Interconexión de VPC

Amazon Virtual Private Cloud

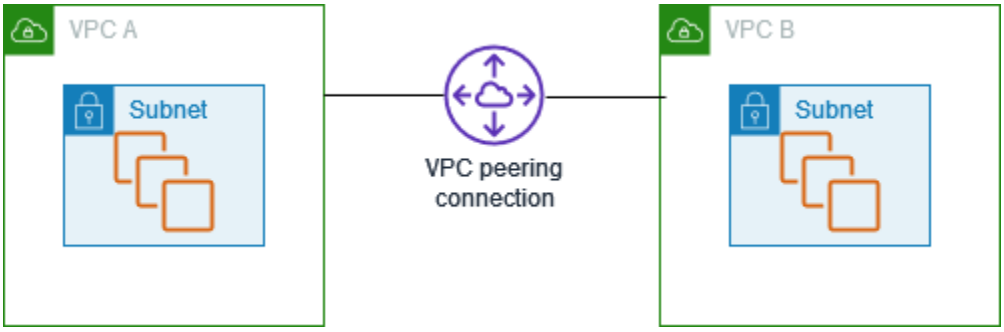
Amazon Virtual Private Cloud: Interconexión de VPC

Table of Contents

¿Qué es una interconexión de VPC?

Una nube privada virtual (VPC) es una red virtual dedicada para su Cuenta de AWS. Esta infraestructura en la nube está aislada lógicamente de otras redes virtuales de la nube de AWS. Puede lanzar recursos de AWS, como instancias de Amazon EC2, en la VPC.

Una interconexión de VPC es una conexión de redes entre dos VPC que permite direccionar tráfico entre ellas mediante direcciones IPv6 o direcciones IPv4 privadas. Las instancias de ambas VPC se pueden comunicar entre sí siempre que se encuentren en la misma red. Puede crear una interconexión de VPC entre sus propias VPC o con una VPC de otra cuenta de AWS. Las VPC pueden encontrarse en regiones distintas (lo que se conoce como conexiones de emparejamiento de VPC entre regiones).



AWS utiliza la infraestructura existente de una VPC para crear una interconexión de VPC. No se trata de ninguna gateway o conexión de VPN y no usa ningún hardware físico individual. Por lo tanto, no existen puntos de error de comunicaciones ni cuellos de botella de ancho de banda.

Una interconexión de VPC le ayuda a facilitar la transferencia de datos. Por ejemplo, si tiene más de una cuenta de AWS, puede interconectar las VPC de dichas cuentas para crear una red de uso compartido de archivos. También puede utilizar la interconexión de VPC para que otras VPC puedan obtener acceso a los recursos que tiene en una de sus VPC.

Al establecer relaciones de emparejamiento entre VPC en diferentes regiones de AWS, los recursos en las VPC (por ejemplo, instancias EC2 y funciones Lambda) en diferentes regiones de AWS pueden comunicarse entre sí mediante direcciones IP privadas, sin usar una puerta de enlace, una conexión VPN o un dispositivo de red. El tráfico permanece en el espacio de dirección IP privada. Todo el tráfico entre regiones se cifra antes de salir de las instalaciones de AWS, sin un único punto de falla ni cuellos de botella de ancho de banda. El tráfico siempre permanece en la red troncal global de AWS y nunca pasa por la red pública de Internet, lo que reduce los vectores de amenazas, como las vulnerabilidades comunes y los ataques DDoS. El emparejamiento de VPC entre regiones

proporciona una forma sencilla y rentable de compartir recursos entre regiones o de replicar datos para obtener redundancia geográfica.

Precios de las interconexiones de VPC

No se aplica ningún cargo por crear un emparejamiento de VPC. Todas las transferencias de datos mediante una conexión de emparejamiento de VPC que permanezca dentro de una zona de disponibilidad son gratuitas, incluso si son entre cuentas distintas. Se aplican cargos por la transferencia de datos a través de conexiones de emparejamiento de VPC entre regiones y zonas de disponibilidad. Para obtener más información, consulte Precios de Amazon EC2.

Cómo funcionan las conexiones de emparejamiento de VPC

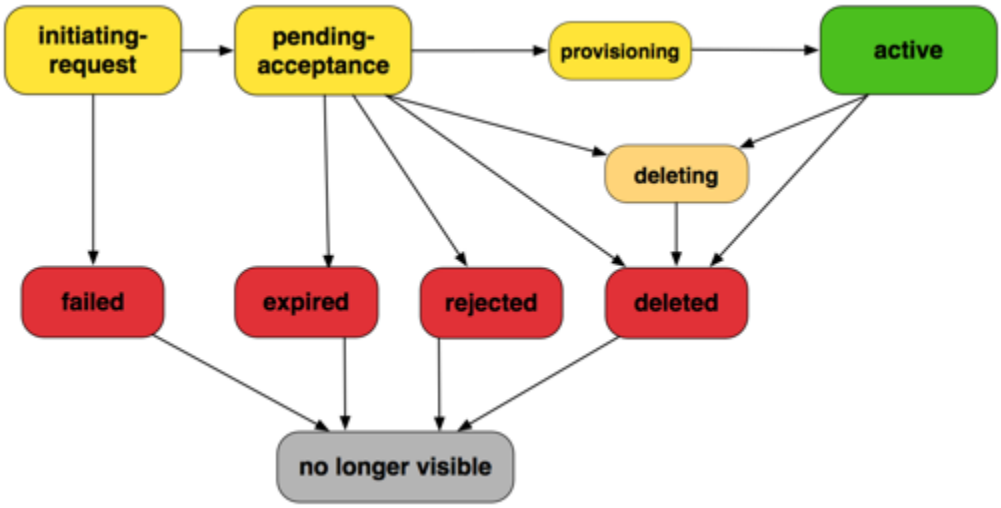
Los siguientes pasos describen el proceso de emparejamiento de VPC:

1. El propietario de la VPC solicitante envía una solicitud al propietario de la VPC que acepta la solicitud para crear la interconexión de VPC. La VPC del que acepta puede ser de su propiedad o de otra cuenta de AWS, y no puede tener un bloque de CIDR que se superponga con el bloque de CIDR de la VPC del solicitante.
2. El propietario de la VPC receptora debe aceptar la solicitud de conexión de emparejamiento de VPC para activar la conexión de emparejamiento de VPC.
3. Para permitir el flujo de tráfico entre VPC mediante direcciones IP privadas, los propietarios de las VPC de la interconexión deben añadir manualmente una ruta a una o varias de las tablas de ruteo de sus VPC que apunten al rango de direcciones IP de la otra VPC (VPC del mismo nivel).
4. Si es necesario, actualice las reglas del grupo de seguridad asociadas a su instancia EC2 para asegurarse de que el tráfico entrante y saliente de la VPC del mismo nivel no se vea afectado. Si ambas VPC se encuentran en la misma región, puede hacer referencia a un grupo de seguridad desde la VPC del mismo nivel como origen o destino de reglas de tráfico entrante o saliente del grupo de seguridad.
5. Con las opciones predeterminadas de conexión de emparejamiento de VPC, si las instancias EC2 de ambos extremos de una conexión de emparejamiento de VPC direccionan el tráfico entre sí utilizando un nombre de host DNS público, el nombre de host se resuelve en la dirección IP pública de la instancia. Para cambiar este comportamiento, habilite la resolución de nombres del host DNS para su conexión de VPC. Después de habilitar la resolución de nombres del host de DNS, si las instancias EC2 de ambos extremos de la conexión de emparejamiento de VPC se comunican entre sí utilizando un nombre de host DNS público, el nombre de host se resuelve en la dirección IP privada de la instancia EC2.

Para obtener más información, consulte Interconexiones de VPC.

Ciclo de vida de las interconexiones de VPC

Las interconexiones de VPC pasan por varias etapas desde que se inicia la solicitud. En cada una de estas fases, se encontrará con acciones que podrá realizar y al final del ciclo de vida, la interconexión de VPC permanecerá visible en la consola de Amazon VPC y en la API o los resultados de la línea de comandos durante un periodo de tiempo.



- Initiating-request: se ha iniciado una solicitud de interconexión de VPC. En esta fase, es posible que se produzca un error en la interconexión o puede ir a `pending-acceptance`.
- Failed: se ha producido un error en la solicitud de interconexión de VPC. Mientras esté en este estado, no se puede aceptar, rechazar o eliminar. La interconexión de VPC con error permanecerá visible al solicitante durante 2 horas.
- Pending-acceptance: la solicitud de interconexión de VPC está pendiente de la aceptación del propietario de la VPC responsable de aceptar la solicitud. Con este estado, el propietario de la VPC solicitante podrá eliminar la solicitud. Por su parte, el propietario de la otra VPC podrá aceptar o rechazar la solicitud. Si no se realiza ninguna acción, la solicitud caducará transcurridos 7 días.
- Expired: la solicitud de interconexión de VPC ha caducado. Con este estado, los propietarios de las VPC no podrán realizar ninguna acción. La interconexión de VPC caducada permanecerá visible para ambos propietarios de VPC durante 2 horas.
- Rejected: el propietario de la VPC responsable de aceptar la solicitud ha rechazado la solicitud de interconexión de VPC con el estado `pending-acceptance`. Mientras esté en este estado, no se puede aceptar la solicitud. La interconexión de VPC rechazada permanecerá visible para el propietario de la VPC solicitante durante 2 días y durante 2 horas para el propietario de la VPC responsable de aceptar la solicitud. Si la solicitud se creó desde la misma cuenta de AWS, la solicitud rechazada permanecerá visible durante 2 horas.
- Provisioning: la solicitud de interconexión de VPC se ha aceptado y pronto pasará al estado `active`.
- Active: la interconexión de VPC está activa y el tráfico puede fluir entre las VPC (siempre que los grupos de seguridad y las tablas de ruteo lo permitan). Mientras se encuentre en este estado,

cualquiera de los propietarios de la VPC puede eliminar la interconexión de VPC, pero no puede rechazarla.

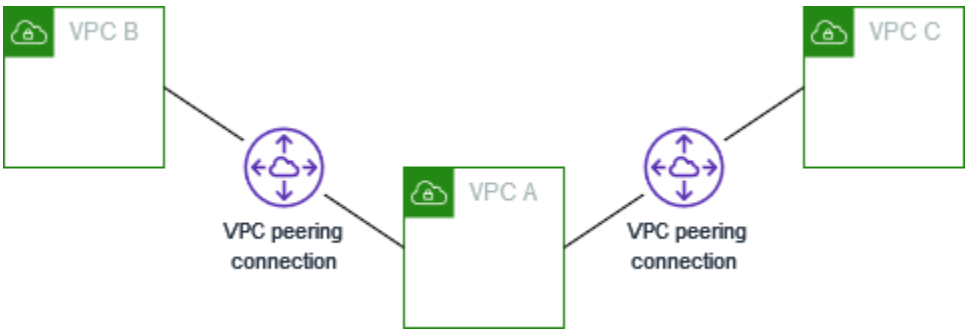
> **Note**
>
> Si ocurre un evento en una región en la que reside una VPC impide el flujo del tráfico, el estado de la conexión de emparejamiento de VPC continúa siendo `Active`.

- Deleting (Eliminar): aplica a una conexión de emparejamiento de VPC entre regiones en proceso de eliminación. El propietario de una de las VPC ha enviado una solicitud para eliminar una interconexión de VPC en estado `active`, o bien el propietario de la VPC solicitante ha enviado una petición para eliminar una solicitud de interconexión de VPC en estado `pending-acceptance`.
- Deleted: un propietario de una de las VPC ha eliminado una interconexión de VPC con el estado `active`, o bien el propietario de la VPC solicitante ha eliminado la solicitud de interconexión de VPC que tenía el estado `pending-acceptance`. Mientras se encuentre en este estado, no se puede aceptar ni rechazar la interconexión de VPC. La interconexión de VPC permanecerá visible para la parte que la eliminó durante 2 horas y durante 2 días para la otra parte. Si la interconexión de VPC se creó desde la misma cuenta de AWS, la solicitud eliminada permanecerá visible durante 2 horas.

Conexiones de emparejamiento de múltiples VPC

Una interconexión de VPC es una relación de uno a uno entre dos VPC. Puede crear conexiones de emparejamiento de múltiples VPC para cada VPC que posea, pero las relaciones de emparejamiento transitivo no están admitidas. No podrá crear relaciones de interconexión con VPC a las que su VPC no esté interconectada directamente.

El diagrama siguiente muestra un ejemplo de una VPC interconectada a varias VPC. Existen dos interconexiones de VPC: la VPC A está interconectada con la VPC B y la VPC C. La VPC B y la VPC C no están interconectadas, por lo que no puede utilizar la VPC A como punto de tránsito para interconectar la VPC B y la VPC C. Si desea habilitar el direccionamiento de tráfico entre la VPC B y la VPC C, debe crear una interconexión de VPC única entre estas VPC.



Limitaciones de interconexión de VPC

Tenga en cuenta las siguientes limitaciones para las conexiones de emparejamiento de VPC. En algunos casos puede usar una conexión de puerta de enlace de tránsito en lugar de una conexión de emparejamiento de VPC. Para obtener más información, consulte Ejemplos de escenarios de la puerta de enlace de tránsito en Puertas de enlace de tránsito de Amazon VPC.

Connections

- Hay una cuota establecida en el número de conexiones de emparejamiento de VPC activas y pendientes por cada VPC. Para obtener más información, consulte Cuotas.
- No puede tener más de una conexión de emparejamiento de VPC entre dos VPC a la vez.
- Las etiquetas que cree para la conexión de emparejamiento de VPC solo se aplicarán en la cuenta o región en las que las haya creado.
- No puede conectarse ni consultar el servidor DNS de Amazon en una VPC del mismo nivel.
- Si el bloque de CIDR de IPv4 de una VPC en una interconexión de VPC queda fuera de los rangos de direcciones IPv4 privadas especificado por RFC 1918, los nombres de host de DNS privada para dicha VPC no se pueden resolver en direcciones IP privadas. Para resolver los nombres de host de DNS privada a direcciones IP privadas, puede habilitar la compatibilidad de resolución DNS para la interconexión de VPC. Para obtener más información, consulte Habilite la resolución de DNS para la interconexión de VPC.
- Es posible habilitar la comunicación mediante IPv6 de los recursos de ambos extremos de una conexión de emparejamiento de VPC. Deberá asociar un bloque de CIDR IPv6 a cada VPC, habilitar la comunicación mediante IPv6 en las instancias de las VPC y direccionar el tráfico IPv6 con destino a la VPC del mismo nivel a la conexión de emparejamiento de VPC.
- No se admite el reenvío de rutas inversas unidifusión en interconexiones de VPC. Para obtener más información, consulte Enrutamiento del tráfico de respuesta.

