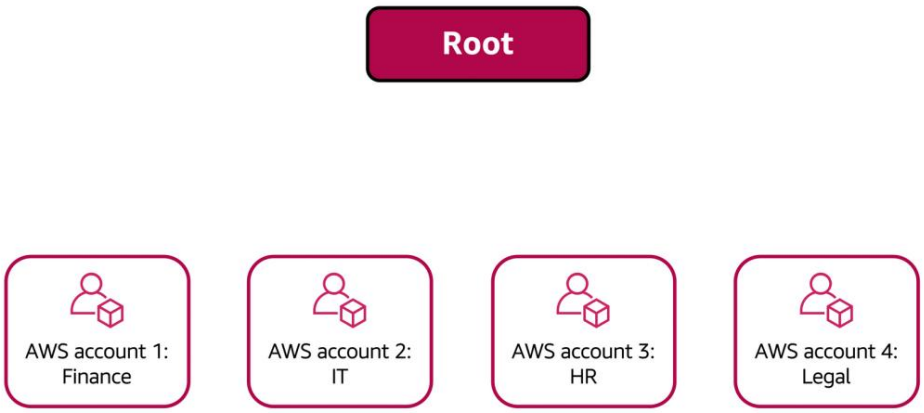
Unidades organizativas En

AWS Organizations, puede agrupar cuentas en unidades organizativas (OU) para facilitar la administración de cuentas con requisitos comerciales o de seguridad similares. Cuando aplica una política a una unidad organizativa, todas las cuentas de la unidad organizativa heredan automáticamente los permisos especificados en la política.

Al organizar cuentas separadas en unidades organizativas, puede aislar más fácilmente las cargas de trabajo o las aplicaciones que tienen requisitos de seguridad específicos. Por ejemplo, si su empresa tiene cuentas que solo pueden acceder a los servicios de AWS que cumplen determinados requisitos reglamentarios, puede poner estas cuentas en una unidad organizativa. Entonces, puede adjuntar una política a la unidad organizativa que bloquee el acceso a todos los demás servicios de AWS que no cumplan los requisitos reglamentarios.

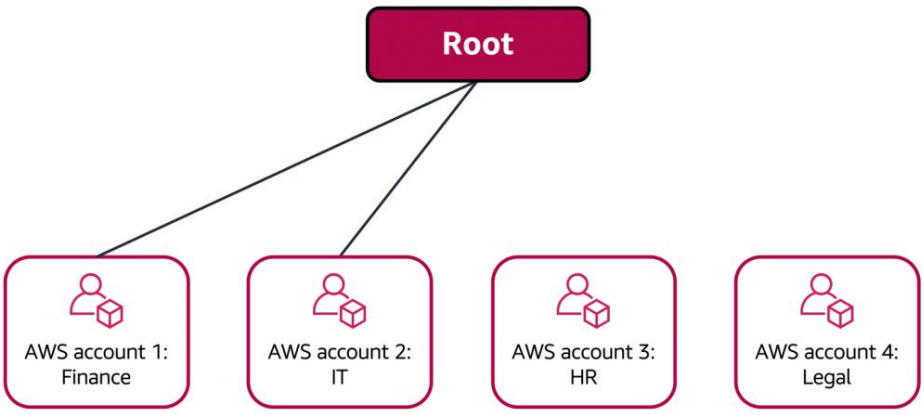
Ejemplo: organizaciones de AWS

Revise un ejemplo de cómo una empresa podría utilizar AWS Organizations:

