



training and
certification

AWS Academy Cloud Foundations (LA)
Module 04 Student Guide

Versión 2.0.16

100-ACCLFO-20-LA-SG

© 2024, Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados.

Este contenido no puede reproducirse ni redistribuirse, total ni parcialmente, sin el permiso previo por escrito de Amazon Web Services, Inc. Queda prohibida la copia, el préstamo o la venta de carácter comercial.

Para correcciones o comentarios relacionados con el curso, contacte con nosotros en
<https://support.aws.amazon.com/#/contacts/aws-training>.

Todas las marcas comerciales pertenecen a sus propietarios.

Contenido

Módulo 4: Seguridad en la nube de AWS

4



Módulo 4: Seguridad en la nube de AWS

AWS Academy Cloud Foundations

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Bienvenido al Módulo 4: Seguridad en la nube de AWS.

La seguridad es la máxima prioridad en Amazon Web Services (AWS). AWS ofrece un entorno de informática en la nube escalable diseñado para proporcionar alta disponibilidad y fiabilidad con herramientas que le permiten ejecutar una amplia variedad de aplicaciones. Además de mantener la confianza de sus clientes, para AWS también es fundamental ayudar a proteger la confidencialidad, integridad y disponibilidad de sus sistemas y datos. Este módulo ofrece una introducción al enfoque de seguridad de AWS, que incluye tanto los controles en el entorno de AWS como algunos de los productos y las características de AWS que los clientes pueden utilizar para cumplir sus objetivos de seguridad.

Información general sobre el módulo

Temas

- Modelo de responsabilidad compartida de AWS
- AWS Identity and Access Management (IAM)
- Protección de una cuenta nueva de AWS
- Protección de cuentas
- Protección de datos en AWS
- Trabajo para garantizar la conformidad

Actividades

- Actividad sobre el modelo de responsabilidad compartida de AWS

Demostración

- Demostración grabada de IAM

Laboratorio

- Introducción a AWS IAM



Revisión de conocimientos



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

2

En este módulo, se abordarán los siguientes temas:

- Modelo de responsabilidad compartida de AWS
- AWS Identity and Access Management (IAM)
- Protección de una cuenta nueva de AWS
- Protección de cuentas
- Protección de datos en AWS
- Trabajo para garantizar la conformidad
- Servicios y recursos de seguridad adicionales

La sección uno incluye una **actividad** impartida por un profesor sobre el modelo de responsabilidad compartida de AWS.

En la sección dos, se incluye una **demonstración de IAM** grabada y, al final de esta misma sección, se incluye un **laboratorio práctico** que le ofrece experiencia en la configuración del IAM mediante el uso de la consola de administración de AWS.

Por último, se le pedirá que complete una **revisión de conocimientos** para comprobar su comprensión de los conceptos clave que se tratan en este módulo.

Objetivos del módulo

Después de completar este módulo, debería ser capaz de lo siguiente:

- Reconocer el modelo de responsabilidad compartida
- Identificar la responsabilidad del cliente y de AWS
- Reconocer usuarios, grupos y roles de IAM
- Describir los diferentes tipos de credenciales de seguridad en IAM
- Identificar los pasos para proteger una nueva cuenta de AWS
- Explorar los usuarios y los grupos de IAM
- Reconocer cómo proteger los datos de AWS
- Reconocer los programas de conformidad de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

3

Después de completar este módulo, debería ser capaz de lo siguiente:

- Reconocer el modelo de responsabilidad compartida
- Identificar la responsabilidad del cliente y de AWS
- Reconocer usuarios, grupos y roles de IAM
- Describir los diferentes tipos de credenciales de seguridad en IAM
- Identificar los pasos para proteger una nueva cuenta de AWS
- Explorar los usuarios y los grupos de IAM
- Reconocer cómo proteger los datos de AWS
- Reconocer los programas de conformidad de AWS

Sección 1: Modelo de responsabilidad compartida de AWS

Módulo 4: Seguridad en la nube de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Presentación de la sección 1: Modelo de responsabilidad compartida de AWS



La seguridad y la conformidad son una responsabilidad compartida entre AWS y el cliente. Este modelo de responsabilidad compartida está diseñado para ayudar a aliviar la carga operativa del cliente. Al mismo tiempo, para proporcionar la flexibilidad y el control del cliente que permite la implementación de soluciones de clientes en AWS, el cliente sigue siendo responsable de algunos aspectos de la seguridad general. La diferencia de quién es responsable entre lo que comúnmente se denomina *seguridad "de" la nube* frente a *seguridad "en" la nube*.

AWS opera, administra y controla los componentes desde la capa de virtualización de software hasta la seguridad física de las instalaciones en las que operan los servicios de AWS. **AWS es responsable** de proteger la infraestructura en la que se ejecutan todos los servicios ofrecidos en la nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

El cliente es responsable del cifrado de los datos en reposo y los datos en tránsito. El cliente también debe asegurarse de que la red esté configurada para la seguridad y de que las credenciales de seguridad y los inicios de sesión se administren de forma segura. Además, el cliente es responsable de la configuración de los grupos de seguridad y de la configuración del sistema operativo que se ejecuta en las instancias informáticas que lanzan (incluidas las actualizaciones y los parches de seguridad).

Responsabilidad de AWS: seguridad *de la nube*



Responsabilidades de AWS:

- Seguridad física de los centros de datos
 - Acceso controlado basado en las necesidades
- Infraestructura de hardware y software
 - Baja de recursos de almacenamiento, registro de acceso del sistema operativo (SO) del host y auditoría
- Infraestructura de red
 - Detección de intrusiones
- Infraestructura de virtualización
 - Aislamiento de instancias



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

6

AWS es responsable de la seguridad *de* la nube. ¿Qué significa esto?

En el modelo de responsabilidad compartida, AWS opera, administra y controla los componentes desde el sistema operativo de alojamiento bare metal y la capa de virtualización del hipervisor hasta la seguridad física de las instalaciones en las que operan los servicios. Esto significa que AWS se encarga de proteger la infraestructura global que ejecuta todos los servicios ofrecidos en la nube de AWS. La infraestructura global incluye regiones de AWS, zonas de disponibilidad y ubicaciones de borde.

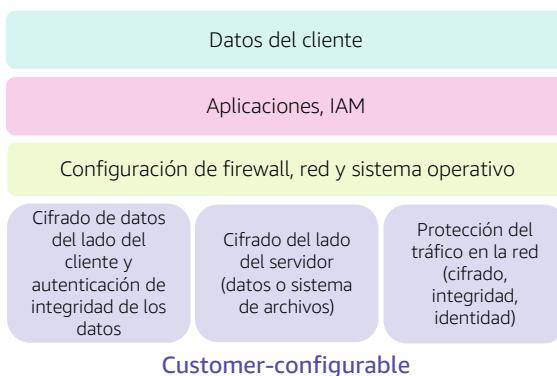
AWS es responsable de la infraestructura física que aloja sus recursos, que incluye lo siguiente:

- Seguridad física de los centros de datos** con acceso controlado basado en las necesidades en instalaciones sin identificación, con guardias de seguridad permanentes, autenticación de dos factores, revisión y registro de accesos, videovigilancia, y destrucción y desmagnetización de discos.
- Infraestructura de hardware**, como servidores, dispositivos de almacenamiento y otros dispositivos de los que dependen los servicios de AWS.
- Infraestructura de software**, que aloja sistemas operativos, aplicaciones de servicios y software de virtualización.
- Infraestructura de red**, como routers, comutadores, balanceadores de carga,

firewalls y cables. AWS también monitorea la red en límites externos, protege los puntos de acceso y proporciona infraestructura redundante con detección de intrusiones de forma constante.

La protección de esta infraestructura es la principal prioridad de AWS. Si bien no puede visitar los centros de datos o las oficinas de AWS para ver esta protección de primera mano, Amazon proporciona numerosos informes de auditores externos que han verificado nuestra conformidad con una variedad de normas y estándares de seguridad informática.

Responsabilidad del cliente: seguridad en la nube



Responsabilidades de los clientes:

- **Sistema operativo** de la instancia de Amazon Elastic Compute Cloud (Amazon EC2)
 - Incluidos los parches y el mantenimiento
- **Aplicaciones**
 - Contraseñas, acceso basado en roles, etc.
- **Configuración del grupo de seguridad**
- SO o **firewalls** basados en host
 - Incluidos los sistemas de detección o prevención de intrusiones
- **Configuraciones de red**
- Administración de cuentas
 - Configuración de inicio de sesión y permisos para cada usuario



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

7

Mientras que AWS protege y mantiene la infraestructura de la nube, los clientes son responsables de la seguridad de todo lo que ponen **en** la nube.

El **cliente es responsable** de lo que se implementa a través del uso de los servicios de AWS y de las aplicaciones que están conectadas a AWS. Los pasos de seguridad que debe tomar dependerán de los servicios que utilice y de la complejidad del sistema.

Las responsabilidades de los clientes incluyen la selección y protección de cualquier sistema operativo de instancias, la protección de las aplicaciones que se lanzan en los recursos de AWS, las configuraciones de grupos de seguridad, las configuraciones de firewall, las configuraciones de red y la administración segura de cuentas.

Cuando los clientes utilizan los servicios de AWS, mantienen un control absoluto sobre su contenido. Los clientes son responsables de administrar los requisitos de seguridad de contenido críticos, entre los que se incluyen los siguientes:

- El contenido que eligen almacenar en AWS
- Los servicios de AWS que se utilizan con el contenido
- En qué país se almacena ese contenido
- El formato y la estructura de ese contenido y si está enmascarado, cifrado o es anónimo
- Quién tiene acceso a ese contenido y cómo se conceden, administran y revocan esos derechos de acceso

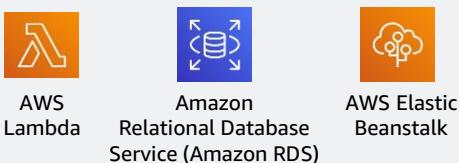
Los usuarios retienen el control de la seguridad que deciden implementar para proteger sus propios datos, entorno, aplicaciones, configuraciones de IAM y sistemas operativos.

Características del servicio y responsabilidad en materia de seguridad

Servicios de ejemplo administrados por el cliente



Servicios de ejemplo administrados por AWS



Infraestructura como servicio (IaaS)

- El cliente tiene más flexibilidad en lo que respecta a la configuración de redes y almacenamiento.
- El cliente es responsable de administrar más aspectos de la seguridad.
- El cliente configura los controles de acceso.

Plataforma como servicio (PaaS)

- El cliente no necesita administrar la infraestructura subyacente.
- AWS gestiona el sistema operativo, la implementación de parches a la base de datos, la configuración del firewall y la recuperación de desastres.
- El cliente puede centrarse en la administración de código o datos.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

8

La infraestructura como servicio (IaaS) se refiere a los servicios que proporcionan bloques de creación básicos para la TI en la nube, que incluyen, por lo general, acceso para configurar redes, equipos (virtuales o en hardware dedicado) y espacio de almacenamiento de datos. Los servicios en la nube que se pueden caracterizar como IaaS proporcionan al cliente el mayor nivel de flexibilidad y control de administración sobre los recursos de TI. Los servicios de IaaS son más similares a los recursos informáticos existentes en las instalaciones con los que muchos departamentos de TI están familiarizados actualmente.

