COLOMBIA POTENCIA DE LA VIDA

TIC

Lección 2
Creación de un entorno de red de AWS

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Amazon VPC

Aprovisione una sección aislada de forma lógica de la nube de AWS donde pueda lanzar recursos de AWS en una red virtual que usted defina.

Utilice su propia red

Amazon Virtual Private Cloud (Amazon VPC) es un servicio de Amazon Web Services que te permite crear un entorno virtual aislado en la nube, conocido como nube virtual privada o VPC, donde puedes lanzar y gestionar tus recursos de AWS de manera segura y controlada.

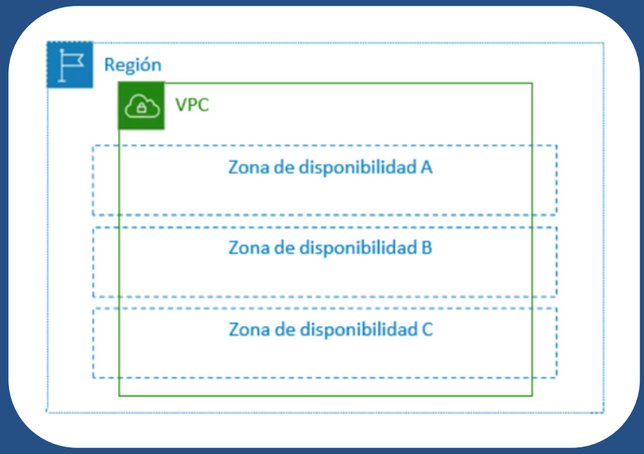
Con Amazon VPC, tienes el poder de definir y controlar todos los aspectos de tu red virtual. Esto incluye la capacidad de elegir tus propios rangos de direcciones IP, crear subredes y configurar la infraestructura de enrutamiento y conectividad de red. Además, tienes la flexibilidad de utilizar tanto IPv4 como IPv6 en tu VPC para garantizar la conectividad segura de tus recursos y aplicaciones.

Una de las ventajas clave de Amazon VPC es la capacidad de personalizar la configuración de red según tus necesidades específicas. Por ejemplo, puedes crear subredes públicas para alojar servidores web que necesiten acceso a Internet, mientras colocas sistemas sensibles, como servidores de aplicaciones o bases de datos, en subredes privadas sin acceso directo a Internet.

Además, Amazon VPC te ofrece diversas capas de seguridad para controlar el acceso a tus instancias de Amazon Elastic Compute Cloud (Amazon EC2) en cada subred. Estas medidas de seguridad incluyen la configuración de grupos de seguridad y listas de control de acceso a la red (ACL de red), que te permiten establecer reglas detalladas sobre qué tráfico está permitido y desde dónde.

Implementación de la VPC

Puede implementar una VPC en cualquier región de AWS.



Las VPC pueden alojar recursos compatibles desde cualquier zona de disponibilidad dentro de su región.

Cada VPC pertenece a una sola región de AWS. Una VPC abarca todas las zonas de disponibilidad de una región, de modo que puede alojar recursos compatibles desde cualquier zona de disponibilidad dentro de su región.

Direccionamiento entre dominios sin clases (CIDR)

0.0.0.0/0	= Todas las direcciones IP
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*

CIDR	Total de direcciones IP
/28	16
...	...
/20	4096
/19	8192
/18	16 384
/17	32 768
/16	65 536

Cuando creas una VPC, decides qué conjunto de direcciones IP privadas utilizarán las instancias dentro de esa VPC. Esto se define mediante un bloque de direccionamiento CIDR (Classless Inter-Domain Routing), por ejemplo, 10.0.0.0/16, que es el bloque CIDR principal de la VPC. Tienes la flexibilidad de asignar tamaños de bloque que van desde /28 (que ofrece 16 direcciones IP) hasta /16 (que proporciona 65,536 direcciones IP).

Amazon VPC permite el uso tanto de direccionamiento IPv4 como IPv6, y existen límites específicos para el tamaño del bloque CIDR para cada uno de ellos. Por defecto, todas las VPC y subredes deben tener bloques CIDR IPv4, una configuración que no se puede modificar. Sin embargo, tienes la opción de asociar un bloque CIDR IPv6 a tu VPC de forma adicional.

