

Amazon Virtual Private Cloud (VPC) allows the users to use AWS resources in a virtual network. The users can customize their virtual networking environment as they like, such as selecting own IP address range, creating subnets, and configuring route tables and network gateways.

The list of AWS services that can be used with Amazon VPC are –

- Amazon EC2
- Amazon Route 53
- Amazon WorkSpaces
- Auto Scaling
- Elastic Load Balancing
- AWS Data Pipeline
- Elastic Beanstalk
- Amazon Elastic Cache
- Amazon EMR
- Amazon OpsWorks
- Amazon RDS
- Amazon Redshift

How to Use Amazon VPC?

Following are the steps to create VPC.

Create VPC

Step 1 – Open the Amazon VPC console by using the following link – <https://console.aws.amazon.com/vpc/>

Step 2 – Select creating the VPC option on the right side of the navigation bar. Make sure that the same region is selected as for other services.

Step 3 – Click the start VPC wizard option, then click VPC with single public subnet option on the left side.

Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

Creates:

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

Select

Step 4 – A configuration page will open. Fill in the details like VPC name, subnet name and leave the other fields as default. Click the Create VPC button.

Step 2: VPC with a Single Public Subnet

IP CIDR block:* (65531 IP addresses available)

VPC name:

Public subnet:* (251 IP addresses available)

Availability Zone:*

Subnet name:

You can add more subnets after AWS creates the VPC.

Enable DNS hostnames:* ☒ Yes ☐ No

Hardware tenancy:*

Cancel and Exit **Back** **Create VPC**

Step 5 – A dialog box will open, showing the work in progress. When it is completed, select the OK button.

The Your VPCs page opens which shows a list of available VPCs. The setting of VPC can be changed here.

Create VPC **Actions**

Search VPCs and their properties... X

1 to 2 of 2 VPCs

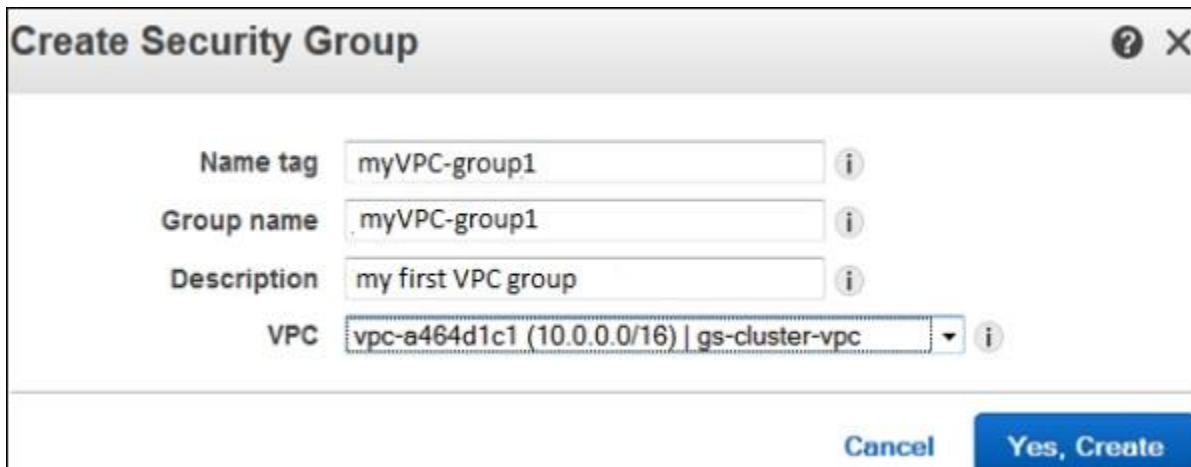
	Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default VPC
	vpc-6f71e...		available	172.31.0.0/16	dopt-6271ed0e	rtb-6071ed0c	acl-6771ed0b	Default	Yes
	my-vpc	vpc-cd65...	available	10.0.0.0/16	dopt-6271ed0e	rtb-b77befd2	acl-0b931c0e	Default	No

Select/Create VPC Group

Step 1 – Open the Amazon VPC console by using the following link
– <https://console.aws.amazon.com/vpc/>

Step 2 – Select the security groups option in the navigation bar, then choose create security group option.