Los servicios de AWS, como **Amazon EC2**, pueden clasificarse como **IaaS** y, por lo tanto, exigir que el cliente realice todas las tareas de configuración y administración de seguridad necesarias. Los clientes que implementan instancias EC2 son responsables de administrar el sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad), cualquier software de aplicación instalado en las instancias y la configuración de los grupos de seguridad proporcionados por AWS.

Plataforma como servicio (PaaS) se refiere a los servicios que eliminan la necesidad de que el cliente administre la infraestructura subyacente (hardware, sistemas operativos, etc.). Los servicios PaaS permiten al cliente enfocarse completamente en la implementación y administración de aplicaciones. Los clientes no tienen que preocuparse por la adquisición de recursos, la planificación de capacidad, el

mantenimiento del software ni la implementación de parches.

Los servicios de AWS, como **AWS Lambda** y **Amazon RDS** pueden clasificarse como **PaaS** porque **AWS opera la capa de infraestructura, el sistema operativo y las plataformas**. Los clientes solo necesitan obtener acceso a los puntos de enlace para almacenar y recuperar datos. Con los servicios PaaS, los clientes son responsables de administrar sus datos, clasificar sus recursos y aplicar los permisos adecuados. Sin embargo, estos servicios actúan más como servicios administrados, ya que AWS se encarga de una mayor parte de los requisitos de seguridad. En lo que respecta a estos servicios, AWS gestiona las tareas de seguridad básicas, como la implementación de parches en la base de datos y el sistema operativo, la configuración del firewall y la recuperación de desastres.

Características del servicio y responsabilidad en materia de seguridad (continuación)

Ejemplos de SaaS



AWS Trusted Advisor



AWS Shield



Amazon Chime

Software como servicio (SaaS)

- El software está alojado de forma centralizada.
- Cuenta con licencia según un modelo de suscripción o de pago por uso.
- Normalmente, el acceso a los servicios se realiza a través de un navegador web, una aplicación móvil o una interfaz de programación de aplicaciones (API).
- Los clientes no necesitan administrar la infraestructura que respalda el servicio.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

9

Software como servicio (SaaS) se refiere a los servicios que proporcionan software alojado de forma centralizada que suele ser accesible a través de un navegador web, una aplicación móvil o una interfaz de programación de aplicaciones (API). El modelo de licencia para ofertas de SaaS suele ser de suscripción o pago por uso. Con las ofertas de SaaS, los clientes no necesitan administrar la infraestructura que respalda el servicio. Algunos servicios de AWS, como **AWS Trusted Advisor**, **AWS Shield** y **Amazon Chime**, podrían clasificarse como ofertas de SaaS, en función de sus características.

AWS Trusted Advisor es una herramienta en línea que analiza su entorno de AWS y proporciona orientación y recomendaciones en tiempo real para ayudarlo a aprovisionar sus recursos siguiendo las prácticas recomendadas de AWS. El servicio Trusted Advisor se ofrece como parte de su plan de AWS Support. Algunas de las características de Trusted Advisor son gratuitas para todas las cuentas, pero los clientes de Business Support y Enterprise Support tienen acceso al conjunto completo de comprobaciones y recomendaciones de Trusted Advisor.

AWS Shield es un servicio administrado de protección contra ataques de denegación de servicio distribuidos (DDoS) que protege las aplicaciones que se ejecutan en AWS. Ofrece detección permanente y mitigaciones directas automáticas que reducen el tiempo de inactividad y latencia de las aplicaciones, por lo que no hay necesidad de contar con AWS Support para disfrutar de la protección de DDoS. AWS Shield

Advanced está disponible para todos los clientes. Sin embargo, para ponerse en contacto con el equipo de respuesta de DDoS, los clientes deben contar con Enterprise Support o Business Support de AWS Support.

Amazon Chime es un servicio de comunicaciones que le permite hacer reuniones, conversar y realizar llamadas empresariales dentro y fuera de su organización, todo con una sola aplicación. Es un servicio de comunicaciones de pago por uso sin tarifas iniciales, compromisos ni contratos a largo plazo.

Actividad: Modelo de responsabilidad compartida de AWS



Photo by Pixabay from Pexels.



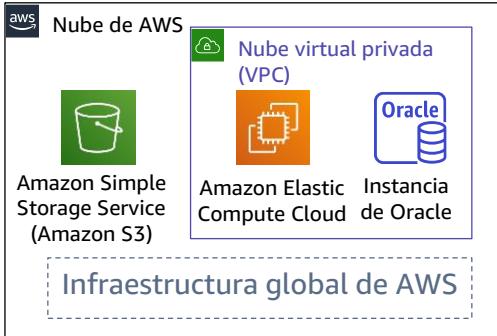
© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

10

En esta actividad impartida por un profesor, se le presentarán dos situaciones. En cada situación, se le harán varias preguntas sobre quién es el responsable (AWS o el cliente) de garantizar la seguridad del elemento en cuestión. El profesor dirigirá la clase en un análisis de cada pregunta y revelará las respuestas correctas una por una.

Actividad: Escenario 1 de 2

Considere esta implementación. ¿Quién es responsable: AWS o el cliente?



1. ¿Actualizaciones y parches del sistema operativo en la instancia de EC2?
2. ¿Seguridad física de los centros de datos?
3. ¿Infraestructura de virtualización?
4. ¿Configuración del grupo de seguridad EC2?
5. ¿Configuración de aplicaciones que se ejecutan en la instancia de EC2?
6. ¿Actualizaciones o parches de Oracle si la instancia de Oracle se ejecuta como una instancia de Amazon RDS?
7. ¿Actualizaciones o parches de Oracle si Oracle se ejecuta en una instancia de EC2?
8. ¿Configuración de acceso al bucket de S3?



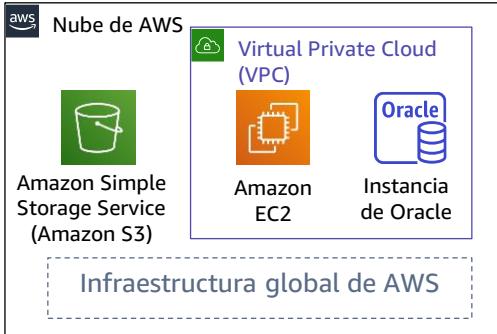
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

11

Considere el caso en el que un cliente utiliza los recursos y servicios de AWS que se muestran aquí. ¿Quién es responsable de mantener la seguridad? ¿AWS o el cliente?

Actividad: escenario 1 de 2

Considere esta implementación. ¿Quién es responsable? ¿AWS o el cliente?



1. ¿Actualizaciones y parches en el sistema operativo en la instancia EC2?
 - **RESPUESTA:** el cliente
2. ¿Seguridad física del centro de datos?
 - **RESPUESTA:** AWS
3. ¿Infraestructura de virtualización?
 - **RESPUESTA:** AWS
4. ¿Configuración de grupos de seguridad de EC2?
 - **RESPUESTA:** el cliente
5. ¿Configuración de las aplicaciones que se ejecutan en la instancia EC2?
 - **RESPUESTA:** el cliente
6. ¿Actualizaciones o parches de Oracle si la instancia de Oracle se ejecuta como una instancia de Amazon RDS?
 - **RESPUESTA:** AWS
7. ¿Actualizaciones o parches de Oracle si Oracle se ejecuta en una instancia EC2?
 - **RESPUESTA:** el cliente
8. ¿Configuración de acceso al bucket de S3?
 - **RESPUESTA:** el cliente



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

12

Considere el caso en el que un cliente utiliza los servicios y recursos de AWS que se muestran aquí. ¿Quién es responsable de mantener la seguridad? ¿AWS o el cliente?

El cliente utiliza Amazon Simple Storage Service (Amazon S3) para almacenar datos. El cliente configuró una nube virtual privada (VPC) con Amazon Virtual Private Cloud (Amazon VPC). La instancia EC2 y la instancia de base de datos de Oracle que crearon se ejecutan en la VPC.

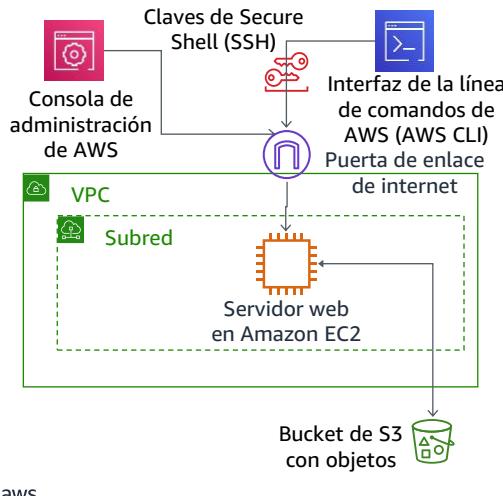
En este ejemplo, el cliente debe administrar el sistema operativo (SO) invitado que se ejecuta en la **instancia EC2**. Con el paso del tiempo, el sistema operativo invitado tendrá que actualizarse y aplicar parches de seguridad. Además, también se debe mantener todo software o utilidad de aplicación que el cliente haya instalado en la instancia de Amazon EC2. El cliente es responsable de configurar el firewall (o grupo de seguridad) de AWS que se aplica a la instancia de Amazon EC2. El cliente también es responsable de las configuraciones de **VPC** que especifican las condiciones de red en las que se ejecuta la instancia de Amazon EC2. Estas tareas son las mismas tareas de seguridad que realizaría el personal de TI, independientemente de dónde se encuentren sus servidores.

La instancia de Oracle de este ejemplo proporciona un caso práctico interesante en términos de responsabilidad de AWS o del cliente. **Si la base de datos se ejecuta en**

una instancia EC2, es responsabilidad del cliente aplicar parches y actualizaciones de software de Oracle. Sin embargo, **si la base de datos se ejecuta como una instancia de Amazon RDS**, AWS es el responsable de aplicar actualizaciones y parches de software de Oracle. Como Amazon RDS es un servicio de base de datos administrado, AWS se encarga de las tareas de administración de bases de datos que consumen mucho tiempo, como el aprovisionamiento, las copias de seguridad, los parches de software, el monitoreo y el escalado de hardware. Para obtener más información, consulte las [prácticas recomendadas para ejecutar la base de datos de Oracle en AWS](#).

Actividad: Escenario 2 de 2

Considere esta implementación. ¿Quién es responsable: AWS o el cliente?



1. ¿Se asegura de que la Consola de administración de AWS no sea pirateada?
2. ¿Configurando la subred?
3. ¿Configurando la VPC?
4. ¿Protección contra las interrupciones de la red en las regiones de AWS?
5. Proteger las claves SSH
6. ¿Garantizar el aislamiento de la red entre los datos de los clientes de AWS?
7. ¿Garantizar una conexión de red de baja latencia entre el servidor web y el bucket de S3?
8. ¿Hacer cumplir la autenticación multifactor para todos los inicios de sesión de los usuarios?

aws

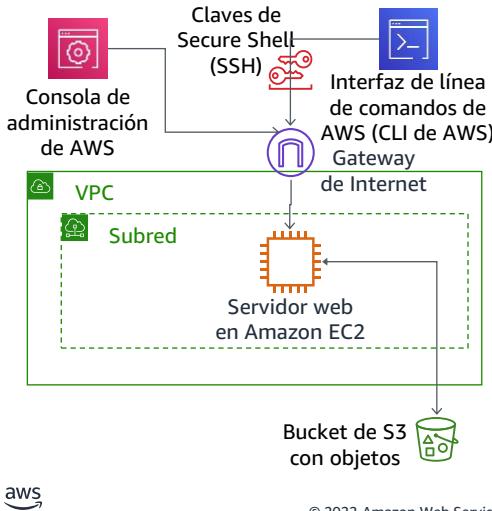
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

13

Ahora, considere este caso adicional en el que un cliente utiliza los servicios y recursos de AWS que se muestran aquí. ¿Quién es responsable de mantener la seguridad? ¿AWS o el cliente?

