Amazon Virtual Private Cloud

VPC Peering

亚马逊云科技

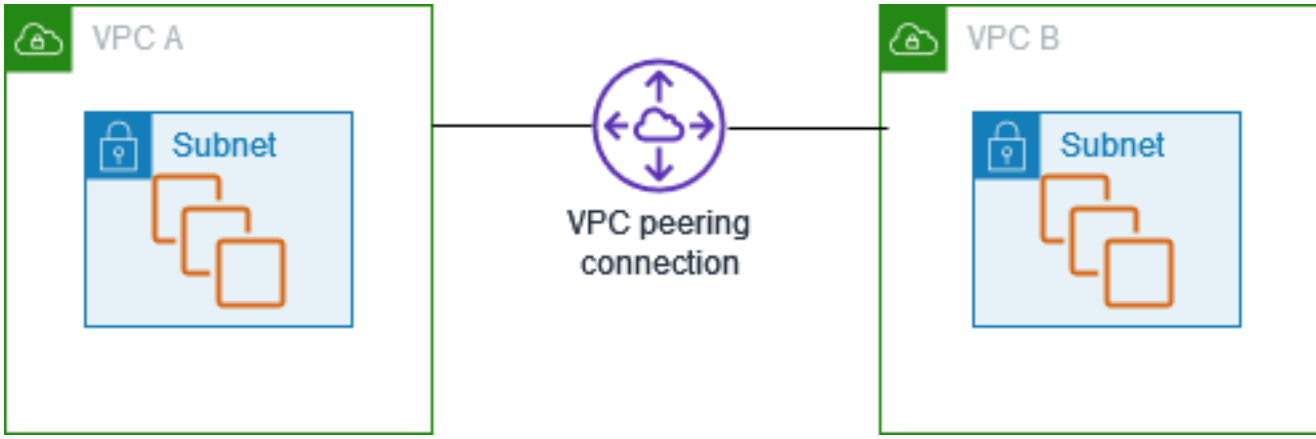
Amazon Virtual Private Cloud: VPC Peering

Table of Contents

What is VPC peering?

A *virtual private cloud* (VPC) is a virtual network dedicated to your Amazon Web Services account. It is logically isolated from other virtual networks in the Amazon Cloud. You can launch Amazon resources, such as Amazon EC2 instances, into your VPC.

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another Amazon account. The VPCs can be in different Regions (also known as an inter-Region VPC peering connection).



Amazon uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

A VPC peering connection helps you to facilitate the transfer of data. For example, if you have more than one Amazon account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

When you establish peering relationships between VPCs across different Amazon Regions, resources in the VPCs (for example, EC2 instances and Lambda functions) in different Amazon Regions can communicate with each other using private IP addresses, without using a gateway, VPN connection, or network appliance. The traffic remains in the private IP space. All inter-Region traffic is encrypted with no single point of failure, or bandwidth bottleneck. Traffic always stays on the global Amazon backbone, and never traverses the public internet, which reduces threats, such as common exploits, and DDoS attacks. Inter-Region VPC peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy.

Pricing for a VPC peering connection

There is no charge to create a VPC peering connection. There is a charge for data transfer across peering connections. For more information, see Amazon EC2 Pricing.

VPC peering basics

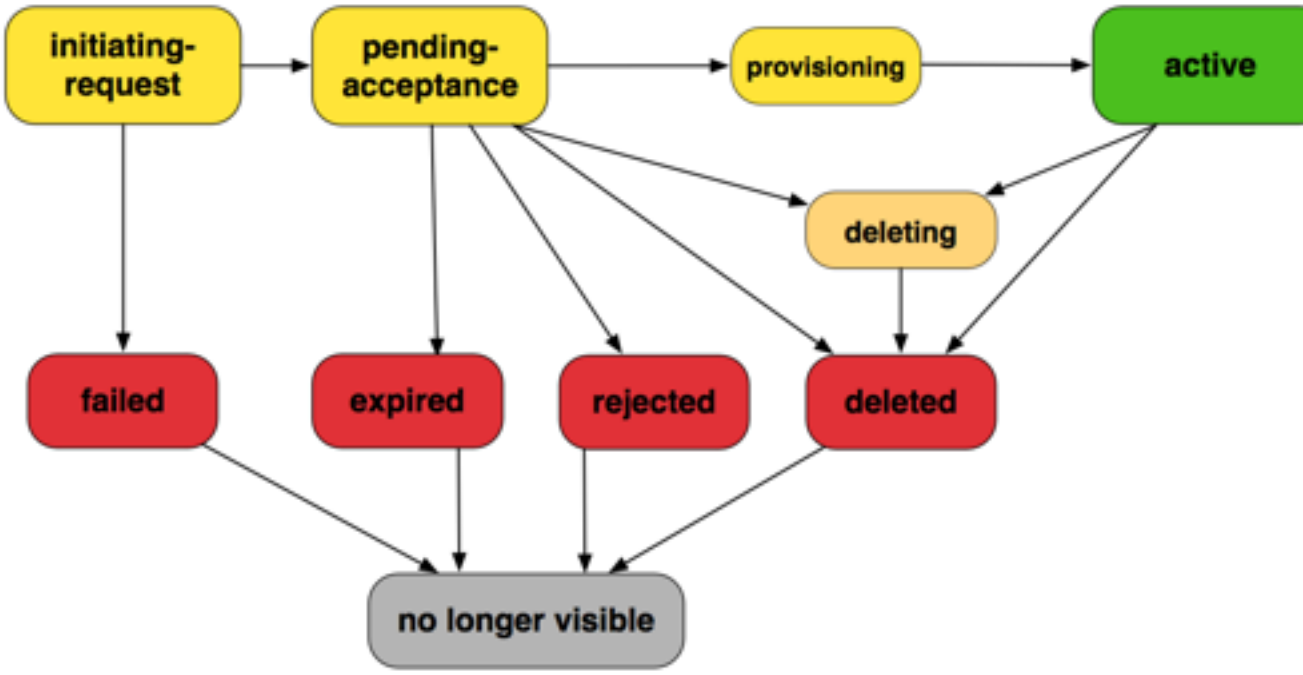
To establish a VPC peering connection, you do the following:

1. The owner of the *requester VPC* sends a request to the owner of the *accepter VPC* to create the VPC peering connection. The accepter VPC can be owned by you, or another Amazon account, and cannot have a CIDR block that overlaps with the CIDR block of the requester VPC.
2. The owner of the accepter VPC accepts the VPC peering connection request to activate the VPC peering connection.
3. To enable the flow of traffic between the VPCs using private IP addresses, the owner of each VPC in the VPC peering connection must manually add a route to one or more of their VPC route tables that points to the IP address range of the other VPC (the peer VPC).
4. If required, update the security group rules that are associated with your instance to ensure that traffic to and from the peer VPC is not restricted. If both VPCs are in the same region, you can reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group rules.
5. With the default VPC peering connection options, if EC2 instances on either side of a VPC peering connection address each other using a public DNS hostname, the hostname resolves to the public IP address of the instance. To change this behavior, enable DNS hostname resolution for your VPC connection. After enabling DNS hostname resolution, if instances on either side of the VPC peering connection address each other using a public DNS hostname, the hostname resolves to the private IP address of the instance.

For more information, see Work with VPC peering connections (p. 7).

VPC peering connection lifecycle

A VPC peering connection goes through various stages starting from when the request is initiated. At each stage, there may be actions that you can take, and at the end of its lifecycle, the VPC peering connection remains visible in the Amazon VPC console and API or command line output for a period of time.



- **Initiating-request**: A request for a VPC peering connection has been initiated. At this stage, the peering connection can fail, or can go to `pending-acceptance`.
- **Failed**: The request for the VPC peering connection has failed. While in this state, it cannot be accepted, rejected, or deleted. The failed VPC peering connection remains visible to the requester for 2 hours.
- **Pending-acceptance**: The VPC peering connection request is awaiting acceptance from the owner of the accepter VPC. During this state, the owner of the requester VPC can delete the request, and the owner of the accepter VPC can accept or reject the request. If no action is taken on the request, it expires after 7 days.
- **Expired**: The VPC peering connection request has expired, and no action can be taken on it by either VPC owner. The expired VPC peering connection remains visible to both VPC owners for 2 days.
- **Rejected**: The owner of the accepter VPC has rejected a `pending-acceptance` VPC peering connection request. While in this state, the request cannot be accepted. The rejected VPC peering connection remains visible to the owner of the requester VPC for 2 days, and visible to the owner of the accepter VPC for 2 hours. If the request was created within the same Amazon account, the rejected request remains visible for 2 hours.
- **Provisioning**: The VPC peering connection request has been accepted, and will soon be in the `active` state.
- **Active**: The VPC peering connection is active, and traffic can flow between the VPCs (provided that your security groups and route tables allow the flow of traffic). While in this state, either of the VPC owners can delete the VPC peering connection, but cannot reject it.

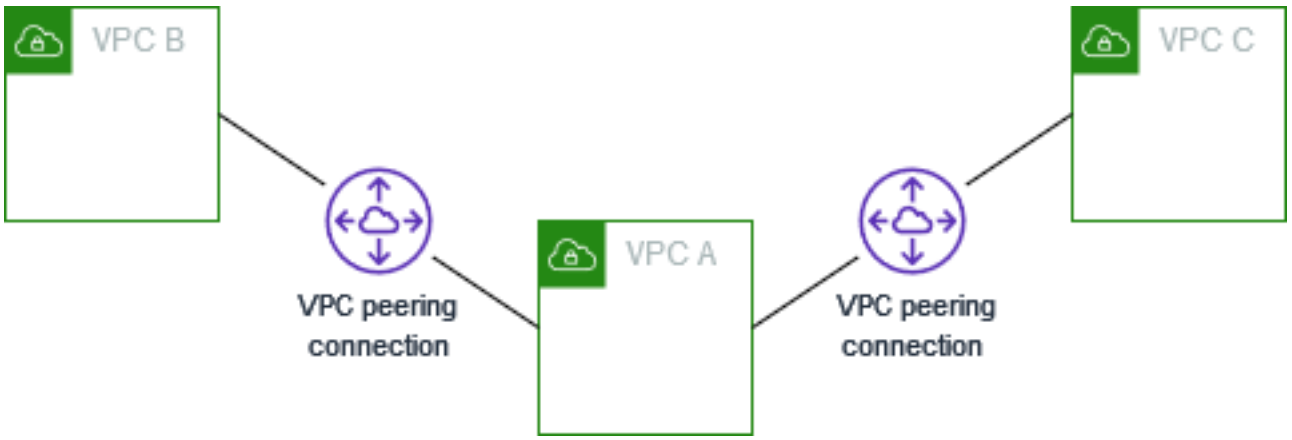
  Note
  If an event in a region in which a VPC resides prevents the flow of traffic, the status of the VPC peering connection remains `Active`.
- **Deleting**: Applies to an inter-Region VPC peering connection that is in the process of being deleted. The owner of either VPC has submitted a request to delete an `active` VPC peering connection, or the owner of the requester VPC has submitted a request to delete a `pending-acceptance` VPC peering connection request.

- **Deleted**: An `active` VPC peering connection has been deleted by either of the VPC owners, or a `pending-acceptance` VPC peering connection request has been deleted by the owner of the requester VPC. While in this state, the VPC peering connection cannot be accepted or rejected. The VPC peering connection remains visible to the party that deleted it for 2 hours, and visible to the other party for 2 days. If the VPC peering connection was created within the same Amazon account, the deleted request remains visible for 2 hours.

