Jonathan A nderson

AWS

Certified Solutions Architect

Associate

The ultimate guide for the

SAA-C03

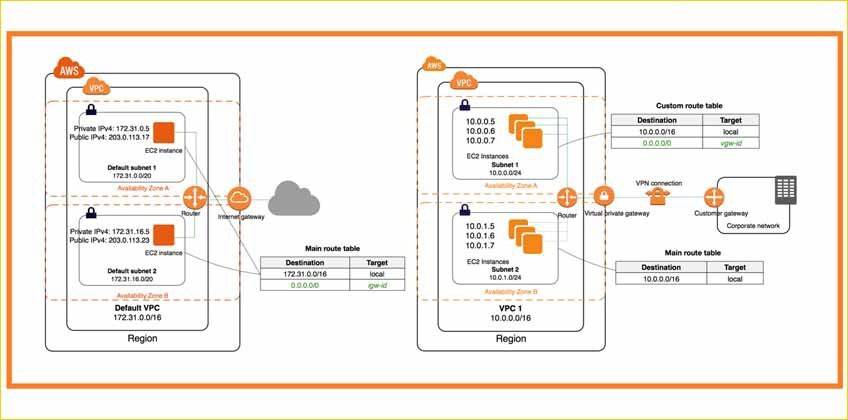
Imagen que contiene lego, juguete

Descripción generada automáticamenteE X A M

# Chapter 3

**Amazon Virtual Private Cloud**

Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual definida personalmente. Esta red virtual es muy similar a la red convencional de su propio centro de datos que puede ejecutar, utilizando la infraestructura escalable de AWS.



**Amazon VPC Concepts**

Amazon VPC es la capa de red de Amazon EC2. Si es nuevo en Amazon EC2, consulte el concepto de Amazon EC2, Para obtener una descripción rápida, consulte la Guía del usuario de Amazon EC2 para instancias de Linux.

Estos son los principales conceptos de las VPC:

* Virtual Private Cloud (VPC): una red virtual solo para su cuenta de AWS.
* Subred: el conjunto de direcciones IP de la VPC.
* Tabla de enrutamiento: un conjunto de reglas denominadas rutas que se utilizan para determinar dónde se enruta el tráfico de red.
* Puerta de enlace de Internet: una puerta de enlace que se asocia con la VPC para habilitar la comunicación entre los recursos de la VPC e Internet.
* VPC Endpoint: le permite conectar de forma privada su VPC a los servicios de AWS compatibles y a los servicios de punto de enlace de la VPC con tecnología privateLink sin necesidad de una gateway de Internet, un equipo NAT, una conexión de AWS Direct Link o Conexión VPN. Para interactuar con determinados servicios, las instancias de la VPC no requieren direcciones IP públicas. El tráfico no sale de la red de Amazon entre su VPC y el otro proveedor.

**Access to Amazon VPC**

Puede crear, acceder y administrar sus VPC utilizando cualquiera de las siguientes interfaces:

* + 1. Consola de administración de AWS: proporciona una interfaz web que puede utilizar para obtener acceso a sus VPC.
    2. AWS Command Line Interface (AWS CLI): ofrece comandos y es compatible con Windows, Mac y Linux para una amplia gama de servicios de AWS, incluida Amazon VPC. Consulte AWS Command Line Interface para obtener más detalles.
    3. SDK de AWS: proporciona API específicas del idioma y admite muchos detalles de conexión, como el cálculo de firmas, el control de intentos de solicitud y el control de errores. Consulte AWS SDK para obtener más información.
    4. API de solicitud: proporciona una evaluación del comportamiento en el nivel inferior de la API que invoca con las solicitudes HTTPS. La forma más directa de navegar por Amazon VPC es utilizar la API de preguntas, sin embargo, requiere que su aplicación maneje detalles de bajo nivel, como generar el hash para firmar la solicitud y controlar los errores. Consulte la referencia de la API de Amazon EC2 para obtener más información.