Actividad: escenario 2 de 2

Considere esta implementación. ¿Quién es responsable? ¿AWS o el cliente?



1. ¿Garantizar que la consola de administración de AWS no sea pirateada?
 - **RESPUESTA:** AWS
2. ¿Configurar la subred?
 - **RESPUESTA:** el cliente
3. ¿Configurar la VPC?
 - **RESPUESTA:** el cliente
4. ¿Proteger frente a interrupciones de red en las regiones de AWS?
 - **RESPUESTA:** AWS
5. ¿Proteger las claves SSH?
 - **RESPUESTA:** el cliente
6. ¿Garantizar el aislamiento de red entre los datos de los clientes de AWS?
 - **RESPUESTA:** AWS
7. ¿Garantizar una conexión de red de baja latencia entre el servidor web y el bucket de S3?
 - **RESPUESTA:** AWS
8. ¿Requerir la autenticación multifactor para todos los inicios de sesión de los usuarios?
 - **RESPUESTA:** el cliente

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

14

Un cliente utiliza Amazon S3 para almacenar datos. El cliente configuró una nube virtual privada con Amazon VPC y está ejecutando un servidor web en una instancia EC2 en la VPC. El cliente configuró una gateway de Internet como parte de la VPC para que se pueda obtener acceso al servidor web mediante la consola de administración de AWS o la interfaz de línea de comandos de AWS (CLI de AWS). Cuando el cliente utiliza la CLI de AWS, la conexión requiere el uso de claves de Secure Shell (SSH).

Aprendizajes clave de la sección 1



- AWS y el cliente comparten responsabilidades en materia de seguridad:
 - AWS es responsable de la seguridad **de la nube**.
 - El cliente es responsable de la seguridad **en la nube**.
- **AWS es responsable de proteger la infraestructura** (incluido el hardware, el software, las redes y las instalaciones) que ejecuta los servicios en la nube de AWS.
- En el caso de los servicios clasificados como infraestructura como servicio (IaaS), el **cliente es responsable de realizar las tareas de configuración y administración de seguridad necesarias**.
 - Por ejemplo, actualizaciones del sistema operativo invitado y configuraciones de parches de seguridad, firewall y grupos de seguridad.

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

15

Estos son algunos de los aprendizajes clave de esta sección del módulo:

- AWS y el cliente comparten responsabilidades en materia de seguridad:
 - AWS es responsable de la seguridad **de la nube**.
 - El cliente es responsable de la seguridad **en la nube**.
- **AWS es responsable de proteger la infraestructura** (incluido el hardware, el software, las redes y las instalaciones) que ejecuta los servicios en la nube de AWS.
- En el caso de los servicios clasificados como infraestructura como servicio (IaaS), el **cliente es responsable de realizar las tareas de configuración y administración de seguridad necesarias**.
 - Por ejemplo, actualizaciones del sistema operativo invitado y configuraciones de parches de seguridad, firewall y grupos de seguridad.

Sección 2: AWS Identity and Access Management (IAM)

Módulo 4: Seguridad en la nube de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Introducción de la sección 2: AWS Identity and Access Management (o IAM)

AWS Identity and Access Management (IAM)

- Utilice **IAM** para administrar el acceso a los **recursos de AWS**:
 - Un recurso es una entidad en una cuenta de AWS con la que puede trabajar.
 - Recursos de ejemplo: una instancia de Amazon EC2 o un bucket de 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 gratuita



AWS Identity and
Access Management
(IAM)



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

17

AWS Identity and Access Management (IAM) le permite controlar el acceso a servicios de informática, almacenamiento, base de datos y aplicaciones en la nube de AWS. IAM se puede utilizar para gestionar la autenticación y para especificar y aplicar políticas de autorización a fin de que usted especifique qué usuarios pueden obtener acceso a cada servicio.

IAM es una herramienta que administra el acceso de forma centralizada para lanzar, configurar, administrar y terminar recursos en su cuenta de AWS. Proporciona un control minucioso sobre el acceso a los recursos, incluida la posibilidad de especificar exactamente qué llamadas a la **API** está autorizado a realizar el usuario a cada servicio. Independientemente de si utiliza la consola de administración de AWS, la CLI de AWS o los kits de desarrollo de software (SDK) de AWS, cada llamada a un servicio de AWS es una llamada a la API.

Con IAM, puede administrar *quién* puede obtener acceso a *qué* recursos y *cómo* se puede obtener acceso a ellos. Puede conceder diferentes permisos a diferentes personas para diferentes recursos. Por ejemplo, puede permitir que algunos usuarios tengan acceso completo a Amazon EC2, Amazon S3, Amazon DynamoDB, Amazon Redshift y otros servicios de AWS. Sin embargo, para otros usuarios, puede permitir el acceso de solo lectura a solo unos cuantos buckets de S3. Del mismo modo, puede conceder permiso a otros usuarios para que solamente administren instancias EC2.

específicas. También puede permitir que algunos usuarios obtengan acceso únicamente a la información de facturación de la cuenta, pero nada más.

IAM es una característica de su cuenta de AWS y se ofrece sin cargos 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



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

18

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

Un **usuario de IAM** es una persona o aplicación definida en una cuenta de AWS que debe realizar llamadas a la API para los 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 de usuario raíz de la cuenta de AWS. Cada usuario está definido en una única cuenta de AWS.

Un **grupo de IAM** es un conjunto de usuarios de IAM. Puede utilizar grupos de IAM para simplificar la especificación y administración de permisos de varios usuarios.

Una **política de IAM** es un documento que define permisos para determinar lo que los usuarios pueden hacer en la cuenta de AWS. Una política normalmente concede acceso a recursos determinados y especifica lo que el usuario puede hacer con esos recursos. Las políticas también pueden denegar explícitamente el acceso.

Un **rol de IAM** es una herramienta para conceder acceso temporal a recursos de AWS específicos 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 con lo siguiente:
 - ID de clave de acceso
 - Clave de acceso secreta
- Proporciona acceso a la CLI de AWS y al SDK de AWS.



CLI de AWS



Herramientas y SDK de AWS

Acceso a la consola de administración de AWS

- Se autentica con lo siguiente:
 - ID 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.



Consola de administración de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

19

La **autenticación** es un concepto básico de seguridad informática: un usuario o sistema debe demostrar primero su identidad. Considere cómo se autentica usted mismo cuando va al aeropuerto y desea pasar por el área de seguridad del aeropuerto para poder tomar su vuelo. En esta situación, debe presentar algún tipo de identificación al oficial de seguridad para demostrar quién es usted antes de poder entrar a un área restringida. Un concepto similar se aplica para obtener acceso a los recursos de AWS en la nube.

Cuando define un usuario de IAM, selecciona qué tipo de acceso puede utilizar el usuario para obtener acceso a los recursos de AWS. Hay dos tipos diferentes de acceso que puede asignar a los usuarios: acceso mediante programación y acceso a la consola de administración de AWS. Puede asignar solo acceso mediante programación, solo acceso a la consola o puede asignar ambos tipos de acceso.

Si concede **acceso mediante programación**, el usuario de IAM deberá presentar un **ID de clave de acceso** y una **clave de acceso secreta** cuando realice una llamada a la API de AWS mediante la CLI de AWS, el SDK de AWS o cualquier otra herramienta de desarrollo.

Si concede **acceso a la consola de administración de AWS**, el usuario de IAM deberá completar los campos que aparecen en la ventana de inicio de sesión del navegador. Se

le pedirá al usuario que proporcione el ID de cuenta de 12 dígitos o el alias de cuenta correspondiente. El usuario también debe escribir su nombre de usuario y contraseña de IAM. Si **Multi-Factor Authentication (MFA)** está habilitada para el usuario, también se le solicitará un código de autenticación.

MFA de IAM

- 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.



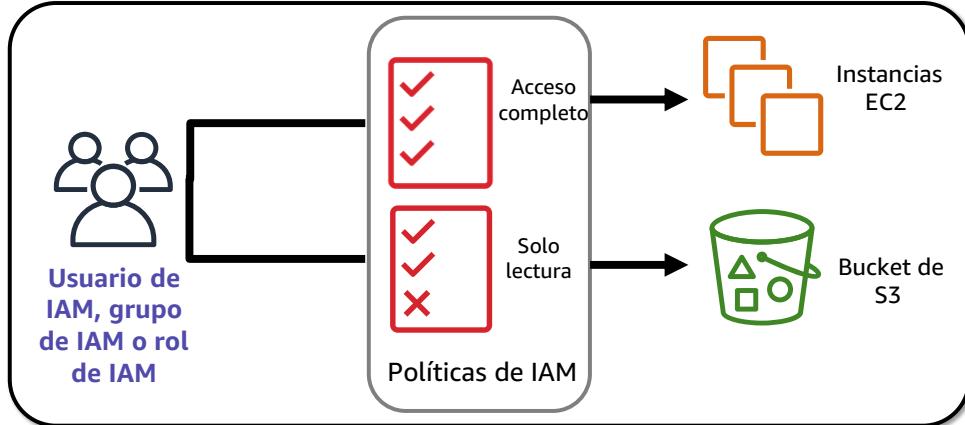
Se puede obtener acceso a los servicios y recursos de AWS mediante la consola de administración de AWS, la CLI de AWS o los SDK y las API. Para mayor seguridad, recomendamos habilitar MFA.

Con MFA, los usuarios y los sistemas deben proporcionar un **token de MFA** (además de las credenciales de inicio de sesión habituales) para poder obtener acceso a los servicios y recursos de AWS.

Las opciones para generar el token de autenticación de MFA incluyen **aplicaciones virtuales conformes con MFA** (como Google Authenticator o Authy 2-Factor Authentication), **dispositivos de clave de seguridad U2F** y **dispositivos MFA físicos**.

Autorización: qué acciones están permitidas

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



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

21

La **autorización** es el proceso de determinar qué permisos debe concederse a un usuario, servicio o aplicación. Una vez que un usuario ha sido autenticado, debe estar autorizado para acceder a un servicio de AWS.

De forma predeterminada, los usuarios de IAM no tienen permiso para obtener acceso a los recursos o los datos en una cuenta de AWS. En su lugar, debe conceder permisos de forma explícita a un usuario, grupo o rol mediante la creación de una *política*, la cual es un documento en formato JavaScript Object Notation (JSON). Una política enumera los permisos que habilitan o deniegan el acceso a los recursos de la cuenta de AWS.

IAM: autorización

- 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**.



Permisos de IAM

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



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

22

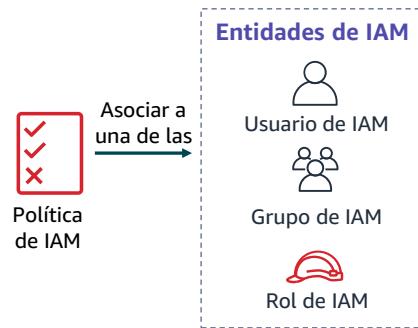
Para asignar un permiso a un usuario, grupo o rol, debe crear una **política de IAM** (o encontrar una política existente en la cuenta). No existen permisos predeterminados. Todas las acciones de la cuenta se deniegan al usuario de forma predeterminada (*denegación implícita*) a menos que dichas acciones se permitan explícitamente. Se denegarán todas las acciones que no se hayan permitido explícitamente. Cualquier acción que deniegue explícitamente, se denegará en todo momento.

