



Documento técnico de AWS

Creación de una infraestructura de red de AWS de varias VPC escalable y segura



Creación de una infraestructura de red de AWS de varias VPC escalable y segura: Documento técnico de AWS

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y de ninguna manera que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Resumen	1
Resumen	1
Introducción	2
Conectividad de VPC a VPC	4
Emparejamiento de VPC	4
Solución de VPC de tránsito	5
Transit Gateway	6
Transit Gateway frente a Transit VPC	7
Transit Gateway frente a emparejamiento de VPC	7
AWS PrivateLink	8
Uso compartido de Amazon VPC	9
Conectividad híbrida	11
VPN	11
Direct Connect	12
Salida centralizada a Internet	15
Seguridad de red centralizada para tráfico de VPC a VPC y local a VPC	19
DNS	22
DNS híbrido	22
Acceso centralizado a puntos de conexión privados de la VPC	25
Puntos de conexión de la VPC de tipo interfaz	25
Conclusión	27
Colaboradores	28
Historial de revisión	29
Avisos	30

Creación de una infraestructura de red de AWS de varias VPC escalable y segura

Fecha de publicación: 10 de junio de 2020 ([Historial de revisión](#))

Resumen

Los clientes de AWS a menudo confían en cientos de cuentas y VPC para segmentar sus cargas de trabajo y ampliar su presencia. Este nivel de escala a menudo crea desafíos en torno al uso compartido de recursos, la conectividad entre VPC y la conectividad local a la VPC.

En este documento técnico se describen las prácticas recomendadas para crear arquitecturas de red escalables y seguras en una red de gran tamaño con servicios de AWS como Amazon VPC, AWS Transit Gateway, AWS PrivateLink y AWS Direct Connect Gateway. Demuestra soluciones para administrar una infraestructura en crecimiento, lo que garantiza la escalabilidad, la alta disponibilidad y la seguridad, al tiempo que mantiene bajos los costes generales.

Introducción

Los clientes de AWS comienzan creando recursos en una sola cuenta de AWS que representa un límite de administración que segmenta los permisos, los costes y los servicios. Sin embargo, a medida que la organización del cliente crece, se necesita una mayor segmentación de los servicios para monitorear los costes, controlar el acceso y facilitar la gestión ambiental. Una solución con varias cuentas resuelve estos problemas al proporcionar cuentas específicas para los servicios de TI y los usuarios de una organización. AWS proporciona varias herramientas para administrar y configurar esta infraestructura, incluidas [AWS Landing Zone](#) y [AWS Control Tower](#).

Figura 1 — Estructura de cuenta de zona de aterrizaje

AWS Landing Zone y AWS Control Tower automatizan la configuración e integración de varios servicios de AWS para proporcionar un entorno básico, altamente controlado y de varias cuentas con administración de identidades y accesos (IAM), gobernanza, seguridad de datos, diseño de redes y registro.

La [solución de zona de aterrizaje de AWS](#) de la figura 1 incluye cuatro cuentas: la cuenta AWS Organizations (utilizada para administrar la configuración y el acceso a las cuentas administradas de la zona de aterrizaje de AWS), la cuenta de servicios compartidos (utilizada para crear servicios compartidos de infraestructura, como servicios de directorio), la cuenta de archivo de registro (registro centralizado en buckets de S3) y la cuenta de seguridad (que el equipo de seguridad y cumplimiento de una empresa utilizará para auditar o realizar operaciones de seguridad de emergencia en caso de un incidente en las cuentas radiales).

Este documento técnico presenta una cuenta de servicios de red propiedad del equipo de redes que administra su infraestructura de AWS. Todas las cuentas y VPC comparten los servicios de red y la infraestructura de red de la cuenta de forma centralizada (similar a un diseño central-radial). Este diseño permite una mejor capacidad de administración para su zona de aterrizaje y ayuda a reducir los costes al eliminar la necesidad de duplicar los servicios de red en cada cuenta y VPC radial.

Note

En este documento técnico, “Zona de aterrizaje” es un término amplio para la configuración de varias cuentas/VPC escalable, segura y eficaz en la que implementa sus cargas de trabajo. Esta configuración se puede crear con cualquier herramienta.

La mayoría de los clientes comienzan con unas cuantas VPC para implementar su infraestructura. La cantidad de VPC que posee un cliente suele estar relacionada con su cantidad de cuentas, usuarios y entornos en etapas (producción, desarrollo, prueba, etc.). A medida que aumenta el uso de la nube, la cantidad de usuarios, unidades de negocio, aplicaciones y regiones con las que interactúa un cliente se multiplica, lo que lleva a la creación de nuevas VPC.

A medida que aumenta el número de VPC, la administración de VPC transversales se vuelve esencial para el funcionamiento de la red en la nube del cliente. Este documento técnico trata las prácticas recomendadas para tres áreas específicas de la conectividad híbrida y de VPC transversal:

- Conectividad de red: interconexión de VPC y redes locales a escala.
- Seguridad de red: creación de puntos de salida centralizados para acceder a Internet y puntos de conexión como NAT Gateway, puntos de conexión de VPC y AWS PrivateLink.
- Administración de DNS: resolución de DNS dentro de la zona de aterrizaje y DNS híbrido.

Conectividad de VPC a VPC

Los clientes pueden usar dos patrones de flujo de VPC diferentes para configurar entornos de varias VPC: de muchos a muchos o central-radial. En el enfoque de muchos a muchos, el tráfico entre cada VPC se administra de forma individual entre cada VPC. En el modelo central-radial, todo el tráfico entre la VPC fluye a través de un recurso central, que dirige el tráfico en función de reglas establecidas.

Temas

- [Emparejamiento de VPC](#)
- [Solución de VPC de tránsito](#)
- [Transit Gateway](#)
- [AWS PrivateLink](#)
- [Uso compartido de Amazon VPC](#)

Emparejamiento de VPC

La forma más sencilla de conectar dos VPC es utilizar el emparejamiento de VPC. En esta configuración, una conexión permite una conectividad bidireccional completa entre las VPC. Esta conexión de emparejamiento se usa para dirigir el tráfico entre las VPC. Las VPC de las cuentas y las regiones de AWS también se pueden emparejar. El emparejamiento de VPC solo incurre en costes por el tráfico que viaja a través de la conexión (no hay una tarifa de infraestructura por hora).

El emparejamiento de VPC es una conectividad punto a punto y no admite el enrutamiento transitivo. Por ejemplo, si tiene una conexión de emparejamiento de VPC entre la VPC A y la VPC B y entre la VPC A y la VPC C, una instancia de la VPC B no puede transitar a través de la VPC A para llegar a la VPC C. Para enrutar paquetes entre la VPC B y la VPC C, debe crear un emparejamiento de VPC directo.

A escala, cuando se tiene de 10 a 100 VPC, interconectarlas mediante el emparejamiento da como resultado una malla de 100 a 1000 conexiones de interconexión, que son difíciles de administrar y escalar. Hay un límite máximo de 125 conexiones de emparejamiento por VPC.