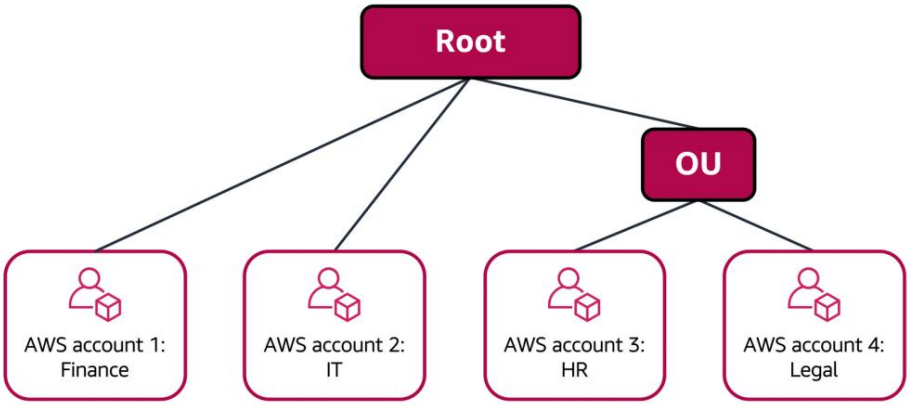


Imagine que su empresa tiene cuentas de AWS separadas para los departamentos de finanzas, tecnología de la información (TI), recursos humanos (HR) y legal. Decide consolidar estas cuentas en una sola organización para poder administrarlas desde una ubicación central. Al crear la organización,
esto establece la raíz.

Al diseñar su organización, tiene en cuenta las necesidades empresariales, de seguridad y reglamentarias de cada departamento. Utilice esta información para decidir qué departamentos se agrupan en unidades organizativas.



Los departamentos de finanzas y TI tienen requisitos que no se superponen con los de ningún otro departamento. Trae estas cuentas a su organización para aprovechar los beneficios, como la facturación consolidada, pero no las coloca en ninguna unidad organizativa.



Los departamentos de recursos humanos y legal necesitan acceder a los mismos servicios y recursos de AWS, por lo que los coloca juntos en una unidad organizativa. Ubicarlos en una unidad organizativa le permite adjuntar políticas que se aplican a las cuentas de AWS de los departamentos de recursos humanos y legal.

Aunque haya colocado estas cuentas en unidades organizativas, puede continuar brindando acceso a usuarios, grupos y roles a través de IAM.

Al agrupar sus cuentas en unidades organizativas, puede brindarles acceso más fácilmente a los servicios y recursos que necesitan. También evita que accedan a cualquier servicio o recurso que no necesiten.

En AWS Organizations, puede aplicar políticas de control de servicios (SCP) a la raíz de la organización, una cuenta de miembro individual o una unidad organizativa. Una SCP afecta a todos los usuarios, grupos y roles de IAM dentro de una cuenta, incluido el usuario raíz de la cuenta de AWS.

Puede aplicar políticas de IAM a usuarios, grupos o roles de IAM. No puede aplicar una política de IAM a AWS usuario raíz de la cuenta

Cumplimiento

Artefacto de AWS

Dependiendo de la industria de su empresa, es posible que deba mantener estándares específicos. Una auditoría o inspección garantizará que la empresa haya cumplido con esos estándares.

AWS Artifact es un servicio que brinda acceso a pedido a informes de cumplimiento y seguridad de AWS y acuerdos en línea selectos. AWS Artifact consta de dos secciones principales: Acuerdos de AWS Artifact e Informes de AWS Artifact.

Acuerdos de AWS Artifact Suponga que su empresa necesita firmar un acuerdo con AWS con respecto al uso de ciertos tipos de información a través de los servicios de AWS. Puede hacerlo a través de acuerdos de artefactos de AWS.

En los acuerdos de AWS Artifact, puede revisar, aceptar y administrar acuerdos para una cuenta individual y para todas sus cuentas en AWS Organizations. Se ofrecen diferentes tipos de acuerdos para abordar las necesidades de los clientes que están sujetos a regulaciones específicas, como la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA).

Informes de AWS Artifact A continuación, suponga que un miembro del equipo de desarrollo de su empresa está creando una aplicación y necesita más información sobre su responsabilidad de cumplir con ciertos estándares normativos. Puede recomendarles que accedan a esta información en AWS Artifact Reports.

AWS Artifact Reports proporciona informes de cumplimiento de auditores externos. Estos auditores han probado y verificado que AWS cumple con una variedad de estándares y regulaciones de seguridad globales, regionales y específicos de la industria. AWS Artifact Reports permanece actualizado con los últimos informes publicados. Puede proporcionar los artefactos de auditoría de AWS a sus auditores o reguladores como prueba de los controles de seguridad de AWS.

Los siguientes son algunos de los informes y normas de cumplimiento que puede encontrar en AWS Artifact.
Cada informe incluye una descripción de su contenido y el período de informe para el cual el documento es válido.

Centro de Cumplimiento del Cliente

El Centro de cumplimiento del cliente contiene recursos para ayudarlo a obtener más información sobre el cumplimiento de AWS.

En el Centro de Cumplimiento de Clientes, puede leer historias de cumplimiento de clientes para descubrir cómo las empresas en industrias reguladas han resuelto varios desafíos de cumplimiento, gobierno y auditoría.