El **principio de mínimo privilegio** es un concepto importante en la seguridad informática. Fomenta que conceda únicamente los privilegios de usuario mínimos que necesita el usuario, en función de las necesidades de los usuarios. Cuando crea políticas de IAM, se recomienda seguir este consejo de seguridad para conceder *privilegios mínimos*. Determine las tareas que tienen que realizar los usuarios y elabore políticas para permitirles realizar *solo* dichas tareas. Comience con un conjunto mínimo de permisos y conceda permisos adicionales según sea necesario. Esto es más seguro que comenzar con permisos que son demasiado amplios y, posteriormente, intentar bloquear los permisos concedidos.

Tenga en cuenta que el alcance de las configuraciones del servicio de IAM es **global**. La configuración no se define en un nivel de región de AWS. Las configuraciones de IAM se aplican en todas las regiones de AWS.

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 un rol de 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).



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

23

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. 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 puede 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

```
{  
    "version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": ["DynamoDB:*", "s3:*"],  
        "Resource": [  
            "arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",  
            "arn:aws:s3:::bucket-name",  
            "arn:aws:s3:::bucket-name/*"]  
    },  
    {  
        "Effect": "Deny",  
        "Action": ["dynamodb:*", "s3:*"],  
        "NotResource": ["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",  
                      "arn:aws:s3:::bucket-name",  
                      "arn:aws:s3:::bucket-name/*"]  
    }]  
}
```

aws

El permiso explícito concede a los usuarios acceso a una tabla específica de DynamoDB y a...
...buckets de Amazon S3.

Explicit deny (denegación explícita) garantiza que los usuarios no puedan usar otras acciones o recursos de AWS que no sean esa tabla y esos buckets.

Una instrucción de denegación explícita prevalece sobre una instrucción de permiso.

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

24

Como se ha mencionado anteriormente, los documentos de políticas de IAM se escriben en JSON.

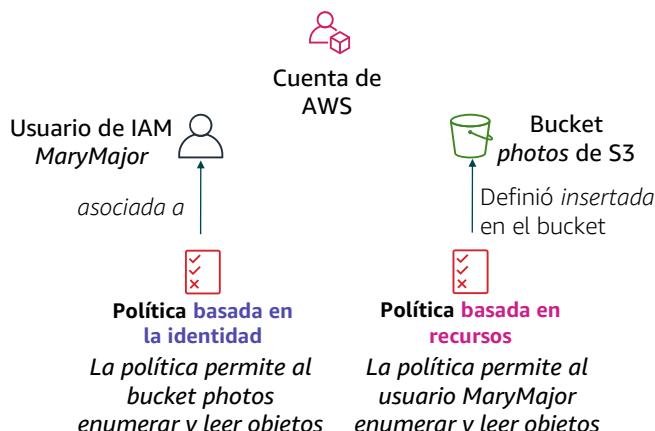
La política de IAM de ejemplo concede a los usuarios acceso únicamente a los siguientes recursos:

- La tabla DynamoDB, cuyo nombre está representado por *table-name*.
- El bucket S3 de la cuenta de AWS, cuyo nombre está representado por *bucket-name* y 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 utilizar ninguna otra acción o recurso de DynamoDB o S3, excepto las acciones y los recursos especificados en la política, aunque se hayan concedido permisos en otra política. Una instrucción de denegación explícita prevalece 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 qué 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



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

25

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.

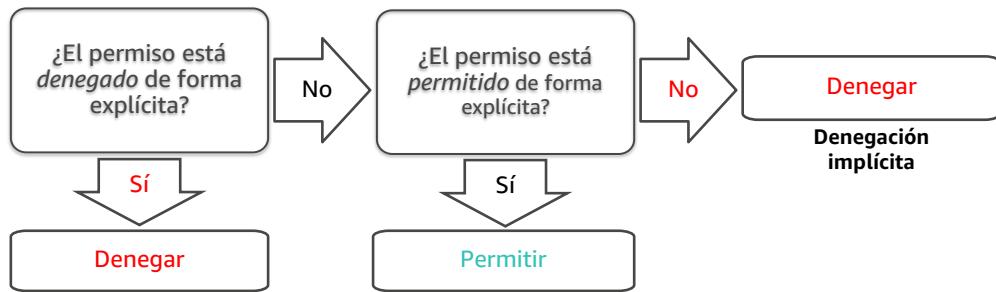
Las políticas basadas en recursos se definen únicamente de forma **directa**, lo que significa que usted define la política en el propio recurso, en lugar de crear un documento de política de IAM independiente. Por ejemplo, para crear una política de bucket de S3 (un tipo de política basada en recurso) 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.

Tenga en cuenta que podría definir una instrucción de denegación en una política de bucket para restringir el acceso a determinados usuarios de IAM, incluso si se concede acceso a los usuarios en una política basada en identidad independiente. Una instrucción de denegación explícita siempre prevalecerá sobre cualquier instrucción de permiso.

Permisos de IAM

Modo en que IAM determina los permisos:



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

26

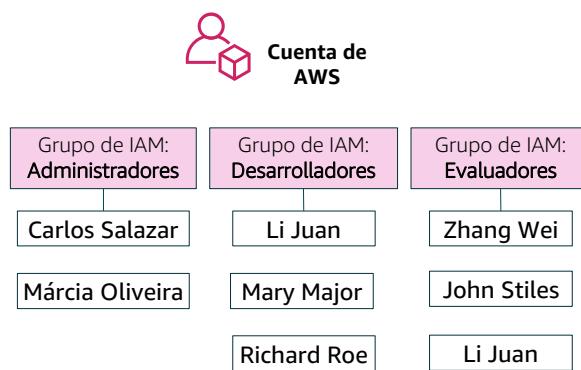
Las políticas de IAM le permiten ajustar los privilegios que se conceden a los usuarios, grupos y funciones de IAM.

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 denegar 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.

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.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

27

Un **grupo de IAM** es un conjunto de usuarios de IAM. Los grupos de IAM ofrecen una forma conveniente para especificar permisos a un conjunto de usuarios, lo que puede facilitar la administración de permisos para dichos usuarios.

Por ejemplo, puede crear un grupo de IAM denominado *Desarrolladores* y asociar una política de IAM o varias políticas de IAM al grupo Desarrolladores que concedan los permisos de acceso a los recursos de AWS que normalmente necesitan dichos desarrolladores. Cualquier usuario que agregue al grupo Desarrolladores tendrá automáticamente los permisos asignados al grupo. En tal caso, no es necesario asociar la política de IAM o las políticas de IAM directamente al usuario. Si un nuevo usuario se une a su organización y se le deben conceder privilegios de desarrollador, solo tiene que agregar a ese usuario al grupo Desarrolladores. Del mismo modo, si una persona cambia de trabajo en su organización, en lugar de editar los permisos de ese usuario, simplemente debe eliminar al usuario del grupo.

Las características importantes de los grupos de IAM son las siguientes:

- Un grupo puede contener muchos usuarios y un usuario puede pertenecer a varios grupos.
- Los grupos no pueden estar anidados. Un grupo solo puede contener usuarios y, a su vez, un grupo no puede contener otros grupos.
- No hay ningún grupo predeterminado que incluya automáticamente a todos los

usuarios de la cuenta de AWS. Si desea tener un grupo con todos los usuarios de la cuenta, debe crear el grupo y agregar cada usuario nuevo.

Roles 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



Rol de IAM



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

28

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.

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 acceso 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.

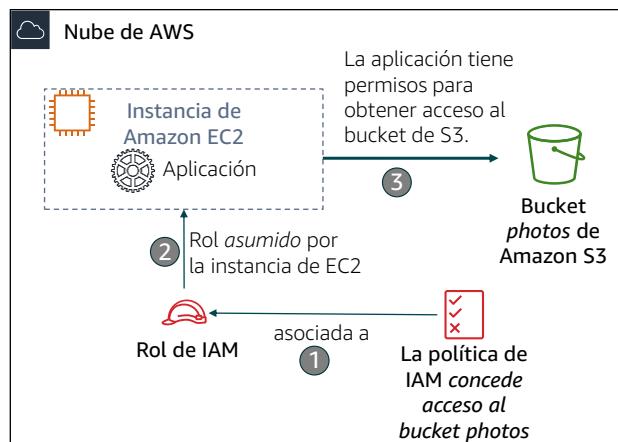
Ejemplo de uso de un rol de IAM

Situación:

- Una aplicación que se ejecuta en una instancia 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



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

29

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](#).

Aprendizajes clave de la sección 2



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

30

- 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.

Estos son algunos de los aprendizajes clave de esta sección del módulo:

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.

Demostración grabada: IAM



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

31

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 sección del módulo.

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

Sección 3: Protección de una cuenta nueva de AWS

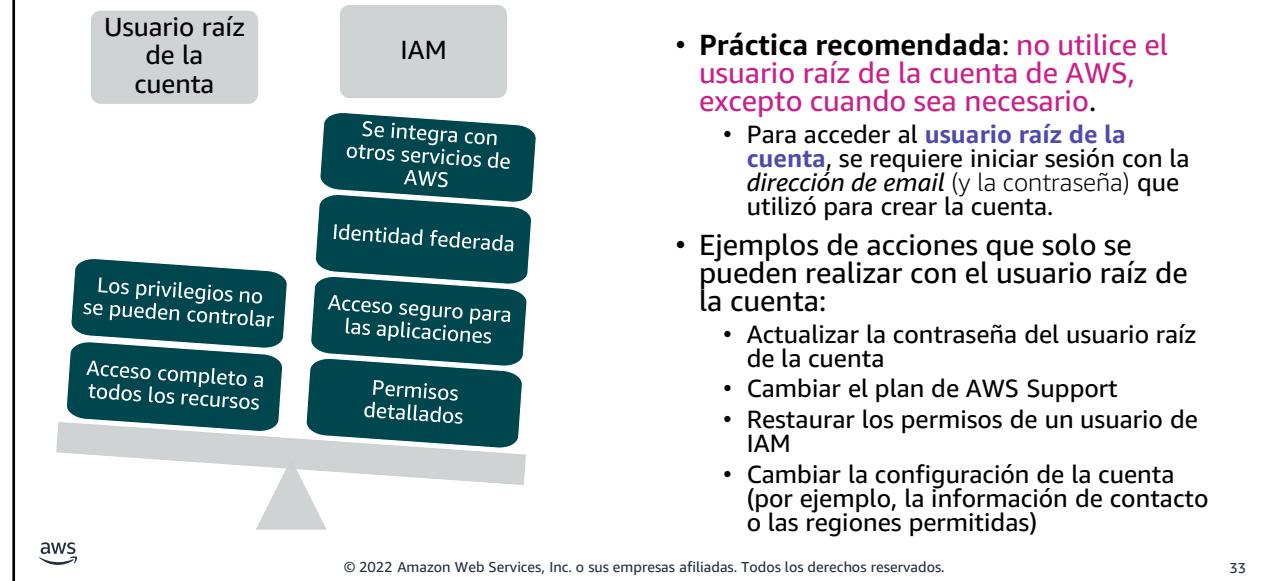
Módulo 4: Seguridad en la nube de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Presentación de la sección 3: Protección de una cuenta nueva de AWS.

