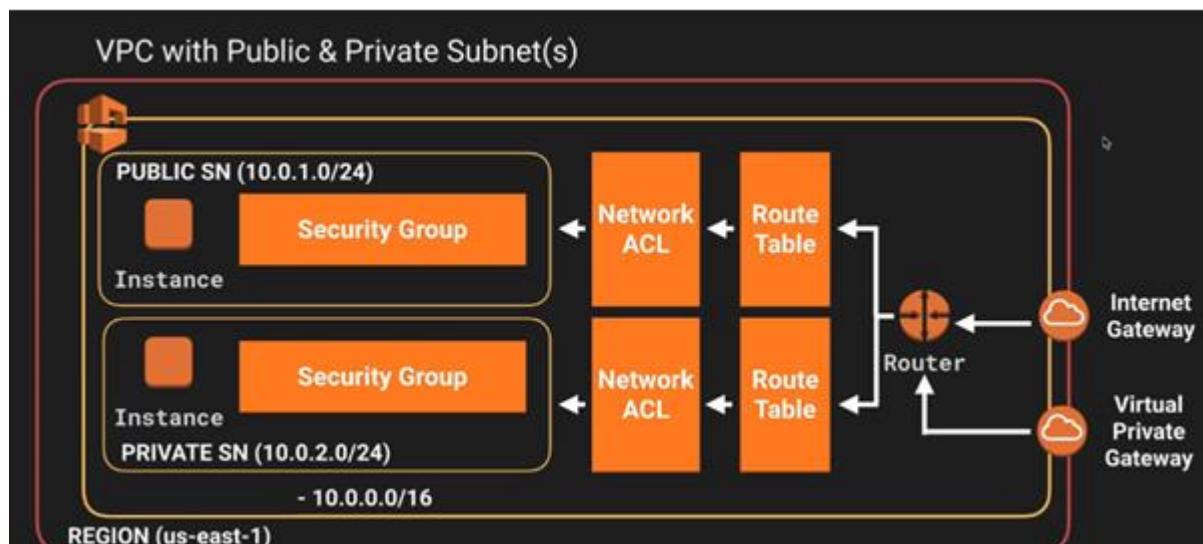


AWS Quick Start Guide: Amazon Virtual Private Cloud Documentation

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

The following are the key concepts for VPCs:

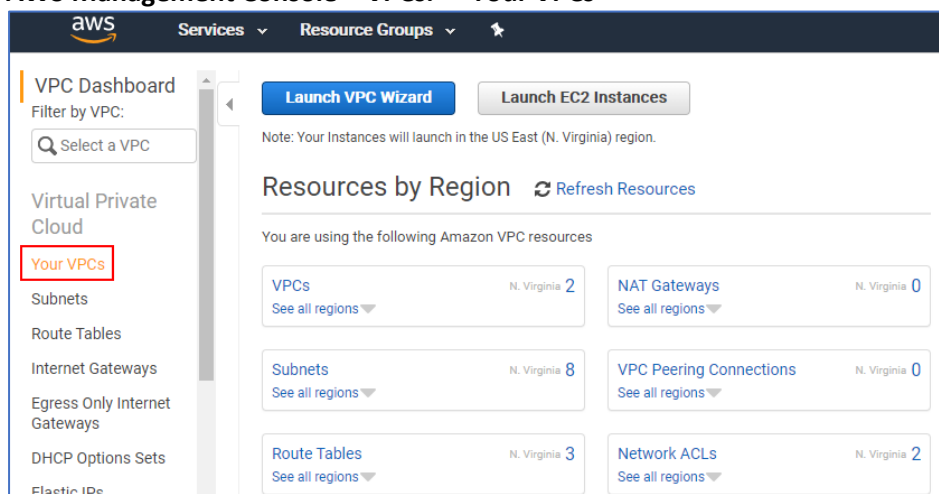
- A *virtual private cloud* (VPC) is a virtual network dedicated to your AWS account.
- A *subnet* is a range of IP addresses in your VPC.
- A *route table* contains a set of rules, called routes, that are used to determine where network traffic is directed.
- An *internet gateway* is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.
- A *VPC endpoint* enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by Private Link without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.