## Amazon VPC Prices

El uso de Amazon VPC no conlleva costos adicionales. Paga tarifas estándar por las instancias y otras características de Amazon EC2 que utilice. Ciertos costos están asociados con el uso de una conexión VPN de sitio a sitio, PrivateLink, duplicación de tráfico y una puerta de enlace NAT.

**Amazon VPC Quota**

Existen cuotas para el número de componentes de Amazon VPC que puede proporcionar. Puede solicitar un aumento para algunas de estas cuotas.

## PCI DSS Compliance

Amazon VPC admite el procesamiento, almacenamiento y transmisión de información de tarjetas de crédito por parte de un comerciante o proveedor de servicios, y ha sido validado como cumple con el Estándar de Seguridad de Datos de la Industria (DSS) y tarjetas de pago (PCI).

Amazon VPC ofrece varias opciones de conectividad de red que puede utilizar en función de sus diseños y requisitos de red actuales. Estas opciones de conectividad implican el uso de Internet o una conexión de AWS Direct Connect como columna vertebral de la red y la finalización de la conexión a AWS o a los puntos de enlace de red administrados por el usuario. Además, AWS le permite elegir cómo se proporciona el enrutamiento de red entre Amazon VPC y sus redes, aprovechando aws o los equipos y rutas de red administrados por el usuario.

Opciones de conectividad de red de usuario para Amazon VPC

* + 1. AWS Managed VPN: describe cómo establecer una conexión VPN entre el equipo de red de una red remota y el equipo de red administrado de AWS conectado a su Amazon VPC.
    2. AWS Direct Connect: describe cómo establecer una conexión lógica privada entre la red remota y Amazon VPC mediante AWS Direct Connect.
    3. AWS Direct Connect + VPN: describe cómo establecer una conexión privada cifrada entre su red remota y Amazon VPC mediante AWS Direct Connect.
    4. AWS VPN CloudHub: describe cómo configurar un modelo estrella para conectar sucursales remotas.
    5. VPN de software: describe cómo establecer una conexión VPN entre su equipo en una red remota y un dispositivo VPN de software administrado por el usuario que se ejecuta en una Amazon VPC.
    6. VPC de tránsito: describe la configuración de una red de tránsito global en AWS mediante una VPN de software junto con una VPN administrada por AWS.

Opciones de conectividad de Amazon VPC a Amazon VPC

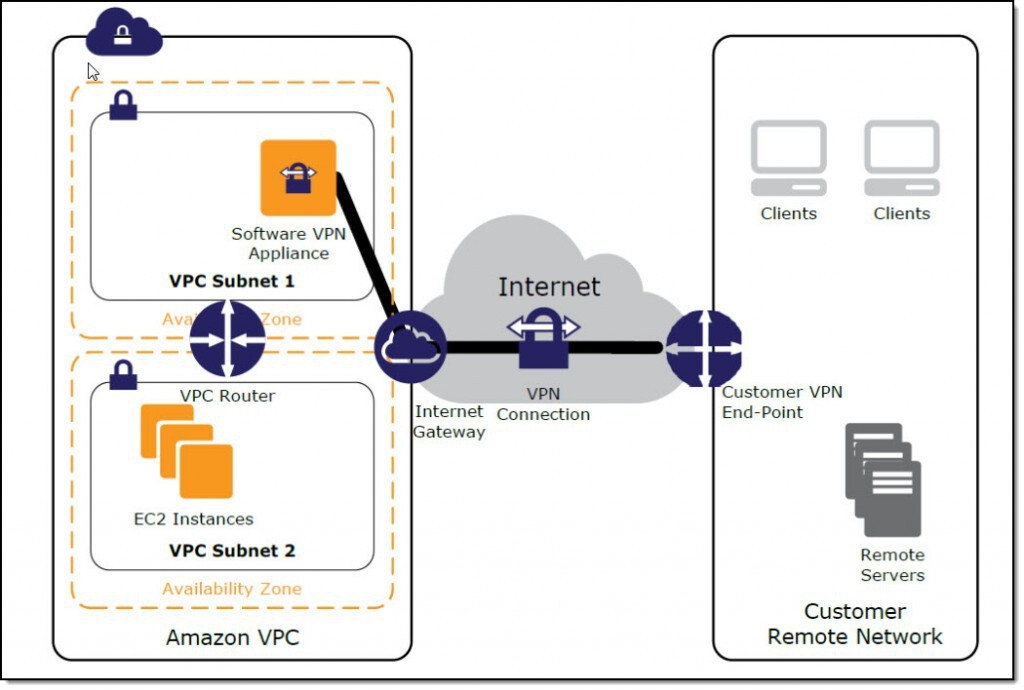
* + 1. Emparejamiento de VPC: describe el enfoque recomendado por AWS para conectar varias VPC de Amazon dentro de las regiones y entre ellas mediante la característica de emparejamiento de Amazon VPC.
    2. VPN de software: describe la conexión entre varias VPC de Amazon mediante conexiones VPN entre dispositivos de software VPN administrados por el usuario que se ejecutan en cada AMAZON VPC.
    3. VPN administrada por software con AWS: describe la conexión entre varias VPC de Amazon con una conexión VPN establecida entre un dispositivo VPN de software administrado por el usuario en una Amazon VPC y un equipo de red administrado por AWS conectado a la otra Amazon VPC.
    4. AWS Managed VPN: describe el vínculo entre varias VPC de Amazon, mediante varias conexiones VPN entre su red remota y cada una de sus VPC de Amazon.
    5. AWS Direct Connect: describe la conexión entre varias AmazonVC, mediante conexiones lógicas en enrutadores de AWS Direct Connect administrados por el cliente.
    6. AWS Private Link: describe la conexión entre varias AmazonVC, mediante puntos de enlace de interfaz de VPC y servicios de punto de enlace de VPC.

