Working with VPCs and subnets

PDF (vpc-ug.pdf#working-with-vpcs)
Kindle (https://www.amazon.com/dp/B07643DHJ1)
RSS (amazon-vpc-release-notes.rss)

The following procedures are for manually creating a VPC and subnets. You also have to manually add gateways and routing tables. Alternatively, you can use the Amazon VPC wizard to create a VPC plus its subnets, gateways, and routing tables in one step. For more information, see Examples for VPC (./VPC_Scenarios.html) .

Tasks

- Creating a VPC (#Create-VPC)
- Creating a subnet in your VPC (#AddaSubnet)
- Viewing your subnet (#view-subnet)
- Associating a secondary IPv4 CIDR block with your VPC (#add-ipv4-cidr)
- Associating an IPv6 CIDR block with your VPC (#vpc-associate-ipv6-cidr)
- Associating an IPv6 CIDR block with your subnet (#subnet-associate-ipv6-cidr)
- Launching an instance into your subnet (#VPC_Launch_Instance)
- Deleting your subnet (#subnet-deleting)
- Disassociating an IPv4 CIDR block from your VPC (#remove-ipv4-cidr)
- Disassociating an IPv6 CIDR block from your VPC or subnet (#vpc-subnet-disassociate-ipv6)
- Deleting your VPC (#VPC_Deleting)

Creating a VPC

You can create an empty VPC using the Amazon VPC console.

To create a VPC using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/ ↗ (https://console.aws.amazon.com/vpc/) .

2. In the navigation pane, choose **Your VPCs**, **Create VPC**.

3. Specify the following VPC details as needed.

   - **Name tag**: Optionally provide a name for your VPC. Doing so creates a tag with a key of `Name` and the value that you specify.

   - **IPv4 CIDR block**: Specify an IPv4 CIDR block for the VPC. The smallest CIDR block you can specify is /28, and the largest is /16. We recommend that you specify a CIDR block from the private (non-publicly routable) IP address ranges as specified in RFC 1918 ↗ (http://www.faqs.org/rfcs/rfc1918.html) ; for example, `10.0.0.0/16`, or `192.168.0.0/16`.

     ⓘNote

     You can specify a range of publicly routable IPv4 addresses. However, we currently do not support direct access to the internet from publicly routable CIDR blocks in a VPC. Windows instances cannot boot correctly if launched into a VPC with ranges from `224.0.0.0` to `255.255.255.255` (Class D and Class E IP address ranges).

- **IPv6 CIDR block**: Optionally associate an IPv6 CIDR block with your VPC. Choose one of the following options, and then choose **Select CIDR**:

  - **Amazon-provided IPv6 CIDR block**: Requests an IPv6 CIDR block from Amazon's pool of IPv6 addresses. For **Network Border Group**, select the group from which AWS advertises IP addresses.

  - **IPv6 CIDR owned by me**: (BYOIP (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-byoip.html)) Allocates an IPv6 CIDR block from your IPv6 address pool. For **Pool,** choose the IPv6 address pool from which to allocate the IPv6 CIDR block.

- **Tenancy**: Select a tenancy option. Dedicated tenancy ensures that your instances run on single-tenant hardware. For more information, see Dedicated instances (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html) in the *Amazon EC2 User Guide for Linux Instances*.

- (Optional) Add or remove a tag.

  [Add a tag] Choose **Add tag** and do the following:

  - For **Key**, enter the key name.

  - For **Value**, enter the key value.

  [Remove a tag] Choose **Remove** to the right of the tag's Key and Value.

4. Choose **Create**.

Alternatively, you can use a command line tool.

To create a VPC using a command line tool

- create-vpc (https://docs.aws.amazon.com/cli/latest/reference/ec2/create-vpc.html) (AWS CLI)

- New-EC2Vpc (https://docs.aws.amazon.com/powershell/latest/reference/items/New-EC2Vpc.html) (AWS Tools for Windows PowerShell)

To describe a VPC using a command line tool

- describe-vpcs (https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-vpcs.html) (AWS CLI)

- Get-EC2Vpc (https://docs.aws.amazon.com/powershell/latest/reference/items/Get-EC2Vpc.html) (AWS Tools for Windows PowerShell)

For more information about IP addresses, see IP Addressing in your VPC (./vpc-ip-addressing.html) .