Acceso de usuario raíz de la cuenta de AWS frente al acceso de IAM



33

Cuando crea una cuenta de AWS por primera vez, comienza con una identidad de inicio de sesión única que tiene acceso total a todos los servicios y recursos de AWS en la cuenta. Esta identidad recibe el nombre de **usuario raíz de la cuenta de AWS** y se obtiene acceso a ella iniciando sesión en la consola de administración de AWS con la dirección de email y la contraseña que utilizó para crear la cuenta. Los usuarios raíz de la cuenta de AWS tienen (y conservan) acceso **completo** a todos los recursos de la cuenta. Por lo tanto, AWS recomienda encarecidamente que no utilice las credenciales de usuario raíz de la cuenta para las interacciones cotidianas con la cuenta.

En su lugar, AWS recomienda utilizar IAM para crear usuarios adicionales y asignar permisos a estos usuarios, de acuerdo con el principio de mínimo privilegio. Por ejemplo, si requiere permisos de administrador, puede crear un usuario de IAM, concederle acceso total y, luego, utilizar esas credenciales para interactuar con la cuenta. Más tarde, si necesita revocar o modificar sus permisos, puede eliminar o modificar cualquier política asociada a ese usuario de IAM.

Además, si tiene varios usuarios que requieren acceso a su cuenta, puede crear credenciales exclusivas para cada uno de ellos y definir quién tendrá acceso a los distintos recursos. Por ejemplo, puede crear usuarios de IAM con acceso de solo lectura a los recursos de su cuenta de AWS y distribuir esas credenciales a los usuarios que requieren acceso de lectura. Debe evitar compartir las mismas credenciales con varios

usuarios.

Aunque el usuario raíz de la cuenta no debe utilizarse para tareas rutinarias, hay algunas tareas que solo se pueden cumplir iniciando sesión como usuario raíz de la cuenta. Puede encontrar una lista completa de estas tareas en la página de documentación de AWS [Tareas que requieren credenciales de usuario raíz de la cuenta de AWS.](#)

Protección de una nueva cuenta de AWS: usuario raíz de la cuenta

Paso 1: Deje de utilizar el usuario raíz de la cuenta tan pronto como sea posible.

- El usuario raíz de la cuenta tiene acceso ilimitado a todos sus recursos.
- Pasos a seguir para dejar de utilizar el usuario raíz de la cuenta:
 1. Inicie sesión como usuario raíz de la cuenta y [cree un usuario de IAM](#) para usted. Guarde las claves de acceso si es necesario.
 2. Cree un grupo de IAM, otórguele permisos totales de administrador y agregue el usuario de IAM al grupo.
 3. Deshabilite y [elimine las claves de acceso de usuario raíz de la cuenta](#), en caso de que existan.
 4. [Habilite una política de contraseñas](#) para los usuarios.
 5. Inicie sesión con sus nuevas credenciales de usuario de IAM.
 6. Guarde las credenciales de usuario raíz de la cuenta en un lugar seguro.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

34

Para dejar de utilizar el usuario raíz de la cuenta, siga los siguientes pasos:

1. Cuando haya iniciado sesión en el usuario raíz de la cuenta, cree un usuario de IAM para usted con el acceso a la consola de administración de AWS habilitado (pero todavía no asocie ningún permiso al usuario). Guarde las claves de acceso de usuario de IAM si es necesario.
2. A continuación, cree un grupo de IAM, asígnele un nombre (como *FullAccess*) y asocie políticas de IAM al grupo que conceda acceso completo a al menos unos pocos de los servicios que utilizará. Luego, agregue al usuario de IAM al grupo.
3. Deshabilite y elimine las claves de acceso de usuario raíz de la cuenta, en caso de que existan.
4. Habilite una política de contraseñas para todos los usuarios. Copie el [enlace de inicio de sesión de los usuarios de IAM](#) desde la página del panel de IAM. A continuación, cierre la sesión como usuario raíz de la cuenta.
5. Vaya al enlace de inicio de sesión de los usuarios de IAM que copió e inicie sesión en la cuenta con las nuevas credenciales de usuario de IAM.
6. Guarde las credenciales de usuario raíz de la cuenta en un lugar seguro.

Para ver instrucciones detalladas sobre cómo configurar su primer usuario y grupo de IAM, consulte [Creación del primer grupo y usuario administrador de IAM](#).

Protección de una nueva cuenta de AWS: MFA

Paso 2: Habilite Multi-Factor Authentication (MFA).

- Exija MFA para **su usuario raíz de la cuenta** y para **todos los usuarios de IAM**.
- También puede usar MFA para controlar el acceso a las API de servicio de AWS.
- Opciones para recuperar el token de MFA:
 - Aplicaciones virtuales compatibles con MFA:
 - Google Authenticator
 - Authy Authenticator (aplicación de Windows Phone)
 - Dispositivos de clave de seguridad U2F:
 - Por ejemplo, YubiKey.
 - Opciones de MFA de hardware:
 - Llavero o tarjeta de visualización ofrecida por [Gemalto](#).



Token de MFA



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

35

Otro paso recomendado para proteger una nueva cuenta de AWS consiste en exigir el uso de Multi-Factor Authentication (MFA) para el inicio de sesión del usuario raíz de la cuenta y para todos los demás inicios de sesión de los usuarios de IAM. También puede utilizar MFA para controlar el acceso mediante programación. Para obtener más información, consulte [Configuración del acceso a la API protegido por MFA](#).

Tiene algunas opciones para recuperar el token de MFA necesario para iniciar sesión cuando la MFA está habilitada. Las opciones incluyen aplicaciones virtuales compatibles con MFA (como Google Authenticator y Authy Authenticator), dispositivos con clave de seguridad U2F y opciones de MFA de hardware que proporcionan un llavero o una tarjeta de visualización.

Protección de una nueva cuenta de AWS: AWS CloudTrail

Paso 3: Utilice AWS CloudTrail.

- CloudTrail realiza un seguimiento de la actividad de los usuarios en su cuenta.
 - Registra todas las solicitudes API para los recursos de todos los servicios admitidos de su cuenta.
 - **El historial básico de eventos de AWS CloudTrail está habilitado de forma predeterminada** y es gratuito.
 - Contiene todos los datos de eventos de administración de los últimos 90 días de actividad de la cuenta.
- Pasos a seguir para obtener acceso a CloudTrail:
 1. Inicie sesión en la **consola de administración de AWS** y seleccione el servicio **CloudTrail**.
 2. Haga clic en **Event history** (Historial de eventos) para ver, filtrar y buscar los últimos 90 días de eventos.
- **Para habilitar los registros de más de 90 días y las alertas de eventos especificados, cree un registro de seguimiento.**
 1. En la página de registros de seguimiento de la consola de CloudTrail, haga clic en **Create trail** (Crear registro de seguimiento).
 2. Asignele un nombre, aplíquelo a todas las regiones y cree un nuevo bucket de Amazon S3 para el almacenamiento de registros.
 3. Configure las restricciones de acceso en el bucket de S3 (por ejemplo, solo los usuarios administradores deben tener acceso).



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

36

AWS CloudTrail es un servicio que registra todas las solicitudes de API a los recursos de su cuenta. De esta forma, permite realizar auditorías operativas en su cuenta.

AWS CloudTrail está habilitado para crear cuentas de forma predeterminada en todas las cuentas de AWS y mantiene un registro de los últimos 90 días de actividad de eventos de administración de cuentas. Puede ver y descargar la actividad de la cuenta de los últimos 90 días con relación a operaciones de *creación, modificación y eliminación* de [servicios compatibles con CloudTrail](#) sin necesidad de crear manualmente otro registro de seguimiento.

Para habilitar la retención de registros de CloudTrail más allá de los últimos 90 días y habilitar las alertas cuando hayan eventos específicos, cree un nuevo registro de seguimiento (descrito en mayor medida en la diapositiva). Para obtener instrucciones detalladas paso a paso sobre cómo crear un registro de seguimiento en AWS CloudTrail, consulte [Creación de un registro de seguimiento](#) en la documentación de AWS.

Protección de una nueva cuenta de AWS: informes de facturación

Paso 4: Habilite un informe de facturación, como el informe de uso y costo de AWS.

- Los informes de facturación proporcionan información sobre el uso de los recursos de AWS y los costos estimados de dicho uso.
- AWS entrega los informes en el bucket de Amazon S3 que especifique.
 - El informe se actualiza al menos una vez al día.
- El **Informe de uso y costo de AWS** hace un seguimiento del uso que hace de AWS y proporciona cargos estimados asociados con su cuenta de AWS, ya sea por hora o por día.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

37

Otro paso recomendado para proteger una nueva cuenta de AWS consiste en habilitar los informes de facturación, como el **informe de uso y costo de AWS**. Los informes de facturación proporcionan información sobre el uso de los recursos de AWS y los costos estimados de dicho uso. AWS envía los informes a un bucket de Amazon S3 que usted especifique y AWS los actualiza al menos una vez al día.

El informe de uso y costo de AWS realiza un seguimiento del uso en la cuenta de AWS y proporciona los cargos estimados, ya sea por hora o por día.

Consulte la documentación de AWS para obtener más información acerca de [cómo crear un informe de uso y costo de AWS](#).

Aprendizajes clave de la sección 3



Prácticas recomendadas para proteger una cuenta de AWS:

- **Proteja** los inicios de sesión con Multi-Factor Authentication (MFA).
- **Elimine** las **claves de acceso** de usuario raíz de la cuenta.
- **Cree** **usuarios de IAM** individuales y otorgue permisos de acuerdo con el principio de mínimo privilegio.
- **Utilice grupos** para asignar permisos a usuarios de IAM.
- **Configure** una **política de contraseñas sólida**.
- **Delegue** el uso de **roles** en lugar del uso compartido de credenciales.
- **Monitoree** la actividad de la cuenta mediante AWS CloudTrail.

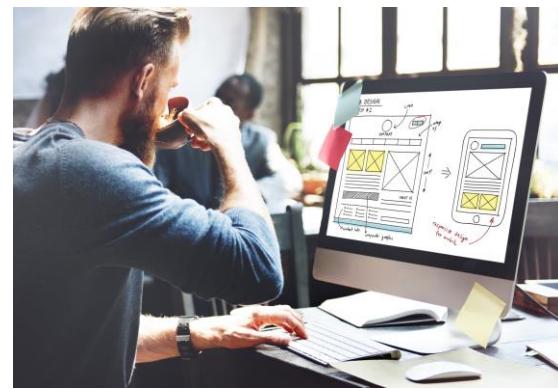
© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

52

Los aprendizajes clave de esta sección del módulo están relacionadas con las prácticas recomendadas para proteger una cuenta de AWS. Estas prácticas recomendadas son las siguientes:

- Proteja los inicios de sesión con Multi-Factor Authentication (MFA).
- Elimine las claves de acceso de usuario raíz de la cuenta.
- Cree usuarios de IAM individuales y otorgue permisos de acuerdo con el principio de mínimo privilegio.
- Utilice grupos para asignar permisos a usuarios de IAM.
- Configure una política de contraseñas sólida.
- Delegue el uso de roles en lugar del uso compartido de credenciales.
- Monitoree la actividad de la cuenta con AWS CloudTrail.

