Instituto Tecnológico de Costa Rica

Base de Datos II - IC4302

Clase Virtual - Viernes 3 de noviembre 2023

Configuracion de una base de datos en un cloud provider(Amazon)

AWS: En equivalente de obtener una cuenta de AWS, podría llamarse comprar un espacio virtual, dentro de este espacio se coloca algo llamado **"VPC (Virtual Private Cloud)"**, se podría ver cómo generar un Switch, para poder trabajar se encuentra algo conocido como **"Redes"**, donde se pueden definir tres tipos de redes, redes privadas, redes públicas y un servicio específico para bases de datos llamado **Database Subnet Group**, este tipo de red, brinda ventajas para realizar análisis de tráfico y de ataques hacia las bases de datos, esto ayuda para poseer más capas de seguridad en la base de datos.

Cuando se definen las redes, hay varios componentes como, **Internet Gateway**, da como salida hacia internet, esto da acceso tanto, de entrada, como de salida, con la posibilidad que desde internet ingrese otra persona. Otro componente seria el **NAT Gateway**, se encarga de dar salida hacia internet, desde las redes privadas, eso quiere decir que es posible tener salida hacia internet, pero no del internet hacia la red. La interacción entre las subredes y los componentes se da mediante un **Route Table**, esto establece reglas de cómo se mueve el tráfico entre los diferentes componentes, a grandes rasgos este componente define el tráfico entre subredes, componentes y salidas a internet según los componentes ya mencionados.

Cada red posee algo llamado **"NAC (Access Control List)"**, en términos generales, limita el tráfico que puede entrar a la red completa, esto se convierte en el primer Firewall que siempre se debe de colocar en una red, una característica importante es que es "Stateless", cuando se tienen dos elementos comunicándose, por ejemplo una base de datos y una aplicación, si la base de datos se encuentra en una red privada y se comunica con un agente externo, por lo tanto la base de datos origina la comunicación, esto quiere decir que se genera un estado en el inicio de la comunicación, al momento de permitir esto puede recibir respuestas por parte del otro elemento, esto podría generar ingresos no permitidos a la base de datos.

Security group: Definición de un firewall dentro de una red, en el caso de una red cloud, tiene características distintas. El security group, ayuda a definir reglas que permitan limitar a un mas quien llega a los servicios, en el caso de AWS es posible tener hasta cinco firewalls propios de cloud a un elemento que utiliza la red. Si se tienen varios firewalls, y permite definir configuraciones lo mas atómicas posibles por cada uno de los firewalls, para luego agregar los firewalls a los elementos que utilizan la red.

Bajo estándares de protección de datos como los de la Unión Europea o los de California, es necesario tener firewalls a nivel de sistema operativo.

AWS WAF (Web Application Firewall): Permanece en la red y observa todo el tráfico de la red, también conocido como Netflow, toma los paquetes que van en el tráfico de red, y verifica si hay algún patrón extraño de algún tipo de ataque, todo el tráfico que entra a la red lo filtra.

