Nadia Arellano
Ingeniera en Informática

Actividad Práctica - Sesión 5: Seguridad en VPNs

Pregunta 1:

¿Cuál es el propósito principal de AWS CloudWatch en el monitoreo de VPNs?

- Respuesta correcta: Supervisar métricas en tiempo real y generar alertas.

AWS CloudWatch permite monitorear el estado de las VPNs, detectar anomalías y optimizar el tráfico. Con este servicio, puedes automatizar respuestas ante eventos críticos y garantizar la estabilidad de la red.

Pregunta 2:

¿Qué métrica mide la cantidad de datos transmitidos en la VPN?

- Respuesta correcta: TunnelDataIn y TunnelDataOut.

Estas métricas permiten evaluar el flujo de datos en la VPN, ayudando a detectar congestión y planificar mejoras en la infraestructura. Monitorearlas con AWS CloudWatch es clave para optimizar el tráfico y prevenir problemas de rendimiento.

Pregunta 3:

¿Cuál de los siguientes factores NO afecta el rendimiento de una VPN?

- Respuesta correcta: Seguridad del firewall.

Aunque la seguridad es crucial, no impacta directamente en el rendimiento de la VPN. Factores como latencia y pérdida de paquetes sí lo hacen. Mantener un equilibrio entre seguridad y rendimiento es clave para una infraestructura eficiente.

Pregunta 4:

¿Qué significa QoS en el contexto de optimización de VPNs?

- Respuesta correcta: Quality of Service.

QoS permite priorizar el tráfico más importante en una red, asegurando un mejor rendimiento para aplicaciones críticas. Su implementación es clave para evitar congestión y mejorar la calidad de la conexión.

Pregunta 5:

¿Cuál de estas opciones ayuda a mitigar ataques de fuerza bruta en VPNs?

- Respuesta correcta: Uso de listas blancas y negras.

Limitar el acceso a direcciones IP confiables es una estrategia eficaz para prevenir ataques de fuerza bruta. Configurar reglas de acceso mejora la seguridad de la VPN y reduce intentos de intrusión.