Opciones de conectividad de usuario interno para Amazon VPC

* + 1. VPN para software de acceso remoto: además de las opciones de conexión de red para que los clientes con Amazon VPC conecten a los usuarios remotos a los recursos de la VPC, en esta sección se describe cómo utilizar una solución de acceso remoto para proporcionar a los usuarios finales acceso VPN a una Amazon VPC.

## Network connection with Amazon VPC

En esta sección, encontrará patrones de diseño que le permitirán vincular redes externas a su entorno de Amazon VPC. Estas opciones son útiles para integrar las herramientas de AWS con sus servicios locales existentes (como seguimiento, autenticación, protección, datos u otros sistemas) mediante la expansión de su sistema interno. Redes en la nube de AWS. Con esta extensión de red, sus usuarios internos también pueden conectarse sin problemas a los recursos alojados en AWS, al igual que cualquier otro recurso interno.



## VPN managed by AWS

Amazon VPC proporciona la capacidad de establecer una conexión VPN IPsec entre redes de clientes remotos y su Amazon VPC en Internet, como se muestra en la siguiente figura. Considere este método si desea aprovechar un punto de enlace VPN administrado por AWS con redundancia automática y revisión de varios centros de datos combinados en el lado de AWS de la conexión VPN. Independientemente de la oscuridad, dos puntos de enlace VPN diferentes sirven a Amazon Virtual Private Gateway, que se encuentran físicamente en centros de datos separados para aumentar la disponibilidad de su conexión VPN.

La puerta de enlace privada virtual también admite y facilita las conexiones a múltiples puertas de enlace de usuario, de modo que, como se muestra en la siguiente figura, puede aplicar la redundancia y la caída en su lado del enlace VPN. Para proporcionar flexibilidad en la configuración de enrutamiento, se ofrecen opciones de enrutamiento dinámico y estático. Para compartir información de enrutamiento entre AWS y estos puntos de enlace remotos, el enrutamiento dinámico utiliza el emparejamiento BGP. El enrutamiento dinámico también le permite especificar prioridades, políticas y ponderaciones de enrutamiento (métricas) en sus anuncios BGP y también puede afectar a la ruta entre sus redes y AWS.

Es importante tener en cuenta que cuando se utiliza BGP, las conexiones IPSec y BGP deben terminar en el mismo equipo que la puerta de enlace de usuario, por lo tanto, las conexiones IPSec y BGP deben terminarse.