Multiple VPC peering connections

A VPC peering connection is a one to one relationship between two VPCs. You can create multiple VPC peering connections for each VPC that you own, but transitive peering relationships are not supported. You do not have any peering relationship with VPCs that your VPC is not directly peered with.

The following diagram is an example of one VPC peered to two different VPCs. There are two VPC peering connections: VPC A is peered with both VPC B and VPC C. VPC B and VPC C are not peered, and you cannot use VPC A as a transit point for peering between VPC B and VPC C. If you want to enable routing of traffic between VPC B and VPC C, you must create a unique VPC peering connection between them.



VPC peering limitations

Consider the following limitations for VPC peering connections. In some cases, you can use a transit gateway attachment instead of a VPC peering connection. For more information, see Examples in *Amazon VPC Transit Gateways*.

Connections

- There is a quota on the number of active and pending VPC peering connections per VPC. For more information, see *Quotas* (p. 51).
- You cannot have more than one VPC peering connection between two VPCs at the same time.
- Any tags that you create for your VPC peering connection are only applied in the account or Region in which you create them.
- You cannot connect to or query the Amazon DNS server in a peer VPC.
- If the IPv4 CIDR block of a VPC in a VPC peering connection falls outside of the private IPv4 address ranges specified by RFC 1918, private DNS hostnames for that VPC cannot be resolved to private IP addresses. To resolve private DNS hostnames to private IP addresses, you can enable DNS resolution support for the VPC peering connection. For more information, see Enable DNS resolution for a VPC peering connection (p. 16).

- You can enable resources on either side of a VPC peering connection to communicate over IPv6. You must associate an IPv6 CIDR block with each VPC, enable the instances in the VPCs for IPv6 communication, and route IPv6 traffic intended for the peer VPC to the VPC peering connection.
- Unicast reverse path forwarding in VPC peering connections is not supported. For more information, see Routing for response traffic (p. 35).
- You can enable IPv4 communication between a linked EC2-Classic instance and instances in a VPC on the other side of a VPC peering connection. However, IPv6 is not supported in EC2-Classic, so you cannot extend this connection for IPv6 communication.

Overlapping CIDR blocks

- You cannot create a VPC peering connection between VPCs that have matching or overlapping IPv4 CIDR blocks.
- You cannot create a VPC peering connection between VPCs that have matching or overlapping IPv6 CIDR blocks.
- If you have multiple IPv4 CIDR blocks, you can't create a VPC peering connection if any of the CIDR blocks overlap, even if you intend to use only the non-overlapping CIDR blocks or only IPv6 CIDR blocks.

Transitive peering

- VPC peering does not support transitive peering relationships. For example, if there are VPC peering connections between VPC A and VPC B, and between VPC A and VPC C, you can't route traffic from VPC B to VPC C through VPC A. To route traffic between VPC B and VPC C, you must create a VPC peering connection between them. For more information, see Three VPCs peered together (p. 23).

Edge to edge routing through a gateway or private connection

- If VPC A has an internet gateway, resources in VPC B can't use the internet gateway in VPC A to access the internet.
- If VPC A has an NAT device that provides internet access to subnets in VPC A, resources in VPC B can't use the NAT device in VPC A to access the internet.
- If VPC A has a VPN connection to a corporate network, resources in VPC B can't use the VPN connection to communicate with the corporate network.
- If VPC A has an Amazon Direct Connect connection to a corporate network, resources in VPC B can't use the Amazon Direct Connect connection to communicate with the corporate network.
- If VPC A has a gateway endpoint that provides connectivity to Amazon S3 to private subnets in VPC A, resources in VPC B can't use the gateway endpoint to access Amazon S3.

Inter-Region VPC peering connections

- You cannot create a security group rule that references a peer VPC security group.
- The Maximum Transmission Unit (MTU) across the VPC peering connection over Regions is 1500 bytes. Jumbo frames (MTUs up to 9001 bytes) are not supported for inter-Region VPC peering connections. They are, however, supported for VPC peering connections in the same Region. For more information about jumbo frames, see Jumbo frames (9001 MTU) in the *Amazon EC2 User Guide for Linux Instances*.
- You must enable DNS resolution support for the VPC peering connection to resolve private DNS hostnames of the peered VPC to private IP addresses, even if the IPv4 CIDR for the VPC falls into the private IPv4 address ranges specified by RFC 1918.
- You cannot enable support for an EC2-Classic instance that's linked to a VPC using ClassicLink to communicate with the peer VPC.

- Inter-Region peering in China is only allowed between the China (Beijing) Region, operated by SINNET and the China (Ningxia) Region, operated by NWCD.

Work with VPC peering connections

Use the following procedures to create and work with VPC peering connections.

Tasks

Create a VPC peering connection

To create a VPC peering connection, first create a request to peer with another VPC. You can request a VPC peering connection with another VPC in your account, or with a VPC in a different Amazon account. For an inter-Region VPC peering connection where the VPCs are in different Regions, the request must be made from the Region of the requester VPC.

To activate the request, the owner of the accepter VPC must accept the request. For an inter-Region VPC peering connection, the request must be accepted in the Region of the accepter VPC. For more information, see the section called “Accept” (p. 9).

Tasks

Prerequisites

- Review the limitations and rules (p. 4) for VPC peering connections.
- Ensure that your VPCs do not have overlapping IPv4 CIDR blocks. If they overlap, the status of the VPC peering connection immediately goes to `failed`. This limitation applies even if the VPCs have unique IPv6 CIDR blocks.

Create with VPCs in the same account and Region

To create a VPC peering connection with VPCs in the same account and Region

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Peering connections**.

3. Choose **Create peering connection**.
4. Configure the following information, and choose **Create Peering Connection** when you are done:
   - **Peering connection name tag**: You can optionally name your VPC peering connection.
   - **VPC (Requester)**: Select the VPC in your account with which you want to create the VPC peering connection.
   - Under **Select another VPC to peer with**: Ensure **My account** is selected, and select another of your VPCs.
   - (Optional) To add a tag, choose **Add new tag** and enter the tag key and value.
5. In the confirmation dialog box, choose **OK**.
6. Select the VPC peering connection that you've created, and choose **Actions**, **Accept Request**.
7. In the confirmation dialog, choose **Yes, Accept**. A second confirmation dialog displays; choose **Modify my route tables now** to go directly to the route tables page, or choose **Close** to do this later.

Create with VPCs in the same account and different Regions

To create a VPC peering connection with VPCs in the same account and different Regions

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Peering connections**.
3. Choose **Create peering connection**.
4. Configure the following information, and choose **Create Peering Connection** when you are done:
   - **Peering connection name tag**: You can optionally name your VPC peering connection. Doing so creates a tag with a key of `Name` and a value that you specify.
   - **VPC (Requester)**: Select the requester VPC in your account with which to request the VPC peering connection.
   - **Account**: Ensure **My account** is selected.
   - **Region**: Choose **Another region**, select the Region in which the accepter VPC resides.
   - **VPC (Accepter)**: Enter the ID of the accepter VPC.
5. In the confirmation dialog box, choose **OK**.
6. In the Region selector, select the Region of the accepter VPC.
7. In the navigation pane, choose **Peering Connections**. Select the VPC peering connection that you've created, and choose **Actions**, **Accept Request**.
8. In the confirmation dialog, choose **Yes, Accept**. A second confirmation dialog displays; choose **Modify my route tables now** to go directly to the route tables page, or choose **Close** to do this later.

Create with VPCs in different accounts and the same Region

To request a VPC peering connection with VPCs in different accounts and the same Region

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Peering connections**.
3. Choose **Create peering connection**.
4. Configure the information as follows, and choose **Create Peering Connection** when you are done:

- **Peering connection name tag**: You can optionally name your VPC peering connection. Doing so creates a tag with a key of `Name` and a value that you specify. This tag is only visible to you; the owner of the peer VPC can create their own tags for the VPC peering connection.
- **VPC (Requester)**: Select the VPC in your account with which to create the VPC peering connection.
- **Account**: Choose **Another account**.
- **Account ID**: Enter the Amazon account ID of the owner of the accepter VPC.
- **VPC (Accepter)**: Enter the ID of the VPC with which to create the VPC peering connection.

5. In the confirmation dialog box, choose **OK**.

Create with VPCs in different accounts and Regions

To request a VPC peering connection with VPCs in different accounts and Regions

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Peering connections**.
3. Choose **Create peering connection**.
4. Configure the information as follows, and choose **Create Peering Connection** when you are done:

   - **Peering connection name tag**: You can optionally name your VPC peering connection. Doing so creates a tag with a key of `Name` and a value that you specify. This tag is only visible to you; the owner of the peer VPC can create their own tags for the VPC peering connection.
   - **VPC (Requester)**: Select the VPC in your account with which to create the VPC peering connection.
   - **Account**: Choose **Another account**.
   - **Account ID**: Enter the Amazon account ID of the owner of the accepter VPC.
   - **Region**: Choose **Another region**, select the Region in which the accepter VPC resides.
   - **VPC (Accepter)**: Enter the ID of the VPC with which to create the VPC peering connection.

5. In the confirmation dialog box, choose **OK**.

Create a VPC peering connection using the command line

You can create a VPC peering connection using the following commands:

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

Accept a VPC peering connection

A VPC peering connection that's in the `pending-acceptance` state must be accepted by the owner of the accepter VPC to be activated. You cannot accept a VPC peering connection request that you've sent to another Amazon account. If you are creating a VPC peering connection in the same Amazon account, you must both create and accept the request yourself.

If the VPCs are in different Regions, the request must be accepted in the Region of the accepter VPC.

Important
Do not accept VPC peering connections from unknown Amazon accounts. A malicious user may have sent you a VPC peering connection request to gain unauthorized network access to your

VPC. This is known as peer phishing. You can safely reject unwanted VPC peering connection requests without any risk of the requester gaining access to any information about your Amazon account or your VPC. For more information, see Reject a VPC peering connection (p. 10). You can also ignore the request and let it expire; by default, requests expire after 7 days.

After you accept the VPC peering connection, you must add an entry to your route tables to enable traffic between the peered VPCs. For more information, see Update your route tables for a VPC peering connection (p. 11).

To accept a VPC peering connection

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. Use the Region selector to choose the Region of the accepter VPC.
3. In the navigation pane, choose **Peering connections**.
4. Select the pending VPC peering connection (the status is `pending-acceptance`), and choose **Actions**, **Accept Request**.

   Note
   If you cannot see the pending VPC peering connection, check the Region. An inter-Region peering request must be accepted in the Region of the accepter VPC.
5. In the confirmation dialog box, choose **Yes, Accept**. A second confirmation dialog displays; choose **Modify my route tables now** to go directly to the route tables page, or choose **Close** to do this later.

Now that your VPC peering connection is active, you must add an entry to your VPC route table to enable traffic to be directed to the peer VPC. For more information, see Update your route tables for a VPC peering connection (p. 11).

To accept a VPC peering connection using the command line or an API

- accept-vpc-peering-connection (Amazon CLI)
- Approve-EC2VpcPeeringConnection (Amazon Tools for Windows PowerShell)
- AcceptVpcPeeringConnection (Amazon EC2 Query API)

Reject a VPC peering connection

You can reject any VPC peering connection request that you've received that's in the `pending-acceptance` state. You should only accept VPC peering connections from Amazon accounts that you know and trust; you can reject any unwanted requests.