Bloques de CIDR solapados

- No puede crear una interconexión de VPC entre VPC con los mismos bloques de CIDR IPv4 o IPv6 o con bloques solapados.
- Si tiene varios bloques de CIDR IPv4, no podrá crear una conexión de emparejamiento de VPC si se superpone cualquiera de los bloques de CIDR, incluso si tiene la intención de usar únicamente bloques de CIDR que no se superpongan o solo bloques de CIDR IPv6.

Interconexión transitiva

- La interconexión de VPC no admite relaciones de interconexión transitivas. Por ejemplo, si hay conexiones de emparejamiento de VPC entre la VPC A y la VPC B y entre la VPC A y la VPC C, no podrá direccionar el tráfico de la VPC B a la VPC C mediante la VPC A. Para direccionar el tráfico entre la VPC B y la VPC C, deberá crear una conexión de emparejamiento de VPC entre ambas. Para obtener más información, consulte Tres VPC interconectadas.

Enrutamiento de borde a borde mediante una gateway o una conexión privada

- Si la VPC A tiene una puerta de enlace de Internet, los recursos de la VPC B no pueden usar la puerta de enlace de Internet de la VPC A para acceder a Internet.
- Si la VPC A tiene un dispositivo NAT que proporciona acceso a Internet a las subredes de la VPC A, los recursos de la VPC B no podrán usar el dispositivo NAT en la VPC A para acceder a Internet.
- Si la VPC A tiene una conexión VPN a una red corporativa, los recursos de la VPC B no pueden usar la conexión VPN para comunicarse con la red corporativa.
- Si la VPC A tiene una conexión Direct Connect a una red corporativa, los recursos de la VPC B no pueden usar la conexión Direct Connect para comunicarse con la red corporativa.
- Si la VPC A tiene un punto de conexión de puerta de enlace que proporciona conectividad a Amazon S3 a subredes privadas en la VPC A, los recursos de la VPC B no pueden usar el punto de conexión de puerta de enlace para acceder a Amazon S3.

Conexiones de emparejamiento de VPC entre regiones

- En el caso de las tramas gigantes, la unidad de transmisión máxima (MTU) entre las conexiones de emparejamiento de VPC dentro de la misma región es de 9001 bytes. La MTU para las conexiones de emparejamiento de VPC entre regiones es de 8500 bytes. Para más información

sobre las tramas gigantes, consulte Tramas gigantes (MTU 9001) en la Guía del usuario de Amazon EC2.

- Debe habilitar la compatibilidad con la resolución de DNS para que la interconexión de VPC resuelva los nombres de host DNS privados de la VPC del mismo nivel en direcciones IP privadas, incluso si el CIDR IPv4 de la VPC está incluido en los intervalos de direcciones IPv4 privadas especificados por RFC 1918.

VPC y subredes compartidas

- Solo los propietarios de una VPC pueden trabajar con conexiones de intercambio de tráfico (describir, crear, aceptar, rechazar, modificar o eliminar). Los participantes no pueden trabajar con conexiones de intercambios de tráfico. Para obtener más información, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon VPC.

Interconexiones de VPC

El emparejamiento de VPC le permite conectar dos VPC en la misma región o en regiones de AWS diferentes. Esto permite que las instancias de una VPC se comuniquen con las instancias de la otra VPC como si todas formaran parte de la misma red.

El emparejamiento de VPC crea una ruta de red directa entre las dos VPC mediante direcciones IPv4 o IPv6 privadas. El tráfico enviado entre las VPC conectadas no viaja por Internet, una conexión VPN o una conexión de AWS Direct Connect. Esto hace que la interconexión de VPC sea una forma segura de compartir recursos, como bases de datos o servidores web, a través de los límites de la VPC.

Para establecer una conexión de emparejamiento de VPC, debe crear una solicitud de conexión de emparejamiento desde una VPC y que la acepte el propietario de la otra VPC. Una vez establecida la conexión, puede actualizar las tablas de enrutamiento para enrutar el tráfico entre las VPC. Esto permite que las instancias de una VPC accedan a los recursos de la otra VPC.

La interconexión de VPC es una herramienta importante para crear arquitecturas de múltiples VPC y compartir recursos más allá de los límites organizacionales en AWS. Proporciona una forma sencilla y de baja latencia de conectar las VPC sin la complejidad de configurar una VPN u otro servicio de red.

Use los siguientes procedimientos para crear y trabajar con conexiones de emparejamiento de VPC.

Tareas

- Creación de una interconexión de VPC
- Acepte o rechace una conexión de emparejamiento de VPC
- Actualice sus tablas de enrutamiento para interconexiones de VPC
- Actualizar grupos de seguridad para que hagan referencia a grupos de seguridad del mismo nivel
- Habilite la resolución de DNS para la interconexión de VPC
- Elimine la interconexión de VPC
- Solución de problemas de conexión de emparejamiento de VPC

Creación de una interconexión de VPC

Para crear una interconexión de VPC, primero debe crear una solicitud de emparejamiento con otra VPC. Para activar la solicitud, el propietario de la VPC debe aceptar la solicitud. Se admiten los siguientes tipos de conexiones de emparejamiento:

- Entre VPC en la misma cuenta y región
- Entre VPC en la misma cuenta y diferentes regiones
- Entre VPC en cuentas diferentes y en la misma región
- Entre VPC en cuentas y regiones diferentes

En el caso de una conexión de emparejamiento de VPC en regiones distintas, la solicitud debe provenir de la región de la VPC solicitante y aceptarse desde la región de la VPC receptora. Para obtener más información, consulte the section called “Aceptar o rechazar”.

Tareas

- Requisitos previos
- Creación de una conexión de emparejamiento mediante la consola
- Creación de una conexión de emparejamiento mediante la línea de comandos

Requisitos previos

- Revise las limitaciones para conexiones de emparejamiento de VPC.
- Asegúrese de que las VPC no tengan bloques de CIDR IPv4 que se solapen. En caso que se superpongan, el estado de la conexión de emparejamiento de VPC cambiará inmediatamente a `failed`. Esta limitación se aplica incluso cuando las VPC tengan bloques de CIDR IPv6.

Creación de una conexión de emparejamiento mediante la consola

Utilice el siguiente procedimiento para crear una conexión de emparejamiento de VPC.

Creación de una conexión de emparejamiento mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Peering Connections (Conexiones de emparejamiento).

3. Elija Create peering connection (Crear conexión de emparejamiento).
4. (Opcional) En Nombre, indique un nombre para la conexión de emparejamiento de VPC. De esta manera, se creará una etiqueta con una clave de Name y el valor que especifique.
5. En ID de VPC (solicitante), seleccione una VPC de la cuenta actual.
6. En Seleccionar otra VPC con la que realizar la conexión, haga lo siguiente:
   a. En Cuenta, para conectarse con una VPC de otra cuenta, elija Otra cuenta e ingrese el ID de la cuenta. De lo contrario, elija Mi cuenta.
   b. En Región, si desea establecer conexiones con una VPC de otra región, seleccione Otra región y elija la región. De lo contrario, elija Esta región.
   c. En ID de VPC (receptora), seleccione una VPC de la cuenta y la región especificadas.
7. (Opcional) Para agregar una etiqueta, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta.
8. Elija Create peering connection (Crear conexión de emparejamiento).
9. El propietario de la cuenta receptora deberá aceptar la solicitud de interconexión. Para obtener más información, consulte the section called “Aceptar o rechazar”.
10. Actualice las tablas de enrutamiento de ambas VPC para permitir la comunicación entre ellas. Para obtener más información, consulte the section called “Actualización de las tablas de ruteo”.

Creación de una conexión de emparejamiento mediante la línea de comandos

Puede crear una conexión de emparejamiento de VPC mediante los siguientes comandos:

- create-vpc-peering-connection (AWS CLI)
- New-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Acepte o rechace una conexión de emparejamiento de VPC

El propietario de la VPC que acepte la interconexión debe aceptar las interconexiones de VPC con el estado `pending-acceptance` para que puedan activarse. Para obtener más información sobre el estado de la conexión de emparejamiento `Deleted`, consulte Ciclo de vida de las interconexiones de VPC. No puede aceptar solicitudes de conexión de emparejamiento de VPC que haya enviado a otra

cuenta de AWS. Para crear una conexión de emparejamiento de VPC entre VPC de la misma cuenta de AWS, deberá crear y aceptar la solicitud usted mismo.

Puede rechazar cualquier solicitud de interconexión de VPC recibida con el estado `pending-acceptance`. Acepte solo conexiones de emparejamiento de VPC de Cuentas de AWS que conozca y que sean de confianza. Rechace las solicitudes no deseadas. Para obtener más información sobre el estado de la conexión de emparejamiento `Rejected`, consulte Ciclo de vida de las interconexiones de VPC.

> **Important**
>
> No acepte interconexiones de VPC de cuentas de AWS que no conozca. ya que los usuarios malintencionados pueden enviar solicitudes de interconexión de VPC para obtener acceso no autorizado a su VPC. Esto se denomina ataques de phishing de interconexión. De este modo, puede rechazar con seguridad las solicitudes de interconexión de VPC sin correr el riesgo de que el solicitante obtenga acceso a información acerca de su cuenta de AWS o su VPC. Para obtener más información, consulte Acepte o rechace una conexión de emparejamiento de VPC. También puede omitir estas solicitudes y dejar que caduquen. De manera predeterminada, las solicitudes a los 7 días.

Aceptación o rechazo de una solicitud de conexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el selector de regiones, seleccione la región de la VPC receptora.
3. En el panel de navegación, elija Peering Connections (Conexiones de emparejamiento).
4. Para aceptar o rechazar una conexión de emparejamiento, seleccione la conexión de emparejamiento de VPC y elija Acciones, Rechazar solicitud. Cuando se le pida confirmación, elija Rechazar solicitud.
5. Para aceptar o rechazar una conexión de emparejamiento, seleccione la conexión de emparejamiento de VPC pendiente (con el estado `pending-acceptance`) y elija Acciones, Aceptar solicitud. Para obtener más información acerca de los estados del ciclo de vida de una conexión de emparejamiento, consulte Ciclo de vida de las interconexiones de VPC.

   Si no hay ninguna conexión de emparejamiento de VPC pendiente, compruebe que ha seleccionado la región de la VPC receptora.
6. Cuando se le pida confirmación, elija Aceptar solicitud.

7. Elija Modificar mis tablas de enrutamiento ahora para agregar una ruta a la tabla de enrutamiento de la VPC y así, poder enviar y recibir tráfico a través de la conexión de emparejamiento. Para obtener más información, consulte Actualice sus tablas de enrutamiento para interconexiones de VPC.

Aceptación de una conexión de emparejamiento mediante la línea de comandos

- accept-vpc-peering-connection (AWS CLI)
- Approve-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Rechazo de una conexión de emparejamiento mediante la línea de comandos

- reject-vpc-peering-connection (AWS CLI)
- Deny-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Actualice sus tablas de enrutamiento para interconexiones de VPC

Para habilitar el tráfico IPv4 privado entre instancias en VPC interconectadas, debe agregar una ruta a las tablas de enrutamiento asociadas a las subredes de ambas instancias. El destino de la ruta es el bloque de CIDR (o parte del bloque de CIDR) de la VPC del mismo nivel y el objetivo es el ID de la conexión de emparejamiento de VPC. Para obtener más información, consulte Configurar tablas de enrutamiento en la Guía del usuario de Amazon VPC.

A continuación se muestra un ejemplo de las tablas de enrutamiento que permiten la comunicación entre instancias en dos VPC interconectadas, VPC A y VPC B. Cada tabla tiene una ruta local y una ruta que envía tráfico de la VPC del mismo nivel a la conexión de emparejamiento de VPC.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR de VPC A*	Local
	CIDR de VPC B	pcx-*11112222*
VPC B	*CIDR de VPC B*	Local
	CIDR de VPC A	pcx-*11112222*

Del mismo modo, si las VPC de la conexión de emparejamiento de VPC tienen asociados bloques de CIDR IPv6, podrá agregar rutas para permitir la comunicación con la VPC del mismo nivel a través de IPv6.

Para obtener más información acerca de las configuraciones de tabla de ruteo compatibles para las interconexiones de VPC, consulte Configuraciones comunes de conexión de emparejamiento de VPC.

Consideraciones

- Si tiene una VPC interconectada con varias VPC con bloques de CIDR IPv4 solapados o que coinciden, asegúrese de que las tablas de ruteo estén configuradas para evitar el envío de tráfico de respuesta desde la VPC a una VPC incorrecta. Actualmente AWS no admite el reenvío de rutas inversas unidifusión en interconexiones de VPC que comprueben la IP de origen de los paquetes y direccionará los paquetes de respuesta de vuelta al origen. Para obtener más información, consulte Enrutamiento del tráfico de respuesta.
- Su cuenta tiene una cuota en el número de entradas que puede agregar por cada tabla de enrutamiento. Si el número de interconexiones de VPC de su VPC supera la cuota de entrada de la tabla de ruteo para una única tabla de ruteo, considere la posibilidad de utilizar varias subredes asociadas a una tabla de ruteo personalizada.
- Puede añadir una ruta para una interconexión de VPC que tenga el estado `pending-acceptance`. Sin embargo, la ruta tendrá el estado de `blackhole` y no tendrá efecto alguno hasta que la conexión de emparejamiento de VPC tenga el estado `active`.

Para añadir una ruta IPv4 para una interconexión de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Tablas de enrutamiento.
3. Seleccione la casilla de verificación al lado de la tabla de enrutamiento asociada a la subred en la que reside su instancia.

   Si no asocia de manera explícita ninguna subred a una tabla de enrutamiento, la subred se asociará de manera implícita a una tabla de enrutamiento principal.
4. Elija Actions (Acciones), Edit routes (Editar rutas).
5. Seleccione Add route (Añadir ruta).
6. En Destination, escriba el rango de direcciones IPv4 al que debe dirigirse el tráfico de red de la interconexión de VPC. Puede especificar el bloque de CIDR IPv4 completo de la VPC del mismo

nivel, un rango específico o una dirección IPv4 individual como, por ejemplo, la dirección IP de la instancia con la que desea comunicarse. Por ejemplo, si el bloque de CIDR de la VPC del mismo nivel es `10.0.0.0/16`, puede especificar una porción `10.0.0.0/24` o una dirección IP específica `10.0.0.7/32`.

