

Redes en AWS: VPC, subredes y gateways

Tecnología e Informática | Informática

Descripción del Curso

El curso de Informática está diseñado para estudiantes mayores de 17 años y se organiza en unidades que combinan fundamentos teóricos con prácticas aplicadas. La unidad 8, Diagrama y guía de implementación para una VPC real, cierra el curso con un proyecto práctico que integra diagramación y despliegue en la nube. En esta unidad se crea un diagrama detallado de una VPC real y se elabora una guía de implementación, describiendo los componentes (VPC, subredes, gateways, tablas de rutas) y las relaciones entre ellos, con énfasis en la claridad y replicabilidad. Objetivo: crear un diagrama y una guía de implementación para una VPC real, describiendo los componentes (VPC, subredes, gateways, tablas de rutas) y las relaciones entre ellos. Específicos: - Elaborar un diagrama claro que represente la VPC, sus subredes, gateways y tablas de rutas, con anotaciones de relación entre componentes. - Redactar una guía de implementación paso a paso que sirva para desplegar una VPC real en AWS, incluyendo consideraciones de seguridad y escalabilidad. - Definir criterios de verificación para validar la conectividad y la seguridad de la VPC implementada. A partir de esta unidad, el curso busca desarrollar habilidades para diseñar soluciones de red en la nube, documentarlas con diagramas precisos y guías reproducibles, evaluar seguridad y rendimiento, y comunicar de forma eficaz procesos técnicos. La unidad se apoya en conceptos de redes, arquitectura en la nube y buenas prácticas de implementación, promoviendo la capacidad de aplicar lo aprendido en contextos reales y en situaciones de resolución de problemas.

Competencias

- Analizar requisitos de redes y nube para diseñar soluciones de VPC de forma segura y escalable. - Aplicar conceptos de VPC, subredes, gateways y tablas de rutas para crear diagramas claros y replicables. - Elaborar diagramas técnicos detallados con anotaciones que faciliten la comprensión de relaciones entre componentes. - Redactar guías de implementación paso a paso para desplegar VPCs reales en AWS, considerando seguridad y rendimiento. - Verificar conectividad, seguridad y cumplimiento de criterios de verificación mediante pruebas y documentación. - Comunicar ideas técnicas de manera clara y colaborativa, favoreciendo la revisión entre pares. - Resolver problemas de diseño y despliegue ajustando configuraciones para escenarios reales y límites de costo.

Requerimientos

- Conocimientos previos en redes básicas y conceptos de nube, especialmente fundamentos de AWS (VPC, subredes, gateways, tablas de rutas, seguridad de red). - Habilidades de lectura de diagramas de arquitectura y de redacción de guías técnicas. - Recursos computacionales: cuenta de AWS (educativa o de prueba) y acceso a herramientas de diagramación (por ejemplo, Draw.io, Lucidchart, Visio). - Acceso a Internet estable y capacidades para documentar y entregar diagramas y guías en formatos editables y/o imágenes. - Compromiso con prácticas de seguridad y cumplimiento de normas éticas en el manejo de entornos de nube.

Unidades del Curso

Unidad 1: Unidad 1: Componentes clave de una VPC en AWS

Objetivos de Aprendizaje

- Reconocer la función de cada componente de una VPC y cómo se interconectan para permitir la conectividad entre recursos.
- Explicar la diferencia entre subredes públicas y privadas y su papel en la seguridad y el tráfico de red.
- Identificar dónde se aloja la información de enrutamiento dentro de la VPC a través de las tablas de rutas.

Contenidos Temáticos

1. **Tema 1:** Conceptos básicos de VPC, componentes principales y su propósito en la conectividad.
2. **Tema 2:** Subredes públicas vs privadas: criterios de diseño y casos de uso.
3. **Tema 3:** Puertas de enlace: Internet Gateway, NAT Gateway y su papel en el tráfico hacia/desde Internet.
4. **Tema 4:** Tablas de rutas: creación, asociaciones y resolución de rutas entre recursos.

Actividades

- **Actividad 1: Mapa de componentes de una VPC** - Construye un diagrama conceptual que muestre la VPC, subredes, objetos de puerta de enlace y tablas de rutas. Se identificarán las relaciones entre cada componente y cómo permiten el flujo de tráfico entre recursos.
- **Actividad 2: Identificación de escenarios** - Analiza diferentes escenarios de conectividad (interno, Internet, recursos públicos) y justifica qué componentes intervienen en cada caso.
- **Actividad 3: Debate corto** - Discute ventajas y desventajas de usar Internet Gateway frente a NAT Gateway para subredes diferentes y qué consideraciones de seguridad guían la elección.

Evaluación

- Pregunta teórica: Identificar y describir los componentes de una VPC y su función en la conectividad.
- Actividad de diagramación: Construir un diagrama correcto de una VPC básica con al menos una subred pública y una privada, e indicar la ubicación de Internet Gateway y las tablas de rutas.
- Rúbrica breve: Explicar cuándo usar Internet Gateway vs NAT Gateway con criterios de seguridad y acceso.