To reject a VPC peering connection

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Peering connections**.
3. Select the VPC peering connection, and choose **Actions**, **Reject Request**.
4. In the confirmation dialog box, choose **Yes, Reject**.

To reject a VPC peering connection using the command line or an API

- reject-vpc-peering-connection (Amazon CLI)
- Deny-EC2VpcPeeringConnection (Amazon Tools for Windows PowerShell)
- RejectVpcPeeringConnection (Amazon EC2 Query API)

View your VPC peering connections

You can view all of your VPC peering connections in the Amazon VPC console. By default, the console displays all VPC peering connections in different states, including those that may have been recently deleted or rejected. For more information about the lifecycle of a VPC peering connection, see VPC peering connection lifecycle (p. 2).

To view your VPC peering connections

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Peering connections**.
3. All of your VPC peering connections are listed. Use the filter search bar to narrow your results.

To describe a VPC peering connection using the command line or an API

- describe-vpc-peering-connections (Amazon CLI)
- Get-EC2VpcPeeringConnections (Amazon Tools for Windows PowerShell)
- DescribeVpcPeeringConnections (Amazon EC2 Query API)

Update your route tables for a VPC peering connection

To enable private IPv4 traffic between instances in peered VPCs, you must add a route to the route tables associated with the subnets for both instances. The route destination is the CIDR block (or portion of the CIDR block) of the peer VPC and the target is the ID of the VPC peering connection. For more information, see Configure route tables in the *Amazon VPC User Guide*.

The following is an example of the route tables that enables communication between instances in two peered VPCs, VPC A and VPC B. Each table has a local route and a route that sends traffic for the peer VPC to the VPC peering connection.

Route table	Destination	Target
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-*11112222*
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-*11112222*

Similarly, if the VPCs in the VPC peering connection have associated IPv6 CIDR blocks, you can add routes that enable communication with the peer VPC over IPv6.

For more information about supported route table configurations for VPC peering connections, see VPC peering configurations (p. 19).

Considerations

- If you have a VPC peered with multiple VPCs that have overlapping or matching IPv4 CIDR blocks, ensure that your route tables are configured to avoid sending response traffic from your VPC to the

incorrect VPC. Amazon currently does not support unicast reverse path forwarding in VPC peering connections that checks the source IP of packets and routes reply packets back to the source. For more information, see Routing for response traffic (p. 35).

- Your account has a quota on the number of entries you can add per route table. If the number of VPC peering connections in your VPC exceeds the route table entry quota for a single route table, consider using multiple subnets that are each associated with a custom route table.
- You can add a route for a VPC peering connection that's in the `pending-acceptance` state. However, the route has a state of `blackhole`, and has no effect until the VPC peering connection is in the `active` state.

To add an IPv4 route for a VPC peering connection

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Route tables**.
3. Select the check box next to the route table that's associated with the subnet in which your instance resides.

   If you do not have a route table explicitly associated with that subnet, the main route table for the VPC is implicitly associated with the subnet.
4. Choose **Actions**, **Edit routes**.
5. Choose **Add route**.
6. For **Destination**, enter the IPv4 address range to which the network traffic in the VPC peering connection must be directed. You can specify the entire IPv4 CIDR block of the peer VPC, a specific range, or an individual IPv4 address, such as the IP address of the instance with which to communicate. For example, if the CIDR block of the peer VPC is `10.0.0.0/16`, you can specify a portion `10.0.0.0/24`, or a specific IP address `10.0.0.7/32`.
7. For **Target**, select the VPC peering connection, and then choose **Save changes**.

The owner of the peer VPC must also complete these steps to add a route to direct traffic back to your VPC through the VPC peering connection.

If you have resources in different Amazon Regions that use IPv6 addresses, you can create an inter-Region peering connection. You can then add an IPv6 route for communication between the resources.

To add an IPv6 route for a VPC peering connection

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Route tables**.
3. Select the check box next to the route table that's associated with the subnet in which your instance resides.

   Note
   If you do not have a route table associated with that subnet, select the main route table for the VPC, as the subnet then uses this route table by default.
4. Choose **Actions**, **Edit routes**.
5. Choose **Add route**.
6. For **Destination**, enter the IPv6 address range for the peer VPC. You can specify the entire IPv6 CIDR block of the peer VPC, a specific range, or an individual IPv6 address. For example, if the CIDR block of the peer VPC is `2001:db8:1234:1a00::/56`, you can specify a portion `2001:db8:1234:1a00::/64`, or a specific IP address `2001:db8:1234:1a00::123/128`.
7. For **Target**, select the VPC peering connection, and then choose **Save changes**.

For more information, see Route Tables in the *Amazon VPC User Guide*.

To add or replace a route using the command line or an API

- create-route (Amazon CLI)
- New-EC2Route (Amazon Tools for Windows PowerShell)
- CreateRoute (Amazon EC2 Query API)
- replace-route (Amazon CLI)
- Set-EC2Route (Amazon Tools for Windows PowerShell)
- ReplaceRoute (Amazon EC2 Query API)

Update your security groups to reference peer security groups

You can update the inbound or outbound rules for your VPC security groups to reference security groups in the peered VPC. Doing so allows traffic to flow to and from instances that are associated with the referenced security group in the peered VPC.

Requirements

- The peer VPC can be a VPC in your account, or a VPC in another Amazon account. To reference a security group in another Amazon account, include the account number in **Source** or **Destination** field; for example, `123456789012/sg-1a2b3c4d`.
- You cannot reference the security group of a peer VPC that's in a different Region. Instead, use the CIDR block of the peer VPC.
- To reference a security group in a peer VPC, the VPC peering connection must be in the `active` state.
- If you configure routes to forward the traffic between two instances in different subnets through a middlebox appliance, you must ensure that the security groups for both instances allow traffic to flow between the instances. The security group for each instance must reference the private IP address of the other instance, or the the CIDR range of the subnet that contains the other instance, as the source. If you reference the security group of the other instance as the source, this does not allow traffic to flow between the instances.

To update your security group rules using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Security groups**.
3. Select the security group, and choose **Inbound Rules** to modify the inbound rules or **Outbound Rules** to modify the outbound rules.
4. Choose **Edit**, **Add another rule**.
5. Specify the type, protocol, and port range as required. For **Source** (or **Destination** for an outbound rule), type the ID of the security group in the peer VPC if it is in the same Region or the CIDR block of the peer VPC if it is in a different Region.

   Note
   Security groups in a peer VPC are not automatically displayed.
6. Choose **Save**.

To update inbound rules using the command line

- authorize-security-group-ingress (Amazon CLI)
- Grant-EC2SecurityGroupIngress (Amazon Tools for Windows PowerShell)

- Revoke-EC2SecurityGroupIngress (Amazon Tools for Windows PowerShell)
- revoke-security-group-ingress (Amazon CLI)

To update outbound rules using the command line

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

For example, to update your security group `sg-aaaa1111` to allow inbound access over HTTP from `sg-bbbb2222` that's in a peer VPC, you can use the following Amazon CLI command:

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

After you've updated the security group rules, use the describe-security-groups command to view the referenced security group in your security group rules.

Identify your referenced security groups

To determine if your security group is being referenced in the rules of a security group in a peer VPC, use one of the following commands for one or more security groups in your account.

- describe-security-group-references (Amazon CLI)
- Get-EC2SecurityGroupReference (Amazon Tools for Windows PowerShell)
- DescribeSecurityGroupReferences (Amazon EC2 Query API)

In the following example, the response indicates that security group `sg-bbbb2222` is being referenced by a security group in VPC `vpc-aaaaaaaa`:

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

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

If the VPC peering connection is deleted, or if the owner of the peer VPC deletes the referenced security group, the security group rule becomes stale.

Work with stale security group rules

A stale security group rule is a rule that references a deleted security group in the same VPC or in a peer VPC, or that references a security group in a peer VPC for which the VPC peering connection has been deleted. When a security group rule becomes stale, it's not automatically removed from your security group—you must manually remove it. If a security group rule is stale because the VPC peering

connection was deleted, the rule will no longer be marked as stale if you create a new VPC peering connection with the same VPCs.

You can view and delete the stale security group rules for a VPC using the Amazon VPC console.

To view and delete stale security group rules

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Security groups**.
3. Choose **Actions**, **Manage stale rules**.
4. For **VPC**, choose the VPC with the stale rules.
5. Choose **Edit**.
6. Choose the **Delete** button next to the rule that you want to delete. Choose **Preview changes**, **Save rules**.

To describe your stale security group rules using the command line or an API

- describe-stale-security-groups (Amazon CLI)
- Get-EC2StaleSecurityGroup (Amazon Tools for Windows PowerShell)
- DescribeStaleSecurityGroups (Amazon EC2 Query API)

In the following example, VPC A (`vpc-aaaaaaaa`) and VPC B were peered, and the VPC peering connection was deleted. Your security group `sg-aaaa1111` in VPC A references `sg-bbbb2222` in VPC B. When you run the `describe-stale-security-groups` command for your VPC, the response indicates that security group `sg-aaaa1111` has a stale SSH rule that references `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"
        }
    ]
}
```

After you've identified the stale security group rules, you can delete them using the revoke-security-group-ingress or revoke-security-group-egress commands.

Modify VPC peering connection options

You can modify a VPC peering connection to do the following:

- Enable one or more EC2-Classic instances that are linked to your VPC via ClassicLink to communicate with instances in the peer VPC, or to enable instances in your VPC to communicate with linked EC2-Classic instances in the peer VPC. For more information, see VPC peering configurations with ClassicLink (p. 40). You cannot enable EC2-Classic instances to communicate with instances in a peer VPC over IPv6.
- Enable a VPC to resolve public IPv4 DNS hostnames to private IPv4 addresses when queried from instances in the peer VPC. For more information, see Enable DNS resolution for a VPC peering connection (p. 16).

Enable DNS resolution for a VPC peering connection

To enable a VPC to resolve public IPv4 DNS hostnames to private IPv4 addresses when queried from instances in the peer VPC, you must modify your existing peering connection.

Both VPCs must be enabled for DNS hostnames and DNS resolution.

You cannot enable DNS resolution support when you create a new peering connection. You can enable DNS resolution support for an existing peering connection that's in the `active` state.

To enable DNS resolution for a peering connection

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Peering connections**.
3. Select the VPC peering connection, and choose **Actions**, **Edit DNS Settings**.
4. To ensure that queries from the peer VPC resolve to private IP addresses in your local VPC, choose the option to enable DNS resolution for queries from the peer VPC. This option is **Requester DNS resolution** or **Accepter DNS resolution**, depending on whether the VPC is the requester or accepter VPC.
5. If the peer VPC is in the same Amazon account, you can enable DNS resolution for both VPCs in the peering connection.
6. Choose **Save**.
7. If the peer VPC is in a different Amazon account or a different Region, the owner of the peer VPC must sign into the VPC console, perform steps 2 through 4, and choose **Save**.

To enable DNS resolution using the command line or an API

- modify-vpc-peering-connection-options (Amazon CLI)
- Edit-EC2VpcPeeringConnectionOption (Amazon Tools for Windows PowerShell)
- ModifyVpcPeeringConnectionOptions (Amazon EC2 Query API)

You must modify the requester VPC peering options if you are the requester of the VPC peering connection, and you must modify the accepter VPC peering options if you are the accepter of the VPC peering connection. You can use the describe-vpc-peering-connections or Get-EC2VpcPeeringConnections commands to verify which VPC is the accepter and the requester for a VPC

peering connection. For inter-Region peering connections, you must use the Region for the requester VPC to modify the requester VPC peering options and the Region for the accepter VPC to modify the accepter VPC peering options.

In this example, you are the requester of the VPC peering connection, therefore modify the peering connection options using the Amazon CLI as follows:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb --
requester-peering-connection-options AllowDnsResolutionFromRemoteVpc=true
```

Delete a VPC peering connection

Either owner of a VPC in a peering connection can delete the VPC peering connection at any time. You can also delete a VPC peering connection that you've requested that is still in the `pending-acceptance` state.