7. En Objetivo, seleccione la conexión de emparejamiento de VPC.
8. Seleccione Save changes (Guardar cambios).

El propietario de la VPC del mismo nivel también debe completar estos pasos para agregar una ruta para dirigir el tráfico de vuelta a la VPC a través de la conexión de pares de VPC.

Si tiene recursos en diferentes regiones de AWS en los que se utilizan direcciones IPv6, puede crear una interconexión entre regiones. Luego, puede agregar una ruta IPv6 para la comunicación entre los recursos.

Para añadir una ruta IPv6 para una interconexión de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Tablas de enrutamiento.
3. Seleccione la casilla de verificación al lado de la tabla de enrutamiento asociada a la subred en la que reside su instancia.

> **Note**
>
> Si no tiene ninguna tabla de ruteo asociada a dicha subred, seleccione la tabla de ruteo principal de la VPC, ya que la subred utilizará dicha tabla de ruteo de manera predeterminada.

4. Elija Actions (Acciones), Edit routes (Editar rutas).
5. Seleccione Add route (Añadir ruta).
6. En Destination, escriba el rango de direcciones IPv6 para la VPC del mismo nivel. Puede especificar el bloque de CIDR IPv6 completo de la VPC del mismo nivel, un rango específico o una dirección IPv6 individual. Por ejemplo, si el bloque de CIDR de la VPC del mismo nivel es `2001:db8:1234:1a00::/56`, puede especificar una porción `2001:db8:1234:1a00::/64` o una dirección IP específica `2001:db8:1234:1a00::123/128`.
7. En Objetivo, seleccione la conexión de emparejamiento de VPC.
8. Seleccione Save changes (Guardar cambios).

Para obtener más información, consulte Tablas de ruteo en la Guía del usuario de Amazon VPC.

Agregado o sustitución de una ruta mediante la línea de comandos

- create-route y replace-route(AWS CLI)
- New-EC2Route y Set-EC2Route(AWS Tools for Windows PowerShell)

Actualizar grupos de seguridad para que hagan referencia a grupos de seguridad del mismo nivel

Puede actualizar las reglas entrantes o salientes de los grupos de seguridad de su VPC para que hagan referencia a los grupos de seguridad de las VPC del mismo nivel. De este modo, garantizará el tráfico entrante y saliente de las instancias asociadas al grupo de seguridad al que se hace referencia en la VPC del mismo nivel.

> **Note**
>
> Los grupos de seguridad de una VPC del mismo nivel no se muestran en la consola para que los seleccione.

Requisitos

- Para hacer referencia a un grupo de seguridad de una VPC del mismo nivel, la interconexión de VPC debe tener el estado `active`.
- La VPC del mismo nivel puede ser una VPC de su cuenta o una VPC de otra cuenta de AWS. Para hacer referencia a un grupo de seguridad que se encuentra en otra cuenta de AWS pero en la misma región, incluya el número de cuenta con el ID del grupo de seguridad. Por ejemplo, `123456789012/sg-1a2b3c4d`.
- No es posible hacer referencia al grupo de seguridad de una VPC del mismo nivel que se encuentra en una región distinta. En lugar de ello, utilice el bloque de CIDR de la VPC del mismo nivel.
- Si configura rutas para reenviar el tráfico entre dos instancias en subredes diferentes a través de un dispositivo de middlebox, debe asegurarse de que los grupos de seguridad de ambas instancias permiten que el tráfico fluya entre las instancias. El grupo de seguridad de cada instancia debe hacer referencia a la dirección IP privada de la otra instancia, o al rango CIDR de la

subred que contiene la otra instancia, como fuente. Si hace referencia al grupo de seguridad de la otra instancia como fuente, esto no permite que el tráfico fluya entre las instancias.

Para actualizar las reglas del grupo de seguridad desde la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Grupos de seguridad.
3. Seleccione el grupo de seguridad y haga una de las operaciones siguientes:
   - Para modificar las reglas de entrada, seleccione Acciones, Editar reglas de entrada.
   - Para modificar las reglas de salida, seleccione Acciones, Editar reglas de salida.
4. Para agregar una regla, elija Agregar regla y especifique el tipo, el protocolo y el rango de puertos. En Origen (regla de entrada) o Destino (regla de salida), haga alguna de las siguientes acciones:
   - Para una VPC del mismo nivel en la misma cuenta y región, ingrese el ID del grupo de seguridad.
   - Para una VPC del mismo nivel en una cuenta diferente pero de la misma región, ingrese el ID de la cuenta y el ID del grupo de seguridad, separados por una barra diagonal (por ejemplo, `123456789012/sg-1a2b3c4d`).
   - Para una VPC del mismo nivel en una región diferente, ingrese el bloque de CIDR de la VPC del mismo nivel.
5. Para editar una regla existente, cambie los valores (por ejemplo, el origen o la descripción).
6. Para eliminar una regla, elija la opción Eliminar situada junto a la regla.
7. Seleccione Guardar reglas.

Para actualizar las reglas de entrada mediante la línea de comandos

- authorize-security-group-ingress y revoke-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress y Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

Por ejemplo, para actualizar el grupo de seguridad `sg-aaaa1111` para permitir el acceso entrante a través de HTTP desde `sg-bbbb2222` en una VPC del mismo nivel, utilice el siguiente comando. Si la VPC del mismo nivel está en la misma región pero en otra cuenta, agregue `--group-owner` *`aws-account-id`*.

```
aws ec2 authorize-security-group-ingress --group-id sg-aaaa1111 --protocol tcp --
port 80 --source-group sg-bbbb2222
```

Para actualizar las reglas de salida mediante la línea de comandos

- authorize-security-group-egress y revoke-security-group-egress (AWS CLI)
- Grant-EC2SecurityGroupEgress y Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Una vez actualizadas las reglas del grupo de seguridad, utilice el comando describe-security-groups para consultar el grupo de seguridad al que se hace referencia en las reglas del grupo de seguridad.

Identifique los grupos de seguridad a los que se hace referencia

Para determinar si se hace referencia a su grupo de seguridad en las reglas de un grupo de seguridad de una VPC del mismo nivel, utilice uno de los comandos siguientes para uno o varios grupos de seguridad de su cuenta.

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

En el siguiente ejemplo, la respuesta indica que un grupo de seguridad de la VPC `sg-bbbb2222` hace referencia al grupo de seguridad `vpc-aaaaaaaa`:

```
aws ec2 describe-security-group-references --group-id sg-bbbb2222
```

```
{
  "SecurityGroupsReferenceSet": [
    {
      "ReferencingVpcId": "vpc-aaaaaaaa",
      "GroupId": "sg-bbbb2222",
      "VpcPeeringConnectionId": "pcx-b04deed9"
    }
  ]
}
```

Si se elimina la interconexión de VPC o si el propietario de la VPC del mismo nivel elimina el grupo de seguridad al que se hace referencia, la regla del grupo de seguridad quedará obsoleta.

Ver y eliminar reglas de grupo de seguridad obsoletas

Las reglas de grupos de seguridad obsoletas son aquellas que hacen referencia a un grupo de seguridad eliminado en la misma VPC o en una VPC del mismo nivel, o que hace referencia a un grupo de seguridad en una VPC del mismo nivel para la que se ha eliminado la conexión de emparejamiento de VPC. Cuando una regla de grupo de seguridad queda obsoleta, esta no se quita automáticamente del grupo de seguridad, sino que debe quitarla manualmente. Si una regla de grupo de seguridad queda obsoleta porque se ha eliminado la interconexión de VPC, esta dejará de marcarse como obsoleto si crea una nueva interconexión de VPC con las mismas VPC.

Puede consultar y eliminar las reglas de grupo de seguridad obsoletas de una VPC mediante la consola de Amazon VPC.

Para ver y eliminar reglas de grupo de seguridad obsoletas

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Security groups (Grupos de seguridad).
3. Elija Actions (Acciones), Manage stale rules (Administrar reglas obsoletas).
4. En VPC, elija la VPC con las reglas obsoletas.
5. Elija Edit.
6. Presione el botón Delete (Eliminar), que se encuentra junto a la regla que desea eliminar. Elija Vista previa de cambios, Guardar reglas.

Descripción de las reglas de grupo de seguridad obsoletas mediante la línea de comandos

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

En el ejemplo siguiente, se creó una interconexión entre la VPC A (`vpc-aaaaaaaa`) y la VPC B y se eliminó la interconexión de VPC. El grupo de seguridad `sg-aaaa1111` de la VPC A hace referencia al grupo `sg-bbbb2222` de la VPC B. Al ejecutar el comando `describe-stale-security-groups` para su VPC, la respuesta indica que el grupo de seguridad `sg-aaaa1111` tiene una regla SSH obsoleta que hace referencia al grupo `sg-bbbb2222`.

```
aws ec2 describe-stale-security-groups --vpc-id vpc-aaaaaaaa
```

```
{
    "StaleSecurityGroupSet": [
        {
            "VpcId": "vpc-aaaaaaaa",
            "StaleIpPermissionsEgress": [],
            "GroupName": "Access1",
            "StaleIpPermissions": [
                {
                    "ToPort": 22,
                    "FromPort": 22,
                    "UserIdGroupPairs": [
                        {
                            "VpcId": "vpc-bbbbbbbb",
                            "PeeringStatus": "deleted",
                            "UserId": "123456789101",
                            "GroupName": "Prod1",
                            "VpcPeeringConnectionId": "pcx-b04deed9",
                            "GroupId": "sg-bbbb2222"
                        }
                    ],
                    "IpProtocol": "tcp"
                }
            ],
            "GroupId": "sg-aaaa1111",
            "Description": "Reference remote SG"
        }
    ]
}
```

Una vez identificadas las reglas de grupo de seguridad obsoletas, puede eliminarlas utilizando los comandos revoke-security-group-ingress o revoke-security-group-egress.

Habilite la resolución de DNS para la interconexión de VPC

La configuración de DNS de una conexión de emparejamiento de VPC determina cómo se resuelven los nombres de host de DNS públicos para las solicitudes que utilizan la conexión de emparejamiento de VPC. Si una instancia de EC2 de un lado de una conexión de emparejamiento de VPC envía una solicitud a una instancia de EC2 del otro lado con el nombre de host de DNS de IPv4 público de la instancia, el nombre de host de DNS se resuelve de la siguiente manera.

Resolución de DNS desactivada (por defecto)

El nombre de host de DNS de IPv4 público basado en IPBN se resuelve en la dirección IPv4 pública de la instancia.

Resolución de DNS activada

El nombre de host de DNS de IPv4 público basado en IPBN se resuelve en la dirección IPv4 privada de la instancia.

Requisitos

- Ambas VPC deben tener habilitados los nombres de host DNS y la resolución de DNS. Para obtener más información, consulte Atributos de DNS para su VPC en la Guía del usuario de Amazon VPC.
- La conexión de emparejamiento de estar en el estado `active`. No se puede activar la compatibilidad con la resolución DNS cuando se crea una conexión de emparejamiento.
- El propietario de la VPC solicitante debe modificar las opciones de conexión de emparejamiento de la VPC solicitante; el propietario de la VPC receptora debe modificar las opciones de emparejamiento de la VPC receptora. Si las VPC se encuentran en la misma cuenta, puede activar la resolución de DNS para la VPC solicitante y la receptora al mismo tiempo. Esto funciona tanto para las conexiones de emparejamiento de VPC de la misma región como entre regiones.

Activación de la resolución de DNS para la conexión de emparejamiento mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Peering Connections (Conexiones de emparejamiento).
3. Seleccione la conexión de emparejamiento de VPC.
4. Elija Acciones, Editar configuración de DNS.
5. Si desea activar la resolución de DNS para las solicitudes de la VPC solicitante, seleccione Resolución de DNS del solicitante y Permitir que la VPC receptora resuelva el DNS de la VPC solicitante.
6. Para garantizar la resolución de DNS para las solicitudes de la VPC receptora, seleccione Resolución de DNS de la receptora y Permitir que la VPC solicitante resuelva el DNS de la VPC receptora.
7. Seleccione Save changes (Guardar cambios).

Habilitación de la resolución de DNS mediante la línea de comandos

- modify-vpc-peering-connection-options (AWS CLI)
- Edit-EC2VpcPeeringConnectionOption (AWS Tools for Windows PowerShell)

Descripción de opciones de conexión de emparejamiento de VPC mediante la línea de comandos

- describe-vpc-peering-connections (AWS CLI)
- Get-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Elimine la interconexión de VPC

Los propietarios de VPC que intervienen en las interconexiones pueden eliminar la interconexión de VPC en cualquier momento. También puede eliminar interconexiones de VPC que haya solicitado y que sigan con el estado `pending-acceptance`.

No se puede eliminar la interconexión de la VPC cuando la interconexión de la VPC está en el estado `rejected`. Se elimina automáticamente la conexión.

Al eliminar una VPC en la consola de Amazon VPC que forme parte de una interconexión de VPC activa también elimina la interconexión de VPC. Si ha solicitado una interconexión de VPC con una VPC de otra cuenta y elimina su VPC antes de que la otra parte haya aceptado la solicitud, la interconexión de VPC también se eliminará. No podrá eliminar las VPC de las cuales tenga una solicitud `pending-acceptance` de una VPC de otra cuenta. Primero debe rechazar la solicitud de interconexión de VPC.

Cuando se elimina una conexión de emparejamiento, el estado se establece en `Deleting` y luego, en `Deleted`. Una vez que se elimina una conexión, no se puede aceptar, rechazar o editar. Para obtener más información sobre cuánto tiempo permanece visible la conexión de emparejamiento, consulte Ciclo de vida de las interconexiones de VPC.

Para eliminar una interconexión de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Peering Connections (Conexiones de emparejamiento).
3. Seleccione la conexión de emparejamiento de VPC.
4. Elija Actions (Acciones), Delete peering connection (Eliminar la interconexión).

5. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Eliminación de una conexión de emparejamiento de VPC mediante la línea de comandos

- delete-vpc-peering-connection (AWS CLI)
- Remove-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

Solución de problemas de conexión de emparejamiento de VPC

Si tiene problemas para conectarse a un recurso de una VPC desde un recurso de una VPC del mismo nivel, haga lo siguiente:

- Para cada recurso de cada VPC, compruebe que la tabla de enrutamiento de su subred contiene una ruta que envía el tráfico destinado a la VPC del mismo nivel a la conexión de emparejamiento de VPC. Esto garantiza que el tráfico de red pueda fluir correctamente entre las dos VPC. Para obtener más información, consulte Actualización de las tablas de ruteo.
- Para cualquier instancia EC2 involucrada, verifique que los grupos de seguridad de esas instancias permiten el tráfico entrante y saliente de la VPC emparejada. Las reglas de los grupos de seguridad controlan qué tráfico puede acceder a las instancias de EC2. Para obtener más información, consulte Referencia a grupos de seguridad del mismo nivel.
- Compruebe que las ACL de red de las subredes que contienen sus recursos permiten el tráfico necesario desde la VPC homóloga. Las ACL de red son una capa de seguridad adicional que filtra el tráfico en el nivel de subred.

Si el problema persiste, puede utilizar el Analizador de accesibilidad. El Analizador de accesibilidad puede ayudar a identificar el componente específico, ya sea una tabla de enrutamiento, un grupo de seguridad o una ACL de red, que causa el problema de conectividad entre las dos VPC. Para obtener más información, consulte la Guía del Analizador de accesibilidad.

Verificar minuciosamente las configuraciones de red de la VPC es fundamental para solucionar cualquier problema de conexión de emparejamiento de VPC que pueda surgir.

Configuraciones comunes de conexión de emparejamiento de VPC

En esta sección se describen dos tipos comunes de configuraciones de emparejamiento de VPC que puede implementar:

- Emparejamientos de VPC con enrutamiento a una VPC completa: en esta configuración, se crea un enrutamiento en cada tabla de enrutamiento de VPC que envía todo el tráfico destinado a la VPC del mismo nivel a la conexión de emparejamiento de VPC. Esto permite que cualquier recurso de una VPC se comunique con cualquier recurso de la VPC homóloga, lo que simplifica la gestión. Sin embargo, también significa que todo el tráfico entre las VPC fluirá a través de la conexión entre pares, lo que podría convertirse en un cuello de botella si el volumen de tráfico es elevado.
- Configuraciones de emparejamiento de VPC con enrutamientos específicos: también puede crear enrutamientos más granulares en la tabla de enrutamiento de cada VPC que solo envíen tráfico a subredes o recursos específicos de la VPC homóloga. Esto le permite limitar el tráfico que fluye a través de la conexión de emparejamiento solo a lo necesario, lo que puede ser más eficiente. Sin embargo, también requiere más mantenimiento, ya que tendrá que actualizar las tablas de enrutamiento cada vez que agregue nuevos recursos en la VPC homóloga que necesiten comunicarse.

El mejor enfoque depende de factores como el tamaño y la complejidad de la arquitectura de la VPC, el volumen de tráfico esperado entre las VPC y las necesidades organizativas en torno a la seguridad y el acceso a los recursos. Muchas empresas utilizan un enfoque híbrido, con enrutamientos amplios para los patrones de tráfico comunes y específicos para los casos de uso más sensibles o con un uso intensivo del ancho de banda.

Configuraciones

- Configuraciones de emparejamiento de VPC con rutas a una VPC completa
- Configuraciones de emparejamiento de VPC con rutas específicas

Configuraciones de emparejamiento de VPC con rutas a una VPC completa

Puede configurar interconexiones con VPC para que sus tablas de ruteo tengan acceso al bloque de CIDR completo de la VPC del mismo nivel. Para obtener más información acerca de escenarios en los que puede necesitar una configuración de interconexión de VPC específica, consulte Escenarios de conexión de emparejamiento de VPC en la red. Para obtener más información acerca de la creación y el uso de interconexiones de VPC; consulte Interconexiones de VPC.

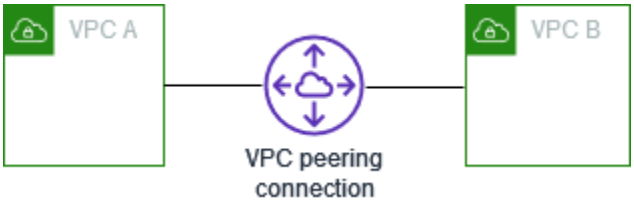
Para obtener más información acerca de la actualización de las tablas de ruteo, consulte Actualice sus tablas de enrutamiento para interconexiones de VPC.

Configuraciones

- Utilización de dos VPC interconectadas
- Una VPC interconectada a dos VPC
- Tres VPC interconectadas
- Varias VPC interconectadas

Utilización de dos VPC interconectadas

En esta configuración, hay una conexión de emparejamiento entre la VPC A y la VPC B (`pcx-11112222`). Las VPC se encuentran en la misma Cuenta de AWS y sus bloques de CIDR no se superponen.



Puede usar este tipo de configuración cuando tiene dos VPC que requieren acceso a sus recursos entre sí. Por ejemplo, puede configurar la VPC A para los registros de contabilidad y la VPC B para los registros financieros. Cada una de las VPC debe poder acceder a todos los recursos de la otra VPC sin restricciones.

CIRD de VPC única

Actualice la tabla de enrutamiento de cada VPC con una ruta que envía el tráfico del bloque de CIDR de la VPC del mismo nivel a la conexión de emparejamiento de VPC.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR de VPC A*	Local
	CIDR de VPC B	pcx-11112222
VPC B	*CIDR de VPC B*	Local
	CIDR de VPC A	pcx-11112222

CIDR de varias VPC IPv4

Si la VPC A y la VPC B tienen varios bloques de CIDR IPv4 asociados, puede actualizar la tabla de enrutamiento de cada VPC con rutas para algunos o todos los bloques de CIDR IPv4 de la VPC del mismo nivel.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR 1 de VPC A*	Local
	CIDR 2 de VPC A	Local
	CIDR 1 de VPC B	pcx-11112222
	CIDR 2 de VPC B	pcx-11112222
VPC B	*CIDR 1 de VPC B*	Local
	CIDR 2 de VPC B	Local
	CIDR 1 de VPC A	pcx-11112222
	CIDR 2 de VPC A	pcx-11112222

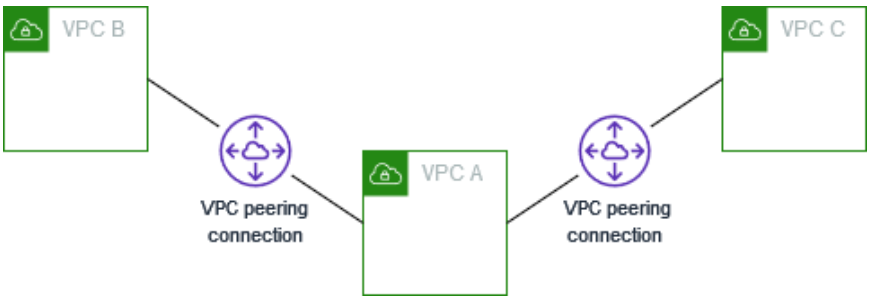
CIDR de VPC IPv4 e IPv6

Si la VPC A y la VPC B tienen bloques de CIDR IPv6 asociados, puede actualizar la tabla de enrutamiento de cada VPC con rutas para los bloques de CIDR IPv4 e IPv6 de la VPC del mismo nivel.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR IPv4 de VPC A*	Local
	CIDR IPv6 de VPC A	Local
	CIDR IPv4 de VPC B	pcx-11112222
	CIDR IPv6 de VPC B	pcx-11112222
VPC B	*CIDR IPv4 de VPC B*	Local
	CIDR IPv6 de VPC B	Local
	CIDR IPv4 de VPC A	pcx-11112222
	CIDR IPv6 de VPC A	pcx-11112222

Una VPC interconectada a dos VPC

En esta configuración, hay una VPC central (VPC A), una conexión de emparejamiento entre la VPC A y la VPC B (`pcx-12121212`) y una conexión de emparejamiento entre la VPC A y la VPC C (`pcx-23232323`). Las tres VPC se encuentran en la misma Cuenta de AWS y sus bloques de CIDR no se superponen.



La VPC B y la VPC C no pueden enviarse tráfico entre sí de forma directa a través de una VPC A, ya que el emparejamiento de VPC no admite las relaciones de emparejamiento transitivas. Puede crear una conexión de emparejamiento de VPC entre la VPC B y la VPC C, tal como se muestra en Tres

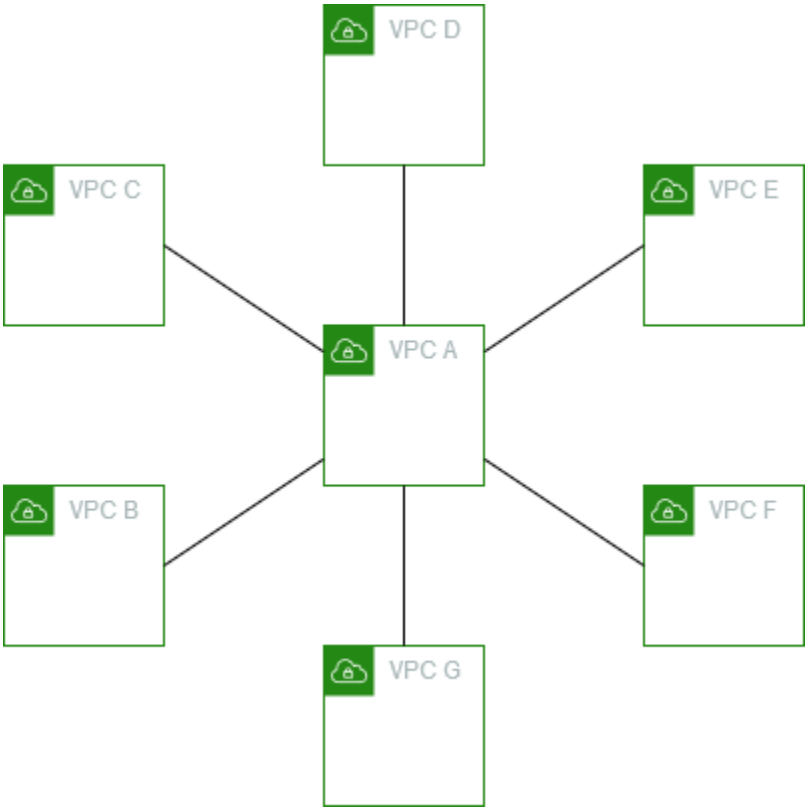
VPC interconectadas. Para obtener más información acerca de los escenarios de interconexión no compatibles, consulte the section called “Limitaciones de interconexión de VPC”.

Puede usar esta configuración cuando tiene recursos en una VPC central, como un repositorio de servicios, al que otras VPC necesitan acceder. Las otras VPC no necesitan tener acceso a los recursos de cada una; solo necesitan tener acceso a los recursos de la VPC central.

Actualice la tabla de enrutamiento para cada VPC de la siguiente manera para implementar esta configuración mediante un bloque de CIDR por VPC.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR de VPC A*	Local
	CIDR de VPC B	pcx-12121212
	CIDR de VPC C	pcx-23232323
VPC B	*CIDR de VPC B*	Local
	CIDR de VPC A	pcx-12121212
VPC C	*CIDR de VPC C*	Local
	CIDR de VPC A	pcx-23232323

Puede extender esta configuración a VPC adicionales. Por ejemplo, la VPC A está emparejada con la VPC B a través de la VPC G mediante CIDR IPv4 e IPv6, pero las demás VPC no están emparejadas entre sí. En este diagrama, las líneas representan las conexiones de emparejamiento de VPC.



Actualice la tabla de enrutamiento de la siguiente manera.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR IPv4 de VPC A*	Local
	CIDR IPv6 de VPC A	Local
	CIDR IPv4 de VPC B	pcx-aaaabbbb
	CIDR IPv6 de VPC B	pcx-aaaabbbb
	CIDR IPv4 de VPC C	pcx-aaaacccc
	CIDR IPv6 de VPC C	pcx-aaaacccc
	CIDR IPv4 de VPC D	pcx-aaaadddd
	CIDR IPv6 de VPC D	pcx-aaaadddd
	CIDR IPv4 de VPC E	pcx-aaaaeeee

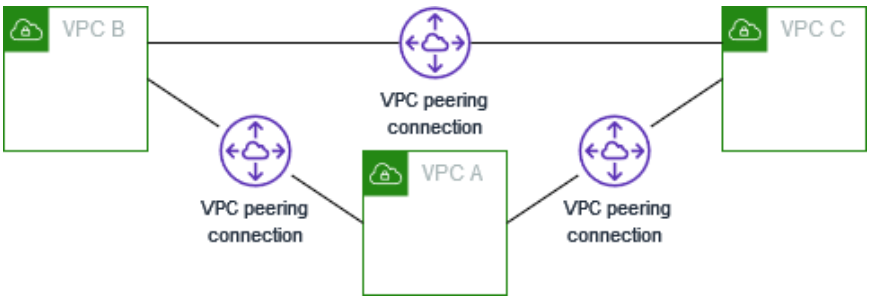
Tabla de enrutamiento	Destino	Objetivo
	CIDR IPv6 de VPC E	pcx-aaaaeeee
	CIDR IPv4 de VPC F	pcx-aaaaffff
	CIDR IPv6 de VPC F	pcx-aaaaffff
	CIDR IPv4 de VPC G	pcx-aaaagggg
	CIDR IPv6 de VPC G	pcx-aaaagggg
VPC B	*CIDR IPv4 de VPC B*	Local
	CIDR IPv6 de VPC B	Local
	CIDR IPv4 de VPC A	pcx-aaaabbbb
	CIDR IPv6 de VPC A	pcx-aaaabbbb
VPC C	*CIDR IPv4 de VPC C*	Local
	CIDR IPv6 de VPC C	Local
	CIDR IPv4 de VPC A	pcx-aaaacccc
	CIDR IPv6 de VPC A	pcx-aaaacccc
VPC D	*CIDR IPv4 de VPC D*	Local
	CIDR IPv6 de VPC D	Local
	CIDR IPv4 de VPC A	pcx-aaaadddd
	CIDR IPv6 de VPC A	pcx-aaaadddd
VPC E	*CIDR IPv4 de VPC E*	Local
	CIDR IPv6 de VPC E	Local
	CIDR IPv4 de VPC A	pcx-aaaaeeee

Tabla de enrutamiento	Destino	Objetivo
	CIDR IPv6 de VPC A	pcx-aaaaeeee
VPC F	*CIDR IPv4 de VPC F*	Local
	CIDR IPv6 de VPC F	Local
	CIDR IPv4 de VPC A	pcx-aaaaffff
	CIDR IPv6 de VPC A	pcx-aaaaffff
VPC G	*CIDR IPv4 de VPC G*	Local
	CIDR IPv6 de VPC G	Local
	CIDR IPv4 de VPC A	pcx-aaaagggg
	CIDR IPv6 de VPC A	pcx-aaaagggg

Tres VPC interconectadas

En esta configuración, hay tres VPC en la misma Cuenta de AWS con bloques de CIDR que no se superponen. Las VPC están emparejadas en una malla completa de la siguiente manera:

- La VPC A está interconectada a la VPC B a través de la interconexión de VPC `pcx-aaaabbbb`
- La VPC A está interconectada a la VPC C a través de la interconexión de VPC `pcx-aaaacccc`
- La VPC B está interconectada a la VPC C a través de la interconexión de VPC `pcx-bbbbcccc`



Puede usar esta configuración cuando tiene VPC que deben compartir recursos entre sí sin restricción. Por ejemplo, como un sistema de intercambio de archivos.