After you've created a VPC, you can create subnets. For more information, see Creating a subnet in your VPC (#AddaSubnet) .

Creating a subnet in your VPC

To add a new subnet to your VPC, you must specify an IPv4 CIDR block for the subnet from the range of your VPC. You can specify the Availability Zone in which you want the subnet to reside. You can have multiple subnets in the same Availability Zone.

You can optionally specify an IPv6 CIDR block for your subnet if an IPv6 CIDR block is associated with your VPC.

To create the subnet in a Local Zone, or a Wavelength Zone, you must enable the Zone. For information about how to enable Wavelength Zones, see Enabling zones (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#enable-zone-group) in the *Amazon EC2 User Guide for Linux Instances*.

To add a subnet to your VPC using the console

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

2. In the navigation pane, choose **Subnets**, **Create subnet**.

3. Specify the subnet details as necessary and choose **Create**.

   - **Name tag**: Optionally provide a name for your subnet. Doing so creates a tag with a key of Name and the value that you specify.

   - **VPC**: Choose the VPC for which you're creating the subnet.

   - **Availability Zone**: Optionally choose a Zone in which your subnet will reside, or leave the default **No Preference** to let AWS choose an Availability Zone for you.

     For information about the Regions and Zones, see Regions and zones (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-available-regions) in the *Amazon EC2 User Guide for Linux Instances*.

   - **IPv4 CIDR block**: Specify an IPv4 CIDR block for your subnet, for example, 10.0.1.0/24. For more information, see VPC and subnet sizing for IPv4 (./VPC_Subnets.html#vpc-sizing-ipv4) .

   - **IPv6 CIDR block**: (Optional) If you've associated an IPv6 CIDR block with your VPC, choose **Specify a custom IPv6 CIDR**. Specify the hexadecimal pair value for the subnet, or leave the default value.

4. (Optional) If required, repeat the steps above to create more subnets in your VPC.

Alternatively, you can use a command line tool.

To add a subnet using a command line tool

- create-subnet (https://docs.aws.amazon.com/cli/latest/reference/ec2/create-subnet.html) (AWS CLI)

- New-EC2Subnet (https://docs.aws.amazon.com/powershell/latest/reference/items/New-EC2Subnet.html) (AWS Tools for Windows PowerShell)

After you create a subnet, you can do the following:

- Configure your routing. To make your subnet a public subnet, you must attach an internet gateway to your VPC. For more information, see Creating and attaching an internet gateway (./VPC_Internet_Gateway.html#Add_IGW_Attach_Gateway) . You can then create a custom route table, and add route to the internet gateway. For more information, see Creating a custom route table (./VPC_Internet_Gateway.html#Add_IGW_Routing) . For other routing options, see Route tables (./VPC_Route_Tables.html) .

- Modify the subnet settings to specify that all instances launched in that subnet receive a public IPv4 address, or an IPv6 address, or both. For more information, see IP addressing behavior for your subnet (./vpc-ip-addressing.html#vpc-ip-addressing-subnet) .

- Create or modify your security groups as needed. For more information, see Security groups for your VPC (./VPC_SecurityGroups.html) .

- Create or modify your network ACLs as needed. For more information, see Network ACLs (./vpc-network-acls.html) .

- Share the subnet with other accounts. For more information, see Sharing a subnet (./vpc-sharing.html#vpc-sharing-share-subnet) .

Viewing your subnet

You van view the details about your subnet.

To view subnet details using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/ ☒ (https://console.aws.amazon.com/vpc/) .