Figura 2: Configuración de red mediante emparejamiento de VPC

Si utiliza el emparejamiento de VPC, se debe establecer una conectividad local (VPN o Direct Connect) en cada VPC. Los recursos de una VPC no pueden llegar a las instalaciones mediante la conectividad híbrida de una VPC emparejada (Figura 2).

El emparejamiento de VPC se utiliza mejor cuando los recursos de una VPC deben comunicarse con los recursos de otra VPC, el entorno de ambas VPC está controlado y protegido, y la cantidad de VPC que se van a conectar es inferior a 10 (para permitir la administración individual de cada conexión). El emparejamiento de VPC ofrece el coste general más bajo en comparación con otras opciones de conectividad entre VPC.

Solución de VPC de tránsito

Las [VPC de tránsito](#) pueden resolver algunas de las deficiencias de la emparejamiento de VPC mediante la introducción de un diseño central y radial para la conectividad entre las VPC. En una red de VPC de tránsito, una VPC central se conecta con todas las demás VPC (VPC radiales) a través de una conexión VPN que, por lo general, aprovecha BGP a través de IPSec. La VPC central contiene instancias de EC2 que ejecutan dispositivos de software que dirigen el tráfico entrante a sus destinos mediante la superposición de VPN (Figura 3). El emparejamiento de VPC en tránsito tiene las siguientes ventajas:

- El enrutamiento transitivo se habilita mediante la red VPN superpuesta, lo que permite un diseño central y radial más simple.
- Cuando se utiliza software de proveedores externos en la instancia de EC2 en la VPC de tránsito central, se puede aprovechar la funcionalidad del proveedor en torno a la seguridad avanzada (firewall/IPS/IDS de capa 7). Si los clientes utilizan el mismo software de forma local, se benefician de una experiencia operativa y de supervisión unificada.

Figura 3: VPC de tránsito con CSR de Cisco

La VPC de tránsito presenta sus propios desafíos, como costes más altos para ejecutar dispositivos virtuales, rendimiento limitado por VPC (hasta 1,25 Gbps por túnel VPN) y sobrecarga adicional de configuración y administración (los clientes deben administrar la disponibilidad y la redundancia de las instancias de EC2).

Transit Gateway

[AWS Transit Gateway](#) proporciona un diseño central y radial para conectar VPC y redes locales como un servicio completamente administrado sin necesidad de aprovisionar dispositivos virtuales como los CSR de Cisco. No se requiere superposición de VPN y AWS administra la alta disponibilidad y la escalabilidad.

Transit Gateway permite a los clientes conectar miles de VPC. Puede conectar toda su conectividad híbrida (conexiones VPN y Direct Connect) a una sola Transit Gateway, lo que consolida y controla toda la configuración de enrutamiento de AWS de su organización en un solo lugar (Figura 4). Transit Gateway controla cómo se dirige el tráfico entre todas las redes radiales conectadas mediante tablas de enrutamiento. Este modelo central y radial simplifica la administración y reduce los costes operativos porque las VPC solo se conectan a Transit Gateway para obtener acceso a las redes conectadas.

Figura 4: Diseño central y radial con AWS Transit Gateway

Transit Gateway es un recurso regional y puede conectar miles de VPC dentro de la misma región de AWS. Puede crear varias Transit Gateways por región, pero las Transit Gateways dentro de una región de AWS no se pueden emparejar entre sí y puede conectarse a un máximo de tres Transit Gateways a través de una sola conexión de Direct Connect para la conectividad híbrida. Por estas razones, debe restringir su arquitectura a una sola Transit Gateway que conecte todas sus VPC en una región determinada y usar tablas de enrutamiento de Transit Gateway para aislarlas donde sea necesario. Existe un caso válido para crear varias Transit Gateways únicamente para limitar el radio de acción de configuración incorrecta.

Coloque la Transit Gateway de su organización en su cuenta de servicios de red. Esto permite la administración centralizada por parte de los ingenieros de red que administran la cuenta de servicios de red Use AWS Resource Access Manager (RAM) para compartir una Transit Gateway para conectar VPC en varias cuentas de su organización de AWS dentro de la misma región. AWS RAM le permite compartir recursos de AWS de manera fácil y segura con cualquier cuenta de AWS o dentro de su AWS Organization. Para obtener más información, consulte la publicación del blog [Automating AWS Transit Gateway attachments to a transit gateway in a central account](#).

Temas

- [Transit Gateway frente a Transit VPC](#)
- [Transit Gateway frente a emparejamiento de VPC](#)

Transit Gateway frente a Transit VPC

Transit Gateway ofrece una serie de ventajas con respecto a Transit VPC:

- Transit Gateway abstrae la complejidad de mantener las conexiones VPN con cientos de VPC.
- Transit Gateway elimina la necesidad de administrar y escalar los dispositivos de software basados en EC2. AWS es responsable de administrar todos los recursos necesarios para dirigir el tráfico.
- Transit Gateway elimina la necesidad de administrar la alta disponibilidad al proporcionar una infraestructura Multi-AZ redundante y de alta disponibilidad.
- Transit Gateway mejora el ancho de banda para la comunicación entre VPC a velocidades de ráfaga de 50 Gbps por zona de disponibilidad.
- Transit Gateway optimiza los costes de los usuarios a un modelo transferido simple por hora por GB.
- Transit Gateway reduce la latencia al eliminar los proxies de EC2 y la necesidad de encapsulación de VPN.

Transit Gateway frente a emparejamiento de VPC

Transit Gateway resuelve la complejidad que implica crear y administrar varios emparejamientos de VPC a escala. Si bien esto hace que TGW sea un buen valor predeterminado para la mayoría de las arquitecturas de red, el emparejamiento de VPC sigue siendo una opción válida debido a las siguientes ventajas que tiene sobre TGW:

- Menor coste: con el emparejamiento de VPC, solo paga los cargos por transferencia de datos. Transit Gateway tiene un cargo por hora por vinculación además de las tarifas de transferencia de datos.
- Sin límites de ancho de banda: con Transit Gateway, el ancho de banda máximo (ráfaga) por conexión VPC es de 50 Gbps. El emparejamiento de VPC no tiene ancho de banda agregado. Los límites de rendimiento de la red de instancias individuales y los límites de flujo (10 Gbps dentro de un grupo de ubicación y 5 Gbps en caso contrario) se aplican a ambas opciones. Solo el emparejamiento de VPC admite grupos de ubicación.
- Latencia: a diferencia del emparejamiento de VPC, Transit Gateway es un salto adicional entre las VPC.
- Compatibilidad con grupos de seguridad: la referencia de grupos de seguridad funciona con el emparejamiento de VPC intrarregional. Actualmente, no funciona con Transit Gateway.

Dentro de la configuración de la zona de aterrizaje, el emparejamiento de VPC se puede utilizar en combinación con el modelo central y radial habilitado por Transit Gateway.