También puede acceder a documentos técnicos y documentación de cumplimiento sobre temas como:

- Respuestas de AWS a preguntas clave sobre cumplimiento
- Una descripción general del riesgo y el cumplimiento de AWS
- Una lista de verificación de seguridad de auditoría

Además, el Centro de Cumplimiento del Cliente incluye una ruta de aprendizaje para auditores. Esta ruta de aprendizaje está diseñada para personas en roles de auditoría, cumplimiento y legales que desean obtener más información sobre cómo sus operaciones internas pueden demostrar el cumplimiento mediante la nube de AWS.

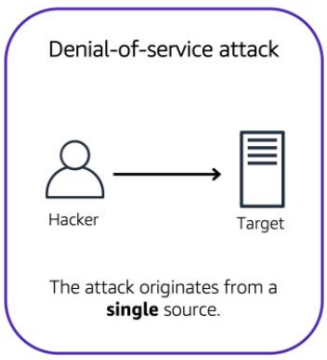
Ataques de denegación de servicio

Los clientes pueden llamar a la cafetería para hacer sus pedidos. Después de atender cada llamada, un cajero toma el pedido y se lo entrega al barista.

Sin embargo, supongamos que un bromista llama varias veces para hacer pedidos, pero nunca recoge sus bebidas. Esto hace que el cajero no esté disponible para atender las llamadas de otros clientes. La cafetería puede intentar detener las solicitudes falsas bloqueando el número de teléfono que está usando el bromista.

En este escenario, las acciones del bromista son similares a un ataque de denegación de servicio Denegación de servicio
Ataques

Un ataque de denegación de servicio (DoS) es un intento deliberado de hacer que un sitio web o una aplicación no estén disponibles a los usuarios

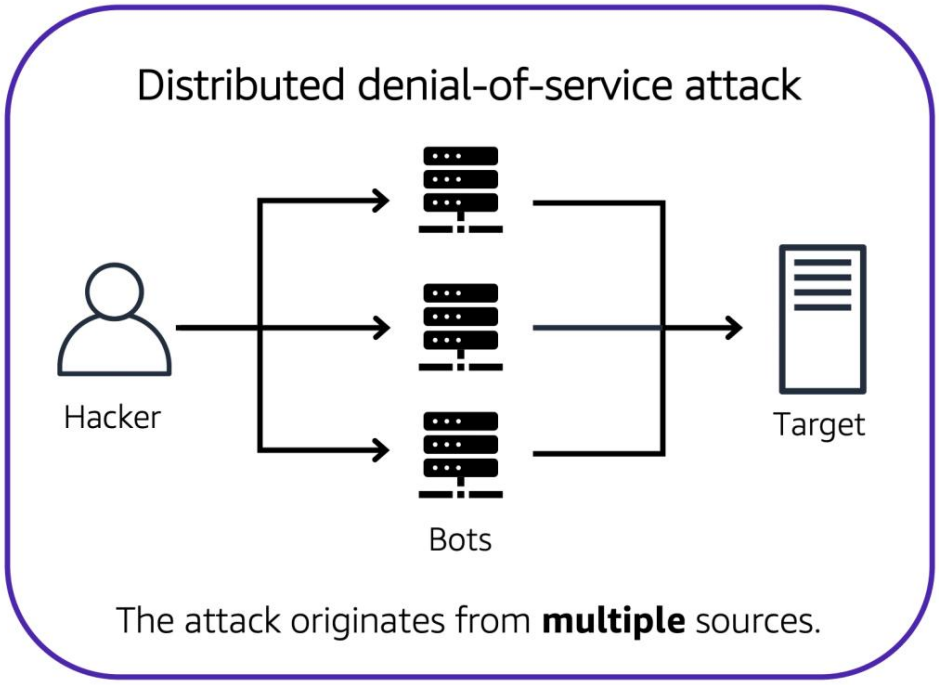


Por ejemplo, un atacante podría inundar un sitio web o una aplicación con un tráfico de red excesivo hasta que el sitio web o la aplicación objetivo se sobrecargue y ya no pueda responder. Si el sitio web o la aplicación no están disponibles, esto niega el servicio a los usuarios que intentan realizar solicitudes legítimas.

Ataques distribuidos de denegación de servicio

Ahora, suponga que el bromista ha solicitado la ayuda de amigos.