2. In the navigation pane, choose **Subnets**.

3. Select the subnet, and then choose **View Details**.

To describe a subnet using a command line tool

- describe-subnets (https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-subnets.html) (AWS CLI)

- Get-EC2Subnet (https://docs.aws.amazon.com/powershell/latest/reference/items/Get-EC2Subnet.html) (AWS Tools for Windows PowerShell)

Associating a secondary IPv4 CIDR block with your VPC

You can add another IPv4 CIDR block to your VPC. Ensure that you have read the applicable restrictions (./VPC_Subnets.html#vpc-resize) .

After you've associated a CIDR block, the status goes to `associating`. The CIDR block is ready to use when it's in the `associated` state.

To add a CIDR block to your VPC using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/ ☒ (https://console.aws.amazon.com/vpc/) .

2. In the navigation pane, choose **Your VPCs**.

3. Select the VPC, and choose **Actions**, **Edit CIDRs**.

4. Choose **Add IPv4 CIDR**, and enter the CIDR block to add; for example, `10.2.0.0/16`. Choose the tick icon.

5. Choose **Close**.

Alternatively, you can use a command line tool.

To add a CIDR block using a command line tool

- associate-vpc-cidr-block (https://docs.aws.amazon.com/cli/latest/reference/ec2/associate-vpc-cidr-block.html) (AWS CLI)

- Register-EC2VpcCidrBlock (https://docs.aws.amazon.com/powershell/latest/reference/items/Register-EC2VpcCidrBlock.html) (AWS Tools for Windows PowerShell)

After you've added the IPv4 CIDR blocks that you need, you can create subnets. For more information, see Creating a subnet in your VPC (#AddaSubnet) .

Associating an IPv6 CIDR block with your VPC

You can associate an IPv6 CIDR block with any existing VPC. The VPC must not have an existing IPv6 CIDR block associated with it.

To associate an IPv6 CIDR block with a VPC using the console

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

2. In the navigation pane, choose **Your VPCs**.

3. Select your VPC, choose **Actions**, **Edit CIDRs**.

4. Choose **Add IPv6 CIDR**.

5. Choose **Add IPv6 CIDR**.

6. For **IPv6 CIDR block**, choose one of the following, and then choose **Select CIDR**:

   - **Amazon-provided IPv6 CIDR block**: Requests an IPv6 CIDR block from Amazon's pool of IPv6 addresses.

   - **IPv6 CIDR owned by me**: (BYOIP) Allocates an IPv6 CIDR block from your IPv6 address pool. For **Pool,** choose the IPv6 address pool from which to allocate the IPv6 CIDR block.

7. If you selected **Amazon-provided IPv6 CIDR block**, from **Network Border Group**, select the group from where AWS advertises the IP addresses.

8. Choose **Select CIDR**.

9. Choose **Close**.

Alternatively, you can use a command line tool.

To associate an IPv6 CIDR block with a VPC using a command line tool

- associate-vpc-cidr-block (https://docs.aws.amazon.com/cli/latest/reference/ec2/associate-vpc-cidr-block.html) (AWS CLI)

- Register-EC2VpcCidrBlock (https://docs.aws.amazon.com/powershell/latest/reference/items/Register-EC2VpcCidrBlock.html) (AWS Tools for Windows PowerShell)

Associating an IPv6 CIDR block with your subnet

You can associate an IPv6 CIDR block with an existing subnet in your VPC. The subnet must not have an existing IPv6 CIDR block associated with it.

To associate an IPv6 CIDR block with a subnet using the console

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

2. In the navigation pane, choose **Subnets**.

3. Select your subnet, choose **Subnet Actions**, **Edit IPv6 CIDRs**.

4. Choose **Add IPv6 CIDR**. Specify the hexadecimal pair for the subnet (for example, 00) and confirm the entry by choosing the tick icon.

5. Choose **Close**.

Alternatively, you can use a command line tool.

To associate an IPv6 CIDR block with a subnet using a command line tool

- associate-subnet-cidr-block (https://docs.aws.amazon.com/cli/latest/reference/ec2/associate-subnet-cidr-block.html) (AWS CLI)

- Register-EC2SubnetCidrBlock (https://docs.aws.amazon.com/powershell/latest/reference/items/Register-EC2SubnetCidrBlock.html) (AWS Tools for Windows PowerShell)

Launching an instance into your subnet

After you've created your subnet and configured your routing, you can launch an instance into your subnet using the Amazon EC2 console.

