Lección 2

Amazon VPC

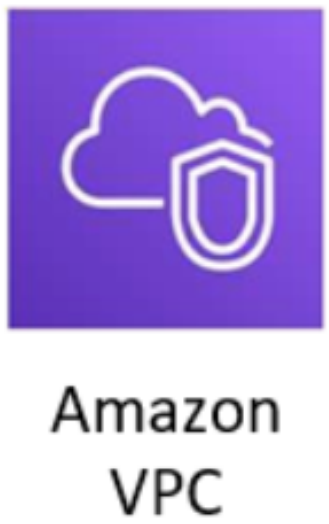
Muchos de los conceptos de una red local se aplican a una red basada en la nube, pero gran parte de la complejidad de configurar una red se ha abstraído sin sacrificar el control, la seguridad y la usabilidad. En esta sección, aprenderá sobre Amazon VPC y los componentes fundamentales de una VPC.

AWS VPC

Le permite aprovisionar una sección aislada de forma lógica de la nube de AWS, donde puede iniciar recursos de AWS en una red virtual que usted defina
Le permite controlar sus recursos de redes virtuales, entre ellos:

- Selección de un rango de direcciones IP
- Creación de subredes
- Configuración de subredes
- Configuración de tablas de enrutamiento y puertas de enlace de red

Le permite personalizar la configuración de red de su VPC
Permite utilizar varios niveles de seguridad



Amazon Virtual Private Cloud (Amazon VPC) es un servicio que permite aprovisionar una sección aislada de forma lógica de la nube de AWS (llamada nube virtual privada o VPC) en la que puede iniciar recursos de AWS.

Amazon VPC le brinda control de todos los recursos de red virtual, incluida la selección de su propio intervalo de direcciones IP, la creación de subredes y la configuración de tablas de enrutamiento y puertas de enlace de red. Puede usar IPv4 e IPv6 en su VPC para un acceso seguro a los recursos y las aplicaciones.

También puede personalizar la configuración de red de su VPC. Por ejemplo, puede crear una subred pública para sus servidores web que puedan acceder a la Internet pública. Puede colocar sus sistemas de backend (como bases de datos o servidores de aplicaciones) en una subred privada sin acceso público a Internet.

Finalmente, puede utilizar varias capas de seguridad, incluidos los grupos de seguridad y las listas de control de acceso (ACL de redes) para ayudar a controlar el acceso a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en cada subred.

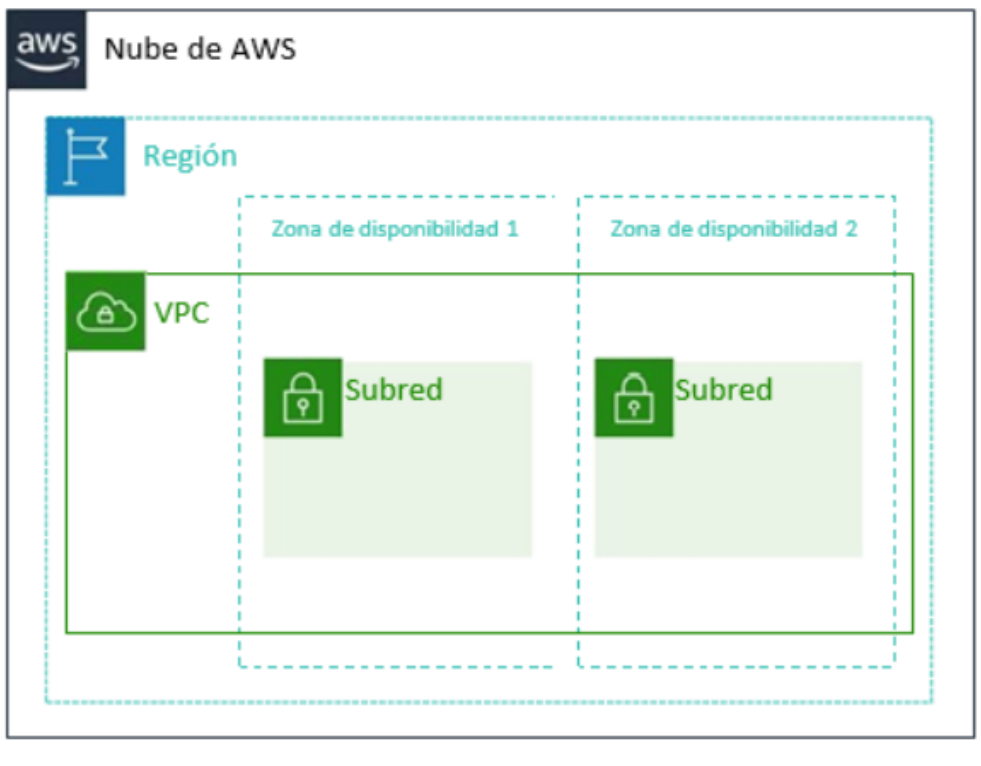
VPC y subredes

VPC:

- Se encuentra aislada de forma lógica de otras VPC
- Dedicada a su cuenta de AWS
- Pertenece a una única región de AWS y puede abarcar varias zonas de disponibilidad

Subredes:

- Intervalo de direcciones IP que divide una VPC
- Pertenece a una única zona de disponibilidad
- Se clasificia como pública o privada

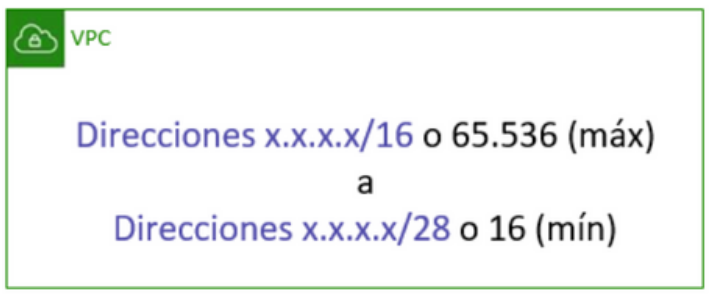


Amazon VPC le permite aprovisionar nubes virtuales privadas (VPC). Una VPC es una red virtual que está aislada de forma lógica de otras redes virtuales en la nube de AWS. Una VPC está dedicada a su cuenta. Las VPC pertenecen a una única región de AWS y puede abarcar varias zonas de disponibilidad.

Después de crear una VPC, puede dividirla en una o más subredes. Una subred es un intervalo de direcciones IP en una VPC. Las subredes pertenecen a una única zona de disponibilidad. Puede crear subredes en diferentes zonas de disponibilidad. Las subredes suelen clasificarse como públicas o privadas. Las subredes públicas tienen acceso a la puerta de enlace de internet; mientras que las subredes privadas no.

Direccionamiento IP

- Al crear una VPC, se le asigna un bloque IPv4 de CIDR (un rango de direcciones IPv4 privadas).
- No puede cambiar el rango de dirección después de crear la VPC.
- El tamaño de bloque de CIDR IPv4 más grande es /16.
- El tamaño de bloque de CIDR IPv4 más pequeño es /28.
- También se admite IPv6 (con un límite de tamaño de bloque diferente).
- Los bloques de CIDR de las subredes no pueden superponerse.



Las direcciones IP habilitan los recursos de su VPC para comunicarse entre sí y con los recursos de Internet. Al crear una VPC, se le asigna un bloque IPv4 de CIDR (un rango de direcciones IPv4 privadas). Después de crear una VPC, no se puede cambiar el rango de direcciones, por lo que es importante elegirlo con cuidado. El bloque de CIDR IPv4 puede ser tan grande como /16 (que son 2(16), o 65.536 direcciones) o tan pequeño como /28 (que son 24(4) o 16 direcciones).

Opcionalmente, puede asociar un bloque de CIDR IPv6 con su VPC y subredes, y asignar direcciones IPv6 de ese bloque a los recursos en su VPC. Los bloques de CIDR IPv6 tienen un límite de tamaño de bloque diferente.

El bloque de CIDR de una subred puede ser el mismo que el bloque de CIDR para la VPC. En este caso, la VPC y la subred tienen el mismo tamaño (la VPC tiene una única subred). Además, el bloque de CIDR de una subred puede ser un subconjunto del bloque de CIDR para la VPC. Esta estructura permite la definición de múltiples subredes. Si crea más de una subred en una VPC, los bloques de CIDR de las subredes no pueden superponerse. No puede tener direcciones IP duplicadas en la misma VPC.

Para obtener más información sobre direccionamiento IP en una VPC, visite https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

Direcciones IP reservadas

Ejemplo: una VPC con un bloque de CIDR IPv4 de 10.0.0.0/16 tiene 65.536 direcciones IP en total. La VPC tiene cuatro subredes del mismo tamaño. Solamente hay 251 direcciones IP disponibles para su uso en cada subred.

Direcciones IP para el bloque de CIDR 10.0.0.0/24	Reservado para
10.0.0.0	Direcciones de red
10.0.0.1	Comunicaciones internas
10.0.0.2	Resolución del sistema de nombres de dominio (DNS)
10.0.0.3	Uso futuro
10.0.0.255	Dirección de difusión de red

Al crear una subred, esta necesita su propio bloque de CIDR. Para cada bloque de CIDR que especifique, AWS reserva cinco direcciones IP dentro de ese bloque y esas direcciones no están disponibles para usarse. AWS se reserva cinco direcciones IP para:

- Direcciones de red
- Enrutador local de la VPC (comunicaciones internas)
- Resolución del sistema de nombres de dominio (DNS)
- Uso futuro
- Dirección de difusión de red

Por ejemplo, supongamos que se crea una subred con un bloque de CIDR IPv4 de 10.0.0.0/24 (que tiene 256 direcciones IP en total). La subred tiene 256 direcciones IP, pero solo 251 están disponibles porque 5 están reservadas.