Accessing Amazon VPC

You can create, access, and manage your VPCs using any of the following interfaces:

1. AWS Management Console – VPCs. -> Your VPCs



2. Create VPC as below:

VPCs > Create VPC

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag:

IPv4 CIDR block*:

IPv6 CIDR block: ☐ No IPv6 CIDR block ☒ Amazon provided IPv6 CIDR block

Tenancy:

* Required

Cancel Create

Note: Route tables, NACLs, security groups are created by default after creation of VPC

3. Now we can create two Subnet -> 1) PublicSubnet 2) PrivateSubnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag:

VPC*: Select the VPC that we created

VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	
	2600:1f18:73:c200::/56	associated	

Availability Zone: Select the the Availability A Zone where this subnet will reside.

IPv4 CIDR block*: The CIDR block that represents the range of IP addresses for the subnet

IPv6 CIDR block:

* Required

Cancel Create

PrivateSubnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag:

VPC*: Select the VPC that we created

VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	
	2600:1f18:73:c200::/56	associated	

Availability Zone: Select the the Availability B Zone where this subnet will reside.

IPv4 CIDR block*: The CIDR block that represents the range of IP addresses for the subnet

IPv6 CIDR block:

* Required

Cancel Create

4. Please create an Internet gateway "MyIGW" and then attached to your VPC

Internet gateways > Create internet gateway

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Name tag:

* Required

Cancel Create

Create internet gateway Actions ²

Filter by tags and attributes

Name	ID	Status	VPC	Owner
MyIGW	igw-06697b956c4...	detached	-	521800872068
	igw-8076c1fb	attached	vpc-92a5e5e8	521800872068

¹ ☒ ³ ☐

Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC*:

AWS Command Line

VPC ID	Name
vpc-0b07598a4a2c11e95	myVPC-Tech

* Required

Cancel Attach

5. Create route table - A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag:

VPC*:

* Required

Cancel Create

6. Now we have to **Subnet Associations**

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Create route table Actions

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Main
	rtb-08cca127dd5af5786	-	Yes
MYRT	rtb-0c291148386877b51	subnet-05bc6698479b8aa64	No
	rtb-6e27e810	-	Yes

Route Table: rtb-0c291148386877b51

Summary Routes **Subnet Associations** Route Propagation Tags

Edit subnet associations

Route table: rtb-0c291148386877b51 (MYRT)

Associated subnets:

Filter by attributes or search by keyword

Subnet ID	IPV4 CIDR	IPV6 CIDR	Current Route Table
subnet-05bc6698479b8aa64 PublicSubnet	10.0.0.0/24	-	rtb-0c291148386877b51
subnet-07c708f2062236fd9 PrivateSubnet	10.0.2.0/24	-	Main

* Required

Cancel Save

7. After this go to Subnets and make your public subnet as auto assign public IP

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Subnets

Create subnet Actions

Filter by tags and attributes or search by keyword

Name	State	VPC
PublicSubnet	available	vpc-0b07598a4a2c11e95 ...
PrivateSubnet	available	vpc-0b07598a4a2c11e95 ...
	available	vpc-92a5e5e8
	available	vpc-92a5e5e8

Subnets > Modify auto-assign IP settings

Modify auto-assign IP settings

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for an instance launched in this subnet. You can override the auto-assign IP settings for an instance at launch time.

Subnet ID: subnet-05bc6698479b8aa64

Auto-assign IPv4 ☒ Enable auto-assign public IPv4 address

* Required

Cancel Save

8. After this launch EC2 instances, in configuration instance tab, choose your **VPC** in network, choose your public subnet.

EC2 – First Instance 10.0.1.0 –us east-1a as public subnet

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the low-cost instance, and more.

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

250 IP Addresses available

Annotations:
 - Select the VPC that we created (points to vpc-0b07598a4a2c11e95)
 - Select the us-east 1 a Subnet that we created (points to subnet-05bc6698479b8aa64)

After this create new security group “SG-1”, ssh and http, HTTPS
 Choose new key pair or you can use the existing one.

