16°

Lab - AWS re/Start

Direcciones IP públicas y privadas

SWIPE

Tarea 01

Investigando el Entorno del cliente

A continuación, se tratarán los siguientes temas:

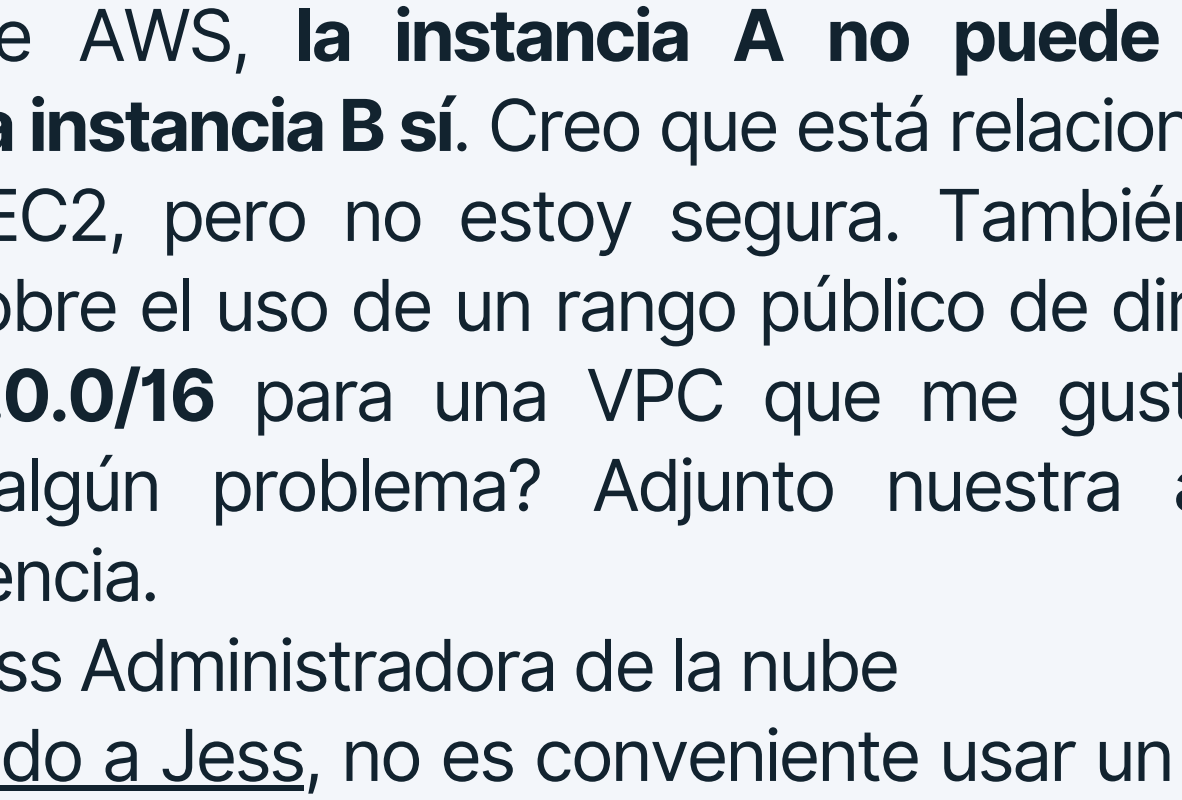
- Resumir e investigar la situación del cliente
- Analizar las diferencias entre una dirección de IP pública y una privada
- Desarrollar una solución al problema del cliente planteado en este laboratorio
- Resumir y describir los hallazgos

Para ello debemos entender el contexto:

Usted es un **ingeniero de soporte** en la nube en Amazon Web Services (**AWS)**. Durante su turno, un cliente de una empresa Fortune 500 solicita **asistencia por un problema de redes** dentro de su infraestructura de AWS. A continuación, figuran el correo y un archivo adjunto de su **arquitectura**

Tarea 01

Este es el ticket del cliente:
En la actualidad, tenemos una Virtual Private Cloud (VPC) con un rango de **CIDR de 10.0.0.0/16**. En esta VPC, tenemos dos instancias de Amazon Elastic Compute Cloud (Amazon **EC2**): **la instancia A y la instancia B**. Aunque ambas están en la **misma subred** y tienen las mismas configuraciones con los recursos de AWS, **la instancia A no puede acceder a Internet y la instancia B sí**. Creo que está relacionado con las instancias EC2, pero no estoy segura. También tenía una pregunta sobre el uso de un rango público de direcciones IP como **12.0.0.0/16** para una VPC que me gustaría lanzar. ¿Causaría algún problema? Adjunto nuestra arquitectura como referencia.
¡Gracias! Jess Administradora de la nube
Respondiendo a Jess, no es conveniente usar un rango CIDR pública para una VPC, puesto que lo que buscas es un pedazo aislado de nube que sea privado.