El bromista y sus amigos llaman repetidamente a la cafetería con solicitudes para hacer pedidos, aunque no tengan la intención de recogerlos. Estas solicitudes provienen de diferentes números de teléfono y es imposible que la cafetería las bloquee todas. Además, la afluencia de llamadas ha hecho que sea cada vez más difícil para los clientes recibir sus llamadas. Esto es similar a un ataque de denegación de servicio distribuido.



En un ataque de denegación de servicio distribuido (DDoS), se utilizan varias fuentes para iniciar un ataque que tiene como objetivo hacer que un sitio web o una aplicación no estén disponibles. Esto puede provenir de un grupo de atacantes, o incluso de un solo atacante. El atacante individual puede usar varias computadoras infectadas (también conocidas como "bots") para enviar tráfico excesivo a un sitio web o aplicación.

Para ayudar a minimizar el efecto de los ataques DoS y DDoS en sus aplicaciones, puede usar AWS Shield.

Escudo AWS

AWS Shield es un servicio que protege las aplicaciones contra ataques DDoS. AWS Shield proporciona dos niveles de protección: Estándar y Avanzado.

Estándar de escudo de AWS

AWS Shield Standard protege automáticamente a todos los clientes de AWS sin costo alguno. Protege sus recursos de AWS de los tipos de ataques DDoS más comunes y frecuentes.

A medida que el tráfico de la red ingresa a sus aplicaciones, AWS Shield Standard utiliza una variedad de técnicas de análisis para detectar el tráfico malicioso en tiempo real y lo mitiga automáticamente.

Escudo de AWS avanzado

AWS Shield Advanced es un servicio pago que proporciona diagnósticos de ataques detallados y la capacidad de detectar y mitigar ataques DDoS sofisticados.

También se integra con otros servicios como Amazon CloudFront, Amazon Route 53 y Elastic Load Balancing. Además, puede integrar AWS Shield con AWS WAF escribiendo reglas personalizadas para mitigar ataques DDoS complejos.

Servicios de seguridad adicionales

Servicio de administración de claves de AWS (AWS KMS)

La cafetería tiene muchos artículos, como máquinas de café, pasteles, dinero en las cajas registradoras, etc. Puede pensar en estos elementos como datos. Los dueños de las cafeterías quieren asegurarse de que todos estos artículos estén seguros, ya sea que estén en la sala de almacenamiento o que se transporten entre tiendas.

De la misma manera, debe asegurarse de que los datos de sus aplicaciones estén seguros mientras se almacenan (cifrado en reposo) y mientras se transmiten, lo que se conoce como cifrado en tránsito.

AWS Key Management Service (AWS KMS) le permite realizar operaciones de cifrado mediante el uso de claves criptográficas. Una clave criptográfica es una cadena aleatoria de dígitos que se utiliza para bloquear (cifrar) y desbloquear (descifrar) datos. Puede utilizar AWS KMS para crear, administrar y utilizar claves criptográficas. También puede controlar el uso de claves en una amplia gama de servicios y en sus aplicaciones.