Step 3 – A form will open, enter the details like group name, name tag, etc. Select ID of your VPC from VPC menu, then select the Yes, create button.



Create Security Group

Name tag: myVPC-group1

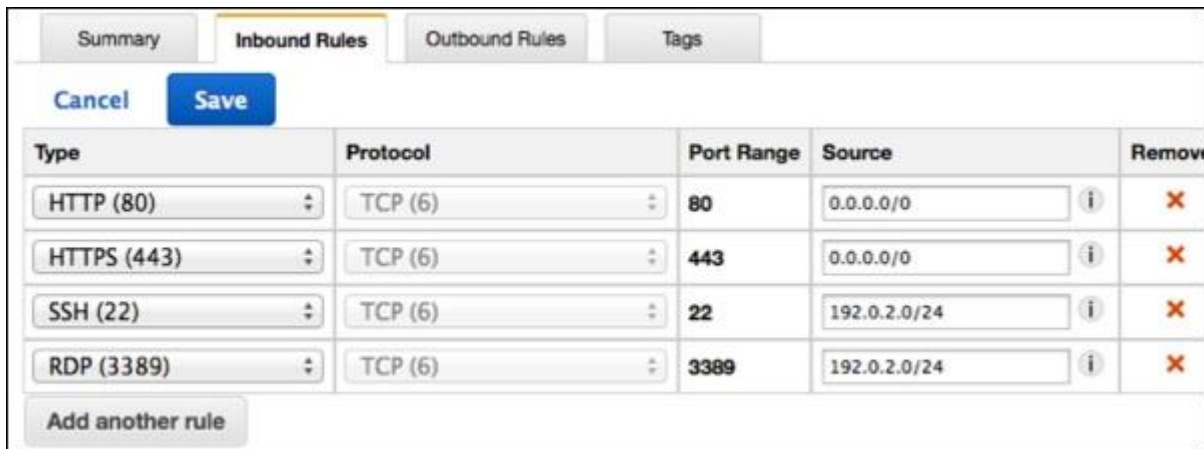
Group name: myVPC-group1

Description: my first VPC group

VPC: vpc-a464d1c1 (10.0.0.0/16) | gs-cluster-vpc

Buttons: Cancel, Yes, Create

Step 4 – The list of groups opens. Select the group name from the list and set rules. Then click the Save button.



Summary | **Inbound Rules** | Outbound Rules | Tags

Buttons: Cancel, Save

Type	Protocol	Port Range	Source	Remove
HTTP (80)	TCP (6)	80	0.0.0.0/0	✗
HTTPS (443)	TCP (6)	443	0.0.0.0/0	✗
SSH (22)	TCP (6)	22	192.0.2.0/24	✗
RDP (3389)	TCP (6)	3389	192.0.2.0/24	✗