Laboratorio 1: Introducción a IAM



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

53

Presentación del laboratorio 1: Introducción a IAM de AWS

Laboratorio 1: tareas

- Tarea 1: analizar los usuarios y los grupos
- Tarea 2: agregar usuarios a los grupos
- Tarea 3: iniciar sesión y probar los usuarios



AWS Identity and
Access Management
(IAM)



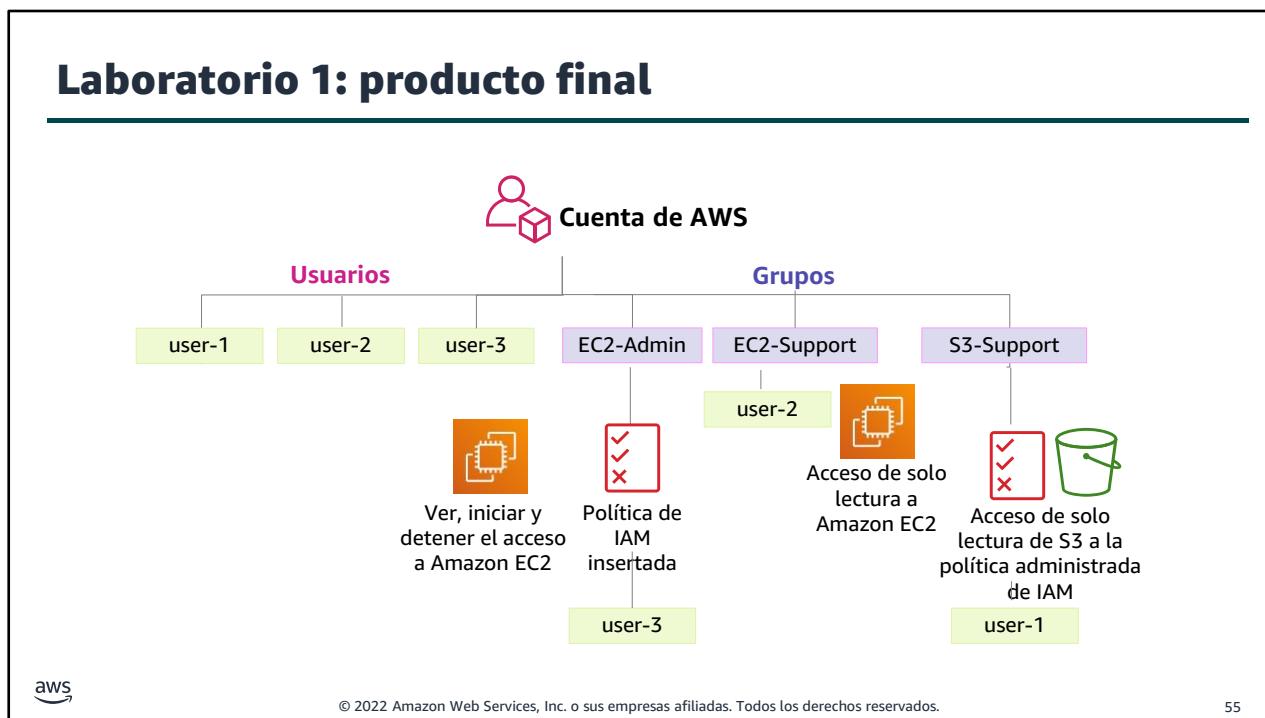
© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

54

En este laboratorio práctico, podrá hacer lo siguiente:

- Analizar usuarios y grupos de IAM creados previamente
- Inspeccionar políticas de IAM a medida que se apliquen a los grupos creados previamente
- Seguir una situación real y agregar usuarios a grupos que tengan capacidades específicas habilitadas
- Ubicar y usar la URL de inicio de sesión de la IAM
- Experimentar con los efectos de las políticas de IAM en el acceso a los recursos de AWS

Laboratorio 1: producto final



En el diagrama, se muestran los recursos que tendrá su cuenta de AWS después de completar los pasos del laboratorio. También, se describe cómo se configurarán los recursos.



~ 40 minutes

Comience el laboratorio 1: Introducción a AWS IAM

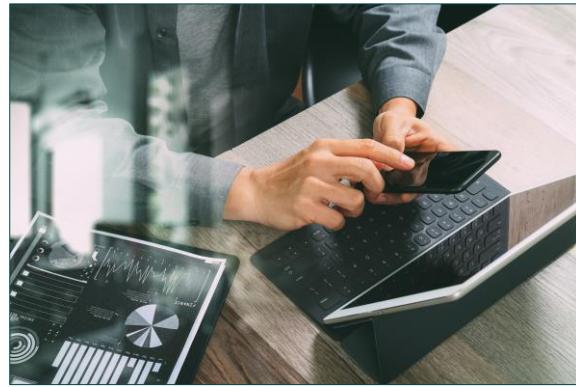
aws

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

56

Ha llegado el momento de iniciar el laboratorio.

Análisis posterior del laboratorio: aprendizajes clave



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

57

El profesor guiará ahora una conversación sobre los aprendizajes clave del laboratorio después de completarlo.

Sección 4: Protección de cuentas

Módulo 4: Seguridad en la nube de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Presentación de la sección 4: Protección de cuentas

AWS Organizations

- **AWS Organizations** le permite consolidar varias cuentas de AWS para que las administre de forma centralizada.



AWS Organizations

- Características de seguridad de AWS Organizations:

- Agrupa las cuentas de AWS en unidades organizativas (OU) y asocian las diferentes políticas de acceso a cada una de ellas.

- Permite integración y compatibilidad con IAM.

- Los permisos para un usuario son la intersección de lo que AWS Organizations permite y lo que IAM concede en esa cuenta.

- Utiliza políticas de control de servicios para establecer el control sobre las acciones de API y los servicios de AWS a los que cada cuenta de AWS puede obtener acceso.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

59

AWS Organizations es un servicio de administración de cuentas que le permite unificar varias cuentas de AWS en una *organización* que crea y administra de manera centralizada. Aquí, nos centraremos en las características de seguridad que ofrece AWS Organizations.

Una característica de seguridad útil es que puede **agrupar cuentas en unidades organizativas** (OU) y asociar diferentes políticas de acceso a cada unidad organizativa. Por ejemplo, si tiene cuentas que deben tener acceso solo a los servicios de AWS que cumplan determinados requisitos normativos, puede colocar esas cuentas en una unidad organizativa. A continuación, puede definir una política que bloquee el acceso de la unidad organizativa a los servicios que no cumplen esos requisitos normativos y, luego, asociar la política a la unidad organizativa.

Otra característica de seguridad es que **AWS Organizations se integra a IAM y lo admite**. Con AWS Organizations, se amplía ese control al nivel de cuenta, ya que le permite controlar lo que pueden hacer los usuarios y roles de una cuenta o grupo de cuentas. Los permisos resultantes son la intersección lógica de lo que permite la configuración de la política de AWS Organizations y los permisos que IAM concede de forma explícita en la cuenta para ese usuario o rol. El usuario solo puede tener acceso a lo que permiten **ambas** políticas: las de AWS Organizations y las de IAM.

Por último, AWS Organizations **proporciona políticas de control de servicios (SCP)** que le permiten especificar los permisos máximos que pueden tener las cuentas miembro de la organización. En las SCP, puede restringir a qué acciones individuales, recursos y servicios de AWS pueden obtener acceso los usuarios y roles de cada cuenta miembro.

Estas restricciones incluso anulan a los administradores de las cuentas miembro.

Cuando AWS Organizations bloquea el acceso a un servicio, un recurso o una acción de la API, ningún usuario o rol de esa cuenta puede obtener acceso a él, aunque un administrador de una cuenta miembro conceda dichos permisos de forma explícita en una política.

AWS Organizations: política de control de servicios

- Las **políticas de control de servicios (SCP)** ofrecen control centralizado sobre las cuentas.
 - Limita los permisos disponibles en una cuenta que forma parte de la organización.
- Garantiza que las cuentas cumplan con las directrices de control de acceso.
- Las SCP son *similares* a las políticas de permisos de IAM:
 - Utilizan una sintaxis similar.
 - Sin embargo, una SCP nunca concede permisos.
 - En su lugar, las SCP **especifican los permisos máximos** para una organización.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

60

Aquí se ofrece un análisis más detallado de la característica de **políticas de control de servicios (SCP)** de AWS Organizations.

Las SCP ofrecen control central de los **permisos máximos disponibles** para todas las cuentas de la organización. De esta manera, le permite asegurarse de que sus cuentas cumplan en todo momento las directrices de control de acceso de la organización. Las SCP solo están disponibles en una organización que tiene todas las características habilitadas, incluida la facturación unificada. Las SCP no están disponibles si su organización ha habilitado únicamente las características de facturación unificada. Para obtener instrucciones sobre cómo habilitar las SCP, consulte Habilitación y deshabilitación de un tipo de política en un nodo raíz.

Las **SCP son similares a las políticas de IAM** y utilizan prácticamente la misma sintaxis. Sin embargo, una SCP nunca concede permisos. Las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). Asociar una SCP al nodo raíz de la organización o a una unidad organizativa (OU) establece una protección para las acciones que pueden realizar las cuentas del nodo raíz de la organización o la unidad organizativa. Sin embargo, no sustituye las configuraciones de IAM bien administradas dentro de cada cuenta. Además, tendrá que asociar políticas de IAM a los usuarios y a los roles de las cuentas de la organización para concederles realmente los permisos.

AWS Key Management Service (AWS KMS)

Características de **AWS Key Management Service (AWS KMS)**:

- Le permite **crear y administrar claves de cifrado**.
- Le permite controlar el uso del cifrado en los servicios de AWS y en sus aplicaciones.
- Se integra con AWS CloudTrail para registrar el uso de todas las claves.
- Utiliza módulos de seguridad de hardware (HSM) validados por *Federal Information Processing Standards* (FIPS, Estándar de procesamiento de la información federal) 140-2 para proteger las claves.



AWS Key Management Service (AWS KMS)



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

61

AWS Key Management Service (AWS KMS) es un servicio que le permite crear y administrar claves de cifrado, así como controlar el uso del cifrado en una amplia gama de servicios de AWS y sus aplicaciones. AWS KMS es un servicio seguro y resistente que utiliza módulos de seguridad de hardware (HSM) validados según el **Estándar de procesamiento de la información federal (FIPS) 140-2** (o en proceso de validación) para proteger sus claves. AWS KMS también se integra AWS CloudTrail para ofrecerle los registros de uso de todas las claves a fin de que satisfagan sus necesidades vinculadas con asuntos normativos y de conformidad.

Las **claves maestras de cliente (CMK)** se utilizan para controlar el acceso a las claves de cifrado de datos que cifran y descifran los datos. Puede crear nuevas claves maestras cuando lo desee y puede administrar quién tiene acceso a estas claves y en qué servicios se pueden utilizar. Además, puede importar claves de su propia infraestructura de administración de claves en AWS KMS.

AWS KMS se integra a la mayoría de los servicios de AWS, lo que significa que puede utilizar claves maestras de AWS KMS para controlar el cifrado de los datos que almacena en estos servicios. Para obtener más información, consulte las [características de AWS Key Management Service](#).

Amazon Cognito

Características de Amazon Cognito:

- Incorpora control de acceso, inicio de sesión y registro de usuarios a sus aplicaciones web y móviles.
- Escala a millones de usuarios.
- Admite el inicio de sesión con proveedores de identidad social, como Facebook, Google y Amazon; y proveedores de identidades empresariales, como Microsoft Active Directory a través del lenguaje de marcado para confirmaciones de seguridad (SAML) 2.0.