Actualice la tabla de enrutamiento de cada VPC de la siguiente manera para implementar esta configuración.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR de VPC A*	Local
	CIDR de VPC B	pcx-aaaabbbb
	CIDR de VPC C	pcx-aaaacccc
VPC B	*CIDR de VPC B*	Local
	CIDR de VPC A	pcx-aaaabbbb
	CIDR de VPC C	pcx-bbbbcccc
VPC C	*CIDR de VPC C*	Local
	CIDR de VPC A	pcx-aaaacccc
	CIDR de VPC B	pcx-bbbbcccc

Si la VPC A y la VPC B tienen bloques de CIDR IPv4 e IPv6, pero la VPC C no tiene un bloque de CIDR IPv6, actualice las tablas de enrutamiento de la siguiente manera. Los recursos en la VPC A y la VPC B pueden comunicarse mediante IPv6 a través de la conexión de emparejamiento de VPC. Sin embargo, la VPC C no puede comunicarse mediante IPv6 ni con la VPC A ni con la VPC B.

Tablas de enrutamiento	Destino	Objetivo
VPC A	*CIDR IPv4 de VPC A*	Local
	CIDR IPv6 de VPC A	Local
	CIDR IPv4 de VPC B	pcx-aaaabbbb
	CIDR IPv6 de VPC B	pcx-aaaabbbb
	CIDR IPv4 de VPC C	pcx-aaaacccc

Tablas de enrutamiento	Destino	Objetivo
VPC B	*CIDR IPv4 de VPC B*	Local
	CIDR IPv6 de VPC B	Local
	CIDR IPv4 de VPC A	pcx-aaaabbbb
	CIDR IPv6 de VPC A	pcx-aaaabbbb
	CIDR IPv4 de VPC C	pcx-bbbbcccc
VPC C	*CIDR IPv4 de VPC C*	Local
	CIDR IPv4 de VPC A	pcx-aaaacccc
	CIDR IPv4 de VPC B	pcx-bbbbcccc

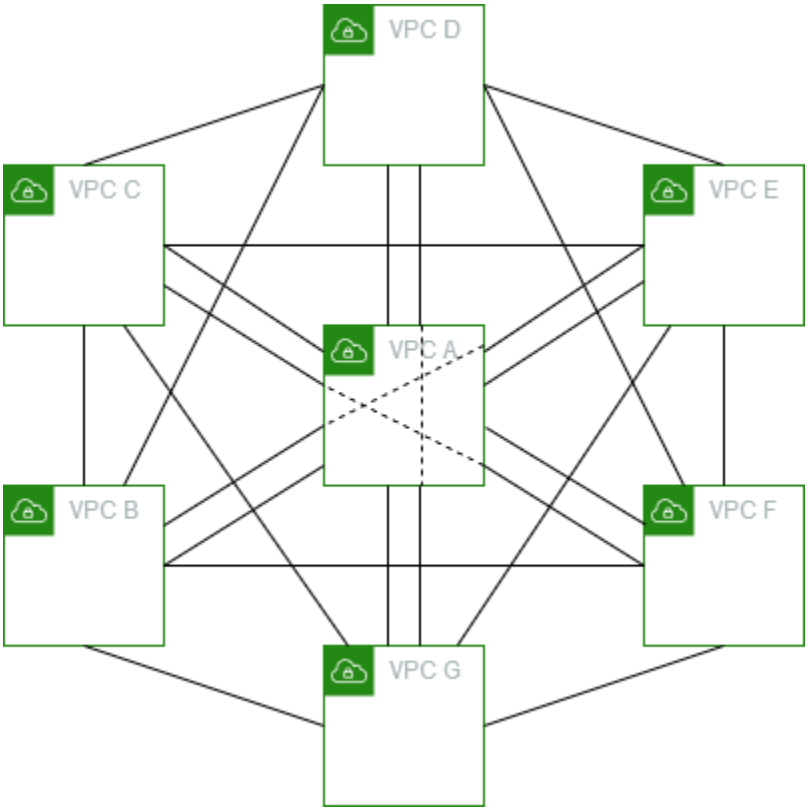
Varias VPC interconectadas

En esta configuración, hay siete VPC emparejadas en una configuración de malla completa. Las VPC se encuentran en la misma Cuenta de AWS y sus bloques de CIDR no se superponen.

VPC	VPC	Interconexión de VPC
A	B	pcx-aaaabbbb
A	C	pcx-aaaacccc
A	D	pcx-aaaadddd
A	E	pcx-aaaaeeee
A	F	pcx-aaaaffff
A	G	pcx-aaaagggg
B	C	pcx-bbbbcccc
B	D	pcx-bbbbdddd

VPC	VPC	Interconexión de VPC
B	E	pcx-bbbbeeee
B	F	pcx-bbbbffff
B	G	pcx-bbbbgggg
C	D	pcx-ccccdddd
C	E	pcx-cccceeee
C	F	pcx-ccccffff
C	G	pcx-ccccgggg
D	E	pcx-ddddeeee
D	F	pcx-ddddffff
D	G	pcx-ddddgggg
E	F	pcx-eeeeffff
E	G	pcx-eeeegggg
F	G	pcx-ffffgggg

Puede utilizar esta configuración cuando tiene varias VPC que necesitan acceder a los recursos de las demás sin restricción. Por ejemplo, como una red de intercambio de archivos. En este diagrama, las líneas representan las conexiones de emparejamiento de VPC.



Actualice la tabla de enrutamiento de cada VPC de la siguiente manera para implementar esta configuración.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR de VPC A*	Local
	CIDR de VPC B	pcx-aaaabbbb
	CIDR de VPC C	pcx-aaaacccc
	CIDR de VPC D	pcx-aaaadddd
	CIDR de VPC E	pcx-aaaaeeee
	CIDR de VPC F	pcx-aaaaffff
	CIDR de VPC G	pcx-aaaagggg
VPC B	*CIDR de VPC B*	Local

Tabla de enrutamiento	Destino	Objetivo
	CIDR de VPC A	pcx-aaaabbbb
	CIDR de VPC C	pcx-bbbbcccc
	CIDR de VPC D	pcx-bbbbdddd
	CIDR de VPC E	pcx-bbbbeeee
	CIDR de VPC F	pcx-bbbbffff
	CIDR de VPC G	pcx-bbbbgggg
VPC C	*CIDR de VPC C*	Local
	CIDR de VPC A	pcx-aaaacccc
	CIDR de VPC B	pcx-bbbbcccc
	CIDR de VPC D	pcx-ccccdddd
	CIDR de VPC E	pcx-ccceeeee
	CIDR de VPC F	pcx-ccccffff
	CIDR de VPC G	pcx-ccccgggg
VPC D	*CIDR de VPC D*	Local
	CIDR de VPC A	pcx-aaaadddd
	CIDR de VPC B	pcx-bbbbdddd
	CIDR de VPC C	pcx-ccccdddd
	CIDR de VPC E	pcx-ddddeeee
	CIDR de VPC F	pcx-ddddffff
	CIDR de VPC G	pcx-ddddgggg

Tabla de enrutamiento	Destino	Objetivo
VPC E	*CIDR de VPC E*	Local
	CIDR de VPC A	pcx-aaaaeeee
	CIDR de VPC B	pcx-bbbbeeee
	CIDR de VPC C	pcx-cccceeee
	CIDR de VPC D	pcx-ddddeeee
	CIDR de VPC F	pcx-eeeeffff
	CIDR de VPC G	pcx-eeeegggg
VPC F	*CIDR de VPC F*	Local
	CIDR de VPC A	pcx-aaaaffff
	CIDR de VPC B	pcx-bbbbffff
	CIDR de VPC C	pcx-ccccffff
	CIDR de VPC D	pcx-ddddffff
	CIDR de VPC E	pcx-eeeeffff
	CIDR de VPC G	pcx-ffffgggg
VPC G	*CIDR de VPC G*	Local
	CIDR de VPC A	pcx-aaaagggg
	CIDR de VPC B	pcx-bbbbgggg
	CIDR de VPC C	pcx-ccccgggg
	CIDR de VPC D	pcx-ddddgggg
	CIDR de VPC E	pcx-eeeegggg

Tabla de enrutamiento	Destino	Objetivo
	CIDR de VPC F	pcx-ffffgggg

Si todas las VPC tienen bloques de CIDR IPv6 asociados, actualice las tablas de enrutamiento de la siguiente manera.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR IPv4 de VPC A*	Local
	CIDR IPv6 de VPC A	Local
	CIDR IPv4 de VPC B	pcx-aaaabbbb
	CIDR IPv6 de VPC B	pcx-aaaabbbb
	CIDR IPv4 de VPC C	pcx-aaaacccc
	CIDR IPv6 de VPC C	pcx-aaaacccc
	CIDR IPv4 de VPC D	pcx-aaaadddd
	CIDR IPv6 de VPC D	pcx-aaaadddd
	CIDR IPv4 de VPC E	pcx-aaaaeeee
	CIDR IPv6 de VPC E	pcx-aaaaeeee
	CIDR IPv4 de VPC F	pcx-aaaaffff
	CIDR IPv6 de VPC F	pcx-aaaaffff
	CIDR IPv4 de VPC G	pcx-aaaagggg
	CIDR IPv6 de VPC G	pcx-aaaagggg
VPC B	*CIDR IPv4 de VPC B*	Local
	CIDR IPv6 de VPC B	Local

Tabla de enrutamiento	Destino	Objetivo
	CIDR IPv4 de VPC A	pcx-aaaabbbb
	CIDR IPv6 de VPC A	pcx-aaaabbbb
	CIDR IPv4 de VPC C	pcx-bbbbcccc
	CIDR IPv6 de VPC C	pcx-bbbbcccc
	CIDR IPv4 de VPC D	pcx-bbbbdddd
	CIDR IPv6 de VPC D	pcx-bbbbdddd
	CIDR IPv4 de VPC E	pcx-bbbbeeee
	CIDR IPv6 de VPC E	pcx-bbbbeeee
	CIDR IPv4 de VPC F	pcx-bbbbffff
	CIDR IPv6 de VPC F	pcx-bbbbffff
	CIDR IPv4 de VPC G	pcx-bbbbgggg
	CIDR IPv6 de VPC G	pcx-bbbbgggg
VPC C	*CIDR IPv4 de VPC C*	Local
	CIDR IPv6 de VPC C	Local
	CIDR IPv4 de VPC A	pcx-aaaacccc
	CIDR IPv6 de VPC A	pcx-aaaacccc
	CIDR IPv4 de VPC B	pcx-bbbbcccc
	CIDR IPv6 de VPC B	pcx-bbbbcccc
	CIDR IPv4 de VPC D	pcx-ccccdddd
	CIDR IPv6 de VPC D	pcx-ccccdddd

Tabla de enrutamiento	Destino	Objetivo
	CIDR IPv4 de VPC E	pcx-ccccceeee
	CIDR IPv6 de VPC E	pcx-ccccceeee
	CIDR IPv4 de VPC F	pcx-ccccffff
	CIDR IPv6 de VPC F	pcx-ccccffff
	CIDR IPv4 de VPC G	pcx-ccccgggg
	CIDR IPv6 de VPC G	pcx-ccccgggg
VPC D	*CIDR IPv4 de VPC D*	Local
	CIDR IPv6 de VPC D	Local
	CIDR IPv4 de VPC A	pcx-aaaadddd
	CIDR IPv6 de VPC A	pcx-aaaadddd
	CIDR IPv4 de VPC B	pcx-bbbbdddd
	CIDR IPv6 de VPC B	pcx-bbbbdddd
	CIDR IPv4 de VPC C	pcx-ccccdddd
	CIDR IPv6 de VPC C	pcx-ccccdddd
	CIDR IPv4 de VPC E	pcx-ddddeeee
	CIDR IPv6 de VPC E	pcx-ddddeeee
	CIDR IPv4 de VPC F	pcx-ddddffff
	CIDR IPv6 de VPC F	pcx-ddddffff
	CIDR IPv4 de VPC G	pcx-ddddgggg
	CIDR IPv6 de VPC G	pcx-ddddgggg

Tabla de enrutamiento	Destino	Objetivo
VPC E	*CIDR IPv4 de VPC E*	Local
	CIDR IPv6 de VPC E	Local
	CIDR IPv4 de VPC A	pcx-aaaaeeee
	CIDR IPv6 de VPC A	pcx-aaaaeeee
	CIDR IPv4 de VPC B	pcx-bbbbeeee
	CIDR IPv6 de VPC B	pcx-bbbbeeee
	CIDR IPv4 de VPC C	pcx-cccceeee
	CIDR IPv6 de VPC C	pcx-cccceeee
	CIDR IPv4 de VPC D	pcx-ddddeeee
	CIDR IPv6 de VPC D	pcx-ddddeeee
	CIDR IPv4 de VPC F	pcx-eeeeffff
	CIDR IPv6 de VPC F	pcx-eeeeffff
	CIDR IPv4 de VPC G	pcx-eeeegggg
	CIDR IPv6 de VPC G	pcx-eeeegggg
VPC F	*CIDR IPv4 de VPC F*	Local
	CIDR IPv6 de VPC F	Local
	CIDR IPv4 de VPC A	pcx-aaaaffff
	CIDR IPv6 de VPC A	pcx-aaaaffff
	CIDR IPv4 de VPC B	pcx-bbbbffff
	CIDR IPv6 de VPC B	pcx-bbbbffff

Tabla de enrutamiento	Destino	Objetivo
	CIDR IPv4 de VPC C	pcx-ccccffff
	CIDR IPv6 de VPC C	pcx-ccccffff
	CIDR IPv4 de VPC D	pcx-ddddffff
	CIDR IPv6 de VPC D	pcx-ddddffff
	CIDR IPv4 de VPC E	pcx-eeeeffff
	CIDR IPv6 de VPC E	pcx-eeeeffff
	CIDR IPv4 de VPC G	pcx-ffffgggg
	CIDR IPv6 de VPC G	pcx-ffffgggg
VPC G	*CIDR IPv4 de VPC G*	Local
	CIDR IPv6 de VPC G	Local
	CIDR IPv4 de VPC A	pcx-aaaagggg
	CIDR IPv6 de VPC A	pcx-aaaagggg
	CIDR IPv4 de VPC B	pcx-bbbbgggg
	CIDR IPv6 de VPC B	pcx-bbbbgggg
	CIDR IPv4 de VPC C	pcx-ccccgggg
	CIDR IPv6 de VPC C	pcx-ccccgggg
	CIDR IPv4 de VPC D	pcx-ddddgggg
	CIDR IPv6 de VPC D	pcx-ddddgggg
	CIDR IPv4 de VPC E	pcx-eeeegggg
	CIDR IPv6 de VPC E	pcx-eeeegggg

Tabla de enrutamiento	Destino	Objetivo
	CIDR IPv4 de VPC F	pcx-ffffgggg
	CIDR IPv6 de VPC F	pcx-ffffgggg

Configuraciones de emparejamiento de VPC con rutas específicas

Puede configurar tablas de enrutamiento para que una conexión de emparejamiento de VPC restrinja el acceso a un bloque de CIDR de subred, un bloque de CIDR concreto (si la VPC tiene varios bloques de CIDR) o a un recurso específico en la VPC. En estos ejemplos se empareja una VPC central con al menos dos VPC que tienen bloques de CIDR superpuestos.