AWS PrivateLink

Es posible que los clientes deseen exponer de forma privada un servicio/aplicación que reside en una VPC (proveedor de servicios) a otras VPC de consumidor dentro de una región de AWS de manera que solo las VPC de consumidor inicien conexiones con la VPC del proveedor de servicios. Un ejemplo de esto es la capacidad de las aplicaciones privadas de acceder a las API de los proveedores de servicios.

Para usar AWS PrivateLink, cree un Network Load Balancer para su aplicación en la VPC y cree una configuración de servicio de punto de conexión de la VPC que apunte a ese equilibrador de carga. A continuación, un consumidor de servicios crea un punto de conexión de interfaz para su servicio. Con ello se creará una interfaz de red elástica en su subred con una dirección IP privada que sirve como punto de entrada al tráfico dirigido al servicio. El consumidor y el servicio no tienen que estar en la misma VPC. Si la VPC es diferente, las VPC del consumidor y del proveedor de servicios pueden tener intervalos de direcciones IP superpuestos. Además de crear el punto de conexión de la VPC de la interfaz para acceder a los servicios de otras VPC, puede crear puntos de conexión de la VPC de la interfaz para acceder de forma privada a los [servicios de AWS compatibles](#) a través de AWS PrivateLink (Figura 5).

Figura 5 – AWS PrivateLink

La elección entre Transit Gateway, emparejamiento de VPC y AWS PrivateLink depende de la conectividad.

AWS PrivateLink: utilice AWS PrivateLink cuando tenga un cliente/servidor configurado en el que desee permitir el acceso unidireccional de una o más VPC de consumidor a un servicio o conjunto de instancias específicos en la VPC del proveedor de servicios. Solo los clientes de la VPC de consumidor pueden iniciar una conexión con el servicio en la VPC del proveedor de servicios. También es una buena opción cuando el cliente y los servidores de las dos VPC tienen direcciones IP superpuestas, ya que AWS PrivateLink aprovecha los ENI dentro de la VPC del cliente para que no haya conflictos de IP con el proveedor de servicios. Puede acceder a los puntos de conexión de AWS PrivateLink a través del emparejamiento de VPC, VPN y AWS Direct Connect.

Emparejamiento de VPC y Transit Gateway: utilice el emparejamiento de VPC y Transit Gateway cuando desee habilitar la conectividad IP de capa 3 entre las VPC.

Su arquitectura contendrá una combinación de estas tecnologías para cumplir con diferentes casos de uso. Todos estos servicios se pueden combinar y operar entre sí. Por ejemplo, AWS PrivateLink gestionando la conectividad cliente-servidor de estilo API, el emparejamiento de VPC gestionando los requisitos de conectividad directa en los casos en los que todavía se desean grupos de colocación dentro de la región o se necesita conectividad entre regiones, y Transit Gateway para simplificar la conectividad de las VPC a escala, así como la consolidación perimetral para la conectividad híbrida.

Uso compartido de Amazon VPC

El uso compartido de VPC es útil cuando el propietario de la VPC no necesita administrar estrictamente el aislamiento de la red entre equipos, pero los usuarios y los permisos del nivel de cuenta sí deben hacerlo. Con la [VPC compartida](#), varias cuentas de AWS crean sus recursos de aplicaciones (como instancias de Amazon EC2) en VPC de Amazon compartidas y administradas de forma centralizada. En este modelo, la cuenta propietaria de la VPC (el propietario) comparte una o varias subredes con otras cuentas (participantes). Después de compartir una subred, los participantes pueden ver, crear, modificar y eliminar los recursos de su aplicación en las subredes compartidas con ellos. Los participantes no pueden ver, modificar ni eliminar recursos que pertenezcan a otros participantes o al propietario de la VPC. La seguridad entre los recursos de las VPC compartidas se administra mediante grupos de seguridad y ACL de red de subred.

Beneficios de uso compartido de VPC:

- Diseño simplificado: sin complejidad en lo que respecta a la conectividad entre VPC
- Menos VPC administradas
- Separación de funciones entre los equipos de red y los propietarios de aplicaciones
- Mejor utilización de direcciones IPv4
- Menores costes: sin cargos por transferencia de datos entre instancias que pertenezcan a diferentes cuentas dentro de la misma zona de disponibilidad


Nota: Cuando se comparte una subred con varias cuentas, sus participantes deben tener cierto nivel de cooperación, ya que comparten el espacio de IP y los recursos de red. Si es necesario, puede elegir compartir una subred diferente para cada cuenta de participante. Una subred por participante permite que la ACL de red proporcione aislamiento de red además de los grupos de seguridad.

La mayoría de las arquitecturas de clientes contendrán varias VPC, muchas de las cuales se compartirán con dos o más cuentas. Transit Gateway y el emparejamiento de VPC se pueden usar

para conectar las VPC compartidas. Por ejemplo, supongamos que tiene 10 aplicaciones. Cada aplicación requiere su propia cuenta de AWS. Las aplicaciones se pueden clasificar en dos carteras de aplicaciones (las aplicaciones dentro de la misma cartera tienen requisitos de red similares, la aplicación 1-5 en "Marketing" y la aplicación 6-10 en "Ventas").

Puede tener una VPC por cartera de aplicaciones (dos VPC en total) y la VPC se comparte con las diferentes cuentas de propietarios de aplicaciones dentro de esa cartera. Los propietarios de aplicaciones implementan aplicaciones en sus respectivas VPC compartidas (en este caso, en las diferentes subredes para la segmentación y el aislamiento de rutas de red mediante NACL). Las dos VPC compartidas se conectan a través de Transit Gateway. Con esta configuración, podría pasar de tener que conectar 10 VPC a solo 2 (Figura 6).

Figura 6: Ejemplo de configuración: VPC compartida

 Note

Los que participan en el uso compartido de VPC no pueden crear todos los recursos de AWS en una subred compartida. Para obtener más información, consulte [Limitaciones de Amazon VPC](#).

Conectividad híbrida

Esta sección se centra en conectar de forma segura los recursos en la nube con los centros de datos locales. Hay dos métodos para habilitar la conectividad híbrida:

1. Conectividad uno a uno: en esta configuración, se crea una conexión VPN o una VIF privada de Direct Connect para cada VPC. Esto se logra aprovechando la puerta de enlace privada virtual (VGW). Esta opción es ideal para pequeñas cantidades de VPC, pero a medida que un cliente escala sus VPC, la administración de la conectividad híbrida por VPC puede resultar difícil.
2. Consolidación perimetral: en esta configuración, los clientes consolidan la conectividad de TI híbrida para varias VPC en un único punto de conexión. Todas las VPC comparten estas conexiones híbridas. Esto se logra mediante el uso de AWS Transit Gateway y Direct Connect Gateway.