You cannot delete the VPC peering connection when the VPC peering connection is in the `rejected` state. We automatically delete the connection for you.

Deleting a VPC in the Amazon VPC console that's part of an active VPC peering connection also deletes the VPC peering connection. If you have requested a VPC peering connection with a VPC in another account, and you delete your VPC before the other party has accepted the request, the VPC peering connection is also deleted. You cannot delete a VPC for which you have a `pending-acceptance` request from a VPC in another account. You must first reject the VPC peering connection request.

When you delete a peering connection, the status is set to `Deleted`. When the connection is in this state, you cannot accept, reject, or edit the DNS settings.

To delete a VPC peering connection

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Peering connections**.
3. Select the VPC peering connection.
4. Choose **Actions**, **Delete peering connection**.
5. In the confirmation dialog box, choose **Yes, Delete**.

To delete a VPC peering connection using the command line or an API

- delete-vpc-peering-connection (Amazon CLI)
- Remove-EC2VpcPeeringConnection (Amazon Tools for Windows PowerShell)
- DeleteVpcPeeringConnection (Amazon EC2 Query API)

Troubleshoot a VPC peering connection

If you're having trouble connecting to a resource in a VPC from a resource in a peer VPC, do the following:

- For each resource in each VPC, verify that the route table for its subnet contains a route that sends traffic destined for the peer VPC to the VPC peering connection. For more information, see Update route tables (p. 11).
- For EC2 instances, verify that the security groups for the EC2 instances allow traffic from the peer VPC. For more information, see Reference peer security groups (p. 13).

- For each resource in each VPC, verify that the network ACL for its subnet allows traffic from the peer VPC.

You can also use VPC Reachability Analyzer to identify the component with a configuration issue, such as a route table, security group, or network ACL. For more information, see the VPC Reachability Analyzer Guide.

VPC peering configurations

The following documentation describes supported VPC peering configurations.

Configurations

VPC peering configurations with routes to an entire VPC

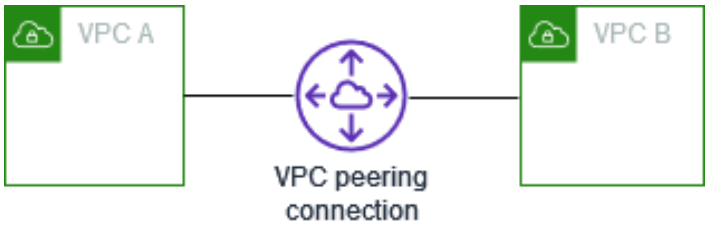
You can configure VPC peering connections so that your route tables have access to the entire CIDR block of the peer VPC. For more information about scenarios in which you might need a specific VPC peering connection configuration, see VPC peering scenarios (p. 45). For more information about creating and working with VPC peering connections, see Work with VPC peering connections (p. 7).

For more information about updating your route tables, see Update your route tables for a VPC peering connection (p. 11).

Configurations

Two VPCs peered together

In this configuration, you have a VPC peering connection, pcx-11112222, between VPC A and VPC B, which are in the same Amazon Web Services account, and do not have overlapping CIDR blocks.



You might use this configuration when you have two VPCs that require access to each others' resources. For example, you set up VPC A for your accounting records and VPC B for your financial records, and these each VPC must be able to access resources from the other VPC without restriction.

Single VPC CIDR

Update the route table for each VPC with a route that sends traffic for the CIDR block of the peer VPC to the VPC peering connection.

Route table	Destination	Target
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-11112222
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-11112222

Multiple IPv4 VPC CIDRs

If VPC A and VPC B have multiple associated IPv4 CIDR blocks, you can update the route table for each VPC with routes for some or all of the IPv4 CIDR blocks of the peer VPC.

Route table	Destination	Target
VPC A	*VPC A CIDR 1*	Local
	VPC A CIDR 2	Local
	VPC B CIDR 1	pcx-11112222
	VPC B CIDR 2	pcx-11112222
VPC B	*VPC B CIDR 1*	Local
	VPC B CIDR 2	Local
	VPC A CIDR 1	pcx-11112222
	VPC A CIDR 2	pcx-11112222

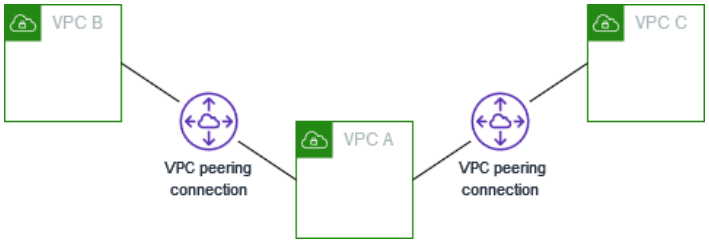
IPv4 and IPv6 VPC CIDRs

If VPC A and VPC B have associated IPv6 CIDR blocks, you can update the route table for each VPC with routes for both the IPv4 and IPv6 CIDR blocks of the peer VPC.

Route table	Destination	Target
VPC A	*VPC A IPv4 CIDR*	Local
	VPC A IPv6 CIDR	Local
	VPC B IPv4 CIDR	pcx-11112222
	VPC B IPv6 CIDR	pcx-11112222
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-11112222
	VPC A IPv6 CIDR	pcx-11112222

One VPC peered with two VPCs

In this configuration, you have a central VPC (VPC A), a VPC peering connection between VPC A and VPC B (pcx-12121212), and a VPC peering connection between VPC A and VPC C (pcx-23232323). All three VPCs are in the same Amazon Web Services account, and do not have overlapping CIDR blocks.



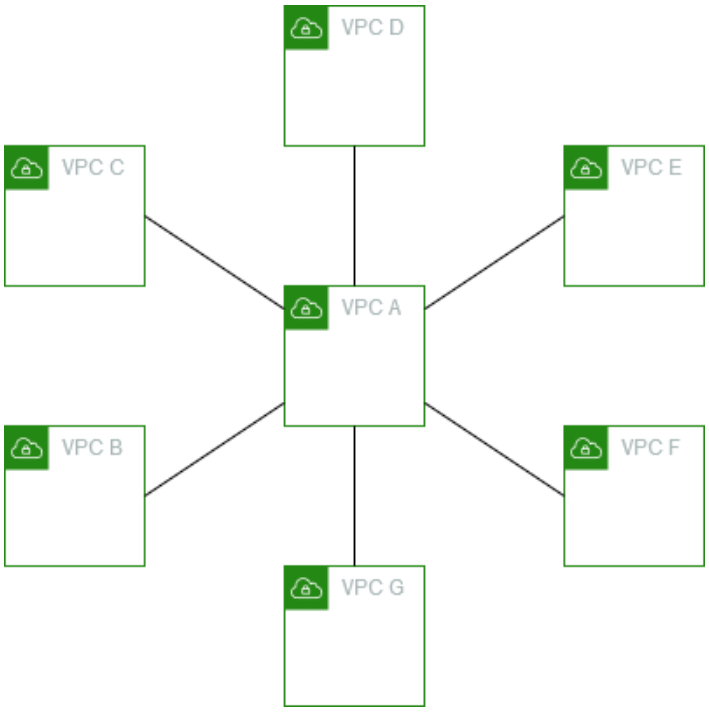
You might use this configuration when you have resources on a central VPC, such as a repository of services, that other VPCs need to access. The other VPCs do not need access to each others' resources; they only need to access resources in the central VPC.

> **Note**
> Spoke VPCs can't send traffic directly to each other through a hub VPC, because VPC peering does not support transitive peering relationships. You can create a VPC peering connection between VPC B and VPC C, as shown in Three VPCs peered together (p. 23). For more information about unsupported peering scenarios, see the section called "VPC peering limitations" (p. 4).

Update the route table for each VPC as follows to implement this configuration using one CIDR block per VPC.

Route table	Destination	Target
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-12121212
	VPC C CIDR	pcx-23232323
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-12121212
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-23232323

You can extend this configuration to additional VPCs. For example, VPC A is peered with VPC B through VPC G using both IPv4 and IPv6 CIDRs, but the other VPCs are not peered to each other. In this diagram, the lines represent VPC peering connections.



Update the route table as follows.

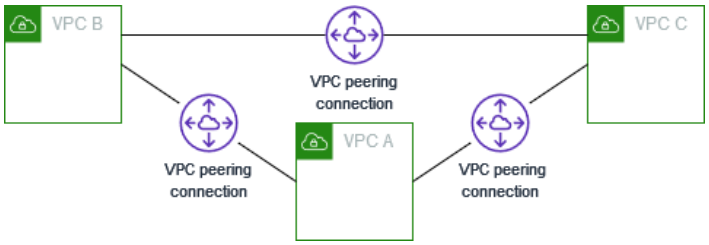
Route table	Destination	Target
VPC A	*VPC A IPv4 CIDR*	Local
	VPC A IPv6 CIDR	Local
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local

Route table	Destination	Target
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
VPC C	*VPC C IPv4 CIDR*	Local
	VPC C IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
VPC D	*VPC D IPv4 CIDR*	Local
	VPC D IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
VPC E	*VPC E IPv4 CIDR*	Local
	VPC E IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaaeeee
	VPC A IPv6 CIDR	pcx-aaaaeeee
VPC F	*VPC F IPv4 CIDR*	Local
	VPC F IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
VPC G	*VPC G IPv4 CIDR*	Local
	VPC G IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg

Three VPCs peered together

In this configuration, you have peered three VPCs together in a full mesh configuration. The VPCs are in the same Amazon Web Services account and do not have overlapping CIDR blocks:

- VPC A is peered to VPC B through VPC peering connection `pcx-aaaabbbb`
- VPC A is peered to VPC C through VPC peering connection `pcx-aaaacccc`
- VPC B is peered to VPC C through VPC peering connection `pcx-bbbbcccc`



You might use this full mesh configuration when you have VPCs that need to share resources with each other without restriction. For example, as a file sharing system.

Update the route table for each VPC as follows to implement this configuration.

Route table	Destination	Target
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc

If VPC A and VPC B have both IPv4 and IPv6 CIDR blocks, but VPC C does not have an IPv6 CIDR block, update the route tables as follows. Resources in VPC A and VPC B can communicate using IPv6 over the VPC peering connection. However, VPC C cannot communicate with either VPC A or VPC B using IPv6.