Amazon Cognito



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

62

Amazon Cognito ofrece soluciones para controlar el acceso a recursos de AWS desde su aplicación. Puede definir los roles y asignar usuarios a diferentes roles para que su aplicación únicamente pueda acceder a los recursos autorizados para cada usuario.

Amazon Cognito utiliza estándares comunes de administración de identidades, como el **lenguaje de marcado para confirmaciones de seguridad (SAML) 2.0**. SAML es un estándar abierto para intercambiar información de identidad y seguridad con aplicaciones y proveedores de servicios. Las aplicaciones y los proveedores de servicios compatibles con SAML le permiten iniciar sesión con las credenciales del directorio corporativo, como el nombre de usuario y la contraseña de Microsoft Active Directory. Con SAML, puede utilizar el inicio de sesión único (SSO) para iniciar sesión en todas las aplicaciones compatibles con SAML mediante un único conjunto de credenciales.

Amazon Cognito lo ayuda a cumplir varios requisitos de seguridad y conformidad, incluidos aquellos a los que deben ajustarse las organizaciones con niveles estrictos de regulación, como las compañías del sector de la sanidad y los comerciantes. Amazon Cognito puede utilizarse con la Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU. ([HIPAA](#)). Además, se puede utilizar para cargas de trabajo que cumplen con el estándar de seguridad de datos del sector de tarjetas de pago ([PCI DSS](#)), el control de organizaciones ([SOC](#)) del Instituto americano de contadores públicos certificados (AICPA), la Organización Internacional de Normalización (ISO) y

los estándares de la Comisión Electrotécnica Internacional (IEC) [ISO/IEC 27001](#), [ISO/IEC 27017](#), e [ISO/IEC 27018](#); e [ISO 9001](#).

AWS Shield

- Características de **AWS Shield**:

- Es un servicio administrado de protección contra ataques de denegación de servicio distribuidos (DDoS).
- Protege las aplicaciones que se ejecutan en AWS.
- Proporciona detección permanente y mitigaciones directas automáticas.
- Se puede habilitar *AWS Shield Standard* sin costo adicional. *AWS Shield Advanced* es un servicio de pago opcional.

- Utilícelo para **minimizar el tiempo de inactividad y la latencia de la aplicación.**



AWS Shield



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

63

AWS Shield es un servicio administrado de protección contra ataques de denegación de servicio distribuidos (DDoS) que protege las aplicaciones ejecutadas en AWS. Ofrece detección permanente y mitigaciones directas automáticas que reducen el tiempo de inactividad y latencia de las aplicaciones, por lo que no hay necesidad de contar con AWS Support para disfrutar de la protección de DDoS.

AWS Shield le ayuda a proteger su sitio web de todos los tipos de ataques DDoS, incluidos los ataques en la capa de la infraestructura (como las inundaciones del protocolo de datagramas de usuario o inundaciones [o UDP]), los ataques de agotamiento de estado (como las inundaciones TCP SYN) y los ataques en la capa de la aplicación (como las inundaciones HTTP GET o POST). Para ver ejemplos, consulte la [guía para desarrolladores de AWS WAF y AWS Shield Advanced](#).

AWS Shield Standard se habilita automáticamente para todos los clientes de AWS sin costo adicional.

AWS Shield Advanced es un servicio de pago opcional. AWS Shield Advanced ofrece protecciones adicionales ante los ataques más grandes y sofisticados para las aplicaciones que se ejecutan en Amazon EC2, Elastic Load Balancing, Amazon CloudFront, AWS Global Accelerator y Amazon Route 53. AWS Shield Advanced está disponible para todos los clientes. Sin embargo, para ponerse en contacto con el

equipo de respuesta de DDoS, los clientes necesitan contar con Enterprise Support o Business Support de AWS Support.

Sección 5: Protección de datos en AWS

Módulo 4: Seguridad en la nube de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Presentación de la sección 5: Protección de datos en AWS

Cifrado de datos en reposo

- El **cifrado** codifica los datos con una **clave secreta**, lo que hace que sean ilegibles.
 - Solo aquellos que tienen la clave secreta pueden descodificar los datos.
 - **AWS KMS** puede administrar sus claves secretas.



- AWS admite el cifrado de **datos en reposo**.

- Datos en reposo = datos almacenados físicamente (en disco o en cinta)
- Puede cifrar los datos almacenados en cualquier servicio compatible con AWS KMS, como los siguientes:
 - Amazon S3
 - Amazon EBS
 - Amazon Elastic File System (Amazon EFS)
 - Bases de datos administradas de Amazon RDS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

65

El **cifrado de datos** es una herramienta esencial cuando desea proteger los datos digitales. El cifrado de datos toma datos legibles y los codifica de forma que sean ilegibles para cualquiera que no tenga acceso a la clave secreta y quiera utilizarla para decodificarlos. Por lo tanto, aunque un atacante obtenga acceso a sus datos, no podrá entenderlos.

Los datos en reposo se refieren a datos que se almacenan físicamente en disco o en cinta.

Puede crear sistemas de archivos cifrados en AWS para que todos sus datos y metadatos se cifren en reposo mediante el algoritmo de cifrado estándar y abierto Advanced Encryption Standard (AES) de 256 bits. Cuando utiliza AWS KMS, el cifrado y el descifrado se gestionan de forma automática y transparente, por lo que no es necesario modificar sus aplicaciones. Si su organización está sujeta a políticas corporativas o normativas que requieren el cifrado de datos y metadatos en reposo, AWS recomienda que habilite el cifrado en todos los servicios que almacenan sus datos. Puede cifrar los datos almacenados en cualquier servicio compatible con AWS KMS. Consulte [cómo los servicios de AWS utilizan AWS KMS](#) para obtener una lista de los servicios admitidos.

Cifrado de datos en tránsito

- Cifrado de **datos en tránsito** (datos que migran a través de una red)
 - **Transport Layer Security (TLS)**, anteriormente SSL, es un protocolo estándar abierto.
 - **AWS Certificate Manager** ofrece una forma de administrar, implementar y renovar certificados TLS o SSL
- HTTP seguro (**HTTPS**) crea un túnel seguro.
 - Utiliza TLS o SSL para el intercambio bidireccional de datos.
- **Los servicios de AWS admiten el cifrado de datos en tránsito.**



- Dos ejemplos:



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

66

Los **datos en tránsito** se refieren a los datos que se mueven a través de la red. El cifrado de los datos en tránsito se realiza mediante el uso de la seguridad de Transport Layer Security (TLS) 1.2 con un cifrado AES de 256 bits estándar abierto. TLS anteriormente se denominaba capa de conexión segura (SSL).

AWS Certificate Manager es un servicio que le permite aprovisionar, administrar e implementar certificados SSL o TLS para su uso con los servicios de AWS y sus recursos internos conectados. Los certificados de SSL o TLS se usan para proteger las comunicaciones por red y para definir la identidad de sitios web mediante Internet y recursos en redes privadas. Con AWS Certificate Manager, puede solicitar un certificado y, luego, implementarlo en recursos de AWS (como平衡adores de carga o distribuciones de CloudFront). AWS Certificate Manager también se encarga de renovar certificados.

El tráfico web que se ejecuta a través de HTTP no es seguro. Sin embargo, el tráfico que se ejecuta a través de **HTTP seguro (HTTPS)** se cifra mediante TLS o SSL. El tráfico HTTPS está protegido contra ataques de acceso no autorizados y ataques de intermediario debido al cifrado bidireccional de la comunicación.

Los servicios de AWS admiten el cifrado de datos en tránsito. Se muestran dos ejemplos de cifrado para datos en tránsito. El primer ejemplo muestra una instancia

EC2 que ha montado un sistema de archivos compartidos de Amazon EFS. Todo el tráfico de datos entre la instancia y Amazon EFS se cifra mediante TLS o SSL. Para obtener más información acerca de esta configuración, consulte [Cifrado de datos de EFS en tránsito](#).

El segundo ejemplo muestra el uso de **AWS Storage Gateway**, un servicio de almacenamiento en la nube híbrida que proporciona acceso en las instalaciones al almacenamiento en la nube de AWS. En este ejemplo, la gateway de almacenamiento está conectada a través de Internet a Amazon S3 y la conexión cifra los datos en tránsito.

Protección de buckets y objetos de Amazon S3

- Los buckets y objetos de S3 recientemente creados son **privados** y están **protegidos** de forma predeterminada.
- Cuando los casos de uso requieren compartir objetos de datos en Amazon S3:
 - Es fundamental administrar y controlar el acceso a los datos.
 - Siga los **permisos que siguen el principio de privilegio mínimo** y considere la posibilidad de utilizar el cifrado de Amazon S3.
- Entre las herramientas y opciones para controlar el acceso a los datos de S3 se incluyen las siguientes:
 - [Característica de Amazon S3 Block Public Access](#): es fácil de usar.
 - Políticas de IAM: son una buena opción cuando el usuario puede autenticarse con IAM.
 - [Políticas de buckets](#)
 - [Listas de control de acceso](#) (ACL): son un mecanismo de control de acceso heredado.
 - Comprobación de permisos del bucket de [AWS Trusted Advisor](#): es una característica gratuita.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

67

De forma predeterminada, todos los buckets de Amazon S3 son privados y *solo* pueden acceder los usuarios a los que se les concede acceso explícitamente. Es fundamental administrar y controlar el acceso a los datos de Amazon S3. AWS proporciona muchas herramientas y opciones para controlar el acceso a sus buckets u objetos de S3, entre los que se incluyen los siguientes:

- El uso de **Amazon S3 Block Public Access**. Esta configuración anula cualquier otra política o permisos de objetos. Habilite **Block Public Access** para todos los buckets que no deseé que sean accesibles públicamente. Esta característica proporciona un método sencillo para evitar la exposición no deseada de datos de Amazon S3.
- La escritura de **políticas de IAM** que especifiquen los usuarios o roles que pueden obtener acceso a buckets y objetos específicos. Este método se ha tratado en detalle anteriormente en este módulo.
- La escritura de **políticas de bucket** que definan el acceso a buckets u objetos específicos. Esta opción se suele utilizar cuando el usuario o el sistema no pueden autenticarse mediante IAM. Las políticas de bucket se pueden configurar para conceder acceso entre cuentas de AWS o para conceder acceso público o anónimo a los datos de Amazon S3. Si se utilizan políticas de bucket, deben escribirse detenidamente y probarse en su totalidad. Puede especificar una instrucción de

denegación en una política de bucket para restringir el acceso. El acceso estará restringido incluso si los usuarios tienen permisos concedidos en una política basada en identidad asociada a los usuarios.

- Configuración de **listas de control de acceso (ACL)** en sus buckets y objetos. Las ACL se utilizan con menos frecuencia (las ACL preceden a la IAM). Si utiliza ACL, no establezca un acceso demasiado abierto o permisivo.
- **AWS Trusted Advisor** proporciona una característica de comprobación de permisos de buckets, que es una herramienta útil para descubrir si alguno de los buckets de su cuenta tiene permisos que conceden acceso global.

Sección 6: Trabajo para garantizar la conformidad

Módulo 4: Seguridad en la nube de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Presentación de la sección 6: Trabajo para garantizar la conformidad.