Temas

- [VPN](#)
- [Direct Connect](#)

VPN

Figura 7: opciones de terminación de AWS VPN

Hay tres maneras de configurar una VPN en AWS:

1. Consolidar la conectividad VPN en Transit Gateway: esta opción aprovecha la conexión de VPN de Transit Gateway en Transit Gateway. Transit Gateway admite la terminación de IPsec para Site-to-Site VPN. Los clientes pueden crear túneles VPN a Transit Gateway y acceder a las VPC conectadas a ella. Transit Gateway admite conexiones VPN dinámicas tanto estáticas como basadas en BGP. Transit Gateway también admite [rutas múltiples de igual coste](#) (ECMP) en vinculaciones de VPN. Cada conexión VPN tiene un rendimiento máximo de 1,25 Gbps y habilitar ECMP permite agregar rendimiento en todas las conexiones VPN. En esta opción, se pagan los precios de Transit Gateway así como los precios de AWS VPN. Recomendamos usar esta opción para la conectividad de VPN. Para obtener más información, consulte la [Información general de AWS VPN](#).

2. Finalizar VPN en la instancia de EC2: los clientes aprovechan esta opción en casos periféricos cuando desean un conjunto de funciones de software de un proveedor en particular (como DMVPN de Cisco o GRE), o si desean coherencia operativa en varias implementaciones de VPN. Puede aprovechar el diseño de VPC de tránsito para la consolidación perimetral, pero es importante recordar que todas las consideraciones clave de la sección de conectividad de VPC a VPC para VPC en tránsito se aplican a la conectividad de VPN híbrida. El cliente es responsable de administrar la alta disponibilidad y pagar los costes de las instancias de EC2, así como las licencias de software de cualquier proveedor.
3. Terminar VPN en una puerta de enlace privada virtual (VGW): esta opción permite un diseño de conectividad uno a uno en el que se crea una conexión VPN (que consiste en un par de túneles de VPN redundantes) por VPC. Esta es una excelente manera de comenzar con la conectividad de VPN en AWS, pero a medida que se escala el número de VPC, el diseño de consolidación perimetral que aprovecha Transit Gateway será una mejor opción. El rendimiento de VPN a una VPC está limitado a 1,25 Gbps y no se admite el balanceador de carga de ECMP. Desde el punto de vista de los precios, solo se paga por los precios de AWS VPN, no hay ningún cargo por ejecutar una VGW. Para obtener más información, consulte [Precios de AWS VPN](#) y [AWS VPN en una puerta de enlace privada virtual](#).

Direct Connect

Si bien la VPN a través de Internet es una excelente opción para comenzar, la conectividad a Internet puede no ser confiable para el tráfico de producción. Debido a esta falta de confiabilidad, muchos clientes eligen [AWS Direct Connect](#), que permite una conectividad de fibra dedicada consistente, de baja latencia y alto ancho de banda entre los centros de datos de los clientes y AWS. Hay cuatro formas de aprovechar AWS Direct Connect para conectar a las VPC:

Figura 8: Cuatro formas de conectar los centros de datos locales a la zona de aterrizaje

- Crear una interfaz virtual privada (VIF) para una VGW conectada a una VPC: puede crear 50 VIF por conexión Direct Connect, lo que le permite conectarse a un máximo de 50 VPC (una VIF proporciona conectividad a una VPC). Hay un emparejamiento de BGP por VPC. La conectividad en esta configuración está restringida a la región de AWS a la que se dirige la ubicación de Direct Connect. La asignación uno a uno de VIF a VPC (y la falta de acceso global) hace que esta sea la forma menos preferida de acceder a las VPC en la zona de aterrizaje.
- Crear una VIF privada en una puerta de enlace de Direct Connect asociada a varias VGW (cada VGW está conectada a una VPC): una puerta de enlace de Direct Connect puede conectarse

a hasta 10 VGW en todo el mundo (excepto China) en cualquier cuenta de AWS. Esta es una excelente opción si una zona de aterrizaje consta de un número reducido de VPC (diez o menos VPC) o si necesita acceso global. Hay un emparejamiento de BGP por puerta de enlace de Direct Connect y por conexión de Direct Connect. La puerta de enlace Direct Connect es solo para el flujo de tráfico norte/sur y no permite la conectividad de VPC a VPC.

- Crear una VIF de tránsito a una puerta de enlace de Direct Connect asociada a Transit Gateway: puede asociar una Transit Gateway a una puerta de enlace de Direct Connect a través de una conexión de Direct Connect dedicada o alojada que se ejecute a 1 Gbps o más. Esta opción permite conectar el centro de datos local a hasta tres Transit Gateways (que se pueden conectar a miles de VPC) en diferentes regiones de AWS y cuentas de AWS a través de un emparejamiento de VIF y BGP. Esta es la configuración más sencilla de las cuatro opciones para conectar varias VPC a escala, pero debe tener en cuenta [las limitaciones de Transit Gateway](#). Un límite clave es que solo puede anunciar 20 rangos de CIDR desde una Transit Gateway hasta un enrutador local a través de la VIF de tránsito. Con las opciones 1 y 2, se pagan los precios de Direct Connect. En el caso de la opción 3, también se pagan los gastos de conexión de puerta de enlace de tránsito y de transferencia de datos. Consulte la documentación de [Asociaciones de la gateway de tránsito en Direct Connect](#) para obtener más información.
- Crear una conexión VPN a Transit Gateway a través de la VIF pública de Direct Connect: una interfaz virtual pública le permite acceder a todos los servicios públicos y puntos de conexión de AWS mediante las direcciones IP públicas. Cuando crea una conexión de VPN en una Transit Gateway, obtiene dos direcciones IP públicas para la terminación de la VPN en el extremo de AWS. Se puede acceder a estas IP públicas a través de la VIF pública. Puede crear tantas conexiones VPN a tantas Transit Gateways como desee a través de VIF pública. Cuando se crea un emparejamiento de BGP en la VIF pública, AWS anuncia todo el rango de IP públicas de AWS en el enrutador. Para asegurarse de que solo permite cierto tráfico (por ejemplo, permitir el tráfico solo a los puntos de conexión de terminación de VPN), se recomienda utilizar un firewall local. Esta opción se puede usar para cifrar su Direct Connect en la capa de red.

Si bien la tercera opción (tránsito de VIF a la puerta de enlace de Direct Connect) puede parecer la mejor opción porque le permite consolidar toda su conectividad local para una región de AWS determinada en un solo punto (Transit Gateway) mediante una sola sesión de BGP por conexión de Direct Connect, dados algunos de los límites y consideraciones en torno a la opción 3, esperamos que los clientes aprovechen tanto la opción 2 como la opción 3 para sus requisitos de conectividad de zona de aterrizaje. La figura 9 ilustra un ejemplo de configuración en el que se usa la VIF de tránsito como método predeterminado para conectarse a las VPC, y se usa una VIF privada para un caso de uso perimetral en el que se debe transferir una gran cantidad de datos desde una DC

local a la VPC de medios. La VIF privada se utiliza para evitar los cargos por transferencia de datos de Transit Gateway. Como práctica recomendada, debe tener al menos dos conexiones en dos ubicaciones de Direct Connect diferentes para obtener la máxima redundancia; en total, cuatro conexiones. Se crea una VIF por conexión para un total de cuatro VIF privadas y cuatro VIF de tránsito. También se crea una VPN como conectividad de respaldo a conexiones de AWS Direct Connect.