Route tables	Destination	Target
VPC A	*VPC A IPv4 CIDR*	Local
	VPC A IPv6 CIDR	Local
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc

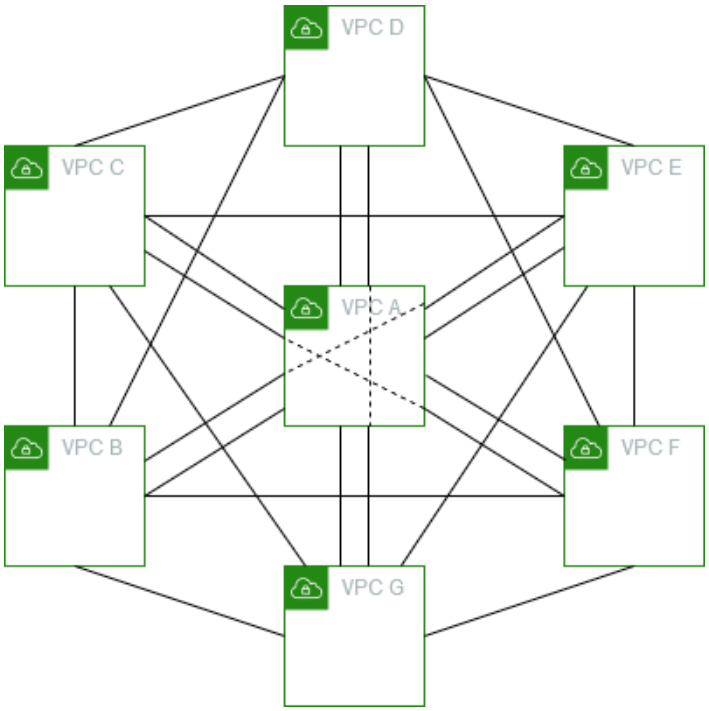
Route tables	Destination	Target
VPC C	*VPC C IPv4 CIDR*	Local
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc

Multiple VPCs peered together

In this configuration, you have seven VPCs peered in a full mesh configuration. The VPCs are in the same Amazon account and do not have overlapping CIDR blocks.

VPC	VPC	VPC peering connection
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
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

You might use this full mesh configuration when you have multiple VPCs that must be able to access each others' resources without restriction. For example, as a file sharing network. In this diagram, the lines represent VPC peering connections.



Update the route table for each VPC as follows to implement this configuration.

Route table	Destination	Target
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	VPC D CIDR	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-bbbbdddd
	VPC E CIDR	pcx-bbbbeeee
	VPC F CIDR	pcx-bbbbffff
	VPC G CIDR	pcx-bbbbgggg

Route table	Destination	Target
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-cccceeee
	VPC F CIDR	pcx-ccccffff
	VPC G CIDR	pcx-ccccgggg
VPC D	*VPC D CIDR*	Local
	VPC A CIDR	pcx-aaaadddd
	VPC B CIDR	pcx-bbbbdddd
	VPC C CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-ddddffff
	VPC G CIDR	pcx-ddddgggg
VPC E	*VPC E CIDR*	Local
	VPC A CIDR	pcx-aaaaeeee
	VPC B CIDR	pcx-bbbbeeee
	VPC C CIDR	pcx-cccceeee
	VPC D CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-eeeegggg
VPC F	*VPC F CIDR*	Local
	VPC A CIDR	pcx-aaaaffff
	VPC B CIDR	pcx-bbbbffff
	VPC C CIDR	pcx-ccccffff
	VPC D CIDR	pcx-ddddffff
	VPC E CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-ffffgggg
VPC G	*VPC G CIDR*	Local
	VPC A CIDR	pcx-aaaagggg
	VPC B CIDR	pcx-bbbbgggg

Route table	Destination	Target
	VPC C CIDR	pcx-ccccgggg
	VPC D CIDR	pcx-ddddgggg
	VPC E CIDR	pcx-eeeegggg
	VPC F CIDR	pcx-ffffgggg

If all VPCs have associated IPv6 CIDR blocks, update the route tables as follows.

Route table	Destination	Target
VPC A	*VPC A IPv4 CIDR*	Local
	VPC A IPv6 CIDR	Local
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPC B	*VPC B IPv4 CIDR*	Local
	VPC B IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc
	VPC C IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-bbbbdddd
	VPC D IPv6 CIDR	pcx-bbbbdddd
	VPC E IPv4 CIDR	pcx-bbbbeeee
	VPC E IPv6 CIDR	pcx-bbbbeeee

Route table	Destination	Target
	VPC F IPv4 CIDR	pcx-bbbbffff
	VPC F IPv6 CIDR	pcx-bbbbffff
	VPC G IPv4 CIDR	pcx-bbbbgggg
	VPC G IPv6 CIDR	pcx-bbbbgggg
VPC C	*VPC C IPv4 CIDR*	Local
	VPC C IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc
	VPC B IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-ccccdddd
	VPC D IPv6 CIDR	pcx-ccccdddd
	VPC E IPv4 CIDR	pcx-cccceeee
	VPC E IPv6 CIDR	pcx-cccceeee
	VPC F IPv4 CIDR	pcx-ccccffff
	VPC F IPv6 CIDR	pcx-ccccffff
	VPC G IPv4 CIDR	pcx-ccccgggg
	VPC G IPv6 CIDR	pcx-ccccgggg
VPC D	*VPC D IPv4 CIDR*	Local
	VPC D IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
	VPC B IPv4 CIDR	pcx-bbbbdddd
	VPC B IPv6 CIDR	pcx-bbbbdddd
	VPC C IPv4 CIDR	pcx-ccccdddd
	VPC C IPv6 CIDR	pcx-ccccdddd
	VPC E IPv4 CIDR	pcx-ddddeeee
	VPC E IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-ddddffff
	VPC F IPv6 CIDR	pcx-ddddffff
	VPC G IPv4 CIDR	pcx-ddddgggg

Route table	Destination	Target
	VPC G IPv6 CIDR	pcx-ddddgggg
VPC E	*VPC E IPv4 CIDR*	Local
	VPC E IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaaeeee
	VPC A IPv6 CIDR	pcx-aaaaeeee
	VPC B IPv4 CIDR	pcx-bbbbeeee
	VPC B IPv6 CIDR	pcx-bbbbeeee
	VPC C IPv4 CIDR	pcx-cccceeee
	VPC C IPv6 CIDR	pcx-cccceeee
	VPC D IPv4 CIDR	pcx-ddddeeee
	VPC D IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-eeeeffff
	VPC F IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-eeeegggg
	VPC G IPv6 CIDR	pcx-eeeegggg
VPC F	*VPC F IPv4 CIDR*	Local
	VPC F IPv6 CIDR	Local
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
	VPC B IPv4 CIDR	pcx-bbbbffff
	VPC B IPv6 CIDR	pcx-bbbbffff
	VPC C IPv4 CIDR	pcx-ccccffff
	VPC C IPv6 CIDR	pcx-ccccffff
	VPC D IPv4 CIDR	pcx-ddddffff
	VPC D IPv6 CIDR	pcx-ddddffff
	VPC E IPv4 CIDR	pcx-eeeeffff
	VPC E IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-ffffgggg
	VPC G IPv6 CIDR	pcx-ffffgggg
VPC G	*VPC G IPv4 CIDR*	Local
	VPC G IPv6 CIDR	Local

Route table	Destination	Target
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg
	VPC B IPv4 CIDR	pcx-bbbbgggg
	VPC B IPv6 CIDR	pcx-bbbbgggg
	VPC C IPv4 CIDR	pcx-ccccgggg
	VPC C IPv6 CIDR	pcx-ccccgggg
	VPC D IPv4 CIDR	pcx-ddddgggg
	VPC D IPv6 CIDR	pcx-ddddgggg
	VPC E IPv4 CIDR	pcx-eeeegggg
	VPC E IPv6 CIDR	pcx-eeeegggg
	VPC F IPv4 CIDR	pcx-ffffgggg
	VPC F IPv6 CIDR	pcx-ffffgggg

VPC peering configurations with specific routes

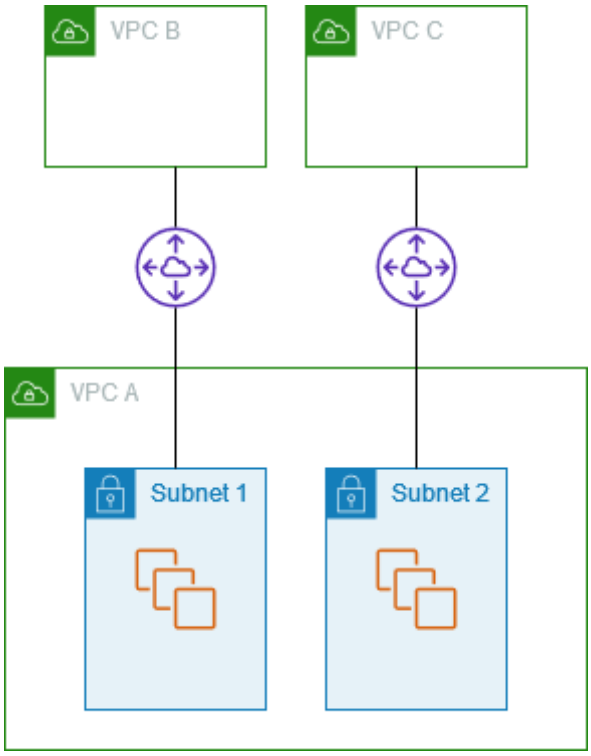
You can configure a VPC peering connections to provide access to part of the CIDR block, a specific CIDR block (if the VPC has multiple CIDR blocks) or a specific instance within the peer VPC. In these examples, a central VPC is peered to two or more VPCs that have overlapping CIDR blocks. For examples of scenarios in which you might need a specific VPC peering connection configuration, see VPC peering scenarios (p. 45). For more information about creating and working with VPC peering connections, see Work with VPC peering connections (p. 7). For more information about updating your route tables, see Update your route tables for a VPC peering connection (p. 11).

Configurations

- Two VPCs peered to two subnets in one VPC (p. 31)
- Two VPCs peered to two different CIDR blocks in one VPC (p. 33)
- One VPC peered to specific subnets in two VPCs (p. 34)
- Instances in one VPC peered to instances in two VPCs (p. 36)
- One VPC peered with two VPCs using longest prefix match (p. 37)
- Multiple VPC configurations (p. 38)

Two VPCs peered to two subnets in one VPC

You have a central VPC (VPC A), and you have a VPC peering connection between VPC A and VPC B (`pcx-aaaabbbb`), and between VPC A and VPC C (`pcx-aaaacccc`). VPC A has two subnets: one for each VPC peering connection.



Use this configuration when you have a central VPC with separate sets of resources in different subnets. Other VPCs may require access to some of the resources, but not all of them.

The route table for subnet 1 points to VPC peering connection `pcx-aaaabbbb` to access the entire CIDR block of VPC B. VPC B's route table points to `pcx-aaaabbbb` to access the CIDR block of only subnet 1 in VPC A. Similarly, the route table for subnet 2 points to VPC peering connection `pcx-aaaacccc` to access the entire CIDR block of VPC C. VPC C's route table points to `pcx-aaaacccc` to access the CIDR block of only subnet 2 in VPC A.

Route table	Destination	Target
Subnet 1 in VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
Subnet 2 in VPC A	*VPC A CIDR*	Local
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	Subnet 1 CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	Subnet 2 CIDR	pcx-aaaacccc

You can extend this configuration to multiple CIDR blocks. Suppose that VPC A and VPC B have both IPv4 and IPv6 CIDR blocks, and that subnet 1 has an associated IPv6 CIDR block. You can enable VPC B to communicate with subnet 1 in VPC A over IPv6 using the VPC peering connection. To do this, add a route

to the route table for VPC A with a destination of the IPv6 CIDR block for VPC B, and a route to the route table for VPC B with a destination of the IPv6 CIDR of subnet 1 in VPC A.