Tipos de direcciones IP públicas

Dirección IPv4 pública

- Asignación manual a través de una dirección IP elástica
- Asignación en forma automática a través de la configuración de dirección IP pública de asignación automática en el nivel de subred

Dirección IP elástica

- Asociada a una cuenta de AWS
- Se puede asignar y reasignar en cualquier momento
- Es posible que se apliquen costos adicionales

Una dirección IP elástica es una dirección de IPv4 estática y pública que está diseñada para el cómputo en la nube dinámico. Puede asociar una dirección IP elástica a cualquier instancia o interfaz de red de cualquier VPC de su cuenta. Con una dirección IP elástica, puede re-asignar rápidamente la dirección a otra instancia de su VPC para enmascarar los errores de una instancia. Asociar la dirección IP elástica con la interfaz de red tiene una ventaja sobre asociarla directamente con la instancia. Puede mover todos los atributos de la interfaz de red de una instancia a otra en un solo paso.

Es posible que se apliquen costos adicionales cuando utilice direcciones IP elásticas, por lo que es importante liberarlas cuando ya no las necesite.

Cuando se crea una VPC, cada instancia de esa VPC obtiene automáticamente una dirección IP privada. También puede solicitar que se asigne una dirección IP pública cuando crea la instancia al modificar las propiedades de asignación automática de dirección IP pública de la subred.

Para obtener más información sobre las direcciones IP elásticas, consulte Direcciones IP elásticas en la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/vpc- eips.html

Tipos de direcciones IP públicas

Una interfaz de red elástica es una interfaz de red virtual que puede:

- Adjuntar a una instancia.
- Desconectar de la instancia y conectarla a otra instancia para redirigir el tráfico de red.

Sus atributos siguen cuando se reasigna a una nueva instancia.
Cada instancia de su VPC tiene una tarjeta de interfaz de red predeterminada a la que se asigna una dirección IPv4 privada del intervalo de direcciones de IPv4 de la VPC.

Una interfaz de red elástica es una interfaz de red virtual que se puede conectar o desconectar de una instancia en una VPC. Los atributos de una interfaz de red la siguen cuando se vuelve a conectar a otra instancia. Cuando se mueve una interfaz de red de una instancia a otra, el tráfico de la red se redirige a la nueva instancia.

Cada instancia de su VPC tiene una interfaz de red predeterminada (la interfaz de red principal) a la que se puede asignar una dirección IPv4 privada del intervalo de su VPC. No se puede desconectar una interfaz de red principal de una instancia. Puede crear y adjuntar una interfaz de red adicional a cualquier instancia de su VPC. El número de interfaces de red que se pueden conectar varía según el tipo de instancia.

Para obtener más información sobre Interfaces de red elástica, consulte la Documentación de AWS en https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html.

Tablas de enrutamiento y rutas

- Una tabla de enrutamiento contiene un conjunto de reglas (o rutas) que puede configurar para dirigir el tráfico de red de su subred.
- Cada ruta especifica un destino y un objetivo.
- De forma predeterminada, cada tabla de enrutamiento contiene una ruta local para la comunicación dentro de la VPC.
- Cada subred de su VPC debe estar asociada a una tabla de enrutamiento (como máximo una).

Tabla de enrutamiento principal (predeterminada)

Destino	Objetivo
10.0.0.0/16	local

Bloque de CIDR de VPC

Una tabla de enrutamiento contiene una serie de reglas (llamadas rutas) que determinan hacia dónde se dirige el tráfico de red de su subred. Cada ruta señala un destino y un objetivo. El destino es el bloque de CIDR de destino, a donde desea que vaya el tráfico de su subred. El objetivo es el objetivo a través del cual se envía el tráfico de destino. De forma predeterminada, cada tabla de enrutamiento que crea contiene una ruta local para la comunicación dentro de la VPC. Puede personalizar las tablas de enrutamiento al agregar rutas. No puede eliminar la entrada de ruta local, que se utiliza para las comunicaciones internas.

Cada subred de su VPC debe estar asociada a una tabla de enrutamiento. La tabla de enrutamiento principal es la tabla de enrutamiento que se asigna automáticamente a su VPC. Esta controla el enrutamiento de todas las subredes que no estén asociadas de forma explícita a ninguna otra tabla de enrutamiento. Una subred puede asociarse solamente a una tabla de enrutamiento por vez, pero pueden asociarse varias subredes a la misma tabla de enrutamiento.

Para obtener más información sobre las tablas de enrutamiento, consulte la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.ht