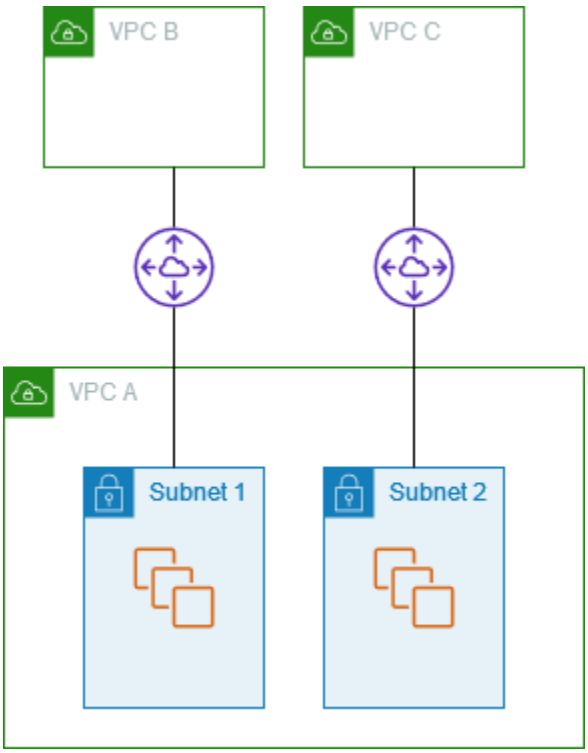
Para obtener ejemplos de escenarios en los que puede necesitar una configuración de interconexión de VPC específica, consulte Escenarios de conexión de emparejamiento de VPC en la red. Para obtener más información sobre el uso de conexiones de emparejamiento de VPC; consulte Interconexiones de VPC. Para obtener más información acerca de la actualización de las tablas de ruteo, consulte Actualice sus tablas de enrutamiento para interconexiones de VPC.

Configuraciones

- Dos VPC que acceden a subredes específicas en una VPC
- Dos VPC que acceden a bloques de CIDR específicos en una VPC
- Una VPC que accede a subredes específicas en dos VPC
- Instancias en una VPC que acceden a instancias específicas en dos VPC
- Una VPC que accede a dos VPC mediante coincidencias con el prefijo de mayor longitud
- Múltiples configuraciones de VPC

Dos VPC que acceden a subredes específicas en una VPC

En esta configuración, hay una VPC central con dos subredes (VPC A), una conexión de emparejamiento entre la VPC A y la VPC B (`pcx-aaaabbbb`) y una conexión de emparejamiento entre la VPC A y la VPC C (`pcx-aaaacccc`). Cada VPC requiere acceso a los recursos de solo una de las subredes en la VPC A.



La tabla de enrutamiento de la subred 1 utiliza la conexión de emparejamiento de VPC `pcx-aaaabbbb` para acceder a todo el bloque de CIDR de la VPC B. La tabla de enrutamiento para la VPC B utiliza `pcx-aaaabbbb` para acceder al bloque de CIDR de la subred 1 en la VPC A. La tabla de enrutamiento de la subred 2 utiliza la conexión de emparejamiento de VPC `pcx-aaaacccc` para acceder a todo el bloque de CIDR de la VPC C. La tabla de enrutamiento para la VPC C utiliza `pcx-aaaacccc` para acceder al bloque de CIDR de la subred 2 en la VPC A.

Tabla de enrutamiento	Destino	Objetivo
Subred 1 (VPC A)	*CIDR de VPC A*	Local
	CIDR de VPC B	pcx-aaaabbbb
Subred 2 (VPC A)	*CIDR de VPC A*	Local
	CIDR de VPC C	pcx-aaaacccc
VPC B	*CIDR de VPC B*	Local
	CIDR de subred 1	pcx-aaaabbbb
VPC C	*CIDR de VPC C*	Local

Tabla de enrutamiento	Destino	Objetivo
	CIDR de subred 2	pcx-aaaacccc

Puede extender esta configuración a varios bloques de CIDR. Supongamos que la VPC A y la VPC B tienen bloques de CIDR IPv4 e IPv6 y que la subred 1 tiene un bloque de CIDR IPv6 asociado. Puede habilitar la VPC B para que se comunique con la subred 1 de la VPC A a través de IPv6 mediante la conexión de emparejamiento de VPC. Para ello, agregue una ruta a la tabla de enrutamiento de la VPC A con destino al bloque de CIDR IPv6 para la VPC B, así como una ruta a la tabla de enrutamiento de la VPC B con destino al bloque de CIDR IPv6 de la subred 1 de la VPC A.

Tabla de enrutamiento	Destino	Objetivo	Notas
Subred 1 de la VPC A	*CIDR IPv4 de VPC A*	Local	
	CIDR IPv6 de VPC A	Local	Ruta local que se añade automáticamente para la comunicación IPv6 en la VPC.
	CIDR IPv4 de VPC B	pcx-aaaabbbb	
	CIDR IPv6 de VPC B	pcx-aaaabbbb	Ruta al bloque de CIDR IPv6 de la VPC B.
Subred 2 de la VPC A	*CIDR IPv4 de VPC A*	Local	
	CIDR IPv6 de VPC A	Local	Ruta local que se añade automáticamente para la

Tabla de enrutamiento	Destino	Objetivo	Notas
			comunicación IPv6 en la VPC.
	CIDR IPv4 de VPC C	pcx-aaaacccc	
VPC B	*CIDR IPv4 de VPC B*	Local	
	CIDR IPv6 de VPC B	Local	Ruta local que se añade automáticamente para la comunicación IPv6 en la VPC.
	CIDR IPv4 de la subred 1	pcx-aaaabbbb	
	CIDR IPv6 de la subred	pcx-aaaabbbb	Ruta al bloque de CIDR IPv6 de la VPC A.
VPC C	*CIDR IPv4 de VPC C*	Local	
	CIDR IPv4 de la subred 2	pcx-aaaacccc	

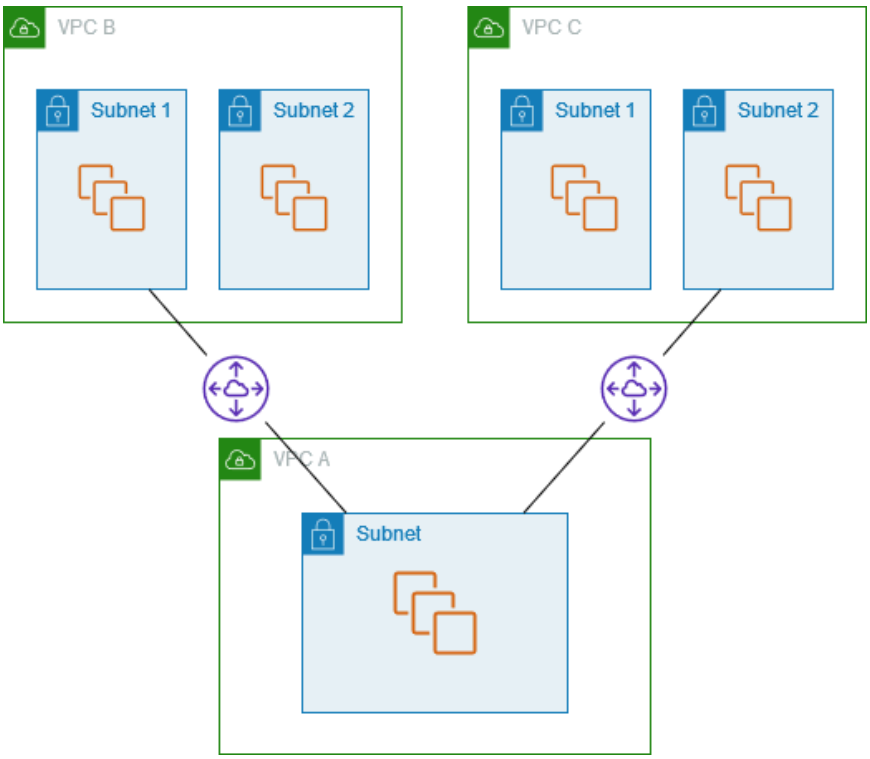
Dos VPC que acceden a bloques de CIDR específicos en una VPC

En esta configuración, hay una VPC central (VPC A), una conexión de emparejamiento entre la VPC A y la VPC B (`pcx-aaaabbbb`) y una conexión de emparejamiento entre la VPC A y la VPC C (`pcx-aaaacccc`). La VPC A tiene un bloque de CIDR por cada conexión de emparejamiento.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR 1 de VPC A*	Local
	CIDR 2 de VPC A	Local
	CIDR de VPC B	pcx-aaaabbbb
	CIDR de VPC C	pcx-aaaacccc
VPC B	*CIDR de VPC B*	Local
	CIDR 1 de VPC A	pcx-aaaabbbb
VPC C	*CIDR de VPC C*	Local
	CIDR 2 de VPC A	pcx-aaaacccc

Una VPC que accede a subredes específicas en dos VPC

En esta configuración, hay una VPC central (VPC A) con una subred, una conexión de emparejamiento entre la VPC A y la VPC B (`pcx-aaaabbbb`) y una conexión de emparejamiento entre la VPC A y la VPC C (`pcx-aaaacccc`). La VPC B y la VPC C tienen dos subredes cada una. La conexión de emparejamiento entre la VPC A y la VPC B utiliza solo una de las subredes en la VPC B. La conexión de emparejamiento entre la VPC A y la VPC C utiliza solo una de las subredes en la VPC C.



Use esta configuración cuando tenga una VPC central con un único conjunto de recursos, como los servicios de Active Directory, a los que otras VPC necesiten tener acceso. La VPC central no requiere acceso completo a las VPC a las que está interconectada.

La tabla de enrutamiento para la VPC A utiliza las conexiones de emparejamiento para acceder solo a subredes específicas en las VPC emparejadas. La tabla de enrutamiento para la subred 1 utiliza la conexión de emparejamiento con la VPC A para acceder a la subred en la VPC A. La tabla de enrutamiento para la subred 2 utiliza la conexión de emparejamiento con la VPC A para acceder a la subred en la VPC A.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR de VPC A*	Local
	CIDR de subred	pcx-aaaabbbb
	CIDR de subred	pcx-aaaacccc
Subred 1 (VPC B)	*CIDR de VPC B*	Local

Tabla de enrutamiento	Destino	Objetivo
	Subred en CIDR de VPC A	pcx-aaaabbbb
Subred 2 (VPC C)	*CIDR de VPC C*	Local
	Subred en CIDR de VPC A	pcx-aaaacccc

Enrutamiento del tráfico de respuesta

Si tiene una VPC emparejada con varias VPC con bloques de CIDR superpuestos o que coinciden, asegúrese de que las tablas de enrutamiento estén configuradas para evitar el envío de tráfico de respuesta desde la VPC a una VPC incorrecta. AWS no admite el reenvío de rutas inversas de unidifusión en conexiones de emparejamiento de VPC que comprueben la IP de origen de los paquetes y direccionen los paquetes de respuesta de vuelta al origen.

Por ejemplo, la VPC A está interconectada con la VPC B y la VPC C. La VPC B y la VPC tiene bloques de CIDR coincidentes al igual que sus respectivas subredes. La tabla de enrutamiento de la subred 2 de la VPC B apunta a la conexión de emparejamiento de VPC `pcx-aaaabbbb` para obtener acceso a la subred de la VPC A. La tabla de enrutamiento de la VPC A está configurada para enviar el tráfico destinado al CIRD de VPC a la conexión de emparejamiento `pcx-aaaaccccc`.

Tabla de enrutamiento	Destino	Objetivo
Subred 2 (VPC B)	*CIDR de VPC B*	Local
	Subred en CIDR de VPC A	pcx-aaaabbbb
VPC A	*CIDR de VPC A*	Local
	CIDR de VPC C	pcx-aaaacccc

Supongamos que una instancia de la subred 2 de la VPC B envía tráfico al servidor de Active Directory de la VPC A mediante la conexión de emparejamiento de VPC `pcx-aaaabbbb`. La VPC A

envía el tráfico de respuesta al servidor de Active Directory. Sin embargo, la tabla de enrutamiento de la VPC A está configurada para enviar todo el tráfico del rango de CIDR de VPC a la conexión de emparejamiento de VPC `pcx-aaaacccc`. Si la subred 2 de la VPC C tiene una instancia con la misma dirección IP que la instancia en la subred 2 de la VPC B, esta recibirá el tráfico de respuesta de la VPC A. La instancia de la subred 2 de la VPC B no recibirá respuesta a las solicitudes que envíe a la VPC A.

Para evitar esto, puede agregar una ruta específica a la tabla de enrutamiento de la VPC A con el CIDR de la subred 2 de la VPC B como destino y objetivo `pcx-aaaabbbb`. La nueva ruta es más específica. Por lo tanto, el tráfico destinado al CIDR de la subred 2 se envía a la conexión de emparejamiento de VPC `pcx-aaaabbbb`.