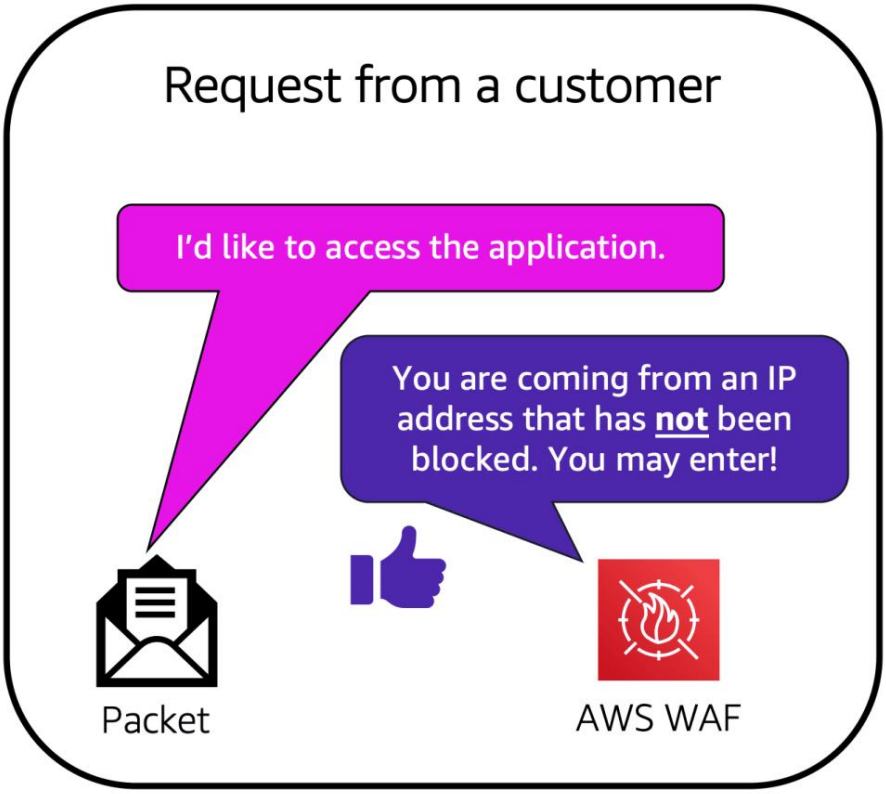
Con AWS KMS, puede elegir los niveles específicos de control de acceso que necesita para sus claves. Por ejemplo, puede especificar qué usuarios y roles de IAM pueden administrar claves. Alternativamente, puede deshabilitar temporalmente las claves para que nadie más las use. Sus claves nunca salen de AWS KMS y usted siempre tiene el control de ellas.

WAF de AWS

AWS WAF es un firewall de aplicaciones web que le permite monitorear las solicitudes de red que ingresan a sus aplicaciones web.

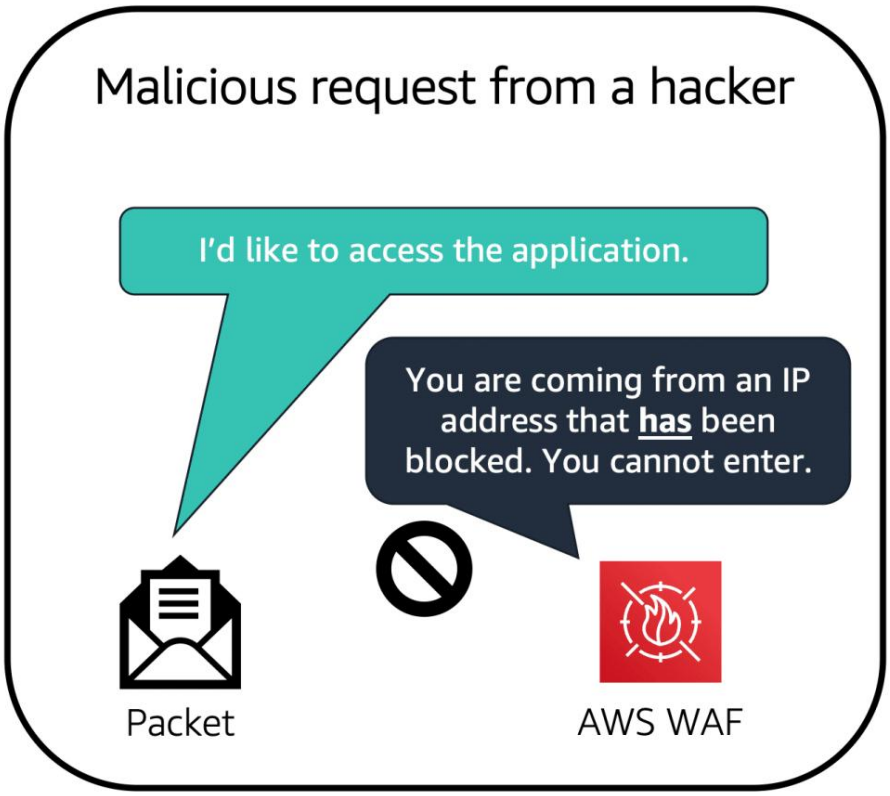
AWS WAF funciona junto con Amazon CloudFront y un balanceador de carga de aplicaciones. Recuerde las listas de control de acceso a la red que aprendió en un módulo anterior. AWS WAF funciona de manera similar para bloquear o permitir el tráfico. Sin embargo, lo hace mediante el uso de una lista de control de acceso web (ACL) para proteger sus recursos de AWS.

Este es un ejemplo de cómo puede usar AWS WAF para permitir y bloquear solicitudes específicas.



