Análisis de Caso

Servicios de red en la nube🛜

Análisis de Caso

Servicios de red en la nube

Este análisis de caso tiene como objetivo que pongas en práctica los conceptos sobre redes en la nube, utilizando la capa gratuita de AWS Academy (o la capa gratuita de AWS). Desarrollarás una VPC, configurarás subredes y reglas de seguridad básicas que permitan comunicación interna y conexión selectiva a Internet.

Situación inicial 📍

La empresa **DataConnect** está expandiendo sus operaciones y desea migrar parte de su infraestructura a la nube para obtener mejor escalabilidad y flexibilidad. Actualmente, cuentan con un entorno on-premise y un sitio web informativo hospedado en un data center local. Sin embargo, para mejorar el rendimiento y la disponibilidad, necesitan diseñar **una red virtual en la nube** que ofrezca aislamiento de recursos, seguridad y la posibilidad de comunicarse con algunos servicios internos.

El equipo de TI propone crear una **VPC** (Virtual Private Cloud) en AWS para alojar un nuevo conjunto de servidores que manejará la parte de análisis de datos de la empresa. Se busca aprovechar la capa gratuita de AWS para reducir costos iniciales y asegurar que la transición sea gradual.

Descripción del Caso 🔎

En tu rol de **Ingeniero de Redes en la Nube**, debes diseñar y configurar una **VPC en AWS** utilizando la capa gratuita o recursos disponibles en AWS Academy. El objetivo es sentar las bases de la infraestructura de redes, asegurando que esté segmentada correctamente (subredes públicas y privadas), con reglas de seguridad adecuadas y posibilidades de conectividad híbrida a futuro (por VPN o Direct Connect, si fuera necesario).

Tendrás que:

- Configurar subredes con acceso restringido a Internet.
- Asegurar la comunicación interna entre instancias de la misma VPC.
- Permitir una ruta de salida a la web (por ejemplo, para actualizaciones de paquetes y parches) sin exponer directamente los servidores privados.

Instrucciones 💡

1. **Creación de la VPC y Subredes**

    - Ingresa a tu cuenta de AWS Academy o AWS Free Tier.
    - Crea una **VPC** con un rango de direcciones IP privado (p. ej., 10.0.0.0/16).
    - Define al menos **dos subredes**: una para la parte pública (por ejemplo, 10.0.1.0/24) y otra para la parte privada (10.0.2.0/24).
2. **Configuración de Gateways y Ruteo**

    - Implementa un **Internet Gateway** asociado a la VPC para permitir conexiones externas (solo en la subred pública).
    - Crea una **Route Table** pública y otra privada, asociando cada una a las subredes correspondientes.
    - (Opcional) Configura un **NAT Gateway** o un NAT Instance en la subred pública para que las instancias privadas puedan obtener actualizaciones sin quedar expuestas directamente a Internet.
3. **Reglas de Seguridad (Security Groups y NACLs)**

    - Diseña un **Security Group** para las instancias en la subred pública, permitiendo acceso HTTP/HTTPS desde cualquier IP, y SSH solo desde tu IP local.
    - Crea un **Security Group** para las instancias de la subred privada, restringiendo la entrada solo a tráfico proveniente de la subred pública o de tu IP específica (si se usa un bastion host).
    - Ajusta las **Network ACLs (NACLs)** si deseas un control granular adicional sobre el tráfico entrante/saliente.
4. **Implementación de Instancias de Prueba**

    - Lanza una instancia en la **subred pública** (tipo t2.micro o t3.micro para cubrir la capa gratuita). Verifica que puedas acceder vía SSH y realices un ping a Internet.
    - Lanza otra instancia en la **subred privada** y revisa que solo se comunique con la instancia de la subred pública (o a Internet por medio del NAT Gateway, si implementaste uno).
5. **Conectividad y Escenarios de Prueba**

    - Comprueba que las reglas de seguridad permitan o bloqueen el tráfico según lo configurado.
    - (Opcional) Explica cómo planearías una **VPN Site-to-Site** para conectar este entorno con la oficina on-premise de DataConnect, resaltando qué recursos necesitarías activar.

6. **Monitoreo y Costos**

    - Revisa métricas básicas en **Amazon CloudWatch** sobre el uso de red de las instancias.
    - Menciona las medidas que tomarías para **evitar costos adicionales**, como finalizar las instancias cuando no estén en uso o eliminar recursos innecesarios (NAT Gateways, etc.).

Entregables 📬

1. **Documento de Diseño de la VPC**

    - Diagrama de la red con la VPC, subredes (públicas y privadas), route tables, y los recursos asociados (Internet Gateway, NAT Gateway si aplica).
    - Explicación de las direcciones IP elegidas y la segmentación.
2. **Informe de Configuración y Seguridad**

    - Descripción de los **Security Groups** y NACLs creados, con los puertos/protocolos permitidos.
    - Justificación de por qué se abrieron o cerraron ciertos puertos (p. ej., puertos HTTP/HTTPS, SSH).
3. **Pruebas de Conectividad**

    - Capturas de pantalla o logs que demuestren la conexión SSH a la instancia de la subred pública.
    - Evidencia de que la instancia en la subred privada se conecta a Internet (si se configuró NAT) o, por el contrario, permanece aislada sin acceso directo (dependiendo de la estrategia elegida).
4. **Posibles Escenarios de Escalabilidad y Conexión Híbrida**

    - Descripción de un plan básico para habilitar una VPN con la infraestructura on-premise (solo conceptual).
    - Ideas para expandir la VPC en caso de crecimiento (más subredes, balanceadores de carga, etc.).
5. **Conclusiones**

    - Reflexiones sobre la experiencia de configurar una VPC en la capa gratuita de AWS, destacando los beneficios de la seguridad, la escalabilidad y el control de costos.

- Recomendaciones sobre pasos siguientes que DataConnect podría tomar para continuar ampliando su infraestructura de red en la nube.

¡Muchas gracias!

Nos vemos en la próxima lección