Figura 9: Ejemplo de arquitectura de referencia para conectividad híbrida

Use la cuenta de servicios de red para crear recursos de Direct Connect que permitan la demarcación de los límites administrativos de la red. La conexión Direct Connect, la puerta de enlace Direct Connect y Transit Gateway pueden residir en una cuenta de servicios de red. Para compartir la conectividad de AWS Direct Connect con su zona de aterrizaje, simplemente comparta la Transit Gateway a través de RAM con otras cuentas.

Salida centralizada a Internet

A medida que implemente aplicaciones en su zona de aterrizaje, muchas aplicaciones requerirán acceso a Internet solo saliente (por ejemplo, al descargar bibliotecas/parches/actualizaciones del sistema operativo). Puede lograr esto preferentemente mediante el uso de una puerta de enlace de traducción de direcciones de red (NAT) o, alternativamente, una instancia de EC2 (configurada con NAT de origen (SNAT)) como salto siguiente para todos los accesos a Internet de salida. Las aplicaciones internas residen en subredes privadas, mientras que las instancias NAT Gateway/EC2 NAT residen en una subred pública.

Utilización de la puerta de enlace de NAT

La implementación de una puerta de enlace de NAT en cada VPC radial puede resultar costosa porque paga un cargo por hora por cada puerta de enlace de NAT que implemente (consulte los [precios de Amazon VPC](#)), por lo que centralizarla podría ser una opción viable. Para centralizar, creamos una VPC de salida en la cuenta de servicios de red y dirigimos todo el tráfico de salida de las VPC radiales a través de una puerta de enlace de NAT ubicada en esta VPC que aprovecha Transit Gateway, como se muestra en la figura 10.

Nota: Cuando se centraliza NAT Gateway con Transit Gateway, se paga un cargo adicional por procesamiento de datos de Transit Gateway, en comparación con el enfoque descentralizado de ejecutar una puerta de enlace de NAT en cada VPC. En algunos casos periféricos, cuando se envían grandes cantidades de datos a través de NAT Gateway desde una VPC, mantener la NAT local en la VPC para evitar el cargo de procesamiento de datos de Transit Gateway puede ser una opción más rentable.

Figura 10: Puerta de enlace de NAT centralizada mediante Transit Gateway (descripción general)

Figura 11: Puerta de enlace de NAT centralizada mediante Transit Gateway (diseño de tabla de enrutamiento)

En esta configuración, las vinculaciones de VPC radiales se asocian a la tabla de enrutamiento 1 (RT1) y se propagan a la tabla de enrutamiento 2 (RT2). Hemos agregado explícitamente una ruta Blackhole para impedir que las dos VPC se comuniquen entre sí. Si desea permitir la comunicación entre VPC, puede eliminar la entrada de ruta "10.0.0.0/8 -> Blackhole" del RT1. Esto les permite comunicarse a través de la puerta de enlace de NAT. También puede propagar las vinculaciones de

VPC radiales a RT1 (o, alternativamente, puede usar una tabla de enrutamiento y asociar/propagar todo a ella), lo que permite el flujo de tráfico directo entre las VPC mediante Transit Gateway.

Añadimos una ruta estática en RT1 que apunta todo el tráfico a la VPC de salida. Debido a esta ruta estática, Transit Gateway envía todo el tráfico de Internet a través de sus ENI en la VPC de salida. Una vez en la VPC de salida, el tráfico sigue las reglas definidas en la tabla de enrutamiento de subred en la que están presentes estos ENI de Transit Gateway. Agregamos una ruta en esta tabla de enrutamiento de subred que apunta todo el tráfico hacia la puerta de enlace de NAT. La tabla de enrutamiento de subred de puerta de enlace de NAT tiene la puerta de enlace de Internet (IGW) como salto siguiente. Para que el tráfico de retorno fluya hacia atrás, debe agregar una entrada de tabla de enrutamiento estática en la tabla de enrutamiento de subred de la puerta de enlace de NAT que señale todo el tráfico vinculado a la VPC radial a Transit Gateway como siguiente salto.

Alta disponibilidad

Para una alta disponibilidad, debe usar dos puertas de enlace de NAT (una en cada zona de disponibilidad). Dentro de una zona de disponibilidad, la puerta de enlace de NAT tiene un SLA de disponibilidad del 99,9 %. AWS gestiona la redundancia contra fallos de componentes dentro de una zona de disponibilidad en virtud del acuerdo de SLA. El tráfico se interrumpe durante el 0,1 % cuando la puerta de enlace de NAT no pueda estar disponible en una zona de disponibilidad. Si una zona de disponibilidad falla por completo, el punto de conexión de Transit Gateway junto con la puerta de enlace de NAT en esa zona de disponibilidad fallarán y todo el tráfico fluirá a través de los extremos de conexión de la puerta de enlace de NAT y Transit Gateway en la otra zona de disponibilidad.

Seguridad

Se confía en los grupos de seguridad de las instancias de origen, las rutas de agujeros negros en las tablas de enrutamiento de Transit Gateway y la ACL de red de la subred en la que se encuentra la puerta de enlace de NAT.

Escalabilidad

Una puerta de enlace NAT puede admitir hasta 55.000 conexiones simultáneas a cada destino único. Desde el punto de vista del rendimiento, está limitado por los límites de rendimiento de la puerta de enlace de NAT. Transit Gateway no es un equilibrador de carga y no distribuirá el tráfico de manera uniforme entre la puerta de enlace de NAT en las distintas zonas de disponibilidad. Si es posible, el tráfico a través de Transit Gateway permanecerá dentro de una zona de disponibilidad. Si el tráfico de inicio de la instancia de EC2 se encuentra en AZ 1, el tráfico saldrá de la interfaz de red elástica de Transit Gateway en la misma AZ 1 en la VPC de salida y fluirá al siguiente salto en función de la

tabla de enrutamiento de subred en la que reside la interfaz de red elástica. Para obtener una lista completa de reglas, consulte [Reglas y límites de la puerta de enlace de NAT](#).

Para obtener más información, consulte la publicación del blog [Creating a single internet exit point from multiple VPCs Using AWS Transit Gateway](#).

Uso de una instancia de EC2 para la salida centralizada

El uso de un dispositivo de firewall basado en software (en EC2)AWS Marketplace como punto de salida es similar a la configuración de la puerta de enlace de NAT. Esta opción se puede utilizar si desea aprovechar las capacidades de firewall de capa 7, prevención de intrusiones y sistemas de detección (IPS/IDS) de las distintas ofertas de proveedores.