Tu VPC puede operar en modo de pila doble, lo que significa que los recursos dentro de ella pueden comunicarse mediante IPv4, IPv6, o ambos protocolos simultáneamente. Cada conjunto de direcciones IPv4 e IPv6 opera de manera independiente, por lo que es necesario configurar la asignación de direcciones y las medidas de seguridad de forma individual para cada protocolo.

Subredes: división de su VPC

- Una subred es un segmento o una partición del intervalo de direcciones IP de una VPC donde puede ubicar un grupo de recursos
- Las subredes no son límites de aislamiento
- Las subredes son un subconjunto del bloque de CIDR de la VPC
- Los bloques de CIDR de las subredes no pueden superponerse
- Todas las subredes se encuentran dentro de una zona de disponibilidad por completo
- Puede agregar una o más subredes en cada zona de disponibilidad o en una zona local
- AWS reserva cinco direcciones IP en cada subred

Ejemplo: una VPC con CIDR/22 incluye un total, de 1024 direcciones IP.

Puede dividir una VPC en una subred o más. Una subred es un segmento o una partición del intervalo de direcciones IP de una VPC, donde se puede asignar un grupo de recursos. Es importante recordar que las subredes no son límites de aislamiento en torno a su aplicación. En cambio, son contenedores para políticas de direccionamiento, sobre las que aprenderá en la siguiente sección de este módulo.

Cuando se crea una subred, se debe especificar el bloque de CIDR que le corresponde, el cual es un subconjunto del bloque de CIDR de la VPC. Los bloques de CIDR de las subredes no pueden superponerse.

Aunque cada subred debe estar dentro de una zona de disponibilidad por completo y no puede abarcar zonas, cada zona de disponibilidad puede tener una o más subredes. Puede elegir agregar subredes en una zona local. Cuando crea una subred en una zona local, la VPC también se extiende a esa zona local. Para obtener más información acerca de cómo extender los recursos de VPC a una zona local, consulte Ampliación de los recursos de VPC a AWS Local Zones en la documentación de AWS.

Como las subredes de la VPC se asignan a zonas de disponibilidad específicas, la ubicación de las subredes implican una forma de garantizar que las instancias de Amazon EC2 se distribuyan de forma adecuada entre distintas ubicaciones.

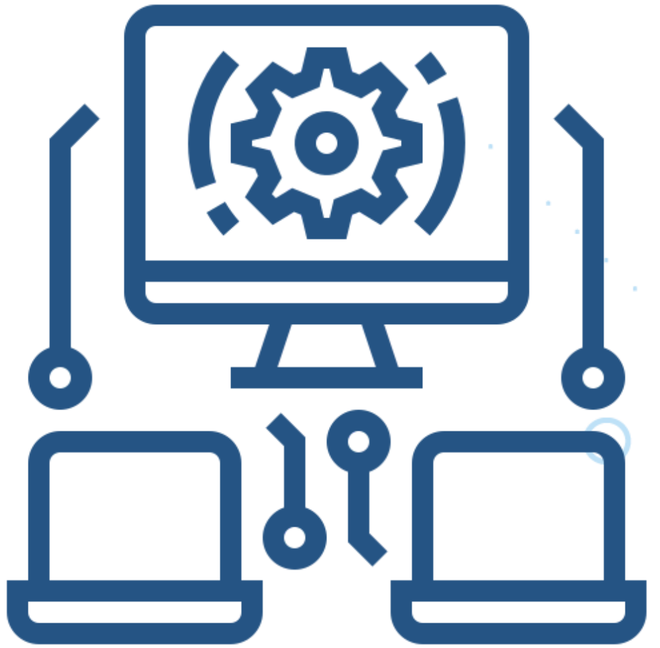
AWS reserva las primeras cuatro direcciones IP y la última del bloque de CIDR de cada subred. Por ejemplo, en una subred con el bloque de CIDR 10.0.0.0/24, AWS reserva las cinco siguientes direcciones IP para sus respectivos usos:

- 10.0.0.0: dirección de red
- 10.0.0.1: enrutador local de la VPC
- 10.0.0.2: resolución del sistema de nombres de dominio (DNS)
- 10.0.0.3: uso futuro
- 10.0.0.255: dirección de transmisión de la red

Para obtener más información acerca de las VPC y las subredes, consulte VPC y subredes en la documentación de AWS.

