COLOMBIA POTENCIA DE LA VIDA

TIC

Lección 3 - Parte 1
Modelo de responsabilidad compartida

Modelo de responsabilidad compartida

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Modelo de responsabilidad compartida de AWS

Modelo de responsabilidad compartida en el que se enumeran las responsabilidades del cliente y de AWS. El cliente es responsable de la seguridad en la nube. Esto incluye los datos del cliente.

Administración de accesos, identidades, plataforma y aplicaciones. Configuración de firewall, red y sistema operativo. Cifrado de datos del lado del cliente e integridad de datos, autenticación. Cifrado del lado del servidor del sistema de archivos y datos. Protección del tráfico de redes, incluidos el cifrado, la integridad y la identidad. AWS es responsable de la seguridad de la nube. Esto incluye los servicios básicos de AWS para cómputo, almacenamiento, bases de datos y redes. Además, incluye la infraestructura global de AWS, que abarca las regiones, las zonas de disponibilidad y las ubicaciones perimetrales.

+INFO

La seguridad y el cumplimiento son responsabilidades compartidas entre AWS y los clientes. AWS opera, administra y controla la seguridad de la nube. Esta responsabilidad incluye asegurar los componentes, desde el sistema operativo del host y la capa de virtualización hasta la seguridad física de las instalaciones donde opera el servicio. AWS es responsable de proteger la infraestructura global que ejecuta todos los servicios que se ofrecen 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.

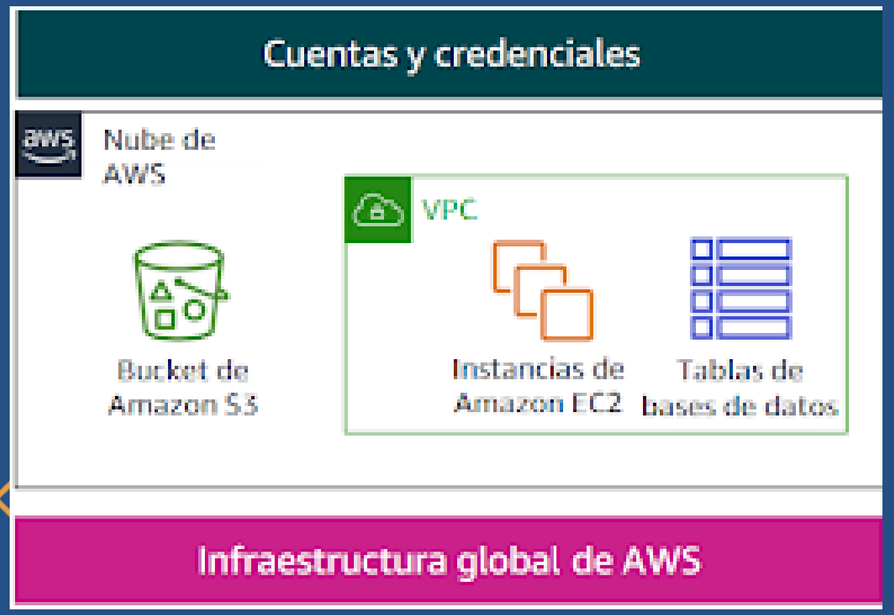
Usted asume la responsabilidad y la administración en la nube. Los pasos de seguridad que deben seguir dependen de los servicios que utilizan y de la complejidad de su sistema. Las responsabilidades del cliente incluyen seleccionar y proteger los sistemas operativos que se ejecutan en instancias EC2 y proteger las aplicaciones que se lanzan en los recursos de AWS. Los clientes también deben seleccionar y manejar configuraciones de grupos de seguridad, configuraciones de firewall, configuraciones de red y administración segura de cuentas. Los clientes también son responsables de administrar sus datos, incluidas las opciones de cifrado.

VOLVER

Para reiterar, AWS protege el hardware, el software, las instalaciones y las redes que ejecutan todos los productos y servicios de AWS. Usted es responsable de lo que implemente mediante el uso de productos y servicios de AWS, y de las aplicaciones que conecte a AWS. Los pasos de seguridad que deben seguir dependen de los servicios que utilizan y de la complejidad de su sistema.