Unidad 2: Unidad 2: Direccionamiento IP y CIDR en VPC

Objetivos de Aprendizaje

- Comprender el esquema CIDR y cómo se aplica en la creación de VPC y subredes.
- Definir rangos de direcciones IPv4 para subredes públicas y privadas sin solapamientos.

- Explicar la relación entre el tamaño de la subred (prefix length) y la cantidad de host disponibles.

Contenidos Temáticos

1. **Tema 1:** Introducción a CIDR, notación y planificación de rangos para VPC.
2. **Tema 2:** Segmentación de la red: creación de subredes públicas y privadas dentro de una VPC.
3. **Tema 3:** Prácticas de diseño de direcciones para escalabilidad y seguridad.

Actividades

- **Actividad 1: Planificador de CIDR** - Dibuja y valida un plan CIDR para una VPC con 2 subredes públicas y 2 privadas en 3 zonas de disponibilidad.
- **Actividad 2: Creación de subredes simuladas** - Asigna rangos CIDR a subredes y verifica que no existan solapamientos, describiendo la justificación de cada elección.
- **Actividad 3: Análisis de capacidad** - Calcula cuántos hosts admite cada subred según el prefix length y planifica crecimiento futuro.

Evaluación

- Pregunta teórica: Explicar CIDR y su efecto en el tamaño de las subredes.
- Actividad práctica: Crear una asignación de CIDR para una VPC con subredes públicas/privadas y justificar la separación.

Unidad 3: Unidad 3: Configuración de una VPC básica con dos subredes y un Internet Gateway

Objetivos de Aprendizaje

- Crear una VPC con rangos CIDR apropiados y establecer subredes públicas y privadas.
- Configurar una Internet Gateway y adjuntarla a la VPC para habilitar acceso a Internet desde la subred pública.
- Crear y asociar una tabla de rutas que permita tráfico hacia Internet desde la subred pública y restringir tráfico de la subred privada.

Contenidos Temáticos

1. **Tema 1:** Creación de la VPC y selección de rangos CIDR.
2. **Tema 2:** Configuración de subredes públicas y privadas y su distribución entre zonas de disponibilidad.
3. **Tema 3:** Internet Gateway: adjuntar a la VPC y asociar rutas para la subred pública.
4. **Tema 4:** Tabla de rutas y pruebas de conectividad básica.

Actividades

- **Actividad 1: Construcción de la VPC** - Realiza la creación de una VPC con CIDR adecuado, crea una subred pública y otra privada y asigna sus respectivas interfaces.
- **Actividad 2: Puerta de enlace e Internet** - Crea un Internet Gateway, adjúntalo a la VPC y añade rutas en la tabla de rutas para permitir Internet desde la subred pública.
- **Actividad 3: Verificación de conectividad** - Realiza pruebas básicas (ping/ACCEPTED) desde una instancia en la subred pública hacia Internet y describe los resultados.

Evaluación

- Demostración práctica: Configurar correctamente VPC, subredes, Internet Gateway y tablas de rutas para permitir Internet desde la subred pública.
- Pregunta de análisis: Explicar por qué la subred privada no debe tener acceso directo a Internet y cómo se puede contactar con Internet de forma controlada.

Unidad 4: Unidad 4: Determinar el gateway adecuado para una subred

Objetivos de Aprendizaje

- Identificar escenarios donde es apropiado exponer recursos directamente a Internet (IGW) frente a requerir NAT para salidas de subredes privadas.
- Explicar cómo NAT Gateway permite acceso saliente a Internet sin exponer recursos privados.

Contenidos Temáticos

1. **Tema 1:** Naturaleza de IGW y NAT Gateway y sus diferencias clave.
2. **Tema 2:** Casos de uso para subredes públicas y privadas y criterios de seguridad.
3. **Tema 3:** Reglas de enrutamiento para dirigir el tráfico adecuado a cada gateway.

Actividades

- **Actividad 1:** Analizar un escenario con una instancia web pública y una base de datos privada; decidir cuál gateway usar y justificar con criterios de seguridad y acceso.
- **Actividad 2:** Configurar en un laboratorio una subred privada con salida a Internet a través de NAT Gateway y describir el flujo de tráfico.

Evaluación

- Pregunta de decisión: Dado un escenario, seleccionar IGW o NAT y justificar la elección con criterios de exposición y seguridad.
- Ejercicio de enrutamiento: Demostrar rutas que redirijan tráfico público a IGW y tráfico privado a través de NAT.

Unidad 5: Unidad 5: Diseño de arquitectura de VPC con comunicación entre subredes y control de acceso a Internet

Objetivos de Aprendizaje

- Crear un diseño de rutas que permita comunicación entre subredes dentro de la VPC, respetando límites de seguridad.
- Asociar subredes a tablas de rutas adecuadas para el control de tráfico hacia Internet o hacia otras subredes.
- Definir políticas básicas de seguridad para permitir o denegar tráfico entre subredes y hacia Internet.

Contenidos Temáticos

1. **Tema 1:** Enrutamiento entre subredes y uso de tablas de rutas compartidas.
2. **Tema 2:** Asociaciones de subred a tablas de rutas y su impacto en el tráfico.
3. **Tema 3:** Seguridad integrada: combinar SGs y NACLs para controlar flujos entre subredes e Internet.