Add another rule

Launch Instance into VPC

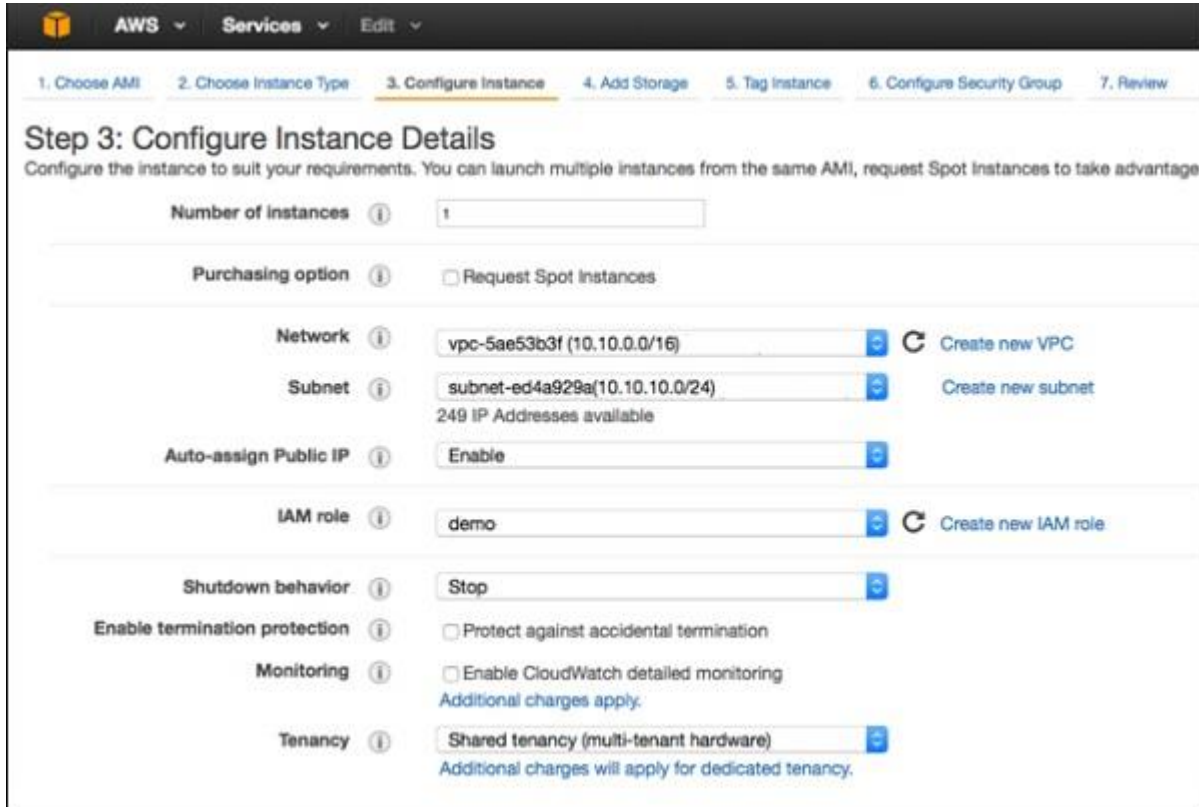
Step 1 – Open the Amazon VPC console using the following link
– <https://console.aws.amazon.com/vpc/>

Step 2 – Select the same region as while creating VPC and security group.

Step 3 – Now select the Launch Instance option in the navigation bar.

Step 4 – A page opens. Choose the AMI which is to be used.

Step 5 – A new page opens. Choose an Instance Type and select the hardware configuration. Then select **Next: Configure Instance Details**.



The screenshot shows the AWS Management Console interface for configuring an instance. The top navigation bar includes the AWS logo, 'Services', and 'Edit'. Below the navigation bar is a progress bar with seven steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (highlighted), 4. Add Storage, 5. Tag Instance, 6. Configure Security Group, and 7. Review. The main heading is 'Step 3: Configure Instance Details' with a subtext: 'Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage'. The form contains several sections: 'Number of Instances' with a dropdown set to '1'; 'Purchasing option' with a checkbox for 'Request Spot Instances'; 'Network' with a dropdown for 'vpc-5ae53b3f (10.10.0.0/16)' and a 'Create new VPC' button; 'Subnet' with a dropdown for 'subnet-ed4a929a (10.10.10.0/24)' and a 'Create new subnet' button; 'Auto-assign Public IP' with a dropdown set to 'Enable'; 'IAM role' with a dropdown for 'demo' and a 'Create new IAM role' button; 'Shutdown behavior' with a dropdown set to 'Stop'; 'Enable termination protection' with a checkbox for 'Protect against accidental termination'; 'Monitoring' with a checkbox for 'Enable CloudWatch detailed monitoring' and a note 'Additional charges apply.'; and 'Tenancy' with a dropdown for 'Shared tenancy (multi-tenant hardware)' and a note 'Additional charges will apply for dedicated tenancy.'