EJEMPLO DE Responsabilidad compartida

VER



Cliente

AWS

Ejemplos de responsabilidad del cliente:

- Configuración del SO invitado
- Seguridad a nivel de aplicación
- Configuración del grupo de seguridad

Considere un ejemplo en el que su empresa utiliza Amazon S3 para almacenar datos. Su entorno de AWS también incluye instancias de EC2 y una instancia de Amazon Relational Database Service (Amazon RDS). Estos recursos ejecutan una base de datos MySQL, que se implementa dentro de una nube virtual privada (VPC). Una instancia de EC2 aloja un servidor web y la aplicación web que se ejecuta en ella utiliza la base de datos para almacenar datos de la aplicación.

En este escenario, AWS es responsable de proteger la infraestructura global, que contiene los servidores físicos que alojan las máquinas virtuales y el hardware de almacenamiento. Estas máquinas virtuales y hardware de almacenamiento alojan su bucket de S3, instancias de EC2 e instancia de base de datos. AWS es responsable de la seguridad de la infraestructura de red física que garantiza que se pueda acceder a estos componentes. AWS también es responsable de la seguridad de la capa del hipervisor que aloja las instancias de EC2. (El hipervisor el sistema operativo del host que ejecuta las instancias de EC2, que son máquinas virtuales que ejecutan sistemas operativos invitados).

VOLVER

Usted (el cliente) es responsable de administrar el sistema operativo huésped que se ejecuta en las instancias de EC2 (incluidas las actualizaciones y los parches de seguridad del sistema operativo Microsoft Windows o Linux). También es responsable de administrar cualquier software de aplicación o utilidades que instale.

Además, es responsable de la configuración de los grupos de seguridad que controlan el acceso a la red a cada instancia de EC2 ya la instancia de la base de datos RDS. También es responsable de configurar la seguridad en el
Bucket de S3 y los objetos que almacena en él. Por ejemplo, podría usar una o más de las funciones de seguridad que proporciona AWS, como políticas de buckets, cifrado de datos y acceso público a buckets de S3.

Para más información puede consultar el siguiente enlace
Modelo de responsabilidad compartida – Amazon Web Services (AWS)

Seguridad en la nube

Consideraciones

- Qué debe almacenar
- Qué servicios de AWS debe usar
- En qué región almacenar datos
- Qué formato de contenido y estructura usar
- Quién tiene acceso

Cliente

Datos del cliente

Plataforma, aplicaciones, administración de identidades y acceso

Configuración del firewall, la red y el sistema operativo

Cifrado de datos del lado del cliente y autenticación de la integridad de los datos

Cifrado del lado del servidor (sistema de archivos o datos

Protección del tráfico de red (cifrado, integridad, identidad)

Si bien AWS asegura y mantiene la infraestructura de la nube, usted es responsable de proteger todo lo que coloca en la nube.

+INFO

Antes de diseñar cualquier carga de trabajo, debe implementar prácticas que influyan en la seguridad. Querrá controlar quién puede hacer qué. Además, desea poder identificar incidentes de seguridad, proteger sus sistemas y servicios y mantener la confidencialidad e integridad de los datos a través de la protección de datos. Debe tener un proceso bien definido y practicado para responder a los incidentes de seguridad. Estas herramientas y técnicas son importantes porque respaldan objetivos, como la prevención de pérdidas financieras o el cumplimiento de obligaciones normativas.

VOLVER

Debido a que AWS protege físicamente la infraestructura que admite nuestros servicios en la nube, como cliente de AWS puede concentrarse en usar los servicios para lograr sus objetivos. La nube de AWS también proporciona un mayor acceso a los datos de seguridad y un enfoque automatizado para responder a los eventos de seguridad.

Al utilizar los servicios de AWS, usted mantiene un control total sobre su contenido y es responsable de administrar los requisitos de seguridad críticos, incluidos los siguientes:

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

Usted conserva el control de la seguridad que elige implementar para proteger sus propios datos, plataforma, aplicaciones, administración de acceso e identidad y sistema operativo. Esto significa que el modelo de responsabilidad compartida cambia según los servicios de AWS que utilice.

INICIO