EC2- Second Instance 10.0.2.0 –us east-1a as private subnet

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the low-cost instance, and more.

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

250 IP Addresses available

Annotations:
 - Select the VPC that we created (points to vpc-0b07598a4a2c11e95)
 - Select the us-east 1 b Subnet that we created for Private (points to subnet-07c708f20622d6fd9)

After this create new security group “SG-1”, ssh and http, HTTPS
 Choose new key pair or you can use the existing one.

- After this connect to public machine **EC2- First Instance** and try to check if it is internet connected or working. By Ping google.com
If Internet is not working, then do below the steps.

We need to enable Internet access.

VPC Dashboard

Filter by VPC:

Virtual Private Cloud
 Your VPCs
 Subnets
Route Tables
 Internet Gateways
 Egress Only Internet Gateways
 DHCP Options Sets
 Elastic IPs
 Endpoints
 Endpoint Services
 NAT Gateways
 Peering Connections
 Security

Create route table [Actions](#)

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Main	VPC ID
	rtb-08cca127dd5af5786	-	Yes	vpc-0b07598a4a2c11e95 ...
<input checked="" type="checkbox"/> MYRT	rtb-0c291148386877b51	subnet-05bc6698479b8aa64	No	vpc-0b07598a4a2c11e95 ...
	rtb-6e27e810	-	Yes	vpc-92a5e5e8

Route Table: rtb-0c291148386877b51

[Summary](#) **[Routes](#)** [Subnet Associations](#) [Route Propagation](#) [Tags](#)

[Edit routes](#)

View:

Destination	Target	Status
10.0.0.0/16	local	active

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
2600:1f18:73:c200::/56	local	active	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="igw-06697b956c4957f5d"/>	active	No
<input type="text" value="::/0"/>	<input type="text" value="igw-06697b956c4957f5d"/>	active	No

[Add route](#) [Cancel](#) [Save routes](#)

Annotations:
 1: Add route
 2: 0.0.0.0/0
 3: Select the Created MyIGW
 4: ::/0
 5: Select the Created MyIGW
 6: Save routes

10. Now try to access your EC2-Second System (PrivateServer) from EC2-First System (PublicServer)
11. [ec2-user@ip-10-0-1-167 ~]\$ vi mynewkey.pem (copy and paste the code from .pem key)
12. [ec2-user@ip-10-0-1-167 ~]\$ chmod 400 mynewkey.pem (Set the permission)
13. [ec2-user@ip-10-0-1-167 ~]\$ ssh -i mynewkey.pem ec2-user@<private_ip_address>
14. After connectivity, elevate privileges and check for command yum update -y
If the Internet is not working on PrivateServer then do below the steps.

NAT Gateways > Create NAT Gateway

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more.](#)

Subnet* 1 2

Elastic IP Allocation ID* 4 3 Create New EIP

* Required

Cancel Create a NAT Gateway 5

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
2600:1f18:73:c200::/56	local	active	No
0.0.0.0/0	igw-06697b956c4957f5d	active	No
::/0	igw-06697b956c4957f5d	active	No
0.0.0.0/0		No	No

Add route

* Required

Cancel Save routes

Egress Only Internet Gateway
Instance
Internet Gateway
NAT Gateway
Network Interface
Peering Connection
Transit Gateway
Virtual Private Gateway

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
2600:1f18:73:c200::/56	local	active	No
0.0.0.0/0	igw-06697b956c4957f5d	active	No
::/0	igw-06697b956c4957f5d	active	No
0.0.0.0/0	nat-	No	No

Add route

* Required

Cancel Save routes

nat-0e25bd614f397d4e3

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
2600:1f18:73:c200::/56	local	active	No
0.0.0.0/0	igw-06697b956c4957f5d	active	No
::/0	igw-06697b956c4957f5d	active	No
0.0.0.0/0	nat-0e25bd614f397d4e3	No	No
::/0	nat-0e25bd614f397d4e3	No	No

Add route

* Required

Cancel Save routes

Done