Route table	Destination	Target	Notes
Subnet 1 in VPC A	*VPC A IPv4 CIDR*	Local	
	VPC A IPv6 CIDR	Local	Local route that's automatically added for IPv6 communication within the VPC.
	VPC B IPv4 CIDR	pcx-aaaabbbb	
	VPC B IPv6 CIDR	pcx-aaaabbbb	Route to the IPv6 CIDR block of VPC B.
Subnet 2 in VPC A	*VPC A IPv4 CIDR*	Local	
	VPC A IPv6 CIDR	Local	Local route that's automatically added for IPv6 communication within the VPC.
	VPC C IPv4 CIDR	pcx-aaaacccc	
VPC B	*VPC B IPv4 CIDR*	Local	
	VPC B IPv6 CIDR	Local	Local route that's automatically added for IPv6 communication within the VPC.
	Subnet 1 IPv4 CIDR	pcx-aaaabbbb	
	Subnet 2 IPv4 CIDR	pcx-aaaabbbb	Route to the IPv6 CIDR block of VPC A.
VPC C	*VPC C IPv4 CIDR*	Local	
	Subnet 2 IPv4 CIDR	pcx-aaaacccc	

Two VPCs peered to two different CIDR blocks in one VPC

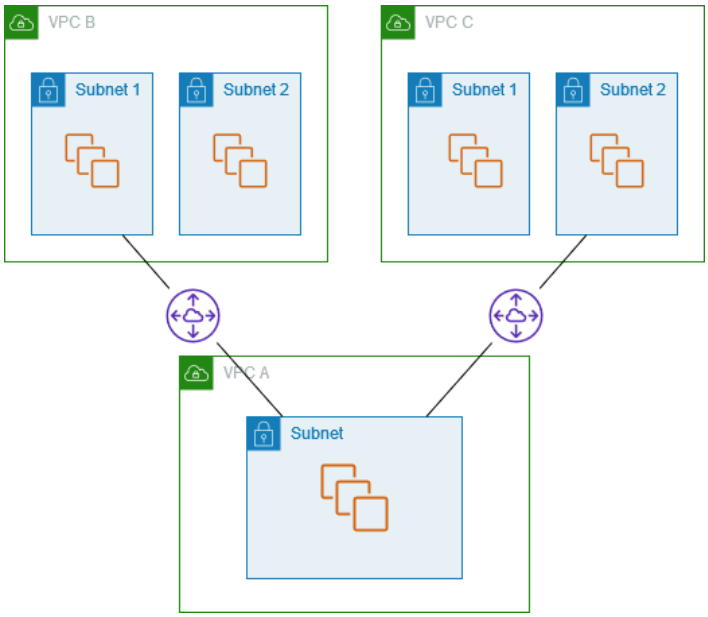
You have a central VPC (VPC A), and you have a VPC peering connection between VPC A and VPC B (`pcx-aaaabbbb`), and between VPC A and VPC C (`pcx-aaaacccc`). VPC A has two CIDR blocks; one for each VPC peering connection.

Route table	Destination	Target
VPC A	*VPC A CIDR 1*	Local
	VPC A CIDR 2	Local
	VPC B CIDR	pcx-aaaabbbb

Route table	Destination	Target
	VPC C CIDR	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	VPC A CIDR 1	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	VPC A CIDR 2	pcx-aaaacccc

One VPC peered to specific subnets in two VPCs

You have a central VPC (VPC A) with one subnet, and you have a VPC peering connection between VPC A and VPC B (`pcx-aaaabbbb`), and between VPC A and VPC C (`pcx-aaaacccc`). VPC B and VPC C each have two subnets, and only one in each is used for the peering connection with VPC A.



Use this configuration when you have a central VPC that has a single set of resources, such as Active Directory services, that other VPCs need to access. The central VPC does not require full access to the VPCs that it's peered with.

The route table for VPC A points to both VPC peering connections to access only specific subnets in VPC B and VPC C. The route tables for the subnets in VPC B and VPC C point to their VPC peering connections to access the VPC A subnet.

Route table	Destination	Target
VPC A	*VPC A CIDR*	Local
	Subnet 1 in VPC B CIDR	pcx-aaaabbbb
	Subnet 2 in VPC C CIDR	pcx-aaaacccc
Subnet 1 in VPC B	*VPC B CIDR*	Local

Route table	Destination	Target
	Subnet in VPC A CIDR	pcx-aaaabbbb
Subnet 2 in VPC C	*VPC C CIDR*	Local
	Subnet in VPC A CIDR	pcx-aaaacccc

Routing for response traffic

If you have a VPC peered with multiple VPCs that have overlapping or matching CIDR blocks, ensure that your route tables are configured to avoid sending response traffic from your VPC to the incorrect VPC. Amazon currently does not support unicast reverse path forwarding in VPC peering connections that checks the source IP of packets and routes reply packets back to the source.

For example, VPC A is peered with VPC B and VPC C. VPC B and VPC C have matching CIDR blocks, and their subnets have matching CIDR blocks. The route table for subnet 2 in VPC B points to the VPC peering connection `pcx-aaaabbbb` to access the VPC A subnet. The VPC A route table is configured to send traffic destined for the VPC CIDR to peering connection `pcx-aaaaccccc`.

Route table	Destination	Target
Subnet 2 in VPC B	*VPC B CIDR*	Local
	Subnet in VPC A CIDR	pcx-aaaabbbb
VPC A	*VPC A CIDR*	Local
	VPC C CIDR	pcx-aaaacccc

Suppose that an instance in subnet 2 in VPC B sends traffic to the Active Directory server in VPC A using VPC peering connection `pcx-aaaabbbb`. VPC A sends the response traffic to Active Directory server. However, the VPC A route table is configured to send all traffic within the VPC CIDR range to VPC peering connection `pcx-aaaacccc`. If subnet 2 in VPC C has an instance with the same IP address as the instance in subnet two of VPC B, it receives the response traffic from VPC A. The instance in subnet 2 in VPC B does not receive a response to its request to VPC A.

To prevent this, you can add a specific route to the VPC A route table with the CIDR of subnet 2 in VPC B as the destination and a target of `pcx-aaaabbbb`. The new route is more specific, therefore traffic destined for the subnet 2 CIDR is routed to the VPC peering connection `pcx-aaaabbbb`

Alternatively, in the following example, the VPC A route table has a route for each subnet for each VPC peering connection. VPC A can communicate with subnet B in VPC B and with subnet A in VPC C. This scenario is useful if you need to add another VPC peering connection with another subnet that falls within the same address range as VPC B and VPC C —you can simply add another route for that specific subnet.

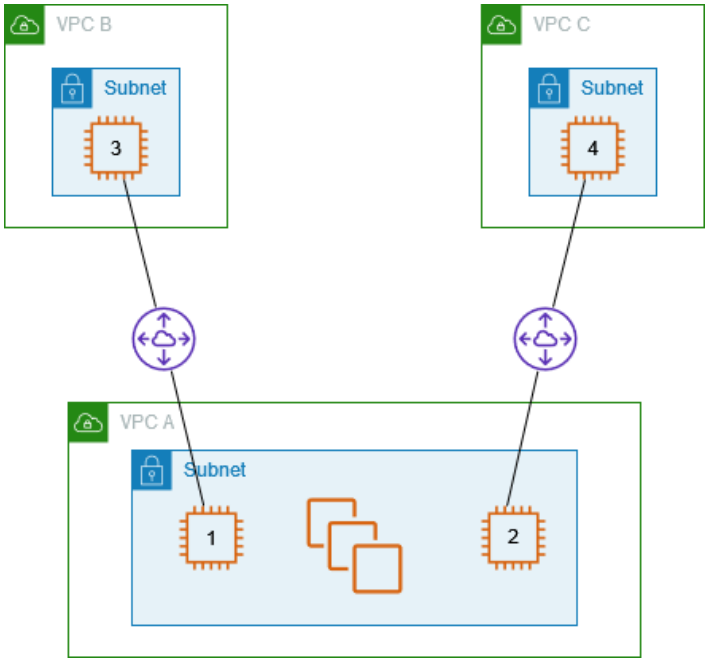
Destination	Target
VPC A CIDR	Local
Subnet 2 CIDR	pcx-aaaabbbb
Subnet 1 CIDR	pcx-aaaacccc

Alternatively, depending on your use case, you can create a route to a specific IP address in VPC B to ensure that traffic routed back to the correct server (the route table uses longest prefix match to prioritize the routes):

Destination	Target
VPC A CIDR	Local
Specific IP address in subnet 2	pcx-aaaabbbb
VPC B CIDR	pcx-aaaacccc

Instances in one VPC peered to instances in two VPCs

You have a central VPC (VPC A) with one subnet, and you have a VPC peering connection between VPC A and VPC B (`pcx-aaaabbbb`), and between VPC A and VPC C (`pcx-aaaacccc`). VPC A has one subnet that has multiple instances; one for each of the VPCs that it's peered with. You can use this configuration to limit peering traffic to specific instances.



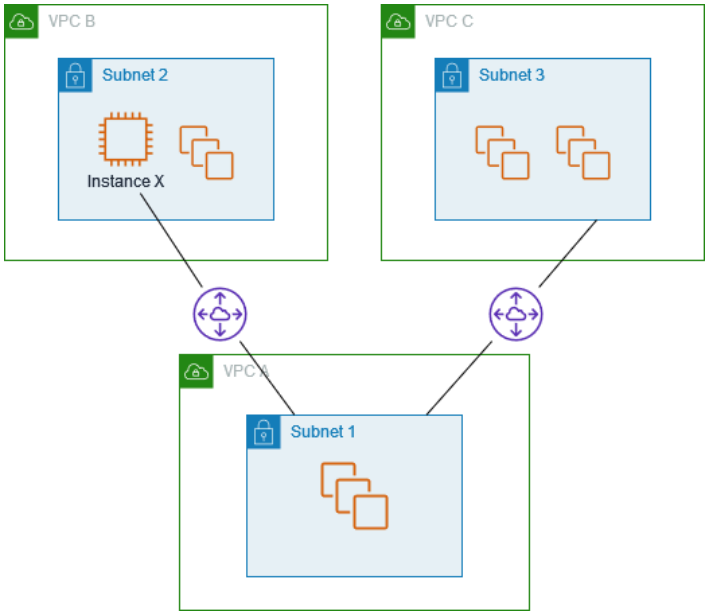
Each VPC route table points to the relevant VPC peering connection to access a single IP address (and therefore a specific instance) in the peer VPC.

Route table	Destination	Target
VPC A	*VPC A CIDR*	Local
	Instance 3 IP address	pcx-aaaabbbb
	Instance 4 IP address	pcx-aaaacccc
VPC B	*VPC B CIDR*	Local
	Instance 1 IP address	pcx-aaaabbbb

Route table	Destination	Target
VPC C	*VPC C CIDR*	Local
	Instance 2 IP address	pcx-aaaacccc

One VPC peered with two VPCs using longest prefix match

You have a central VPC (VPC A) with one subnet, a VPC peering connection between VPC A and VPC B (pcx-aaaabbbb), and a VPC peering connection between VPC A and VPC C (pcx-aaaacccc). VPC B and VPC C have matching CIDR blocks. You want to use VPC peering connection pcx-aaaabbbb to route traffic between VPC A and specific instance in VPC B. All other traffic destined for the CIDR address range shared by VPC B and VPC C is routed to VPC C through pcx-aaaacccc.



