NIVEL INTEGRADOR - MÓDULO 1 - UNIDAD 1 - Lección 3

ACTIVIDAD

Ahora completará una actividad sobre el modelo de responsabilidad compartida y las responsabilidades de AWS y el cliente.

ACTIVIDAD
Escenario 1 de 2

Considere ¿Quién es responsable: AWS o el cliente?

Para consolidar las respuestas ingrese al cuestionario online.

El diagrama arquitectónico muestra un cuadro de la nube de AWS que contiene un área de infraestructura global de AWS, así como un bucket de Amazon S3 y, finalmente, una VPC que contiene una instancia de Amazon EC2y una instancia de Oracle.

Considere el caso en el que un cliente utiliza los recursos y servicios de AWS que se muestran aquí. El cliente utiliza Amazon S3 para almacenar datos. El cliente administra una VPC que contiene una instancia de EC2 y una instancia de Amazon
RDS para Oracle Database.

¿Quién es responsable de mantener la seguridad de cada componente? ¿AWS o el cliente?

ACTIVIDAD

Respuestas escenario 1 de 2

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

1 ¿Actualizaciones de parches del sistema operativo en la instancia de EC2?

Respuesta: El cliente

2 ¿Seguridad física de los centros de datos?

Respuesta: AWS

3 ¿Infraestructura de virtualización?

Respuesta: AWS

4 ¿Configuración del grupo de seguridad EC2?

Respuesta: El cliente

5 ¿Configuración de aplicaciones que se ejecutan en la instancia de 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 de EC2?

Respuesta: El cliente

8 ¿Configuraciones de acceso al bucket de S3?

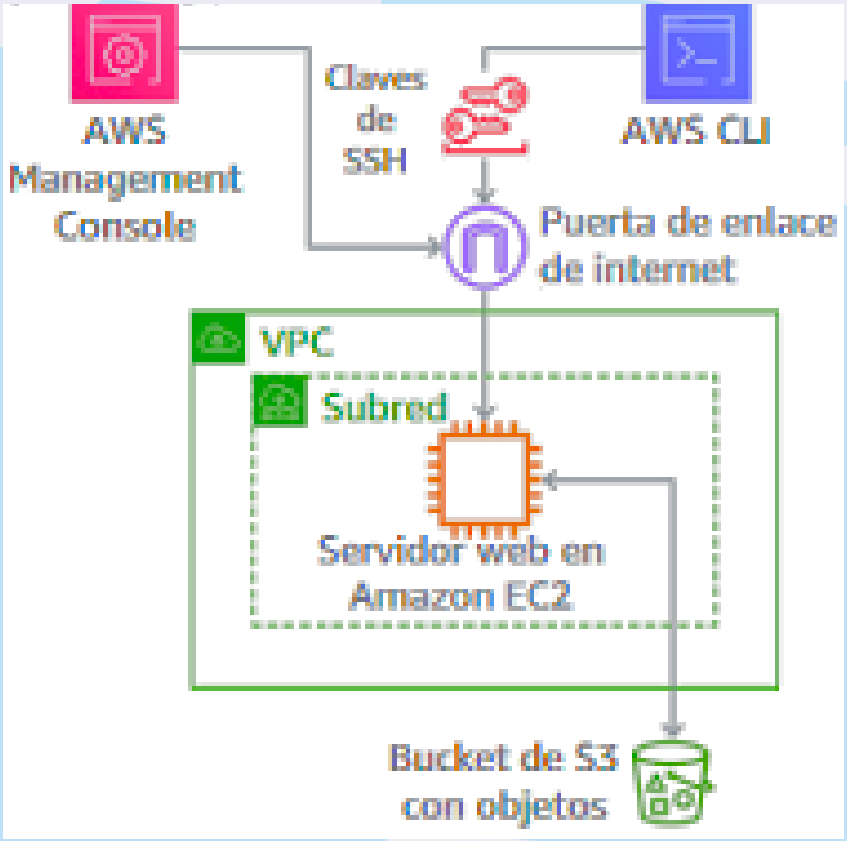
Respuesta: El cliente

El diagrama arquitectónico muestra un cuadro de la nube de AWS que contiene un área de infraestructura global de AWS, así como un bucket de Amazon S3 y, finalmente, una VPC que contiene una instancia de Amazon EC2 y una instancia de Oracle.