To launch an instance into your subnet using the console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/ ☒ (https://console.aws.amazon.com/ec2/) .

2. On the dashboard, choose **Launch Instance**.

3. Follow the directions in the wizard. Select an AMI and an instance type and choose **Next: Configure Instance Details**.

   ⓘNote

   If you want your instance to communicate over IPv6, you must select a supported instance type. All current generation instance types support IPv6 addresses.

4. On the **Configure Instance Details** page, ensure that you have selected the required VPC in the **Network** list, then select the subnet in to which to launch the instance. Keep the other default settings on this page and choose **Next: Add Storage**.

5. On the next pages of the wizard, you can configure storage for your instance, and add tags. On the **Configure Security Group** page, choose from any existing security group that you own, or follow the wizard directions to create a new security group. Choose **Review and Launch** when you're done.

6. Review your settings and choose **Launch**.

7. Select an existing key pair that you own or create a new one, and then choose **Launch Instances** when you're done.

Alternatively, you can use a command line tool.

To launch an instance into your subnet using a command line tool

- run-instances (https://docs.aws.amazon.com/cli/latest/reference/ec2/run-instances.html) (AWS CLI)

- New-EC2Instance (https://docs.aws.amazon.com/powershell/latest/reference/items/New-EC2Instance.html) (AWS Tools for Windows PowerShell)

Deleting your subnet

If you no longer need your subnet, you can delete it. You must terminate any instances in the subnet first.

To delete your subnet using the console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/ 🗗 (https://console.aws.amazon.com/ec2/) .

2. Terminate all instances in the subnet. For more information, see Terminate Your Instance (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html) in the *EC2 User Guide*.

3. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/ 🗗 (https://console.aws.amazon.com/vpc/) .

4. In the navigation pane, choose **Subnets**.

5. Select the subnet to delete and choose **Actions**, **Delete subnet**.

6. In the **Delete Subnet** dialog box, choose **Delete subnet**.

Alternatively, you can use a command line tool.

To delete a subnet using a command line tool

- delete-subnet (https://docs.aws.amazon.com/cli/latest/reference/ec2/delete-subnet.html) (AWS CLI)

- Remove-EC2Subnet (https://docs.aws.amazon.com/powershell/latest/reference/items/Remove-EC2Subnet.html) (AWS Tools for Windows PowerShell)

Disassociating an IPv4 CIDR block from your VPC

If your VPC has more than one IPv4 CIDR block associated with it, you can disassociate an IPv4 CIDR block from the VPC. You cannot disassociate the primary IPv4 CIDR block. You can only disassociate an entire CIDR block; you cannot disassociate a subset of a CIDR block or a merged range of CIDR blocks. You must first delete all subnets in the CIDR block.

To remove a CIDR block from a VPC using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/ 🗗 (https://console.aws.amazon.com/vpc/) .

2. In the navigation pane, choose **Your VPCs**.

3. Select the VPC, and choose **Actions**, **Edit CIDRs**.

4. Under **VPC IPv4 CIDRs**, choose the delete button (a cross) for the CIDR block to remove.

5. Choose **Close**.

Alternatively, you can use a command line tool.

To remove an IPv4 CIDR block from a VPC using a command line tool

- disassociate-vpc-cidr-block (https://docs.aws.amazon.com/cli/latest/reference/ec2/disassociate-vpc-cidr-block.html) (AWS CLI)

- Unregister-EC2VpcCidrBlock (https://docs.aws.amazon.com/powershell/latest/reference/items/Unregister-EC2VpcCidrBlock.html) (AWS Tools for Windows PowerShell)

Disassociating an IPv6 CIDR block from your VPC or subnet

If you no longer want IPv6 support in your VPC or subnet, but you want to continue using your VPC or subnet for creating and communicating with IPv4 resources, you can disassociate the IPv6 CIDR block.