En la figura 12, sustituimos la puerta de enlace de NAT por una instancia de EC2 (con SNAT habilitada en la instancia de EC2). Hay algunas consideraciones clave con esta opción:

Alta disponibilidad

En esta configuración, es responsable de supervisar la instancia de EC2, detectar errores y reemplazar la instancia de EC2 por una instancia de copia de seguridad/en espera. La mayoría de los proveedores de AWS tienen automatización prediseñada para su software implementado en esta configuración. Esa automatización puede controlar lo siguiente:

- Detectar errores en la instancia de EC2-1 principal
- Cambie la tabla de enrutamiento "Route Table Egx 1" para que apunte todo el tráfico a la instancia de EC2-2 de seguridad en caso de que falle la instancia principal. Esto también se debe hacer para las subredes de la AZ 2.

Figura 12: NAT centralizada mediante instancias de EC2 y Transit Gateway

Escalabilidad

Transit Gateway no es un equilibrador de carga y no distribuirá el tráfico de manera uniforme entre las instancias de las dos zonas de disponibilidad. Si es posible, el tráfico a través de Transit Gateway permanecerá dentro de una zona de disponibilidad. Está limitado por las capacidades de ancho de banda de una sola instancia de EC2. Puede escalar verticalmente esta instancia de EC2 a medida que aumenta el uso.

Si el proveedor que elija para la inspección del tráfico de salida no admite la automatización para la detección de errores, o si necesita un escalado horizontal, puede usar un diseño alternativo. En este diseño (Figura 13), no creamos una vinculación de VPC en la puerta de enlace de tránsito para la VPC de salida, sino que creamos una conexión de VPN de IPsec y creamos una VPN de IPsec desde Transit Gateway a las instancias de EC2 que aprovechan BGP para intercambiar rutas.

Ventajas

- Detección de errores y reenrutamiento del tráfico gestionado por BGP. No se requiere la automatización de tablas de enrutamiento de subredes de VPC.
- El ECMP de BGP se puede utilizar para equilibrar la carga del tráfico en varias instancias de EC2; es posible el escalado horizontal.

Figura 13: NAT centralizada mediante instancias de EC2 y VPN de Transit Gateway

Consideraciones clave

- Sobrecarga de administración de VPN en instancias de EC2
- El ancho de banda en Transit Gateway está limitado a 1,25 Gbps por túnel de VPN. Con ECMP Transit Gateway puede admitir un ancho de banda de VPN total de hasta 50 Gbps. Las capacidades de procesamiento de paquetes y VPN del dispositivo del proveedor pueden ser un factor limitante.
- Este diseño supone que la instancia de EC2 de FW funciona con la misma interfaz de red elástica para el tráfico entrante y saliente.
- Si habilita el balanceador de carga de ECMP del tráfico en varias instancias de EC2, debe convertir con SNAT el tráfico en la instancia de EC2 para garantizar la simetría del flujo de retorno, lo que significa que el destino no conocerá el verdadero origen.

Seguridad de red centralizada para tráfico de VPC a VPC y local a VPC

AWS proporciona grupos de seguridad y NACLs de subred para implementar la seguridad de la red en su zona de aterrizaje. Son firewalls de capa 4. Puede haber situaciones en las que un cliente quiera implementar un firewall/IPS/ID de capa 7 dentro de su zona de aterrizaje para inspeccionar el tráfico que fluye entre las VPC o entre un centro de datos local y una VPC. Esto se puede lograr con Transit Gateway y dispositivos de software de terceros que se ejecutan en instancias de EC2. Con la arquitectura de la figura 14, podemos permitir que el tráfico de VPC a VPC y de local a VPC fluya a través de las instancias de EC2. La configuración es similar a la que ya hemos analizado en la figura 12, pero además eliminamos la ruta de agujero negro en la tabla de enrutamiento 1 para permitir el flujo de tráfico de VPC interna y asociamos la conexión de VPN y/o la vinculación de Direct Connect GW a la tabla de enrutamiento 1 para permitir el flujo de tráfico híbrido. Esto permite que todo el tráfico procedente de los radios fluya a la VPC de salida antes de enviarse al destino. Necesita rutas estáticas en la tabla de enrutamiento de subred de VPC de salida (donde residen los dispositivos EC2 de firewall) para enviar tráfico destinado a VPC radiales y CIDR local a través de Transit Gateway después de la inspección del tráfico.

Note

La información de ruta no se propaga dinámicamente desde Transit Gateway a la tabla de enrutamiento de subred y se debe introducir de forma estática. Hay un límite flexible de 50 rutas estáticas en una tabla de enrutamiento de subred.

Figura 14: Control de tráfico de VPC a VPC y de VPC a local

Consideraciones clave al enviar tráfico a instancias de EC2 para su inspección en línea:

- Cargos de procesamiento de datos adicionales de Transit Gateway
- El tráfico debe pasar por dos saltos adicionales (instancia de EC2 y Transit Gateway)
- Potencial de cuellos de botella de rendimiento y ancho de banda
- Complejidad adicional de mantener, administrar y escalar instancias de EC2:
 - Detección de fallos y conmutación por error a modo de espera

- Uso de seguimiento y escalado horizontal/vertical
- Configuración de firewall, administración de parches
- Traducción de direcciones de red de origen (SNAT) del tráfico cuando se equilibra la carga para garantizar un flujo simétrico

Debe ser selectivo en cuanto al tráfico que pasa a través de estas instancias de EC2. Una forma de proceder es definir las zonas de seguridad e inspeccionar el tráfico entre las zonas que no son de confianza. Una zona que no es de confianza puede ser un sitio remoto administrado por un tercero, una VPC de proveedor que no controla o en la que no confía o una VPC de entorno aislado o de desarrollo, que tiene un marco de seguridad más relajado en comparación con el resto del entorno. En la figura 15 se permite el flujo de tráfico directo entre redes de confianza mientras se inspecciona el flujo de tráfico hacia/desde redes que no son de confianza mediante instancias de EC2 en línea. En este ejemplo, hemos creado tres zonas:

- Zona no confiable: para cualquier tráfico procedente de la “VPN a un sitio remoto que no es de confianza” o la VPC de un proveedor externo.
- Zona de producción: contiene el tráfico de la VPC de producción y de la DC del cliente local.
- Zona de desarrollo: contiene el tráfico de las dos VPC de desarrollo.

A continuación, se muestran ejemplos de reglas que definimos para la comunicación entre zonas:

1. Zona no confiable - Zona de producción: no se permite la comunicación
2. Zona de producción - Zona de desarrollo: se permite la comunicación a través de dispositivos FW de EC2 en la VPC de salida
3. Zona no confiable - Zona de desarrollo: se permite la comunicación a través de dispositivos FW de EC2 en la VPC de salida
4. Zona de producción - Zona de producción y Zona de desarrollo - Zona de desarrollo: comunicación directa mediante Transit Gateway

Esta es una configuración que tiene tres zonas de seguridad, pero puede que tengas más. Puede utilizar varias tablas de enrutamiento y rutas de agujeros negros para lograr un aislamiento de seguridad y un flujo de tráfico óptimo. La elección de las zonas correctas depende de la estrategia general de diseño de la zona de aterrizaje (estructura de la cuenta, diseño de la VPC). Puede tener zonas para permitir el aislamiento entre unidades de negocio, aplicaciones, entornos, etc.