SWIPE

Tarea 01

Como análisis de los rangos de dirección (CIDR), podemos ver el mínimo y máximo de cada uno, asimismo ver sus respectivas clases.
10.0.0.0/16 - Los 16 primeros bits son fijos
00001010.00000000.xxxxxxxx.xxxxxxxx
Min: 10.0.0.0 Max: 10.0.255.255

Notas:

- Una dirección IP pública es aquella a la que se puede acceder a través de internet. Mientras que una dirección IP privada se asigna a los equipos dentro de una red privada (VPC), los cuales no pueden ser accedidos via internet.
- Para ver la clase de la dirección IP, nos fijamos en el primer octeto de bits. Recordar que los *bits de red son los fijos*

Valor del primer octeto	Clase	Ejemplo de dirección IP	Bits IPv4 para tamaños de ID de red
0 - 126	Clase A	34.126.35.125	8
128 - 191	Clase B	134.23.45.123	16
192 - 223	Clase C	212.11.123.3	24
224 - 239	Clase D	225.2.3.40	Se utilizan para multidifusión y no se pueden usar para el tráfico normal de Internet
240 - 255	Clase E	245.192.1.123	Están reservados y no se pueden usar en la Internet pública

SWIPE

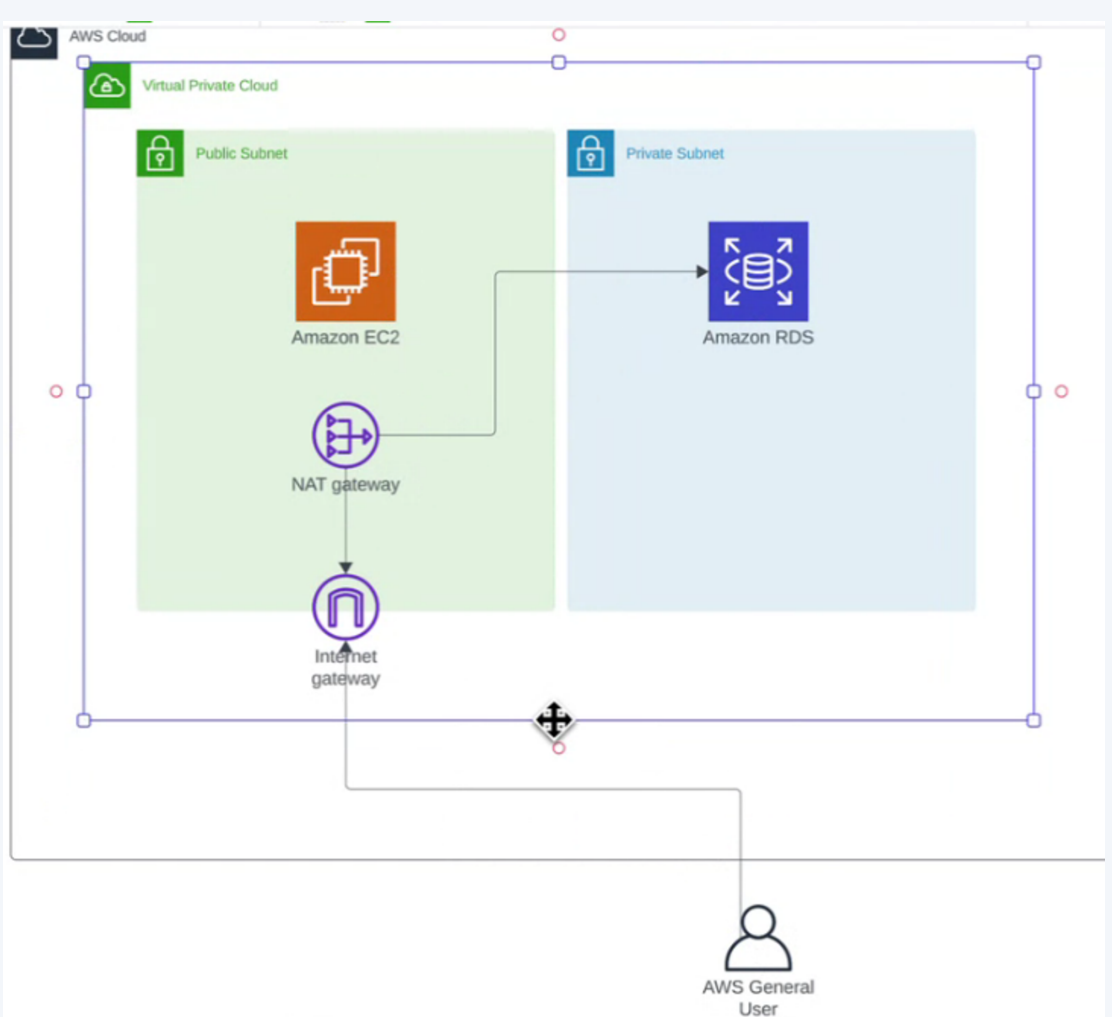
Tarea 01

A continuación los posibles **rangos de direcciones IP (CIDR) privadas**.