Actividades

- **Actividad 1:** Diseñar una arquitectura con al menos 3 subredes (pública A, pública B, privada) y definir rutas entre ellas para permitir acceso entre recursos.
- **Actividad 2:** Configurar reglas básicas de seguridad (grupos de seguridad y NACLs) para permitir tráfico autorizado entre subredes y hacia Internet.

Evaluación

- Evaluación de diseño: presentar un diagrama y justificar las rutas y asociaciones de subredes para lograr comunicación deseada y seguridad.
- Caso práctico: aplicar reglas de seguridad para un flujo entre una instancia de frontend y una base de datos en una subred privada.

Unidad 6: Unidad 6: Seguridad básica en VPC: Grupos de seguridad y NACLs

Objetivos de Aprendizaje

- Explicar la diferencia entre grupos de seguridad y NACLs, incluyendo su ámbito de aplicación (instancias vs subredes).
- Configurar reglas básicas de grupos de seguridad limitando acceso entrante y saliente para recursos específicos.
- Definir reglas de NACL para controlar el tráfico hacia y desde las subredes y entender sus impactos de orden de evaluación.

Contenidos Temáticos

1. **Tema 1:** Conceptos de seguridad en VPC: SGs y NACLs y sus diferencias.
2. **Tema 2:** Configuración de grupos de seguridad para instancias y recursos clave.
3. **Tema 3:** Configuración de NACLs con reglas de entrada/salida y reglas por subred.

Actividades

- **Actividad 1:** Crear grupos de seguridad para una instancia web y una base de datos, definiendo permisos mínimos necesarios.
- **Actividad 2:** Definir NACLs para una subred privada y establecer reglas de tráfico entrante y saliente acorde a políticas de seguridad.
- **Actividad 3:** Realizar una simulación de flujo de tráfico entre subredes y evaluar si las reglas permiten o bloquean el acceso.

Evaluación

- Ejercicio práctico: Aplicar SGs y NACLs para garantizar el acceso autorizado entre servicios y bloquear accesos no deseados.
- Pregunta de reflexión: Comparar SGs y NACLs, cuando usar cada uno y por qué.

Unidad 7: Unidad 7: Escalabilidad y alta disponibilidad en VPC

Objetivos de Aprendizaje

- Explicar el papel de las AZs (zonas de disponibilidad) y cómo distribuir subredes para tolerancia a fallos.
- Proponer diseños con subredes en varias AZs para servicios frontend y backend y para NAT/egress resiliente.
- Identificar consideraciones de escalabilidad, como tamaños de subred y límites de recursos en AWS.

Contenidos Temáticos

1. **Tema 1:** Arquitecturas multi-AZ: distribución de subredes en AZs.
2. **Tema 2:** Escalabilidad de rutas y NATs en entornos de alta disponibilidad.
3. **Tema 3:** Patrones de resiliencia y recuperación ante fallos a nivel de red.

Actividades

- **Actividad 1:** Diseñar una VPC con al menos 3 AZs, creando subredes públicas y privadas distribuidas para una aplicación de dos capas.
- **Actividad 2:** Proponer y describir una estrategia de continuidad (failover) a nivel de enrutamiento y puertas de enlace.
- **Actividad 3:** Analizar límites de servicios y dimensionamiento para soportar picos de tráfico entre AZs.

Evaluación

- Proyecto: Presentar la arquitectura multi-AZ con diagrama y explicación de la elección de subredes, gateways y rutas para alta disponibilidad.
- Ejercicio de resiliencia: Simular fallos y describir la respuesta de la red ante cada escenario.

Unidad 8: Diagrama y guía de implementación para una VPC real

Objetivos de Aprendizaje

- Elaborar un diagrama claro que represente la VPC, sus subredes, gateways y tablas de rutas, con anotaciones de relación entre componentes.
- Redactar una guía de implementación paso a paso que sirva para desplegar una VPC real en AWS, incluyendo consideraciones de seguridad y escalabilidad.
- Definir criterios de verificación para validar la conectividad y la seguridad de la VPC implementada.

Contenidos Temáticos

1. **Tema 1:** Herramientas de diagramación y notación de arquitectura de red (diagrama lógico de VPC).
2. **Tema 2:** Guía de implementación: pasos, recursos, permisos y validación.
3. **Tema 3:** Verificación de conectividad y seguridad post-implementación.

Actividades

- **Actividad 1:** Crear un diagrama de arquitectura de VPC real, con anotaciones sobre componentes y relaciones.
- **Actividad 2:** Redactar una guía de implementación detallada que describa el despliegue de la VPC, la creación de subredes, gateways y tablas de rutas paso a paso.
- **Actividad 3:** Elaborar un plan de verificación de conectividad y seguridad para validar la VPC implementada.

Evaluación

- Entrega del diagrama y la guía de implementación, evaluando claridad, precisión y capacidad de replicación.
- Cuadro de verificación de conectividad y seguridad con criterios de éxito y métricas de rendimiento.