En este ejemplo, terminamos la VPN remota que no es de confianza en Transit Gateway y enviamos todo el tráfico a los dispositivos FW de software en EC2 para su inspección. Como alternativa, puede terminar estas VPN directamente en las instancias de EC2 en lugar de hacerlo en Transit Gateway. Con este enfoque, el tráfico de VPN que no es de confianza nunca interactúa directamente con Transit Gateway. La cantidad de saltos en el flujo de tráfico se reduce en 1 y se ahorra en costes de AWS VPN. Para habilitar los intercambios de rutas dinámicas (para que Transit Gateway aprenda el CIDR de la VPN remota a través de BGP), las instancias de firewall deben conectarse a Transit Gateway a través de una VPN. En el modelo de conexión TGW nativo, debe agregar rutas estáticas en la tabla de enrutamiento TGW para VPN CIDE con el siguiente salto como la VPC de seguridad/salida. En nuestra configuración (Figura 15), tenemos una ruta predeterminada a la VPC de salida para todo el tráfico, de modo que no hay que añadir explícitamente ninguna ruta estática específica. Con este enfoque, pasa de un punto de conexión de terminación de VPN de Transit Gateway completamente administrado a una instancia de EC2 autoadministrada, lo que agrega sobrecarga de administración de VPN y carga adicional en la instancia de EC2 en términos de computación y memoria.

Figura 15: Aislamiento del tráfico mediante Transit Gateway y definición de zonas de seguridad

DNS

Al lanzar una instancia en una VPC que no es predeterminada, AWS ofrece la instancia con un nombre de host DNS privado (posiblemente un nombre de host DNS público) en función de los [atributos de DNS](#) que especifique para la VPC y de si su instancia tiene una dirección IPv4 pública. Cuando el atributo “enableDnsSupport” se establece en true, se obtiene una resolución de DNS dentro de la VPC desde Route 53 Resolver (desplazamiento de IP +2 al CIDR de la VPC). De forma predeterminada Route 53 Resolver responde a las consultas de DNS de los nombres de dominio de la VPC como nombres de dominios para instancias de EC2 o balanceadores de carga de Elastic Load Balancing. Con el emparejamiento de VPC, los hosts de una VPC pueden resolver nombres de host de DNS públicos en direcciones IP privadas para instancias en VPC emparejadas, siempre que esté habilitada la opción de hacerlo. Lo mismo se aplica a las VPC conectadas a través de AWS Transit Gateway. Para obtener más información, consulte [Habilitación de la resolución de DNS para el emparejamiento de VPC](#).

Si desea asignar sus instancias a un nombre de dominio personalizado, puede usar Amazon Route 53 para crear un registro de asignación de DNS a IP personalizado. Una zona alojada de Amazon Route 53 es un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios. Las zonas alojadas públicas contienen información de DNS que se puede resolver en Internet pública, mientras que las zonas alojadas privadas son una implementación específica que solo presenta información a las VPC que se han adjuntado a la zona alojada privada específica. En una configuración de zona de aterrizaje en la que tiene varias VPC o cuentas, puede asociar una única zona alojada privada con varias VPC en las cuentas de AWS y en todas las regiones. Los hosts finales de las VPC utilizan su IP de Route 53 Resolver respectiva (desplazamiento +2 del CIDR de la VPC) como servidor de nombres para las consultas de DNS. Route 53 Resolver en la VPC solo acepta consultas de DNS de los recursos dentro de una VPC.

DNS híbrido

La coordinación de la resolución de DNS entre la configuración de la zona de aterrizaje de AWS y los recursos locales es una de las piezas más importantes de una red híbrida. Los clientes que implementan entornos híbridos suelen tener un sistema de resolución de DNS ya implementado y desean una solución de DNS que funcione en conjunto con su sistema actual. Cuando integra un DNS en las VPC de una región de AWS con un DNS en su red, necesita un punto de conexión de entrada de Route 53 Resolver (para las consultas de DNS que reenvía a las VPC) y un punto

de conexión de salida de Route 53 Resolver (para las consultas que reenvía desde las VPC a la red). Como se muestra en la Figura 16, puede configurar puntos de conexión salientes de Resolver para que reenvíen las consultas que reciba de las instancias de EC2 de las VPC a los servidores de DNS de la red. Para reenviar las consultas seleccionadas, desde una VPC a local, cree reglas de Route 53 Resolver que especifiquen los nombres de dominio para las consultas de DNS que quiere reenviar (como example.com) y las direcciones IP de los solucionadores de DNS en la red a las que desea reenviar las consultas. Para las consultas entrantes desde las zonas locales a las alojadas de Route 53, los servidores de DNS de la red pueden reenviar consultas a los puntos de conexión entrantes de Resolver en una VPC especificada.

Figura 16: Resolución de DNS híbrida con el Route 53 Resolver

Esto permite a los solucionadores de DNS locales resolver fácilmente los nombres de dominio para recursos de AWS como registros o instancias de EC2 en una zona alojada privada de Route 53 asociada con esa VPC.

No se recomienda crear puntos de conexión de Route 53 Resolver en todas las VPC de la zona de aterrizaje. Centralícelos en una VPC de salida central (en la cuenta de servicios de red). Este enfoque permite una mejor capacidad de administración a la vez que mantiene los costes bajos (se cobra una tarifa por hora por cada punto de conexión de entrada/salida que cree). Se comparte el punto de conexión de entrada y salida centralizado con el resto de la zona de aterrizaje.

Resolución de salida: use la cuenta de servicios de red para escribir reglas de resolución (en función de las consultas de DNS que se reenviarán a los servidores de DNS locales). Con Resource Access Manager (RAM), comparta estas reglas de Route 53 Resolver con varias cuentas (y asócielas a las VPC de las cuentas). Las instancias de EC2 en VPC radiales pueden enviar consultas de DNS a Route 53 Resolver y Route 53 Resolver Service reenviará estas consultas al servidor de DNS local a través de los puntos de conexión de salida de Route 53 Resolver en la VPC de salida. No necesita emparejar las VPC radiales a la VPC de salida ni conectarlas a través de Transit Gateway. No utilice la IP del punto de conexión de resolución saliente como DNS principal en las VPC radiales. Las VPC radiales deben usar Route 53 Resolver (para compensar el CIDR de la VPC) en su VPC.

Figura 17: Centralización de los puntos de conexión de Route 53 Resolver en la VPC de salida

Resolución de DNS de entrada: cree puntos de conexión de entrada de Route 53 Resolver en una VPC centralizada y asocie todas las zonas alojadas privadas de su zona de aterrizaje con esta VPC centralizada. Para obtener más información, consulte [Associating More VPCs with a Private](#)

[Hosted Zone](#). Varias zonas alojadas privadas (PHZ) asociadas a una VPC no se pueden superponer. Como se muestra en la figura 17, esta asociación de PHZ con la VPC centralizada permitirá que los servidores locales resuelvan el DNS para cualquier entrada en cualquier zona alojada privada (asociada a la VPC central) mediante el punto de conexión de entrada en la VPC centralizada. Para obtener más información sobre las configuraciones de DNS híbridas, consulte [Administración centralizada de DNS de la nube híbrida con Amazon Route 53 y AWS Transit Gateway](#) y [Opciones de DNS de nube híbrida para Amazon VPC](#).