De manera alternativa, en el ejemplo siguiente, la tabla de enrutamiento de la VPC A tiene una ruta para cada subred de cada conexión de emparejamiento de VPC. La VPC A puede comunicarse con la subred 2 de la VPC B y con la subred 1 de la VPC C. Esta situación es útil si necesita agregar otra conexión de emparejamiento de VPC con otra subred que se encuentra en el mismo intervalo de dirección IP que las VPC B y VPC C; basta con agregar otra ruta para dicha subred específica.

Destino	Objetivo
CIDR de VPC A	Local
CIDR de subred 2	pcx-aaaabbbb
CIDR de subred 1	pcx-aaaacccc

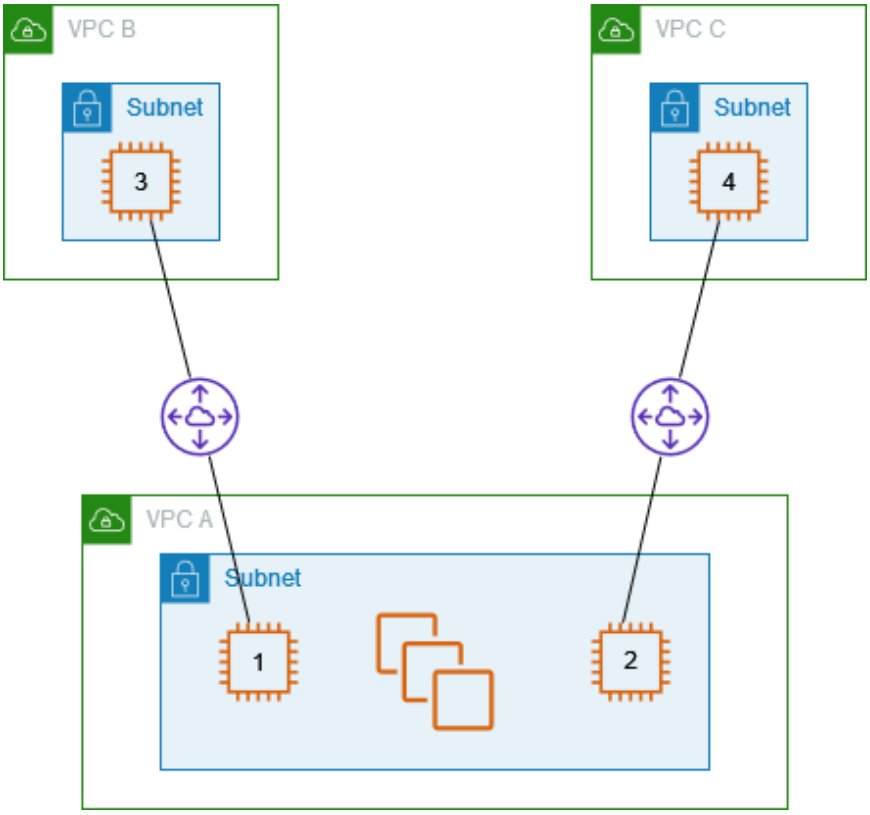
De manera alternativa, dependiendo de su caso, puede crear una ruta a una dirección IP específica de la VPC B para asegurarse de que el tráfico se direccione de nuevo al servidor correcto (la tabla de ruteo utiliza la coincidencia con el prefijo de mayor longitud para establecer una prioridad en las rutas):

Destino	Objetivo
CIDR de VPC A	Local
Dirección IP específica en la subred 2	pcx-aaaabbbb

Destino	Objetivo
CIDR de VPC B	pcx-aaaacccc

Instancias en una VPC que acceden a instancias específicas en dos VPC

En esta configuración, hay una VPC central (VPC A) con una subred, una conexión de emparejamiento entre la VPC A y la VPC B (`pcx-aaaabbbb`) y una conexión de emparejamiento entre la VPC A y la VPC C (`pcx-aaaacccc`). La VPC A tiene una subred con una instancia para cada conexión de emparejamiento. Puede usar esta configuración para limitar el tráfico de emparejamiento a instancias específicas.



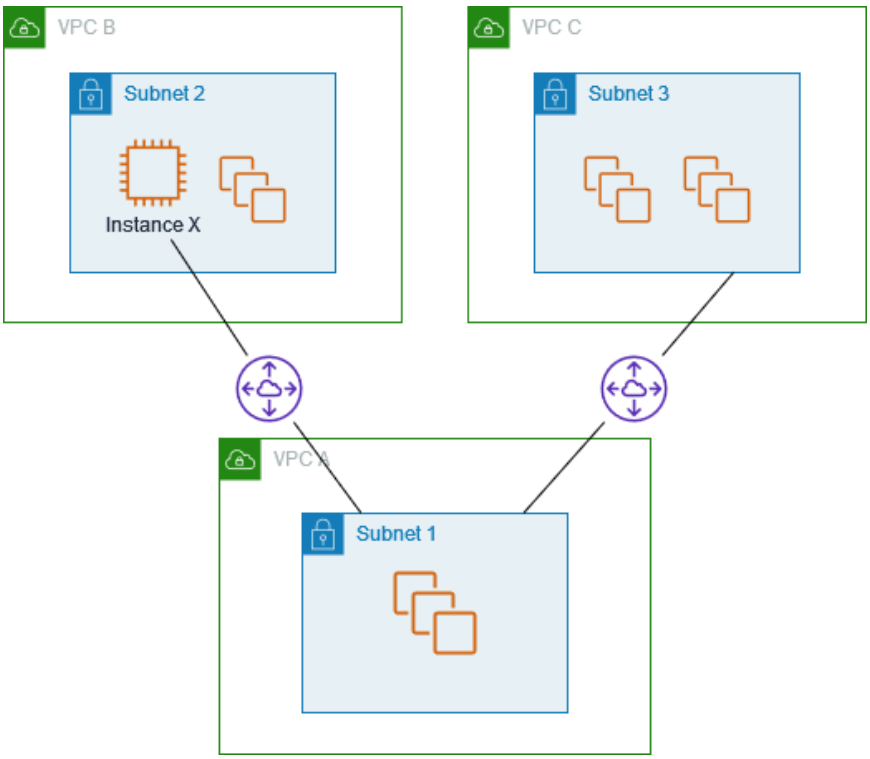
Cada tabla de ruteo de VPC apunta a la interconexión de VPC relevante para obtener acceso a una única dirección IP (y, por lo tanto, a una instancia específica) de la VPC interconectada.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR de VPC A*	Local

Tabla de enrutamiento	Destino	Objetivo
	Dirección IP de la instancia 3	pcx-aaaabbbb
	Dirección IP de la instancia 4	pcx-aaaacccc
VPC B	*CIDR de VPC B*	Local
	Dirección IP de la instancia 1	pcx-aaaabbbb
VPC C	*CIDR de VPC C*	Local
	Dirección IP de la instancia 2	pcx-aaaacccc

Una VPC que accede a dos VPC mediante coincidencias con el prefijo de mayor longitud

En esta configuración, hay una VPC central (VPC A) con una subred, una conexión de emparejamiento entre la VPC A y la VPC B (`pcx-aaaabbbb`) y una conexión de emparejamiento entre la VPC A y la VPC C (`pcx-aaaacccc`). La VPC B y la VPC C tienen bloques de CIDR coincidentes. Utiliza la conexión de emparejamiento de VPC `pcx-aaaabbbb` para dirigir el tráfico entre la VPC A y una instancia específica en la VPC B. El resto del tráfico con destino al rango de dirección de CIDR compartido entre la VPC B y la VPC C se direcciona hacia la VPC C mediante `pcx-aaaacccc`.



Las tablas de ruteo de la VPC utilizan la coincidencia con el prefijo de mayor longitud para seleccionar la ruta más específica en la interconexión de VPC. El resto del tráfico se direcciona mediante la siguiente ruta coincidente; en este caso, la interconexión de VPC `pcx-aaaacccc`.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*Bloque de CIDR de VPC A*	Local
	Dirección IP de la instancia X	pcx-aaaabbbb
	Bloque de CIDR de VPC C	pcx-aaaacccc
VPC B	*Bloque de CIDR de VPC B*	Local
	Bloque de CIDR de VPC A	pcx-aaaabbbb

Tabla de enrutamiento	Destino	Objetivo
VPC C	*Bloque de CIDR de VPC C*	Local
	Bloque de CIDR de VPC A	pcx-aaaacccc

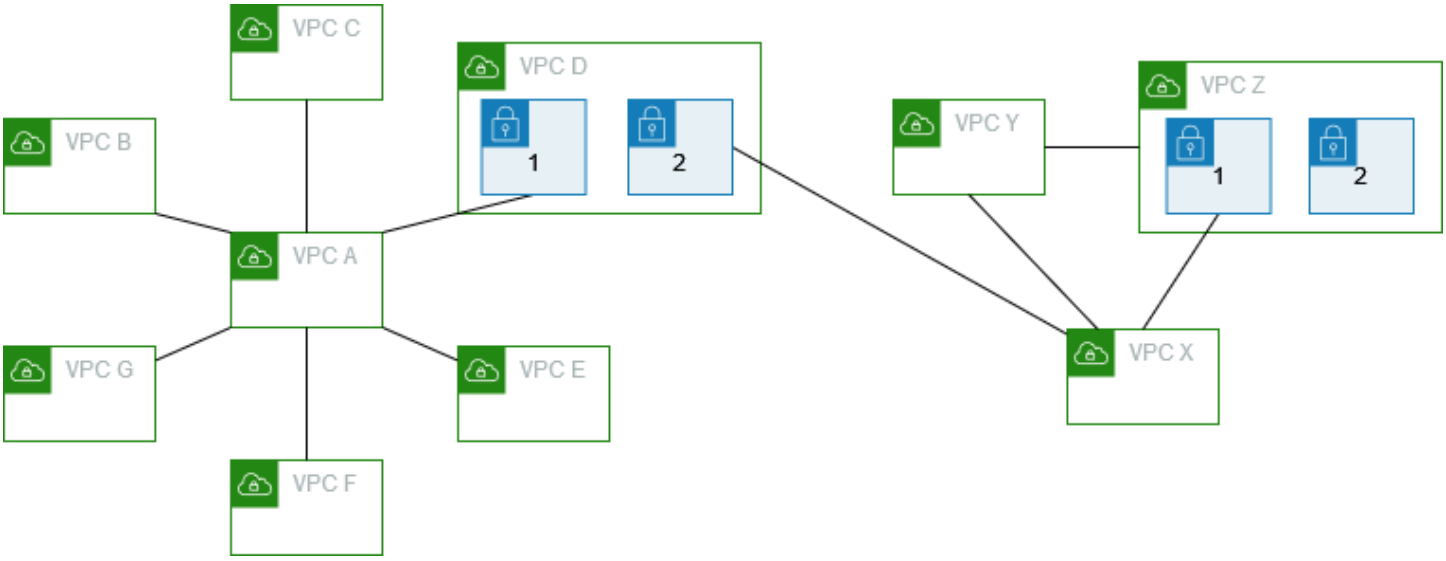
> **Important**
>
> Si una instancia distinta a la instancia X de la VPC B envía tráfico a la VPC A, es posible que el tráfico de respuesta se direccione a la VPC C en lugar de a la VPC B. Para obtener más información, consulte Enrutamiento del tráfico de respuesta.

Múltiples configuraciones de VPC

En esta configuración, hay una VPC central (VPC A) que está emparejada a múltiples VPC en una configuración radial. También tiene tres VPC (VPC X, Y y Z) emparejadas en una configuración de malla completa.

La VPC D también tiene una conexión de emparejamiento de VPC con la VPC X (`pcx-ddddxxxx`). La VPC A y la VPC X tienen bloques de CIDR superpuestos. Esto significa que el tráfico de emparejamiento entre la VPC A y la VPC D está limitado a una subred específica (subred 1) en la VPC D. Esto garantiza que, si la VPC D recibe una solicitud desde la VPC A o la VPC X, el tráfico de respuesta se enviará a la VPC correcta. AWS no admite el reenvío de rutas inversas unidifusión en conexiones de emparejamiento de VPC que comprueben la IP de origen de los paquetes y direccionen los paquetes de respuesta de vuelta al origen. Para obtener más información, consulte Enrutamiento del tráfico de respuesta.

Del mismo modo, la VPC D y la VPC Z tienen bloques de CIDR superpuestos. El tráfico de emparejamiento entre la VPC D y la VPC X está limitado a la subred 2 de la VPC D y el tráfico de emparejamiento entre la VPC X y la VPC Z está limitado a la subred 1 de la VPC Z. De este modo, se garantiza que, si la VPC X recibe tráfico de emparejamiento de la VPC D o la VPC Z, el tráfico de respuesta se enviará de nuevo a la VPC correcta.



Las tablas de enrutamiento de las VPC B, C, E, F y G apuntan a las conexiones de emparejamiento relevantes para obtener acceso al bloque de CIDR completo de la VPC A. Asimismo, la tabla de enrutamiento de la VPC A apunta a las conexiones de emparejamiento relevantes de las VPC B, C, E, F y G para obtener acceso a sus bloques de CIDR completos. Para la conexión de emparejamiento `pcx-aaaadddd`, la tabla de enrutamiento de la VPC A direcciona el tráfico solo a la subred 1 de la VPC D y la tabla de enrutamiento de la subred 1 de la VPC D apunta al bloque de CIDR completo de la VPC A.

La tabla de enrutamiento de la VPC Y apunta a las conexiones de emparejamiento relevantes para obtener acceso a los bloques de CIDR completos de la VPC X y la VPC Z. Asimismo, la tabla de enrutamiento de la VPC Z apunta a la conexión de emparejamiento relevante para obtener acceso al bloque de CIDR completo de la VPC Y. La tabla de enrutamiento de la subred 1 de la VPC Z apunta a la conexión de emparejamiento relevante para obtener acceso al bloque de CIDR completo de la VPC Y. La tabla de enrutamiento de la VPC X apunta a la conexión de emparejamiento relevante para obtener acceso a la subred 2 de la VPC D y a la subred 1 de la VPC Z.