Rango de RFC 1918	Ejemplo de bloque de CIDR de Amazon VPC
10.0.0.0 - 10.255.255.255	10.0.0.0/16
172.16.0.0 - 172.31.255.255	172.31.0.0/16
192.168.0.0 - 192.268.255.255	192.168.0.0/16

Como un breve análisis a la arquitectura vemos que:

- Hay un VPC vinculada a una región.
- Luego una subred pública, recordando que solo puede haber una subred por AZ (Zona de disponibilidad). Dentro de esta subred tenemos dos instancia del servicio EC2.
- Es correcto el uso de una puerta de enlace de Internet (Internet Gateway) para conectar los servicios de la red pública a internet. En caso tuvieramos algunos servicios que quisieramos conectar a internet y se encuentran dentro de una subred privada. Deberíamos usar también una puerta de enlace NAT

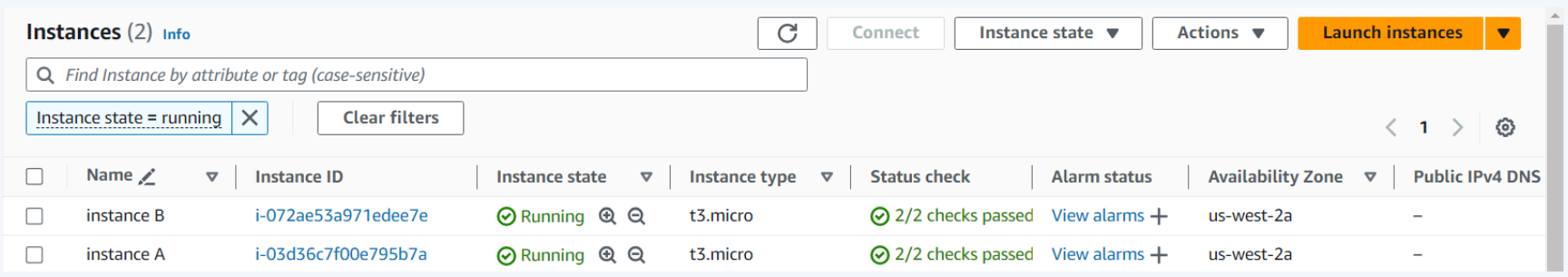


Tarea 01

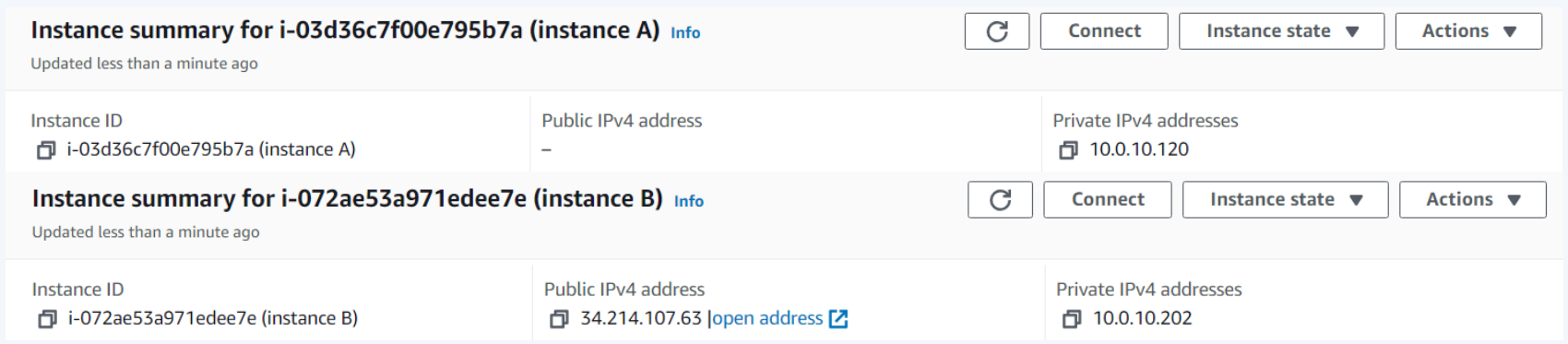
Para solucionar el problema, podemos ir indagando lo siguiente:

- Fallas en regiones o zona de disponibilidad
- Configuraciones de tablas de enrutamiento, puertas de enlace y subredes.
- Permisos de Grupos de Seguridad y Lista de control de acceso (NACL)
- Configuración de networking de las instancias EC2
- Algún error en los servidores web y aplicaciones

Entonces, exploremos dichas instancias:



Veamos sus direcciones IP de cada una:



Notamos que la intancia A no tiene definida una dirección IP pública que le permita conectarse a internet.

SWIPE