VPC route tables use longest prefix match to select the most specific route across the intended VPC peering connection. All other traffic is routed through the next matching route, in this case, across the VPC peering connection pcx-aaaacccc.

Route table	Destination	Target
VPC A	*VPC A CIDR block*	Local
	Instance X IP address	pcx-aaaabbbb
	VPC C CIDR block	pcx-aaaacccc
VPC B	*VPC B CIDR block*	Local
	VPC A CIDR block	pcx-aaaabbbb
VPC C	*VPC C CIDR block*	Local
	VPC A CIDR block	pcx-aaaacccc

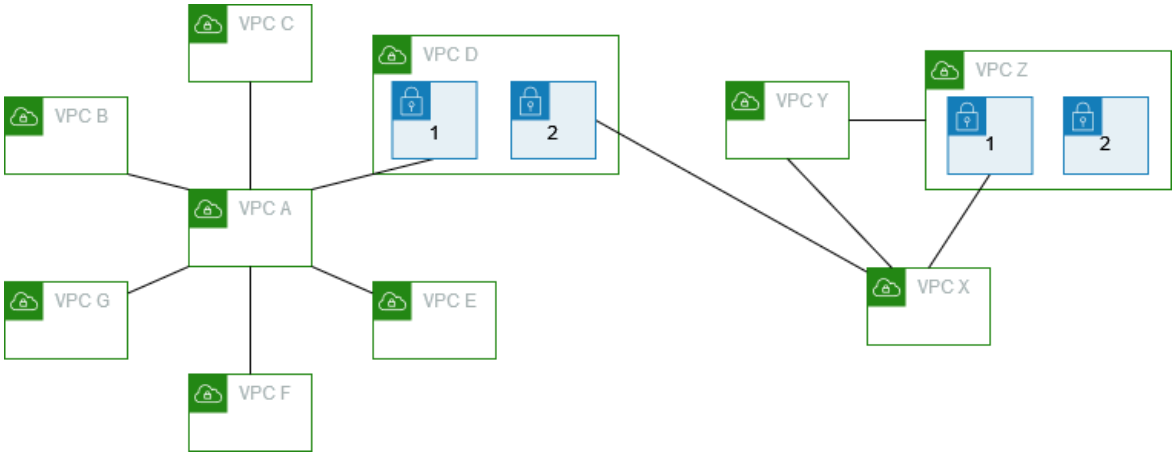
Important
If an instance other than instance X in VPC B sends traffic to VPC A, the response traffic may be routed to VPC C instead of VPC B. For more information, see Routing for response traffic (p. 35).

Multiple VPC configurations

In this example, a central VPC (VPC A) is peered with multiple VPCs in a spoke configuration. You also have three VPCs (VPCs X, Y, and Z) peered in a full mesh configuration.

VPC D also has a VPC peering connection with VPC X (`pcx-ddddxxxx`). VPC A and VPC X have overlapping CIDR blocks. This means that peering traffic between VPC A and VPC D is limited to a specific subnet (subnet 2) in VPC D. This is to ensure that if VPC D receives a request from VPC A or VPC X, it sends the response traffic to the correct VPC. Amazon currently does not support unicast reverse path forwarding in VPC peering connections that checks the source IP of packets and routes reply packets back to the source. For more information, see Routing for response traffic (p. 35).

Similarly, VPC D and VPC Z have overlapping CIDR blocks. Peering traffic between VPC D and VPC X is limited to subnet 2 in VPC D, and peering traffic between VPC X and VPC Z is limited to subnet 1 in VPC Z. This is to ensure that if VPC X receives peering traffic from VPC D or VPC Z, it sends the response traffic back to the correct VPC.



The route tables for VPCs B, C, E, F, and G point to the relevant peering connections to access the full CIDR block for VPC A, and the VPC A route table points to the relevant peering connections for VPCs B, C, E, F, and G to access their full CIDR blocks. For peering connection `pcx-aaaadddd`, the VPC A route table routes traffic only to subnet 1 in VPC D and the subnet 1 route table in VPC D points to the full CIDR block of VPC A.

The VPC Y route table points to the relevant peering connections to access the full CIDR blocks of VPC X and VPC Z, and the VPC Z route table points to the relevant peering connection to access the full CIDR block of VPC Y. The subnet 1 route table in VPC Z points to the relevant peering connection to access the full CIDR block of VPC Y. The VPC X route table points to the relevant peering connection to access subnet 2 in VPC D and subnet 1 in VPC Z.

Route table	Destination	Target
VPC A	*VPC A CIDR*	Local
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc

Route table	Destination	Target
	Subnet 1 CIDR in VPC D	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg
VPC B	*VPC B CIDR*	Local
	VPC A CIDR	pcx-aaaabbbb
VPC C	*VPC C CIDR*	Local
	VPC A CIDR	pcx-aaaacccc
Subnet 1 in VPC D	*VPC D CIDR*	Local
	VPC A CIDR	pcx-aaaadddd
Subnet 2 in VPC D	*VPC D CIDR*	Local
	VPC X CIDR	pcx-ddddxxxx
VPC E	*VPC E CIDR*	Local
	VPC A CIDR	pcx-aaaaeeee
VPC F	*VPC F CIDR*	Local
	VPC A CIDR	pcx-aaaaffff
VPC G	*VPC G CIDR*	Local
	VPC A CIDR	pcx-aaaagggg
VPC X	*VPC X CIDR*	Local
	Subnet 2 CIDR in VPC D	pcx-ddddxxxx
	VPC Y CIDR	pcx-xxxxyyyy
	Subnet 1 CIDR in VPC Z	pcx-xxxxzzzz
VPC Y	*VPC Y CIDR*	Local
	VPC X CIDR	pcx-xxxxyyyy
	VPC Z CIDR	pcx-yyyyzzzz
VPC Z	*VPC Z CIDR*	Local
	VPC Y CIDR	pcx-yyyyzzzz
	VPC X CIDR	pcx-xxxxzzzz

VPC peering configurations with ClassicLink

We are retiring EC2-Classic. We recommend that you migrate from EC2-Classic to a VPC.

If you have a VPC peering connection between two VPCs, and there are one or more EC2-Classic instances that are linked to one or both of the VPCs using ClassicLink, you can extend the VPC peering connection to enable communication between the EC2-Classic instances and the instances in the VPC on the other side of the VPC peering connection. This enables the EC2-Classic instances and the instances in the VPC to communicate using private IP addresses. To do this, you enable a local VPC to communicate with a linked EC2-Classic instance in a peer VPC, or you enable a local linked EC2-Classic instance to communicate with VPC instances in a peer VPC.

Communication over ClassicLink only works if both VPCs in the VPC peering connection are in the same Region.

Important
EC2-Classic instances cannot be enabled for IPv6 communication. You can enable VPC instances on either side of a VPC peering connection to communicate with each other over IPv6; however, an EC2-Classic instance that's ClassicLinked with a VPC can communicate with VPC instances on either side of the VPC peering connection over IPv4 only.

To enable your VPC peering connection for communication with linked EC2-Classic instances, you must modify the requester VPC peering options if you are the requester of the VPC peering connection, and you must modify the accepter VPC peering options if you are the accepter of the VPC peering connection. You can use the describe-vpc-peering-connections command to verify which VPC is the accepter and the requester for a VPC peering connection.

You can modify the VPC peering connection options as follows:

- **Enable a local linked EC2-Classic instance to communicate with instances in a peer VPC**

  In this case, you modify the VPC peering connection options to enable outbound communication from the local ClassicLink connection to the peer VPC on the other side of the VPC peering connection. The owner of the peer VPC modifies the VPC peering connection options to enable outbound communication from their local VPC to the remote ClassicLink connection.
- **Enable a local VPC to communicate with a linked EC2-Classic instance in a peer VPC**

  In this case, you modify the VPC peering connection options to enable outbound communication from your local VPC to the remote ClassicLink connection on the other side of the VPC peering connection. The owner of the peer VPC with the linked EC2-Classic instance modifies the VPC peering connection options to enable outbound communication from their local ClassicLink connection to the remote VPC.

When you enable a local linked EC2-Classic instance to communicate with instances in a peer VPC, you must manually add a route to the main route table of your local VPC with a destination of the peer VPC CIDR block, and a target of the VPC peering connection. The linked EC2-Classic instance is not associated with any subnet in the VPC; it relies on the main route table for communication with the peer VPC.

Important
The route for the VPC peering connection must be added to the main route table, regardless of any custom route tables with existing routes to the peering connection. If not, the EC2-Classic instance cannot communicate with the peer VPC.

When you enable a local VPC for communication with a remote ClassicLink connection, a route is automatically added to all the local VPC route tables with a destination of `10.0.0.0/8` and a target of

`Local`. This enables communication with the remote linked EC2-Classic instance. If your route table has an existing static route in the `10.0.0.0/8` IP address range (including VPC peering connection routes), you cannot enable the local VPC for communication with the remote ClassicLink connection.

Region Support

You can modify the VPC peering connection options in the following Regions:

- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Europe (Ireland)
- Asia Pacific (Tokyo)
- Asia Pacific (Singapore)
- South America (São Paulo)
- Asia Pacific (Sydney)

Enable communication between an EC2-Classic instance and a peer VPC

In this scenario, we have the following:

- VPC A is enabled for ClassicLink, and EC2-Classic instance A is linked to VPC A using ClassicLink.
- VPC B is in a different Amazon account, and is peered to VPC A using VPC peering connection `pcx-aaaabbbb`. The VPC peering connection was requested by VPC A and accepted by VPC B.
- VPC B can either be a VPC in an account that supports EC2-Classic, or an account that supports EC2-VPC only.

Use the following route tables so that instance A can communicate with instances in VPC B, and instances in VPC B can communicate with instance A.

Route table	Destination	Target	Notes
VPC A	*VPC A CIDR*	Local	Default local route for VPC A.
	VPC B CIDR	pcx-aaaabbbb	Route manually added for the peering connection between VPC A and VPC B.
	10.0.0.0/8	Local	Route automatically added to enable ClassicLink communication (added when you linked the instance to VPC A).
VPC B	*VPC B CIDR*	Local	Default local route for VPC B.

Route table	Destination	Target	Notes
	VPC A CIDR	pcx-aaaabbbb	Route manually added for the peering connection between VPC A and VPC B.

The owner of VPC A must modify the VPC peering connection to enable instance A to communicate with VPC B, and update the main route table. The owner of VPC B must modify the VPC peering connection to enable VPC B to communicate with instance A.

For more information about adding routes, see Adding and Removing Routes from a Route Table in the *Amazon VPC User Guide*.

Tasks

- Modify the VPC peering connection for VPC A (p. 42)
- Modify the VPC peering connection for VPC B (p. 42)
- View VPC peering connection options (p. 43)

Modify the VPC peering connection for VPC A

To enable communication from the EC2-Classic instance to VPC B, the Amazon account owner of VPC A must modify the VPC peering connection options to enable the local ClassicLink connection to send traffic to instances in the peer VPC.

To modify the VPC peering connection using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.

   The owner of VPC A must sign in to the console.
2. In the navigation pane, choose **Peering Connections**.
3. Select the VPC peering connection, and choose **Actions**, **Edit ClassicLink Settings**.
4. Choose the option to allow local linked EC2-Classic instances to communicate with the peer VPC, and choose **Save**.