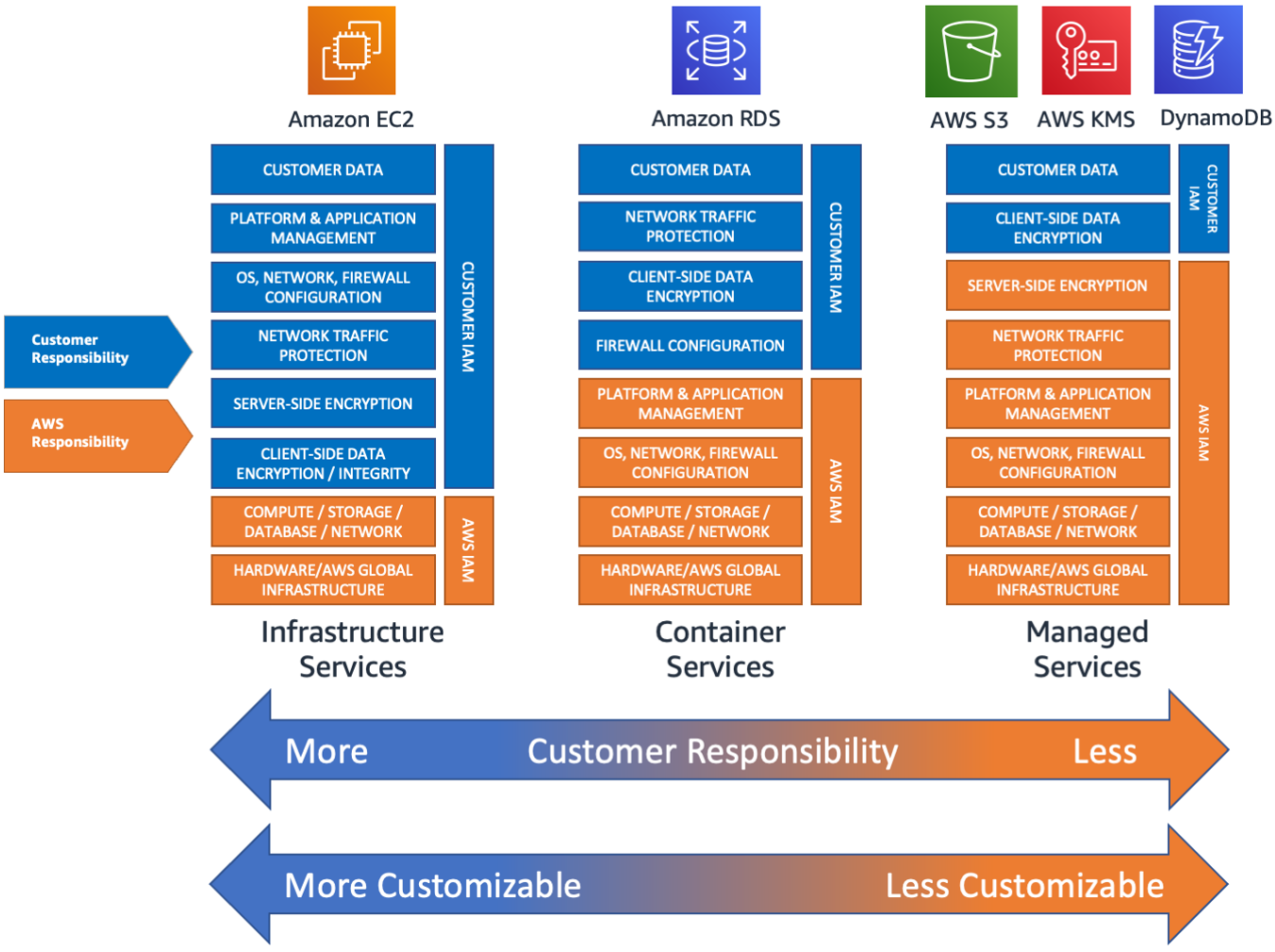
Guard: Analiza el trafico tratando de identificar DoS(Denial of Service), brinda ayuda mediante inteligencia artificial.

Seguridad de base de datos en términos de disponibilidad

Para asegurar disponibilidad, en una misma región, como mínimo se debe tener tres datacenters, que están a una distancia de cien kilómetros como mínimo, si se hace una red para la base de datos, esa red se debe replicar a los otros datacenters, esto para asegurar máxima disponibilidad, para todo esto se debe expandir el VPC, generando así **Availabity Zones**.

- **Infrasture Services:** Como cliente se tiene mucha responsabilidad.
- **Container Services:** Transmite gran parte de la responsabilidad al Cloud Provider.
- **Managed Services:** Proveen todo lo necesario, donde únicamente el cliente recibe y entrega datos, la responsabilidad de inscripción de redes y del envió de datos son responsabilidad del cloud provider.

A continuación, se presenta una imagen con el modelo de responsabilidades de AWS que fue mencionado en clases.



Amazon como todos los cloud provider, utiliza la red que nosotros realizamos, si se crea una maquina mediante Amazon, el disco se encuentra físicamente a la máquina. En un cloud provider mueven el disco a una red separada y esto implica es que la maquina corre en una red y mediante la red ingresa al disco, como ventaja se tiene es que están separados los datos de donde corren las aplicaciones, con esto visualizando patrones de acceso al disco. Si le disco se tiene en el servidor y logran ingresar al mismo, la base de datos se ve muy comprometida y poniendo en riesgo de hackeo a la base de datos.

El disco que siempre va a estar separado de la máquina, va a tener Server-side encryption (SSE), que será manejado por el servicio **KSM**, este servicio maneja las llaves de encriptadas que pueden utilizar los diferentes elementos de una red en la nube, esto garantiza trazabilidad, todo a aquel elemento de la infraestructura que utilice una llave encriptada va a grabar un evento; estos eventos entran a una base de dato "timeseries", y es posible reconstruir todos los eventos hasta el punto de que sea atacada la base de datos.

Como una ventaja del Cloud es la generación de snapshots a nivel de discos de red, también a nivel de las instalaciones, facilitando la creación de backups que proporciona el cloud.