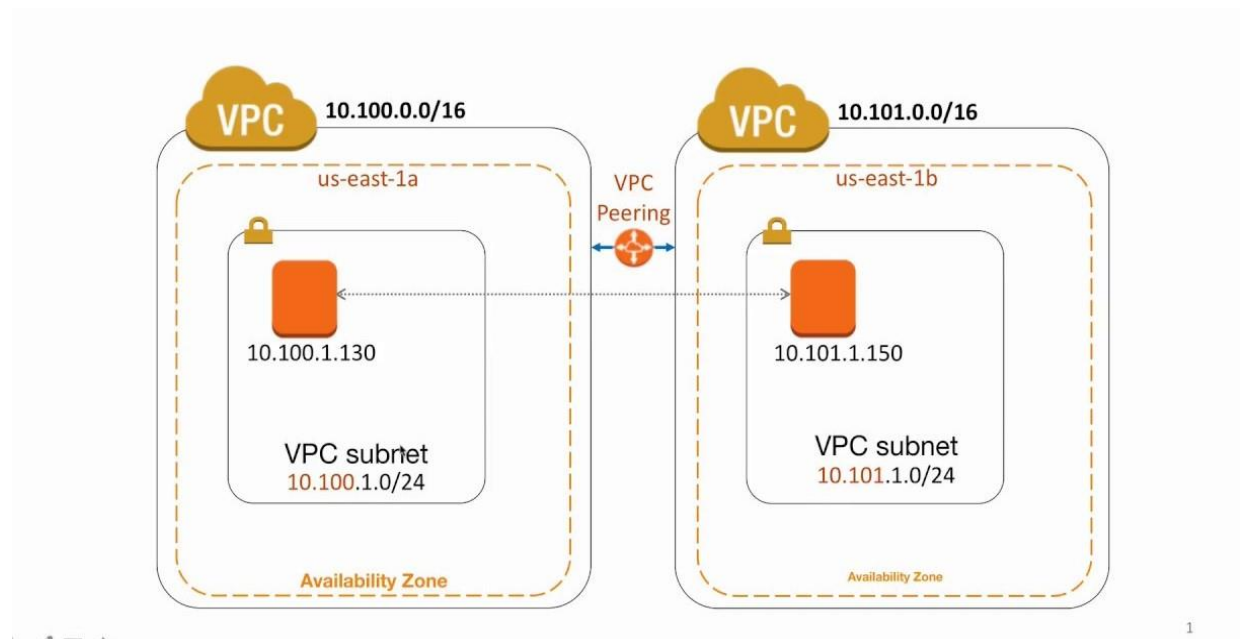


# What is VPC Peering

1. Peering connection is a part in VPC
2. Peering connection means interconnection between two VPC's
3. It is called as two-way connection

## VPC Peering architecture



## Steps to create peering connection

### Step 1:

1. Go to VPC services
2. Create two VPC's with different CIDR block range
3. First create one VPC
4. Click on create VPC
  - Select VPC only
  - Give the name for VPC as VPC 1
  - Give the CIDR block range as (10.0.0.0/16)
  - Finally click on create VPC as shown in below figure

**VPC settings**

Resources to create [Info](#)  
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

Name tag - *optional*  
Creates a tag with a key of 'Name' and a value that you specify.

vpc1

IPv4 CIDR block [Info](#)  
☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR  
10.0.0.0/16  
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)  
☒ No IPv6 CIDR block  
☐ IPAM-allocated IPv6 CIDR block  
☐ Amazon-provided IPv6 CIDR block  
☐ IPv6 CIDR owned by me

Tenancy [Info](#)  
Default

## Step 2:

1. Create second VPC
2. Click on create VPC
  - Select VPC only
  - Give the name for second VPC as VPC 2
  - Give the CIDR block range as (20.0.0.0/16)
  - Finally click on create VPC as shown in below figure

**VPC settings**

Resources to create [Info](#)  
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

Name tag - *optional*  
Creates a tag with a key of 'Name' and a value that you specify.

vpc2

IPv4 CIDR block [Info](#)  
☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR  
20.0.0.0/16  
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)  
☒ No IPv6 CIDR block  
☐ IPAM-allocated IPv6 CIDR block  
☐ Amazon-provided IPv6 CIDR block  
☐ IPv6 CIDR owned by me