To disassociate an IPv6 CIDR block, you must first unassign any IPv6 addresses that are assigned to any instances in your subnet. For more information, see Unassigning an IPv6 address from an instance (./vpc-ip-addressing.html#vpc-unassign-ipv6-instance) .

To disassociate an IPv6 CIDR block from a subnet using the console

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

2. In the navigation pane, choose **Subnets**.

3. Select your subnet, choose **Actions**, **Edit IPv6 CIDRs**.

4. Remove the IPv6 CIDR block for the subnet by choosing the cross icon.

5. Choose **Close**.

To disassociate an IPv6 CIDR block from a VPC using the console

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

2. In the navigation pane, choose **Your VPCs**.

3. Select your VPC, choose **Actions**, **Edit CIDRs**.

4. Remove the IPv6 CIDR block by choosing the cross icon.

5. Choose **Close**.

ⓘNote

Disassociating an IPv6 CIDR block does not automatically delete any security group rules, network ACL rules, or route table routes that you've configured for IPv6 networking. You must manually modify or delete these rules or routes.

Alternatively, you can use a command line tool.

To disassociate an IPv6 CIDR block from a subnet using a command line tool

- disassociate-subnet-cidr-block (https://docs.aws.amazon.com/cli/latest/reference/ec2/disassociate-subnet-cidr-block.html) (AWS CLI)

- Unregister-EC2SubnetCidrBlock (https://docs.aws.amazon.com/powershell/latest/reference/items/Unregister-EC2SubnetCidrBlock.html) (AWS Tools for Windows PowerShell)

To disassociate an IPv6 CIDR block from a VPC using a command line tool

- disassociate-vpc-cidr-block (https://docs.aws.amazon.com/cli/latest/reference/ec2/disassociate-vpc-cidr-block.html) (AWS CLI)

- Unregister-EC2VpcCidrBlock (https://docs.aws.amazon.com/powershell/latest/reference/items/Unregister-EC2VpcCidrBlock.html) (AWS Tools for Windows PowerShell)

Deleting your VPC

To delete a VPC using the VPC console, you must first terminate or delete the following components:

- All instances in the VPC - For information about how to terminate an instance, see Terminate your instance (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html) in the *Amazon EC2 User Guide for Linux Instances*.

- VPC peering connections

- Interface endpoints

- NAT gateways

When you delete a VPC using the VPC console, we also delete the following VPC components for you:

- Subnets

- Security groups

- Network ACLs

- Route tables

- Gateway endpoints

- Internet gateways

- Egress-only internet gateways

- DHCP options

If you have a AWS Site-to-Site VPN connection, you don't have to delete it or the other components related to the VPN (such as the customer gateway and virtual private gateway). If you plan to use the customer gateway with another VPC, we recommend that you keep the Site-to-Site VPN connection and the gateways. Otherwise, you must configure your customer gateway device again after you create a new Site-to-Site VPN connection.

To delete your VPC using the console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/ ⧉ (https://console.aws.amazon.com/ec2/) .

2. Terminate all instances in the VPC. For more information, see Terminate Your Instance (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html) in the *Amazon EC2 User Guide for Linux Instances*.

3. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/ ⧉ (https://console.aws.amazon.com/vpc/) .

4. In the navigation pane, choose **Your VPCs**.

5. Select the VPC to delete and choose **Actions**, **Delete VPC**.

6. If you have a Site-to-Site VPN connection, select the option to delete it; otherwise, leave it unselected. Choose **Delete VPC**.

Alternatively, you can use a command line tool. When you delete a VPC using the command line, you must first terminate all instances, and delete or detach all associated resources, including subnets, custom security groups, custom network ACLs, custom route tables, VPC peering connections, endpoints, the NAT gateway, the internet gateway, and the egress-only internet gateway.

To delete a VPC using a command line tool

- delete-vpc (https://docs.aws.amazon.com/cli/latest/reference/ec2/delete-vpc.html) (AWS CLI)

- Remove-EC2Vpc (https://docs.aws.amazon.com/powershell/latest/reference/items/Remove-EC2Vpc.html) (AWS Tools for Windows PowerShell)