Prácticas recomendadas para el diseño de VPC

- Cree una subred por zona de disponibilidad utilizables por cada grupo de alojamientos que tenga requisitos de direccionamiento exclusivos.
- Divida el intervalo de red de la VPC de manera equitativa entre todas las zonas de disponibilidad utilizables en una región.
- No asigne todas las direcciones de res a la vez. En cambio, asegúrese de reservar un espacio de direcciones para su uso en el futuro.
- Ajuste el tamaño del CIDR de su VPC y las subredes de modo que admitan un crecimiento significativo de las cargas de trabajo esperadas.
- Asegúrese de que el intervalo de red de VPC (bloque de CIDR) no se superponga con los demás intervalos de res privada de su organización.



Cuando configure cualquier red de equipos, tenga en cuenta los siguientes principios universales para el diseño de redes:

- Cree una subred por zona de disponibilidad utilizable por cada grupo de alojamientos que tenga requisitos de direccionamiento exclusivos.
- Divida el intervalo de red de la VPC de manera equitativa entre todas las zonas de disponibilidad utilizables en una región.
- No asigne todas las direcciones de red a la vez. En cambio, asegúrese de reservar un espacio de direcciones para su uso en el futuro.
- Ajuste el tamaño del CIDR de su VPC y las subredes de modo que admitan un crecimiento significativo de las cargas de trabajo esperadas.
- Asegúrese de que el intervalo de red de VPC (bloque de CIDR) no se superponga con los demás intervalos de red privada de su organización.

Para obtener más información sobre el diseño y el ajuste de tamaño de las VPC individuales, consulte Diseño de una VPC en AWS.

COLOMBIA POTENCIA DE LA VIDA

TIC

Presionar cada tema para ver si contenido

- Implementación de una única VPC
- Múltiples VPC
- Cuentas múltiples
- Cuentas de Amazon VPC

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Implementación de una única VPC

Existen casos de uso limitados en los que la implementación de una VPC podrúa ser adecuada:

- pequeñas aplicaciones individuales que administra un equipo reducido
- informática de alto rendimiento (HPC)
- administración de identidades

Cuando diseña y crea su entorno de red, hay un número limitado de casos de uso en los que el entorno de una sola VPC podría ser adecuado:

- pequeñas aplicaciones individuales que administra un equipo reducido
- entornos de informática de alto rendimiento (HPC) (como simulaciones de física): un entorno de una sola VPC tiene una latencia más baja que la de los entornos distribuidos entre varias VPC
- entornos de administración de identidades: una sola VPC puede proporcionar el mejor nivel de seguridad

Sin embargo, para la mayoría de los casos de uso, se requiere un entorno de múltiples VPC. Puede crear varias VPC dentro de la misma región o en diferentes regiones. También puede crear varias VPC en la misma cuenta de AWS o en cuentas de AWS distintas.

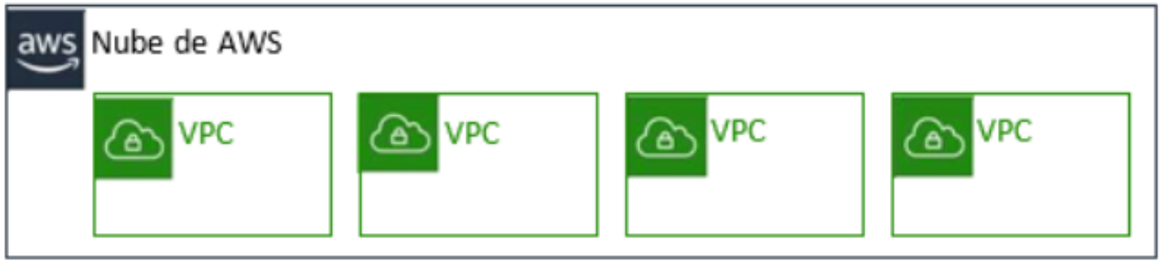
Múltiples VPC

Adecuado para lo siguiente:

- Equipos u organizaciones individuales, como los proveedores de servicios administrados
- Equipos limitados, lo que facilita el mantenimiento de los estándares y la administración del acceso

Excepción:

- Los estándares de control y conformidad pueden requerir aún más aislamiento de las cargas de trabajo sea cual sea el nivel de complejidad de la organización



La opción de utilizar múltiples VPC es más adecuada para situaciones en las que un solo equipo o una organización tiene un control completo sobre el aprovisionamiento y la gestión de todos los recursos en cada entorno de aplicación.

+INFO

Por ejemplo, esto podría ser relevante para un equipo que desarrolla una aplicación de comercio electrónico a gran escala, donde los desarrolladores tienen acceso completo a los entornos de desarrollo y producción. Este enfoque también es común en los proveedores de servicios administrados (MSP) que gestionan todos los recursos en entornos de prueba y producción.

Para obtener más detalles sobre los servicios disponibles y las mejores prácticas asociadas con la implementación de múltiples VPC, puedes consultar los recursos indicados a continuación:

- Conectividad a VPC múltiples en una sola región
- Conectividad a VPC múltiples en regiones diferentes

Cuentas múltiples

Adecuado para lo siguiente:

- Organizaciones grandes y con varios equipos de TI
- Organizaciones de tamaño mediano que prevén un crecimiento acelerado

¿Por qué?:

- Puede resultar más complicado administrar el acceso y los estándares en las organizaciones más complejas

Como se explicó anteriormente, tienes la opción de crear múltiples VPC dentro de la misma cuenta de AWS o en cuentas separadas.

Los modelos de cuentas múltiples son más apropiados para clientes u organizaciones empresariales que gestionan aplicaciones administradas por varios equipos. Por ejemplo, considera una organización que respalda a dos o más equipos de desarrollo. Estos equipos pueden optar por utilizar este modelo para permitir que los desarrolladores tengan acceso total a los recursos en el entorno de desarrollo, pero acceso restringido o nulo al entorno de producción.

Cuotas de Amazon VPC

Cuota predeterminada: 5 VPC por región y cuenta*

Tenga en cuenta las cuotas de Amazon VPC.
La cuota predeterminada es 5 VPC por región.
Sin embargo, puede solicitar un aumento.

*La cuota predeterminada es de 5 VPC por región, pero puede solicitar un aumento de cuota.

Para obtener más información sobre los límites de servicio de Amazon VPC, consulte Cuotas de Amazon VPC en la documentación de AWS.

Estos son algunos de los aprendizajes clave de esta lección 2 de la unidad 1:

- Amazon VPC le permite aprovisionar VPC, que son secciones aisladas de forma lógica de la nube de AWS donde puede lanzar sus recursos de AWS.
- Las VPC pertenecen a una sola región y se dividen en subredes.
- Las subredes pertenecen a una zona de disponibilidad o zona local. Son subconjuntos del bloque de CIDR de la VPC.
- Puede crear varias VPC en la misma región o en regiones diferentes, además de en la misma cuenta o en cuentas distintas.

- Siga estas prácticas recomendadas a la hora de diseñar su VPC:
  - Cree una subred por zona de disponibilidad para cada grupo de alojamientos que tenga requisitos de direccionamiento exclusivos.
  - Divida el intervalo de red de la VPC de manera equitativa entre todas las zonas de disponibilidad utilizables en una región.
  - No asigne todas las direcciones de red a la vez. En cambio, asegúrese de reservar un espacio de direcciones para su uso en el futuro.
  - Ajuste el tamaño del CIDR de su VPC y las subredes de modo que admitan un crecimiento significativo de las cargas de trabajo esperadas.
  - Asegúrese de que el intervalo de red de la VPC no se superponga con los demás intervalos de red privada de su organización.

INICIO