Acceso centralizado a puntos de conexión privados de la VPC

Un punto de conexión de la VPC le permite conectar su VPC de forma privada a los servicios de AWS compatibles sin necesidad de una puerta de enlace de Internet o un dispositivo NAT. Las instancias de la VPC no requieren direcciones IP públicas para comunicarse con los puntos de conexión del servicio de AWS con este punto de conexión de la interfaz. El tráfico entre su VPC y otros servicios no abandona la red troncal de AWS. Actualmente se pueden aprovisionar dos tipos de puntos de conexión: puntos de conexión de interfaz (con tecnología AWS PrivateLink) y puntos de conexión de puerta de enlace. Los puntos finales de puerta de enlace se pueden aprovisionar de forma gratuita y no hay un caso de uso sólido para la centralización.

Puntos de conexión de la VPC de tipo interfaz

Un [puntos de conexión de interfaz](#) es una más interfaces de red elástica con una dirección IP privada que actúan como punto de entrada para el tráfico dirigido a un servicio de AWS compatible. Cuando se aprovisiona un punto de conexión de interfaz, los usuarios incurren en un coste por cada hora en que se ejecute el punto de conexión. De forma predeterminada, se crea un punto de conexión de interfaz en cada VPC desde la que se desee acceder al servicio de AWS. Esto puede resultar caro y difícil de administrar en la configuración de la zona de aterrizaje, en la que un cliente quiere interactuar con un servicio de AWS específico en varias VPC. Para evitarlo, puede alojar los puntos de conexión de la interfaz en una VPC centralizada. Todas las VPC radiales usarán estos puntos de conexión centralizados.

Cuando se crea un punto de conexión de la VPC para un servicio de AWS, puede habilitar el DNS privado. Cuando se habilita, la configuración crea una zona alojada privada (PHZ) de Route 53 administrada por AWS que permite la resolución del punto de conexión del servicio público de AWS a la IP privada del punto de conexión de la interfaz. El PHZ administrado solo funciona dentro de la VPC con el punto de conexión de la interfaz. En nuestra configuración, cuando queremos que las VPC radiales puedan resolver el DNS de punto conexión de VPC alojado en una VPC centralizada, el PHZ administrado no funcionará. Para solucionar esto, deshabilite la opción que crea automáticamente el DNS privado cuando se crea un punto conexión de interfaz. Como alternativa, puede [crear manualmente un PHZ de Route 53](#) y agregar un registro Alias con el nombre completo del punto de conexión del servicio de AWS apuntando al punto de conexión de interfaz, como se muestra en la Figura 18.

Figura 18 — PHZ creado manualmente

[Asociamos](#) esta zona alojada privada con otras VPC dentro de la zona de aterrizaje. Esta configuración permite que las VPC radiales resuelvan los nombres de punto de conexión de servicio completo en los puntos de conexión de la interfaz en la VPC centralizada.

Note

Para acceder a la zona alojada privada compartida, los hosts de las VPC radiales deben usar la IP de Route 53 Resolver de su VPC. También se puede acceder a los puntos de conexión de interfaz desde redes locales a través de VPN y Direct Connect. Use reglas de reenvío condicional para enviar todo el tráfico de DNS para los nombres de punto de conexión de servicio completo a los puntos de conexión entrantes de Route 53 Resolver, que resolverá las solicitudes de DNS de acuerdo con la zona alojada privada.

En la Figura 19, Transit Gateway permite el flujo de tráfico desde las VPC radiales a los puntos de conexión de la interfaz centralizada. Cree puntos de conexión de VPC y la zona alojada privada para ello en la cuenta de servicios de red y compártalos con las VPC radiales en las cuentas radiales. Para obtener más información sobre cómo compartir información de puntos de conexión con otras VPC, consulte la publicación del blog [Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver](#).

Nota: Un enfoque de punto de conexión de VPC distribuida, es decir, un punto de conexión por VPC, permite aplicar políticas de privilegios mínimos en los puntos de conexión de VPC. En un enfoque centralizado, aplicará y administrará políticas para todos los accesos a VPC radiales en un único punto de conexión. Con el número creciente de VPC, puede aumentar la complejidad de mantener los privilegios mínimos con un solo documento de política. Un único documento de política también da como resultado un radio de explosión mayor. También tiene restricciones en cuanto al tamaño del documento de la política (20 480 caracteres).

Figura 19: Centralización de puntos de conexión de VPC de la interfaz

Conclusión

A medida que se escala el uso de AWS y se implementan aplicaciones en la zona de aterrizaje de AWS, aumenta el número de VPC y componentes de red. En este documento técnico se explica cómo podemos administrar esta infraestructura en crecimiento garantizando la escalabilidad, la alta disponibilidad y la seguridad, a la vez que mantenemos los costes bajos. Es fundamental tomar las decisiones de diseño correctas al aprovechar servicios como Transit Gateway, VPC compartida, AWS Direct Connect, puntos de conexión de VPC y dispositivos de software de terceros. Es importante comprender las consideraciones clave de cada enfoque y trabajar de forma retroactiva a partir de sus requisitos y analizar qué opción o combinación de opciones se adapta mejor a sus necesidades.

Colaboradores

Las siguientes personas participaron en la elaboración de este documento:

- Sidhartha Chauhan, arquitecto de soluciones, Amazon Web Services
- Amir Abu-akeel, arquitecto de infraestructura en la nube, Amazon Web Services
- Sohaib Tahir, arquitecta de soluciones, Amazon Web Services

Historial de revisión

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

update-history-change	update-history-description	update-history-date
Actualización menor	Se ha actualizado la sección Transit Gateway frente a un emparejamiento de VPC.	2 de abril de 2021
Documento técnico actualizado	Se ha corregido el texto para que coincida con las opciones ilustradas en la figura 7	10 de junio de 2020
Actualización menor	Se ha corregido el texto para que coincida con las opciones ilustradas en la figura 7	10 de junio de 2020
Publicación inicial	Documento técnico publicado.	15 de noviembre de 2019

Avisos

Los clientes son responsables de realizar sus propias evaluaciones de la información contenida en este documento. Este documento: (a) solo tiene fines informativos, (b) representa las prácticas y las ofertas de productos vigentes de AWS, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía de AWS y sus empresas filiales, proveedores o concesionarios de licencias. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, representaciones ni condiciones de ningún tipo, ya sean explícitas o implícitas. Las responsabilidades y las obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS. Además, este documento no forma parte de ningún acuerdo entre AWS y sus clientes ni lo modifica.

© 2019, Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.