Reto Técnico Ingeniero Cloud

Aspirante: Santiago Fuentes

Preguntas teóricas:

1. **¿Cuál es la diferencia entre nube pública, privada e hibrida?**

Una nube pública está disponible su acceso por internet y esta manejado por proveedores como Amazon (AWS), Microsoft (Azure) o Google (GCP) entre las más conocidas, tiene modelos de economía de escala y se paga únicamente por los recursos que se utiliza. El usuario no se encarga de manejar el hardware de los diferentes servicios, esto está del lado del proveedor. Una nube privada es solo accesible por una organización en específico y es gestionado y personalizado por esta misma organización, es decir, esta organización se encarga de la compra del hardware y su configuración. Una nube hibrida es la mezcla de ambos mundos, donde una parte de los recursos que ocupa una organización está en sus propios servidores y otra parte en los servidores de las nubes públicas. Esto puede ser por temas regulatorios y/o seguridad que tenga la empresa dependiendo del negocio.

2. **Describa tres prácticas de seguridad en la nube.**

- El control de tráfico desde internet hacia los recursos en la nube debe ser controlado y monitoreado de tal forma que no se pueda acceder a recursos privados desde internet, todos los servicios deben estar protegidos con grupos de seguridad correctamente configurados y los servicios a ser accedidos deben ser expuestos con servicios propios para este fin.
- Se debe habilitar MFA para todos los usuarios de las diversas cuentas de acceso a recursos en la nube, ya que agrega una capa nueva de seguridad para realizar tareas específicas.
- Realizar el cifrado de los datos tanto en tránsito como en reposo, para evitar la filtración de datos sensibles que las aplicaciones manejan.

3. **¿Qué es la IaC, y cuáles son sus principios beneficios? Mencione 2 herramientas de IaC y sus principales características.**

IaC, Infraestructura como código en español, es la práctica de gestionar y desplegar infraestructura usando herramientas de código, teniendo los siguientes beneficios:

- Reducir errores humanos al tener todo estandarizado y puesto en código.
- Automatización de despliegue de recursos

- Obtener despliegues consistentes cada vez que se aplique el código.
- Se puede versionar la infraestructura con la ayuda de herramientas como Git.

Entre las principales herramientas se tiene:

Pulumi

- IaC compatible con leguajes de programación conocidos como Python o JavaScript.
- Se puede tener componentes reutilizables.
- Gran integración con herramientas de despliegue continuo

Terraform

- Gran soporte de diversos proveedores cloud y diversas herramientas como DataDog
- Reutilización de código con la utilización de módulos que pueden ser públicos o privados.
- Rastreo de la infraestructura con un archivo llamado Estado, que permite mantener el trackeo entre el código y la infraestructura real
- Es capaz de rastrear cambios realizados fuera de la herramienta.

4. **¿Qué métricas considera esenciales para el monitoreo de soluciones en la nube?**

- La latencia, es una métrica importante ya que tiene un gran impacto en la experiencia de uso del usuario, la entrega de los servicios al usuario tiene que ser lo más rápida y eficiente posible.
- Utilización de la CPU, permite ver cuánto de los recursos computacionales provisionados en realidad de esta usando y de esta forma identificar áreas en donde se pueda reducir la cantidad para abaratar costos debido a la falta de uso o áreas en donde se necesite más porque la carga está siendo intensa y con más recursos se puede mejorar el rendimiento.
- Utilización de la memoria. Permite ver cuánto de memoria están usando los procesos de la aplicación y de igual forma aumentar o disminuir su cantidad dependiendo el caso y la necesidad.
- Solicitudes por minuto, permite ver cuál es el uso de la aplicación en un determinado espacio de tiempo y puede ser útil para identificar patrones de uso y tener la infraestructura lista para estos patrones, con más recursos en momentos o fechas determinadas y menos para un uso normal.