To modify the VPC peering connection using the Amazon CLI

You can use the modify-vpc-peering-connection-options command. In this case, VPC A was the requester of the VPC peering connection; therefore, modify the requester options as follows:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb --
requester-peering-connection-options AllowEgressFromLocalClassicLinkToRemoteVpc=true
```

Modify the VPC peering connection for VPC B

Next, the Amazon account owner of VPC B must modify the VPC peering connection options to enable VPC B to send traffic to EC2-Classic instance A.

To modify the VPC peering connection using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.

   The owner of VPC B must sign in to the console.

2. In the navigation pane, choose **Peering Connections**.
3. Select the VPC peering connection, and choose **Actions**, **Edit ClassicLink Settings**.
4. Choose the option to allow local VPC instances to communicate with EC2-Classic instances in the peer VPC, and choose **Save**.

To modify the VPC peering connection using the Amazon CLI

VPC B accepted the VPC peering connection; therefore, modify the accepter options as follows:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb --
accepter-peering-connection-options AllowEgressFromLocalVpcToRemoteClassicLink=true
```

View VPC peering connection options

You can view the VPC peering connection options for the accepter VPC and requester VPC using the Amazon VPC console or the Amazon CLI.

To view VPC peering connection options using the console

1. Open the Amazon VPC console at https://console.amazonaws.cn/vpc/.
2. In the navigation pane, choose **Peering Connections**.
3. Select the VPC peering connection, and choose **ClassicLink**. Information about the enabled or disabled VPC peering connection options is displayed.

To view VPC peering connection options using the Amazon CLI

You can use the describe-vpc-peering-connections command:

```
aws ec2 describe-vpc-peering-connections --vpc-peering-connection-id pcx-aaaabbbb
```

```
{
    "VpcPeeringConnections": [
        {
            "Status": {
                "Message": "Active",
                "Code": "active"
            },
            "Tags": [
                {
                    "Value": "MyPeeringConnection",
                    "Key": "Name"
                }
            ],
            "AccepterVpcInfo": {
                "PeeringOptions": {
                    "AllowEgressFromLocalVpcToRemoteClassicLink": true,
                    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
                    "AllowDnsResolutionFromRemoteVpc": false
                },
                "OwnerId": "123456789101",
                "VpcId": "vpc-80cb52e4",
                "CidrBlock": "172.31.0.0/16"
            },
            "VpcPeeringConnectionId": "pcx-aaaabbbb",
            "RequesterVpcInfo": {
                "PeeringOptions": {
                    "AllowEgressFromLocalVpcToRemoteClassicLink": false,
```

```
                    "AllowEgressFromLocalClassicLinkToRemoteVpc": true,
                    "AllowDnsResolutionFromRemoteVpc": false
                },
                "OwnerId": "111222333444",
                "VpcId": "vpc-f527be91",
                "CidrBlock": "192.168.0.0/16"
            }
        }
    ]
}
```

VPC peering scenarios

There are a number of reasons you might need to set up a VPC peering connection between your VPCs, or between a VPC that you own and a VPC in a different Amazon account. The following scenarios can help you determine which configuration is best suited to your networking requirements.

Scenarios

Peering two or more VPCs to provide full access to resources

In this scenario, you have two or more VPCs that you want to peer to enable full sharing of resources between all VPCs. The following are some examples:

- Your company has a VPC for the finance department, and another VPC for the accounting department. The finance department requires access to all resources that are in the accounting department, and the accounting department requires access to all resources in the finance department.
- Your company has multiple IT departments, each with their own VPC. Some VPCs are located within the same Amazon account, and others in a different Amazon account. You want to peer together all VPCs to enable the IT departments to have full access to each others' resources.

For more information about how to set up the VPC peering connection configuration and route tables for this scenario, see the following documentation:

- Two VPCs peered together (p. 19)
- Three VPCs peered together (p. 23)
- Multiple VPCs peered together (p. 25)

For more information about creating and working with VPC peering connections in the Amazon VPC console, see Work with VPC peering connections (p. 7).

Peering to one VPC to access centralized resources

In this scenario, you have a central VPC that contains resources that you want to share with other VPCs. Your central VPC may require full or partial access to the peer VPCs, and similarly, the peer VPCs may require full or partial access to the central VPC. The following are some examples:

- Your company's IT department has a VPC for file sharing. You want to peer other VPCs to that central VPC, however, you do not want the other VPCs to send traffic to each other.
- Your company has a VPC that you want to share with your customers. Each customer can create a VPC peering connection with your VPC, however, your customers cannot route traffic to other VPCs that are peered to yours, nor are they aware of the other customers' routes.

- You have a central VPC that is used for Active Directory services. Specific instances in peer VPCs send requests to the Active Directory servers and require full access to the central VPC. The central VPC does not require full access to the peer VPCs; it only needs to route response traffic to the specific instances.

For more information about creating and working with VPC peering connections in the Amazon VPC console, see Work with VPC peering connections (p. 7).

Peering with ClassicLink

You can modify a VPC peering connection to enable one or more EC2-Classic instances that are linked to your VPC via ClassicLink to communicate with instances in the peer VPC. Similarly, you can modify a VPC peering connection to enable instances in your VPC to communicate with linked EC2-Classic instances in the peer VPC.

For more information about how to set up the VPC peering connection configuration and route tables for this scenario, see VPC peering configurations with ClassicLink (p. 40).

Identity and access management for VPC peering

By default, IAM users cannot create or modify VPC peering connections. To grant access to VPC peering resources, attach an IAM policy to an IAM identity, such as a user, group, or role.

Examples

For a list of Amazon VPC actions, and the supported resources and conditions keys for each action, see Actions, resources, and condition keys for Amazon EC2 in the *Service Authorization Reference*.

Example: Create a VPC peering connection

The following policy grants users permission to create VPC peering connection requests using VPCs that are tagged with `Purpose=Peering`. The first statement applies a condition key (`ec2:ResourceTag`) to the VPC resource. Note that the VPC resource for the `CreateVpcPeeringConnection` action is always the requester VPC.

The second statement grants users permission to create the VPC peering connection resources, and therefore uses the * wildcard in place of a specific resource ID.

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws-cn:ec2:region:account-id:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws-cn:ec2:region:account-id:vpc-peering-connection/*"
    }
  ]
}
```

The following policy grants users in the specified Amazon account permission to create VPC peering connections using any VPC in the specified Region, but only if the VPC that accepts the peering connection is a specific VPC in specific account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws-cn:ec2:region:account-id-1:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws-cn:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws-cn:ec2:region:account-id-2:vpc/vpc-id"
        }
      }
    }
  ]
}
```

Example: Accept a VPC peering connection

The following policy grants users permission to accept VPC peering connection requests from a specific Amazon account. This helps to prevent users from accepting VPC peering connection requests from unknown accounts. The statement uses the `ec2:RequesterVpc` condition key to enforce this.

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws-cn:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:RequesterVpc": "arn:aws-cn:ec2:region:account-id-2:vpc/*"
        }
      }
    }
  ]
}
```

The following policy grants users permission to accept VPC peering requests if the VPC has the tag `Purpose=Peering`.

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws-cn:ec2:region:account-id:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    }
```

```
  ]
}
```

Example: Delete a VPC peering connection

The following policy grants users in the specified account permission to delete any VPC peering connection, except those that use the specified VPC, which is in the same account. The policy specifies both the `ec2:AccepterVpc` and `ec2:RequesterVpc` condition keys, as the VPC might have been the requester VPC or the peer VPC in the original VPC peering connection request.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": "ec2:DeleteVpcPeeringConnection",
      "Resource": "arn:aws-cn:ec2:region:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnNotEquals": {
          "ec2:AccepterVpc": "arn:aws-cn:ec2:region:account-id:vpc/vpc-id",
          "ec2:RequesterVpc": "arn:aws-cn:ec2:region:account-id:vpc/vpc-id"
        }
      }
    }
  ]
}
```

Example: Work within a specific account

The following policy grants users permission to work with VPC peering connections within a specific account. Users can view, create, accept, reject, and delete VPC peering connections, provided they are all within the same Amazon account.

The first statement grants users permission to view all VPC peering connections. The `Resource` element requires a * wildcard in this case, as this API action (`DescribeVpcPeeringConnections`) currently does not support resource-level permissions.

The second statement grants users permission to create VPC peering connections, and access to all VPCs in the specified account in order to do so.

The third statement uses a * wildcard as part of the `Action` element to grant permission for all VPC peering connection actions. The condition keys ensure that the actions can only be performed on VPC peering connections with VPCs that are part of the account. For example, a user is cannot delete a VPC peering connection if either the accepter or requester VPC is in a different account. A user cannot create a VPC peering connection with a VPC in a different account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeVpcPeeringConnections",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": ["ec2:CreateVpcPeeringConnection","ec2:AcceptVpcPeeringConnection"],
      "Resource": "arn:aws-cn:ec2:*:account-id:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:*VpcPeeringConnection",
      "Resource": "arn:aws-cn:ec2:*:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws-cn:ec2:*:account-id:vpc/*",
          "ec2:RequesterVpc": "arn:aws-cn:ec2:*:account-id:vpc/*"
        }
      }
    }
  ]
}
```

Example: Manage VPC peering connections using the console

To view VPC peering connections in the Amazon VPC console, users must have permission to use the `ec2:DescribeVpcPeeringConnections` action. To use the **Create Peering Connection** page, users must have permission to use the `ec2:DescribeVpcs` action. This grants them permission to view and select a VPC. You can apply resource-level permissions to all the `ec2:*PeeringConnection` actions, except `ec2:DescribeVpcPeeringConnections`.

The following policy grants users permission to view VPC peering connections, and to use the **Create VPC Peering Connection** dialog box to create a VPC peering connection using a specific requester VPC only. If users try to create a VPC peering connection with a different requester VPC, the request fails.

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

VPC peering connection quotas

The following table lists the quotas, formerly referred to as limits, for VPC peering connections for your Amazon account. Unless indicated otherwise, you can request an increase for these quotas.

Name	Default	Adjustable
Active VPC peering connections per VPC	50	Yes (up to 125)
Outstanding VPC peering connection requests	25	Yes
Expiry time for an unaccepted VPC peering connection request	1 week (168 hours)	No

For more information about the rules for using VPC peering connections, see VPC peering limitations (p. 4).

For additional quotas for Amazon VPC, see Amazon VPC quotas in the *Amazon VPC User Guide*.

Document history for the Amazon VPC Peering Guide

The following table describes the documentation releases for the *Amazon VPC Peering Guide*.

Change	Description	Date
Tag on create (p. 52)	You can add tags when you create a VPC peering connection and route table.	July 20, 2020
Inter-Region peering	DNS hostname resolution is supported for inter-Region VPC peering connections in the Asia Pacific (Hong Kong) Region.	August 26, 2019
Inter-Region peering	You can create a VPC peering connection between VPCs in different Amazon Regions.	November 29, 2017
DNS resolution support for VPC peering	You can enable a local VPC to resolve public DNS hostnames to private IP addresses when queried from instances in the peer VPC.	July 28, 2016
Stale security group rules	You can identify if your security group is being referenced in the rules of a security group in a peer VPC and you can identify stale security group rules.	May 12, 2016
Using ClassicLink over a VPC peering connection	You can modify your VPC peering connection to enable local linked EC2-Classic instances to communicate with instances in a peer VPC, or vice versa.	April 26, 2016
VPC peering	You can create a VPC peering connection between two VPCs, which allows instances in either VPC to communicate with each other using private IP addresses	March 24, 2014