Suponga que su aplicación ha estado recibiendo solicitudes de red maliciosas de varias direcciones IP. Desea evitar que estas solicitudes continúen accediendo a su aplicación, pero también desea asegurarse de que los usuarios legítimos aún puedan acceder a ella. Configura la ACL web para permitir todas las solicitudes, excepto las de las direcciones IP que ha especificado.

Cuando llega una solicitud a AWS WAF, se compara con la lista de reglas que configuró en la ACL web. Si una solicitud no provino de una de las direcciones IP bloqueadas, permite el acceso a la aplicación.



Sin embargo, si una solicitud proviene de una de las direcciones IP bloqueadas que especificó en la ACL web, se le niega el acceso.

Amazon Inspector Suponga

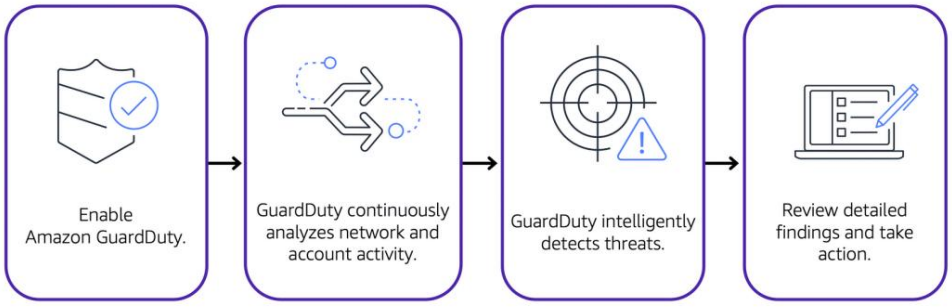
que los desarrolladores de la cafetería están desarrollando y probando una nueva aplicación de pedidos.
Quieren asegurarse de que están diseñando la aplicación de acuerdo con las mejores prácticas de seguridad. Sin
embargo, tienen varias otras aplicaciones para desarrollar, por lo que no pueden dedicar mucho tiempo a realizar evaluaciones
manuales. Para realizar evaluaciones de seguridad automatizadas, deciden utilizar Amazon Inspector.

Amazon Inspector ayuda a mejorar la seguridad y el cumplimiento de las aplicaciones mediante la ejecución de evaluaciones de
seguridad automatizadas. Comprueba las aplicaciones en busca de vulnerabilidades de seguridad y desviaciones de las
mejores prácticas de seguridad, como el acceso abierto a las instancias de Amazon EC2 y las instalaciones de software vulnerable.
versiones.

Después de que Amazon Inspector haya realizado una evaluación, le proporciona una lista de hallazgos de seguridad.
La lista prioriza por nivel de gravedad, incluida una descripción detallada de cada problema de seguridad y una
recomendación sobre cómo solucionarlo. Sin embargo, AWS no garantiza que seguir las recomendaciones proporcionadas
resuelva todos los posibles problemas de seguridad. Según el modelo de responsabilidad compartida, los clientes son
responsables de la seguridad de sus aplicaciones, procesos y herramientas que se ejecutan en AWS
servicios.

Servicio de guardia de Amazon

Amazon GuardDuty es un servicio que brinda detección inteligente de amenazas para su infraestructura y recursos de AWS. Identifica amenazas al monitorear continuamente la actividad de la red y el comportamiento de la cuenta dentro de su entorno de AWS.



Después de habilitar GuardDuty para su cuenta de AWS, GuardDuty comienza a monitorear la actividad de su red y cuenta. No tiene que implementar ni administrar ningún software de seguridad adicional. Luego, GuardDuty analiza continuamente los datos de varias fuentes de AWS, incluidos los registros de flujo de VPC y los registros de DNS.

Si GuardDuty detecta amenazas, puede revisar los hallazgos detallados sobre ellas desde la Consola de administración de AWS. Los hallazgos incluyen pasos recomendados para la remediación. También puede configurar las funciones de AWS Lambda para tomar medidas de remediación automáticamente en respuesta a los hallazgos de seguridad de GuardDuty.

ESTAS NOTAS CREÉ DEL CURSO:

https://www.coursera.org/learn/aws-cloud-practitioner-essentials

NOTAS DE ALMACENAMIENTO DE AWS:

https://www.linkedin.com/feed/update/urn:li:actividad:6801249080908550144/