Programas de conformidad de AWS

- Los clientes están sujetos a diferentes reglamentos y requisitos de seguridad y conformidad.
 - AWS colabora con organismos de certificación y auditores independientes para ofrecer a los clientes información detallada sobre las políticas, los procesos y los controles que establece y aplica AWS.**
- Los programas de conformidad pueden clasificarse en las siguientes categorías generales:
- Certificaciones y acreditaciones**
 - Evaluadas por un auditor de terceros independiente
 - Ejemplos: ISO 27001, 27017, 27018 e ISO/IEC 9001
 - Leyes, regulaciones y privacidad**
 - AWS ofrece características de seguridad y acuerdos legales para respaldar la conformidad
 - Ejemplos: Reglamento General de Protección de Datos (GDPR) de la UE, HIPAA
 - Alineaciones y marcos de trabajo**
 - Requisitos de conformidad o seguridad específicos de cada sector o función
 - Ejemplos: Centro de seguridad en Internet (CIS), certificado por el Escudo de la privacidad UE-EE. UU.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

69

AWS colabora con organismos de certificación externos y auditores independientes para ofrecer a los clientes información sobre las políticas, los procesos y los controles que establece y aplica AWS.

Se encuentra disponible una [lista de los programas de conformidad de AWS](#) en su totalidad. Además, para obtener más información acerca de qué servicios de AWS están incluidos en el ámbito de los programas de garantía de AWS, consulte [Servicios de AWS en el ámbito del programa de conformidad](#).

Como ejemplo de una **certificación** en la que puede utilizar los servicios de AWS para cumplir sus objetivos de conformidad, considere la certificación **ISO/IEC 27001:2013**. Específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de administración de seguridad de la información. La base de esta certificación es el desarrollo y la implementación de un programa de seguridad riguroso, que incluye el desarrollo y la implementación de un sistema de administración de seguridad de la información. El sistema de administración de la seguridad de la información define cómo AWS administra constantemente la seguridad de una manera integral.

AWS también ofrece características de seguridad y acuerdos legales diseñados para ayudar a los clientes con regulaciones y leyes comunes. Un ejemplo es el reglamento

de la **Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA)**. Otro ejemplo es el **Reglamento General de Protección de Datos (RGPD)** de la Unión Europea (UE), que protege el derecho fundamental a la privacidad y la protección de datos personales de los titulares de datos pertenecientes a la Unión Europea. Introduce requisitos estrictos que reforzarán y armonizarán las normas de protección de datos, seguridad y conformidad. El [Centro del GDPR](#) contiene muchos recursos para ayudar a los clientes a cumplir sus requisitos de conformidad con esta normativa.

AWS Config

Ejemplo de la vista del panel de AWS Config



The screenshot shows the AWS Config dashboard with the following details:

- Resources:** Total resource count: 48
- Config rule compliance:** Noncompliant rule(s): 1
- Resource compliance:** Noncompliant resource(s): 35
- Noncompliant rules:**

Rule name	Compliance
required-tags	25+ noncompliant resources

Below the dashboard, there is a table of contents for AWS Config documentation.

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados. 70

AWS Config es un servicio que le permite analizar, auditar y evaluar las configuraciones de sus recursos de AWS. AWS Config monitorea y registra constantemente las configuraciones de sus recursos de AWS y le permite automatizar la evaluación de las configuraciones registradas frente a las configuraciones deseadas. Con AWS Config, puede revisar los cambios en las configuraciones y las relaciones entre los recursos de AWS, revisar los históricos detallados de configuración de recursos y determinar la conformidad general con respecto a las configuraciones especificadas en sus pautas internas. Esto le permite simplificar las auditorías de conformidad, los análisis de seguridad, la administración de cambios y la resolución de problemas operativos.

Como puede ver en la captura de pantalla del panel de AWS Config que se muestra aquí, AWS Config mantiene una lista de inventario de todos los recursos que existen en la cuenta y, a continuación, comprueba la conformidad de las reglas de configuración y de los recursos. Se marcan los recursos que se consideran no conformes, lo cual le avisa de los problemas de configuración que deben resolverse en la cuenta.

AWS Config es un servicio regional. Para realizar un seguimiento de los recursos entre regiones, habilítelo en todas las regiones que utilice. AWS Config ofrece una característica de agregador que puede mostrar una vista agregada de recursos en varias regiones e incluso en varias cuentas.

AWS Artifact



AWS Artifact

- **Es un recurso destinado a la información relacionada con la conformidad.**
- Proporciona acceso a informes de seguridad y conformidad, así como también a acuerdos en línea seleccionados.
- Puede obtener acceso a descargas de ejemplo:
 - Certificaciones ISO de AWS
 - Informes del sector de tarjetas de pago (PCI) y del control de organizaciones de servicios (SOC)
- Puede acceder a AWS Artifact directamente desde la consola de administración de AWS
 - En **Security, Identify & Compliance** (Seguridad, identidad y conformidad), haga clic en **Artifact**.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

71

AWS Artifact proporciona descargas bajo demanda de documentos de seguridad y conformidad de AWS, como certificaciones ISO de AWS e informes del sector de tarjetas de pago (PCI) y del control de organizaciones de servicios (SOC). Puede enviar los documentos de seguridad y conformidad (también conocidos como *artefactos de auditoría*) a sus auditores o reguladores para demostrar la seguridad y el cumplimiento de la infraestructura y los servicios de AWS que utiliza. También puede usar estos documentos como directrices para evaluar su propia arquitectura en la nube y evaluar la efectividad de los controles internos de su empresa. AWS Artifact solo proporciona documentos sobre AWS. Los clientes de AWS son los responsables de desarrollar u obtener documentos que demuestren la seguridad y la conformidad de sus empresas.

Puede utilizar AWS Artifact para revisar, aceptar y realizar un seguimiento del estado de los acuerdos de AWS, como el Acuerdo para socio empresarial (BAA). Un BAA suele ser necesario para las empresas sujetas al HIPAA a fin de garantizar la protección adecuada de la información sanitaria protegida (PHI). Con AWS Artifact, puede aceptar los acuerdos con AWS; y designar cuentas de AWS que puedan procesar legalmente información restringida. Puede aceptar un acuerdo en nombre de varias cuentas. Para aceptar acuerdos de varias cuentas, cree una organización con AWS Organizations. Para obtener más información, consulte [Administración de sus acuerdos en AWS Artifact](#).

Aprendizajes clave de la sección 6



- Los **programas de conformidad de seguridad de AWS** proporcionan información acerca de las políticas, los procesos y los controles que establece y opera AWS.
- **AWS Config** se utiliza para analizar, auditar y evaluar las configuraciones de los recursos de AWS.
- **AWS Artifact** proporciona acceso a informes de seguridad y conformidad.

© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

72

Estos son algunos de los aprendizajes clave de esta sección del módulo:

- Los programas de conformidad de seguridad de AWS proporcionan información acerca de las políticas, los procesos y los controles que establece y opera AWS.
- AWS Config se utiliza para analizar, auditar y evaluar las configuraciones de los recursos de AWS.
- AWS Artifact proporciona acceso a informes de seguridad y conformidad.

Conclusión del módulo

Módulo 4: Seguridad en la nube de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Ha llegado el momento de hacer un repaso del módulo y concluir con una revisión de conocimientos y un debate sobre una pregunta del examen de certificación como práctica

Resumen del módulo

En resumen, en este módulo, aprendió a hacer lo siguiente:

- Reconocer el modelo de responsabilidad compartida
- Identificar la responsabilidad del cliente y de AWS
- Reconocer usuarios, grupos y roles de IAM
- Describir los diferentes tipos de credenciales de seguridad en IAM
- Identificar los pasos para proteger una nueva cuenta de AWS
- Explorar los usuarios y los grupos de IAM
- Reconocer cómo proteger los datos de AWS
- Reconocer los programas de conformidad de AWS



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

77

En resumen, en este módulo, aprendió a hacer lo siguiente:

- Reconocer el modelo de responsabilidad compartida
- Identificar la responsabilidad del cliente y de AWS
- Reconocer usuarios, grupos y roles de IAM
- Describir los diferentes tipos de credenciales de seguridad en IAM
- Identificar los pasos para proteger una nueva cuenta de AWS
- Explorar los usuarios y los grupos de IAM
- Reconocer cómo proteger los datos de AWS
- Reconocer los programas de conformidad de AWS

Complete la revisión de conocimientos



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

78

Ha llegado el momento de completar la revisión de conocimientos de este módulo.



Pregunta de examen de ejemplo

¿Cuál de las siguientes opciones es responsabilidad de AWS en virtud del Modelo del responsabilidad compartida de AWS?

Opción Respuesta

- A** Configuración de aplicaciones de terceros
- B** Mantenimiento del hardware físico
- C** Protección del acceso a la aplicación y de los datos
- D** Administración de las imágenes de máquina de Amazon (AMI) personalizadas.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

79

Mire las opciones de respuesta y descártelas según las palabras clave.



Respuesta a la pregunta de examen de ejemplo

¿Cuál de las siguientes opciones es responsabilidad de AWS en virtud del Modelo del responsabilidad compartida de AWS?

La respuesta correcta es la B.

Las palabras clave de la pregunta son “responsabilidad de AWS” y “modelo de responsabilidad compartida de AWS”.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

80

Las siguientes son las palabras clave que se deben reconocer: **“Responsabilidad de AWS” y “Modelo de responsabilidad compartida de AWS”**.

La respuesta correcta es la B.

Este ejemplo de pregunta de examen proviene del documento de preguntas de ejemplo de AWS Certified Cloud Practitioner al que se puede acceder desde la página principal de información del examen AWS Certified Cloud Practitioner en <https://aws.amazon.com/certification/certified-cloud-practitioner/>.

Recursos adicionales

- Página de inicio de Seguridad en la nube de AWS: <https://aws.amazon.com/security/>
- Recursos de seguridad de AWS: https://aws.amazon.com/security/security-learning/?cards-top.sort-by=item.additionalFields.sortDate&cards-top.sort-order=desc&awsf.Types=*all
- Blog de seguridad de AWS: <https://aws.amazon.com/blogs/security/>
- Boletines de seguridad: https://aws.amazon.com/security/security-bulletins/?card-body.sort-by=item.additionalFields.bulletinId&card-body.sort-order=desc&awsf.bulletins-flag=*all&awsf.bulletins-year=*all
- Pruebas de intrusión y vulnerabilidad: <https://aws.amazon.com/security/penetration-testing/>
- Marco de Buena Arquitectura de AWS: pilar de seguridad:
<https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf>
- Documentación de AWS: prácticas recomendadas de IAM:
<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

81

- Página de inicio de Seguridad en la nube de AWS: <https://aws.amazon.com/security/>
- Recursos de seguridad de AWS: https://aws.amazon.com/security/security-learning/?cards-top.sort-by=item.additionalFields.sortDate&cards-top.sort-order=desc&awsf.Types=*all
- Blog de seguridad de AWS: <https://aws.amazon.com/blogs/security/>
- Boletines de seguridad: https://aws.amazon.com/security/security-bulletins/?card-body.sort-by=item.additionalFields.bulletinId&card-body.sort-order=desc&awsf.bulletins-flag=*all&awsf.bulletins-year=*all
- Pruebas de intrusión y vulnerabilidad: <https://aws.amazon.com/security/penetration-testing/>
- Marco de Buena Arquitectura de AWS: pilar de seguridad:
<https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf>
- Documentación de AWS: prácticas recomendadas de IAM:
<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

Gracias

Todas las marcas comerciales pertenecen a sus propietarios.



© 2022 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

82

Gracias por completar este módulo.