Step 6 – Select the recently created VPC from the Network list, and the subnet from the Subnet list. Leave the other settings as default and click Next till the Tag Instance page.

Step 7 – On the Tag Instance page, tag the instance with the Name tag. This helps to identify your instance from the list of multiple instances. Click Next: Configure Security Group.

Step 8 – On the Configure Security Group page, select the recently created group from the list. Then, select Review and Launch button.

Step 9 – On the Review Instance Launch page, check your instance details, then select Launch.

Step 10 – A dialog box appears. Choose the option Select an existing key pair or create a new key pair, then click the Launch Instances button.

Step 11 – The confirmation page open which shows all the details related to instances.

Assign Elastic IP Address to VPC Instances

Step 1 – Open the Amazon VPC console using the following link
– <https://console.aws.amazon.com/vpc/>

Step 2 – Select Elastic IP's option in the navigation bar.

Step 3 – Select Allocate New Address. Then select Yes, Allocate button.

Step 4 – Select your Elastic IP address from the list, then select Actions, and then click the Associate Address button.

Step 5 – A dialog box will open. First select the Instance from the Associate with list. Then select your instance from the Instance list. Finally click the Yes, Associate button.

Associate Address Cancel X

Select the instance or network interface to which you wish to associate this IP address (54.208.9.154).

Instance: i-d69845b8 - ns1.example.com

Private IP address: 10.0.0.10*
* denotes the primary private IP address

or

Network Interface: Select a network interface

Private IP address:
* denotes the primary private IP address

☒ Allow Reassociation

Cancel Yes, Associate

Delete a VPC

There are several steps to delete VPC without losing any resources associated with it. Following are the steps to delete a VPC.

Step 1 – Open the Amazon VPC console using the following link
– <https://console.aws.amazon.com/vpc/>

Step 2 – Select Instances option in the navigation bar.

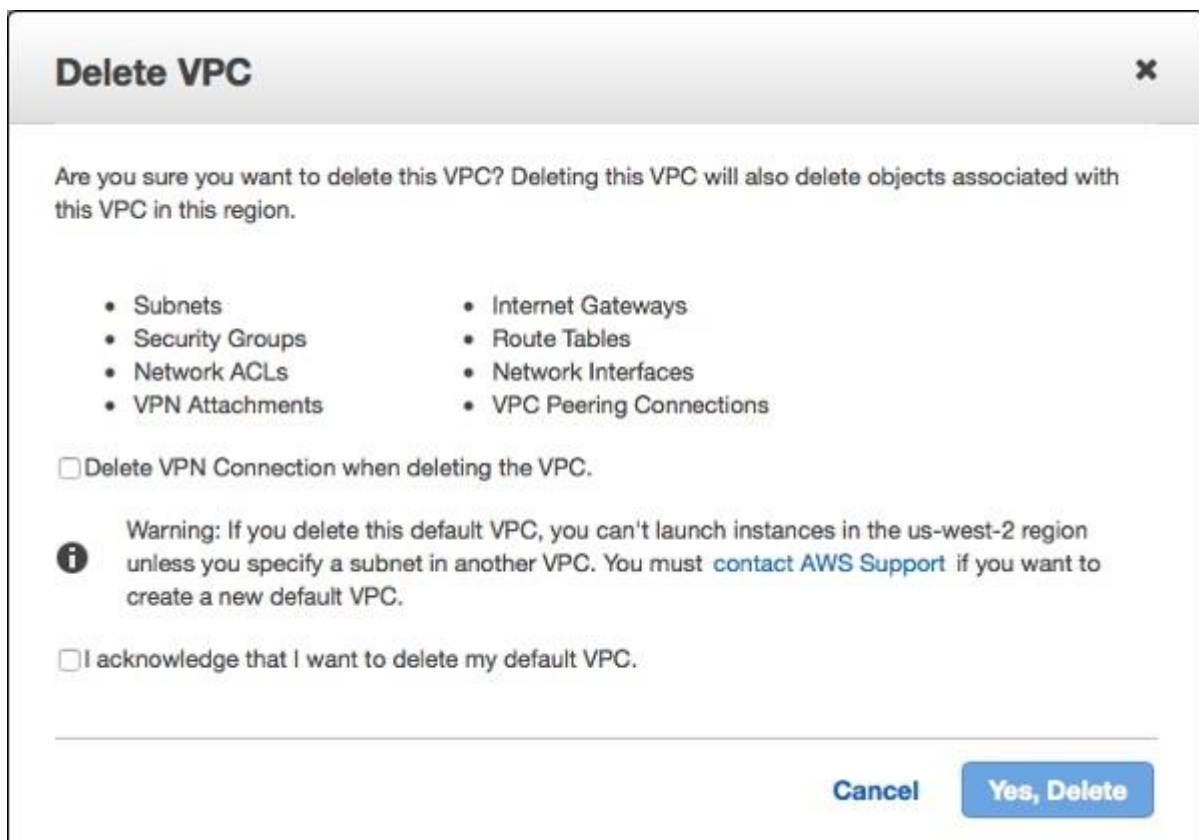
Step 3 – Select the Instance from the list, then select the Actions → Instance State → Terminate button.