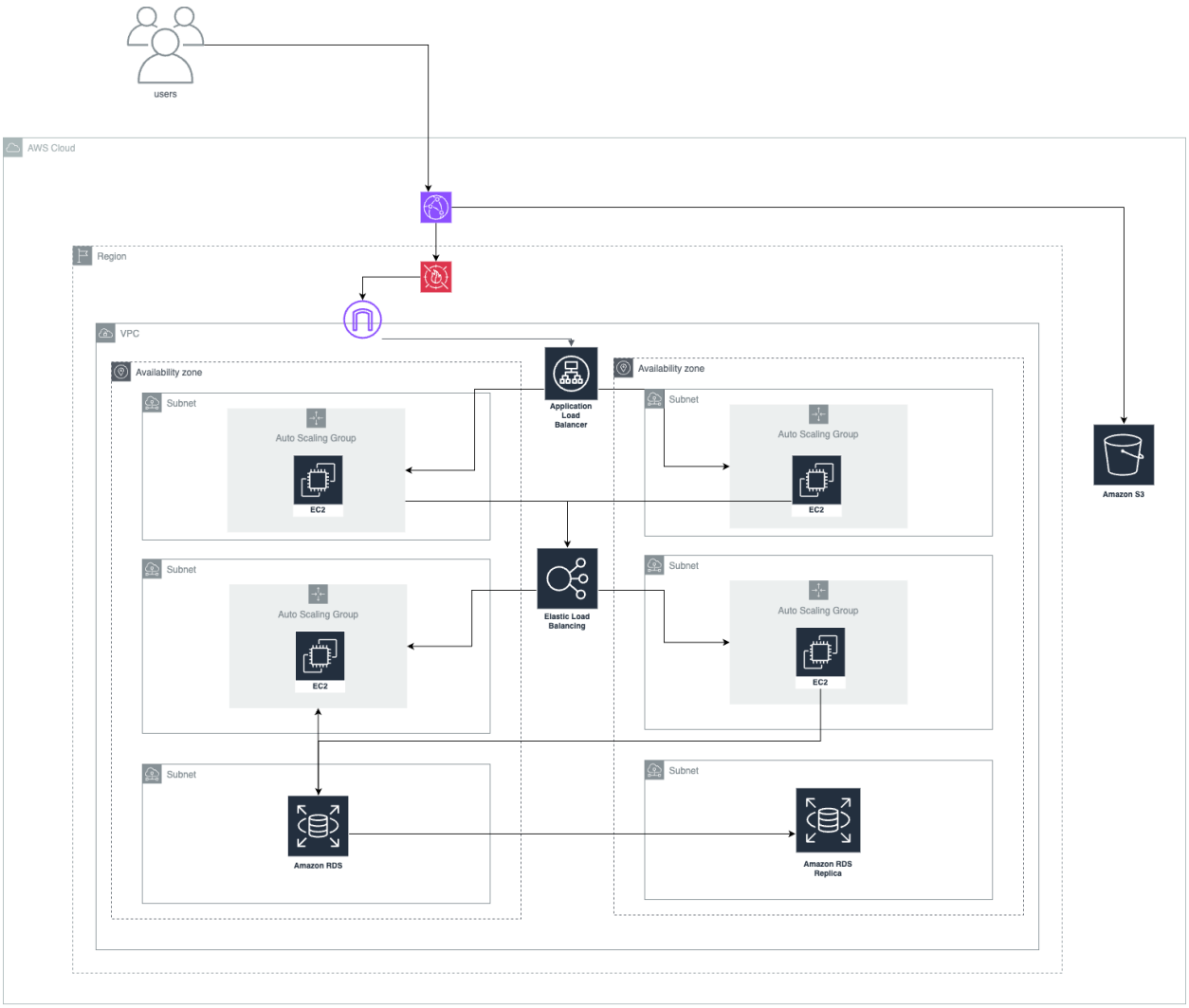
5. **¿Qué es Docker y cuáles son sus componentes principales?**

Es una herramienta que permite implementar una aplicación dentro de contenedores, lo que permite su portabilidad y ejecución en diversos ambientes de manera consistente.

Dentro de sus principales componentes se tiene:

- Docker Engine
- Las imágenes
- Los contendores
- Interfaz de comandos CLI

6. **Caso práctico**



Para el caso práctico, se selecciona AWS debido a la familiaridad con la herramienta y las buenas experiencias utilizando los servicios para aplicaciones variadas.

En este caso, la infraestructura cuenta con un cloud front que va a hacer el punto de entrada a la aplicación y por donde lo usuarios consumirán la aplicación, detrás se encuentra un firewall que permitirá controlar el tráfico que ingrese, añadiendo una capa de seguridad a la aplicación y que permite evitar tráfico malicioso.

Con eso entra a los recursos utilizando un internet Gateway que a su vez redirige el tráfico a una balanceador de carga que distribuirá el tráfico entre las dos zonas para mantener la aplicación con alta disponibilidad, en cada zona se encuentra un grupo de auto escalamiento con instancias computaciones EC2 para la parte del front, esta se comunica con el backend enviando el tráfico a un balanceador de carga que los distribuirá entre las dos zonas y que también tiene grupos de auto escalamiento en cada zona.

Esta capa, se comunicará con la base de datos principal en una de las zonas y esta a su vez, tendrá una réplica en la zona secundaria, para tener una mejor disponibilidad de datos en caso de desastre o falla en la zona principal.

Además, se tiene un bucket s3 para servir los archivos estáticos directamente al cloud front.

Finalmente, hay que tomar en cuenta que se omiten grupos de seguridad para todas las instancias, bases de datos y balanceadores por temas de simplicidad del diagrama, además, cabe mencionar que las diferentes capaz de la aplicación, se encuentran en su propia subnet, siendo todas privadas y controlando el tráfico de tal forma que solo se pueden comunicar con la capa inmediatamente inferior con el uso de route tables.