El cliente controla la seguridad en la nube. En el escenario anterior, esto incluye actualizar y parchear el sistema operativo huésped y el software de la aplicación asociada en la instancia de EC2, y la configuración del firewall del grupo de seguridad proporcionado por AWS. Debido a que la responsabilidad del cliente está determinada por los servicios de la nube de AWS que seleccione, las actualizaciones o los parches de Oracle serán responsabilidad del cliente si ejecuta la base de datos de Oracle en una instancia de EC2. El cliente también es responsable de utilizar las herramientas de IAM para aplicar los permisos correctos en el nivel de la plataforma, como para los buckets de S3, y en el nivel de usuario o grupo de IAM.
AWS administra la seguridad de la nube al garantizar que la infraestructura de AWS cumpla con los requisitos reglamentarios y las prácticas recomendadas globales y regionales. AWS opera, administra y controla los componentes desde el sistema operativo del host y la capa de virtualización hasta la seguridad física de las instalaciones en las que opera el servicio.
En este ejemplo, AWS es responsable de la seguridad física del centro de datos y la infraestructura de virtualización. Si la instancia de Oracle se ejecuta como una instancia de Amazon RDS, AWS es responsable de las actualizaciones y los parches de Oracle. Amazon RDS automatiza tareas administrativas comunes, como realizar copias de seguridad y aplicar parches al software que alimenta su base de datos.

ACTIVIDAD
Escenario 2 de 2

Considere ¿Quién es responsable: AWS o el cliente?



Para consolidar las respuestas ingrese al cuestionario online.

El diagrama arquitectónico en el que se muestra un servidor web que se ejecuta en EC2 dentro de una subred y VPC. El servidor web se conecta a un bucket de S3. Se puede acceder al servidor web a través de una puerta de enlace de Internet, ya sea mediante la consola de administración de AWS o mediante la Command Line Interface de AWS, que utiliza claves SSH.

Ahora, considere este caso adicional en el que un cliente utiliza los servicios y recursos de AWS que se muestran aquí.
Un cliente utiliza Amazon S3 para almacenar datos. El cliente configuró una nube virtual privada (VPC) con Amazon VPC y está ejecutando un servidor web en una instancia de EC2 en la VPC. El cliente configuró una puerta de enlace de Internet como parte de la VPC para que se pueda acceder al servidor web mediante la consola de administración de AWS o Command Line Interface de AWS (AWS CLI). Cuando el cliente utiliza la AWS CLI, la conexión requiere el uso de claves de
Secure Shell (SSH).

¿Quién es responsable de mantener la seguridad de cada componente? ¿AWS o el cliente?

ACTIVIDAD

Respuestas 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 pirata?
   Respuesta: AWS

2. ¿Configurando la subred?
   Respuesta: El cliente

3. ¿Configurando la VPC?
   Respuesta: El cliente

4. ¿Protección contra las interrupciones de la red en las regiones AWS?
   Respuesta: AWS

5. ¿Proteger las claves SSH?
   Respuesta: El cliente

6. ¿Garantizar el aislamiento de la 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. ¿Hacer cumplir la autenticación multifactor para todos los inicios de sesión de los usuarios?
   Respuesta: El cliente

El diagrama arquitectónico en el que se muestra un servidor web que se ejecuta en EC2 dentro de una subred y VPC. El servidor web se conecta a un bucket de S3. Se puede acceder al servidor web a través de una puerta de enlace de Internet, ya sea mediante la consola de administración de AWS o mediante la Command Line Interface de AWS, que utiliza claves SSH.

En el modelo de responsabilidad compartida, el cliente es responsable de lo que implementa al usar AWS y de las aplicaciones que están conectadas a la nube de AWS. En este ejemplo, el cliente es responsable de configurar la VPC y la subred, proteger las claves SSH y aplicar la autenticación multifactor para todos los inicios de sesión de los usuarios.

Recuerde que los clientes son responsables de la seguridad del contenido que colocan en la nube de AWS o que conectan a su infraestructura de AWS. Esto incluye contenido almacenado y procesado en almacenamiento, bases de datos u otros servicios de AWS. Como cliente de AWS, usted controla todo el ciclo de vida de su contenido en AWS y puede administrar su contenido de acuerdo con sus necesidades específicas, incluida la clasificación de contenido, el control de acceso, la retención y la eliminación.

Como se describe en el modelo de responsabilidad compartida, AWS es responsable de proteger la infraestructura global que ejecuta toda la nube de AWS. Esto incluye la infraestructura física que aloja sus recursos.
En este ejemplo, AWS es responsable de lo siguiente:

- Asegurarse de que la consola no esté pirateada
- Proteger la infraestructura contra interrupciones de la red en las regiones de AWS
- Garantizar el aislamiento de la red entre los datos de los clientes de AWS
- Garantizar una conexión de red de baja latencia entre el servidor web y el Bucket de S3