Step 4 – A new dialog box opens. Expand the Release attached Elastic IPs section, and select the checkbox next to the Elastic IP address. Click the Yes, Terminate button.

Step 5 – Again open the Amazon VPC console using the following link – <https://console.aws.amazon.com/vpc/>

Step 6 – Select the VPC from the navigation bar. Then select Actions & finally click the Delete VPC button.

Step 7 – A confirmation message appears. Click the Yes, Delete button.



The screenshot shows a 'Delete VPC' dialog box with a close button (X) in the top right corner. The main text asks: 'Are you sure you want to delete this VPC? Deleting this VPC will also delete objects associated with this VPC in this region.' Below this, there are two columns of bulleted items representing associated resources: Subnets, Security Groups, Network ACLs, VPN Attachments, Internet Gateways, Route Tables, Network Interfaces, and VPC Peering Connections. There is a checkbox labeled 'Delete VPN Connection when deleting the VPC.' Below that is a warning message with an information icon: 'Warning: If you delete this default VPC, you can't launch instances in the us-west-2 region unless you specify a subnet in another VPC. You must [contact AWS Support](#) if you want to create a new default VPC.' At the bottom left, there is another checkbox: 'I acknowledge that I want to delete my default VPC.' At the bottom right, there are two buttons: 'Cancel' and 'Yes, Delete'.

Features of VPC

- **Many connectivity options** – There are various connectivity options that exist in Amazon VPC.
 - Connect VPC directly to the Internet via public subnets.

- Connect to the Internet using Network Address Translation via private subnets.
 - Connect securely to your corporate datacenter via encrypted IPsec hardware VPN connection.
 - Connect privately to other VPCs in which we can share resources across multiple virtual networks through AWS account.
 - Connect to Amazon S3 without using an internet gateway and have good control over S3 buckets, its user requests, groups, etc.
 - Combine connection of VPC and datacenter is possible by configuring Amazon VPC route tables to direct all traffic to its destination.
- **Easy to use** – Ease of creating a VPC in very simple steps by selecting network set-ups as per requirement. Click "Start VPC Wizard", then Subnets, IP ranges, route tables, and security groups will be automatically created.
 - **Easy to backup data** – Periodically backup data from the datacenter into Amazon EC2 instances by using Amazon EBS volumes.
 - **Easy to extend network using Cloud** – Move applications, launch additional web servers and increase storage capacity by connecting it to a VPC.