Tabla de enrutamiento	Destino	Objetivo
VPC A	*CIDR de VPC A*	Local
	CIDR de VPC B	pcx-aaaabbbb
	CIDR de VPC C	pcx-aaaacccc

Tabla de enrutamiento	Destino	Objetivo
	CIDR de subred 1 en VPC D	pcx-aaaadddd
	CIDR de VPC E	pcx-aaaaeeee
	CIDR de VPC F	pcx-aaaaffff
	CIDR de VPC G	pcx-aaaagggg
VPC B	*CIDR de VPC B*	Local
	CIDR de VPC A	pcx-aaaabbbb
VPC C	*CIDR de VPC C*	Local
	CIDR de VPC A	pcx-aaaacccc
Subred 1 de la VPC D	*CIDR de VPC D*	Local
	CIDR de VPC A	pcx-aaaadddd
Subred 2 de la VPC D	*CIDR de VPC D*	Local
	CIDR de VPC X	pcx-ddddxxxx
VPC E	*CIDR de VPC E*	Local
	CIDR de VPC A	pcx-aaaaeeee
VPC F	*CIDR de VPC F*	Local
	CIDR de VPC A	pcx-aaaaffff
VPC G	*CIDR de VPC G*	Local
	CIDR de VPC A	pcx-aaaagggg
VPC X	*CIDR de VPC X*	Local

Tabla de enrutamiento	Destino	Objetivo
	CIDR de subred 2 en VPC D	pcx-ddddxxxx
	CIDR de VPC Y	pcx-xxxxyyyy
	CIDR de subred 1 en VPC Z	pcx-xxxxzzzz
VPC Y	*CIDR de VPC Y*	Local
	CIDR de VPC X	pcx-xxxxyyyy
	CIDR de VPC Z	pcx-yyyyzzzz
VPC Z	*CIDR de VPC Z*	Local
	CIDR de VPC Y	pcx-yyyyzzzz
	CIDR de VPC X	pcx-xxxxzzzz

Escenarios de conexión de emparejamiento de VPC en la red

Hay diversos motivos por los que podría necesitar configurar una conexión de emparejamiento de VPC entre sus VPC o entre una VPC propia y una VPC de otra cuenta de AWS. Los siguientes escenarios pueden ayudarlo a determinar qué configuración se adapta mejor a sus necesidades de redes.

Escenarios

- Interconexión de dos o más VPC para proporcionar acceso completo a los recursos
- Interconexión de una VPC para obtener acceso a recursos centralizados

Interconexión de dos o más VPC para proporcionar acceso completo a los recursos

En este escenario, tiene dos o más VPC que desea interconectar para poder compartir por completo los recursos entre todas las VPC. A continuación se muestran algunos ejemplos:

- Su empresa tiene una VPC para el departamento de finanzas, y otra VPC para el departamento de contabilidad. El departamento de finanzas necesita obtener acceso a todos los recursos del departamento de contabilidad, y el departamento de contabilidad necesita obtener acceso a todos los recursos del departamento de finanzas.
- Su empresa tiene varios departamentos de TI, cada uno con su propia VPC. Algunas VPC se encuentran en la misma cuenta de AWS, mientras que otras están en una cuenta de AWS diferente. Desea interconectar todas las VPC para permitir que los departamentos de TI tengan acceso completo a los recursos de los demás.

Para obtener más información acerca de cómo configurar los ajustes de interconexión con VPC y las tablas de ruteo para este escenario, consulte la siguiente documentación:

- Utilización de dos VPC interconectadas
- Tres VPC interconectadas
- Varias VPC interconectadas

Para obtener más información acerca de la creación y el uso de interconexiones de VPC en la consola de Amazon VPC, consulte Interconexiones de VPC.

Interconexión de una VPC para obtener acceso a recursos centralizados

En este escenario, dispone de una VPC central que contiene recursos que desea compartir con otras VPC. Su VPC central puede necesitar un acceso completo o parcial a las VPC del mismo nivel y, de forma similar, estas VPC del mismo nivel pueden necesitar un acceso completo o parcial a la VPC central. A continuación se muestran algunos ejemplos:

- El departamento de TI de su empresa tiene una VPC para el uso compartido de archivos. Desea interconectar otras VPC a esa VPC central, pero no desea que las otras VPC se envíen tráfico entre sí.
- Su empresa tiene una VPC que desea compartir con sus clientes. Cada cliente puede crear una interconexión de VPC con su VPC; sin embargo, sus clientes no pueden direccionar el tráfico a otras VPC interconectadas con la suya, ni conocen las rutas de otros clientes.
- Tiene una VPC central que se utiliza para servicios de Active Directory. Las instancias específicas de las VPC del mismo nivel envían solicitudes a los servidores de Active Directory y requieren acceso completo a la VPC central. La VPC central no necesita acceso completo a las VPC del mismo nivel; solo necesita direccionar el tráfico de respuesta a las instancias específicas.

Para obtener más información acerca de la creación y el uso de interconexiones de VPC en la consola de Amazon VPC, consulte Interconexiones de VPC.

Administración de identidades y accesos para la interconexión de VPC

De forma predeterminada, los usuarios no pueden crear ni modificar interconexiones de VPC. Para conceder acceso a recursos de emparejamiento de VPC, asocie una política de IAM a una identidad de IAM como, por ejemplo, un rol.

Ejemplos

- Ejemplo: crear una conexión de emparejamiento de VPC
- Ejemplo: aceptar una conexión de emparejamiento de VPC
- Ejemplo: eliminar una conexión de emparejamiento de VPC
- Ejemplo: trabajar con una cuenta específica
- Ejemplo: administrar conexiones de emparejamiento de VPC mediante la consola

Para obtener una lista de las acciones de Amazon VPC y las claves de condiciones y recursos compatibles para cada acción, consulte Acciones, recursos y claves de condición para Amazon EC2 en la Referencia de autorización de servicios.

Ejemplo: crear una conexión de emparejamiento de VPC

La siguiente política otorga permiso a los usuarios para crear solicitudes de conexión de emparejamiento de VPC mediante VPC con la etiqueta `Purpose=Peering`. La primera instrucción aplica una clave de condición (`ec2:ResourceTag`) al recurso de la VPC. Tenga en cuenta que el recurso de la VPC de la acción `CreateVpcPeeringConnection` corresponde siempre a la VPC solicitante.

La segunda instrucción otorga a los usuarios permiso para crear recursos de conexión de emparejamiento de VPC y, por lo tanto, usa el carácter comodín * en lugar de un ID de recurso específico.

JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*"
    }
  ]
}
```

La siguiente política otorga permiso a los usuarios de la cuenta de AWS especificada para crear conexiones de emparejamiento de VPC mediante cualquier VPC de la región especificada, pero solo si la VPC que aceptará la conexión de emparejamiento es una VPC determinada en otra cuenta específica.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcPeeringConnection",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcPeeringConnection",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-
connection/*",
            "Condition": {
                "ArnEquals": {
```

```
                    "ec2:AccepterVpc": "arn:aws:ec2:us-
east-1:111122223333:vpc/vpc-1234567890abcdef0"
                }
            }
        }
    ]
}
```

Ejemplo: aceptar una conexión de emparejamiento de VPC

La siguiente política otorga permiso a los usuarios para aceptar solicitudes de conexión de emparejamiento de VPC de una cuenta de AWS específica. Esto ayuda a evitar que los usuarios acepten solicitudes de interconexión de VPC de cuentas desconocidas. La instrucción utiliza la clave de condición `ec2:RequesterVpc` para hacer que esto se cumpla.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:RequesterVpc": "arn:aws:ec2:us-east-1:111122223333:vpc/*"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
    }
  ]
}
```

La siguiente política otorga permiso a los usuarios para aceptar solicitudes de emparejamiento solo si la VPC tiene la etiqueta `Purpose=Peering`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-connection/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    }
  ]
}
```

Ejemplo: eliminar una conexión de emparejamiento de VPC

La siguiente política otorga permiso a los usuarios de la cuenta especificada para eliminar cualquier conexión de emparejamiento de VPC, salvo aquellas que usen la VPC especificada, la cual se encuentra en la misma cuenta. La política especifica las claves de condición `ec2:AccepterVpc` y `ec2:RequesterVpc`, ya que es posible que la VPC haya sido la VPC solicitante o la VPC del mismo nivel en la solicitud de interconexión de VPC original.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVpcPeeringConnection",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:vpc-peering-
connection/*",
            "Condition": {
                "ArnNotEquals": {
                    "ec2:AccepterVpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0",
                    "ec2:RequesterVpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-0abcdef1234567890"
                }
            }
        }
    ]
}
```

Ejemplo: trabajar con una cuenta específica

La siguiente política otorga permiso a los usuarios para usar conexiones de emparejamiento de VPC de una cuenta específica. La política permite a los usuarios ver, crear, aceptar, rechazar y eliminar interconexiones de VPC siempre que se encuentren en la misma cuenta de AWS.

La primera instrucción otorga permiso a los usuarios para ver todas las conexiones de emparejamiento de VPC. El elemento `Resource` requiere el carácter comodín * en este caso, ya que la acción de la API (`DescribeVpcPeeringConnections`) no admite actualmente los permisos de nivel de recurso.

La segunda instrucción otorga permiso a los usuarios para crear conexiones de emparejamiento de VPC y permite para ello el acceso a todas las VPC de la cuenta especificada.

La tercera instrucción usa el carácter comodín * como parte del elemento `Action` para otorgar permiso para todas las acciones de conexión de emparejamiento de VPC. Las claves de condición aseguran que las acciones solo se puedan realizar en interconexiones de VPC con VPC que forman parte de la cuenta. Por ejemplo, un usuario no puede eliminar una conexión de emparejamiento de VPC si la VPC solicitante o responsable de aceptar la solicitud se encuentran en cuentas distintas. Los usuarios no podrán crear interconexiones de VPC con VPC de otras cuentas distintas.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeVpcPeeringConnections",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection"
            ],
            "Resource": "arn:aws:ec2:*:111122223333:vpc/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:*VpcPeeringConnection",
            "Resource": "arn:aws:ec2:*:111122223333:vpc-peering-connection/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:AccepterVpc": "arn:aws:ec2:*:111122223333:vpc/*",
                    "ec2:RequesterVpc": "arn:aws:ec2:*:111122223333:vpc/*"
                }
            }
        }
    ]
}
```

Ejemplo: administrar conexiones de emparejamiento de VPC mediante la consola

Para consultar las interconexiones de VPC en la consola de Amazon VPC, los usuarios deben tener permiso para utilizar la acción `ec2:DescribeVpcPeeringConnections`. Para poder utilizar la página Create Peering Connection (Crear interconexiones), los usuarios deben tener permiso para utilizar la acción `ec2:DescribeVpcs`. Esto les concede permiso para visualizar y seleccionar una

VPC. Puede aplicar permisos de nivel de recurso a todas las acciones `ec2:*PeeringConnection` excepto `ec2:DescribeVpcPeeringConnections`.

La siguiente política otorga permiso a los usuarios para ver conexiones de emparejamiento de VPC y usar el cuadro de diálogo Create VPC Peering Connection (Crear conexiones de emparejamiento de VPC) para crear una conexión de emparejamiento de VPC que use solo una VPC solicitante específica. Si los usuarios intentan crear una interconexión de VPC con una VPC solicitante distinta, se producirá un error en la solicitud.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeVpcPeeringConnections", "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": [
        "arn:aws:ec2:*:*:vpc/vpc-1234567890abcdef0",
        "arn:aws:ec2:*:*:vpc-peering-connection/*"
      ]
    }
  ]
}
```

Cuotas de conexión de emparejamiento de VPC para una cuenta

El emparejamiento de la VPC le permite conectar dos VPC. Esto permite que los recursos de una VPC se comuniquen con los recursos de la otra VPC como si estuvieran en la misma red. El emparejamiento de la VPC es una característica útil para conectar sus VPC, tanto si se encuentran en la misma región de AWS como en regiones diferentes. En esta sección se describen las cuotas que debe tener en cuenta al trabajar con conexiones de emparejamiento de la VPC.

En la tabla siguiente se muestran las cuotas, antes llamadas límites, para las conexiones de emparejamiento de VPC para su cuenta de AWS. A no ser que se indique lo contrario, puede solicitar un aumento de estas cuotas.

Si descubre que sus requisitos actuales de conexión de emparejamiento de VPC superan las cuotas predeterminadas, le recomendamos que envíe una solicitud de aumento del límite de servicio. Revisaremos su caso de uso y trabajaremos con usted para ajustar las cuotas en consecuencia, garantizando que su entorno de VPC pueda satisfacer sus crecientes necesidades empresariales.

Nombre	Valor predeterminado	Ajustable
Interconexiones de VPC activas por VPC	50	Sí (hasta 125)
Solicitudes de interconexión de VPC pendientes	25	Sí
Tiempo de caducidad de una solicitud de interconexión de VPC no aceptada	1 semana (168 horas)	No

Para obtener más información sobre las reglas de uso de conexiones de emparejamiento de VPC, consulte Limitaciones de interconexión de VPC. Para obtener más información acerca de las cuotas de Amazon VPC, consulte Cuotas de Amazon VPC en la Guía del usuario de Amazon VPC.

Historial de documentos para la Guía de emparejamiento de VPC de Amazon

En la siguiente tabla, se describe la documentación de esta versión de la Guía de emparejamiento de VPC de Amazon.

Cambio	Descripción	Fecha
Etiqueta al crear	Puede añadir etiquetas al crear una conexión de emparejamiento de VPC y una tabla de enrutamiento.	20 de julio de 2020
Emparejamiento entre regiones	La resolución de nombres de host DNS se admite para las conexiones de emparejamiento de VPC entre regiones en la región Asia-Pacífico (Hong Kong).	26 de agosto de 2019
Emparejamiento entre regiones	Puede crear una interconexión de VPC entre VPC de distintas regiones de AWS.	29 de noviembre de 2017
Soporte para la resolución de DNS para la interconexión de VPC	Puede habilitar una VPC local para resolver nombres de host DNS públicos en direcciones IP privadas al consultar desde instancias en la VPC del mismo nivel.	28 de julio de 2016
Reglas antiguas de los grupos de seguridad	Puede identificar si se está haciendo referencia a su grupo de seguridad en las reglas de un grupo de seguridad de una VPC del mismo nivel y puede identificar	12 de mayo de 2016

	las reglas antiguas del grupo de seguridad.	
Uso de ClassicLink a través de una interconexión de VPC	Puede modificar su interconexión de VPC para permitir que las instancias locales vinculadas de EC2-Classic se comuniquen con las instancias de una VPC del mismo nivel y viceversa.	26 de abril de 2016
Interconexión con VPC	También puede crear una interconexión VPC entre dos VPC, que permitirá a las instancias de las dos VPC comunicarse entre sí utilizando direcciones IP privadas.	24 de marzo de 2014