Working with VPC Peering

Creating and Accepting 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 AWS 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.

Before you begin, ensure that you are aware of the limitations and rules for a VPC peering connection.

Tasks

- Creating a VPC Peering Connection with Another VPC in Your Account
- Creating a VPC Peering Connection with a VPC in Another AWS Account
- Accepting a VPC Peering Connection
- Viewing Your VPC Peering Connections

Creating a VPC Peering Connection with Another VPC in Your Account

To request a VPC peering connection with a VPC in your account, ensure that you have the IDs of the VPCs with which you are creating the VPC peering connection. You must both create and accept the VPC peering connection request yourself to activate it.

You can create a VPC peering connection with a VPC in the same region, or a different region.

Important

Ensure that your VPCs do not have overlapping IPv4 CIDR blocks. If they do, the status of the VPC peering connection immediately goes to `failed`. This limitation applies even if the VPCs have unique IPv6 CIDR blocks. Communication over IPv6 is not supported for an inter-region VPC peering connection.

To create a VPC peering connection with a VPC in the same region

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Peering Connections**, **Create Peering Connection**.
3. 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 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.
4. In the confirmation dialog box, choose **OK**.
5. Select the VPC peering connection that you've created, and choose **Actions**, **Accept Request**.
6. 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.

To create a VPC peering connection with a VPC in a different region

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Peering Connections**, **Create Peering Connection**.
3. 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.

4. In the confirmation dialog box, choose **OK**.
5. In the region selector, select the region of the accepter VPC.
6. In the navigation pane, choose **Peering Connections**. 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.

Now that your VPC peering connection is active, you must add an entry to your VPC route tables to enable traffic to be directed between the peered VPCs. For more information, see Updating Your Route Tables for a VPC Peering Connection.

Creating a VPC Peering Connection with a VPC in Another AWS Account

You can request a VPC peering connection with a VPC that's in another AWS account. Before you begin, ensure that you have the AWS account number and VPC ID of the VPC to peer with. After you've created the request, the owner of the accepter VPC must accept the VPC peering connection to activate it.

You can create a VPC peering connection with a VPC in the same region, or a different region.

Important

If the VPCs have overlapping IPv4 CIDR blocks, or if the account ID and VPC ID are incorrect or do not correspond with each other, the status of the VPC peering connection immediately goes to `failed`.

To request a VPC peering connection with a VPC in another account in the same region

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Peering Connections**, **Create Peering Connection**.

3. 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 AWS 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.

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

To request a VPC peering connection with a VPC in another account in a different region

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Peering Connections**, **Create Peering Connection**.
3. 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 AWS 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.

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

The VPC peering connection that you've created is not active. To activate it, the owner of the accepter VPC must accept the VPC peering connection request.

Accepting 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 AWS account. If you are creating a VPC peering connection in the same AWS 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 AWS 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 AWS account or your VPC.

To accept a VPC peering connection

1. Open the Amazon VPC console at https://console.aws.amazon.com/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.

Viewing 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.

To view your VPC peering connections

1. Open the Amazon VPC console at https://console.aws.amazon.com/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.

Rejecting 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 AWS 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.aws.amazon.com/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**.

Updating Your Route Tables for a VPC Peering Connection

To send private IPv4 traffic from your instance to an instance in a peer VPC, you must add a route to the route table that's associated with your subnet in which your instance resides. The route points to the CIDR block (or portion of the CIDR block) of the peer VPC in the VPC peering connection, and specifies the VPC peering connection as the target.

Similarly, if the VPCs in the VPC peering connection have associated IPv6 CIDR blocks, you can add a route to your route table to enable communication with the peer VPC over IPv6.
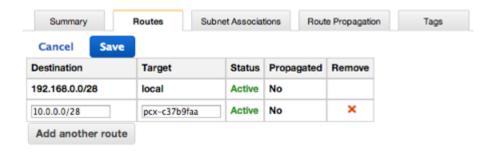
To add an IPv4 route for a VPC peering connection

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Route Tables**.
3. Select 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 **Routes**, **Edit**, **Add Route**.
5. 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 `10.0.0.0/28`, or a specific IP address `10.0.0.7/32`.
6. Select the VPC peering connection from **Target**, and then choose **Save**.

Summary	Routes	Subnet Associations	Route Propagation	Tags

Cancel **Save**

Destination	Target	Status	Propagated	Remove
192.168.0.0/28	local	Active	No	
10.0.0.0/28	pcx-c37b9faa	Active	No	✕

Add another route

If both VPCs in the VPC peering connection are in the same region, have IPv6 CIDR blocks, and the resources in the VPC are enabled to use IPv6, you can also add a route for IPv6 communication.