Tenancy [Info](#)  
Default

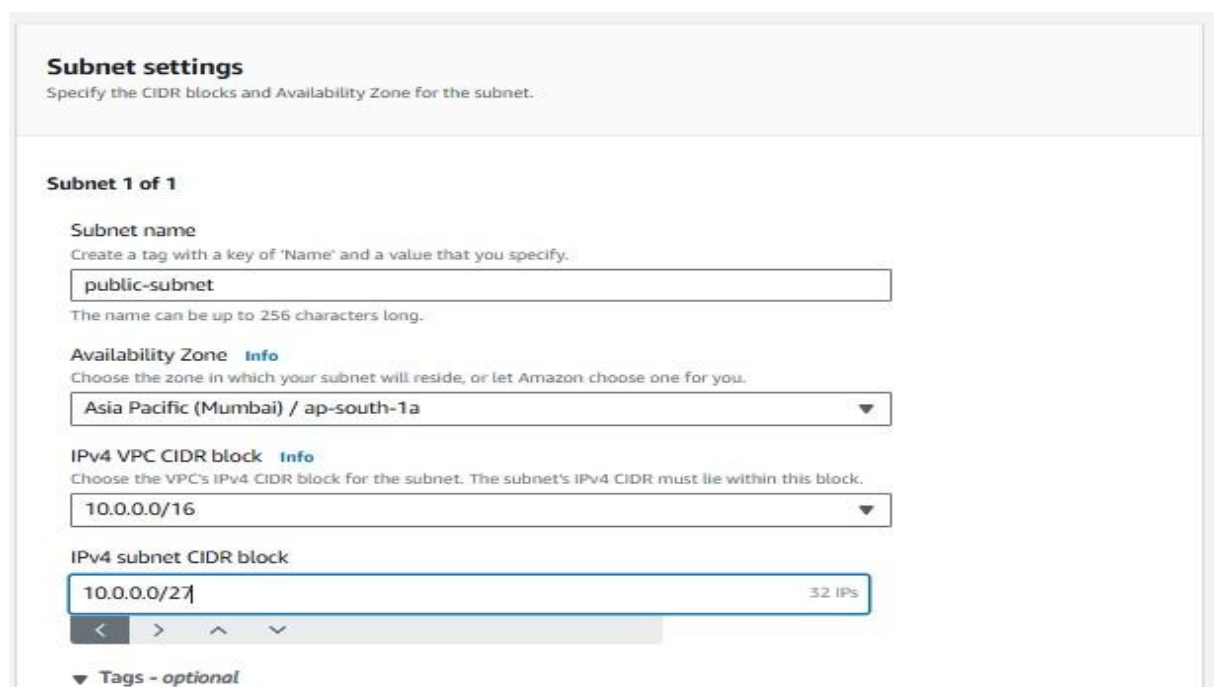
### Step 3:

1. Go to subnets
2. Create two subnets one is public subnet with created VPC 1 and another one is private subnet with created VPC 2
3. Click on create subnet
  - Select created VPC 1



The screenshot shows the 'VPC' configuration page. Under 'VPC ID', there is a dropdown menu with the value 'vpc-0b2a44ef00cd67c2b (vpc1)'. Below this, under 'Associated VPC CIDRs', there is a table with one entry: 'IPv4 CIDRs' with the value '10.0.0.0/16'.

- Edit subnet settings
- Give the name for subnet as public subnet
- Select the availability zone
- Select subnet CIDR block range as (10.0.0.0/27)
- Finally create the subnet as shown in below figure



The screenshot shows the 'Subnet settings' page. It includes the following fields and options:

- Subnet name:** A text input field containing 'public-subnet'.
- Availability Zone:** A dropdown menu showing 'Asia Pacific (Mumbai) / ap-south-1a'.
- IPv4 VPC CIDR block:** A dropdown menu showing '10.0.0.0/16'.
- IPv4 subnet CIDR block:** A text input field containing '10.0.0.0/27', with a '32 IPs' label to its right.
- Tags - optional:** A section at the bottom with a dropdown arrow.

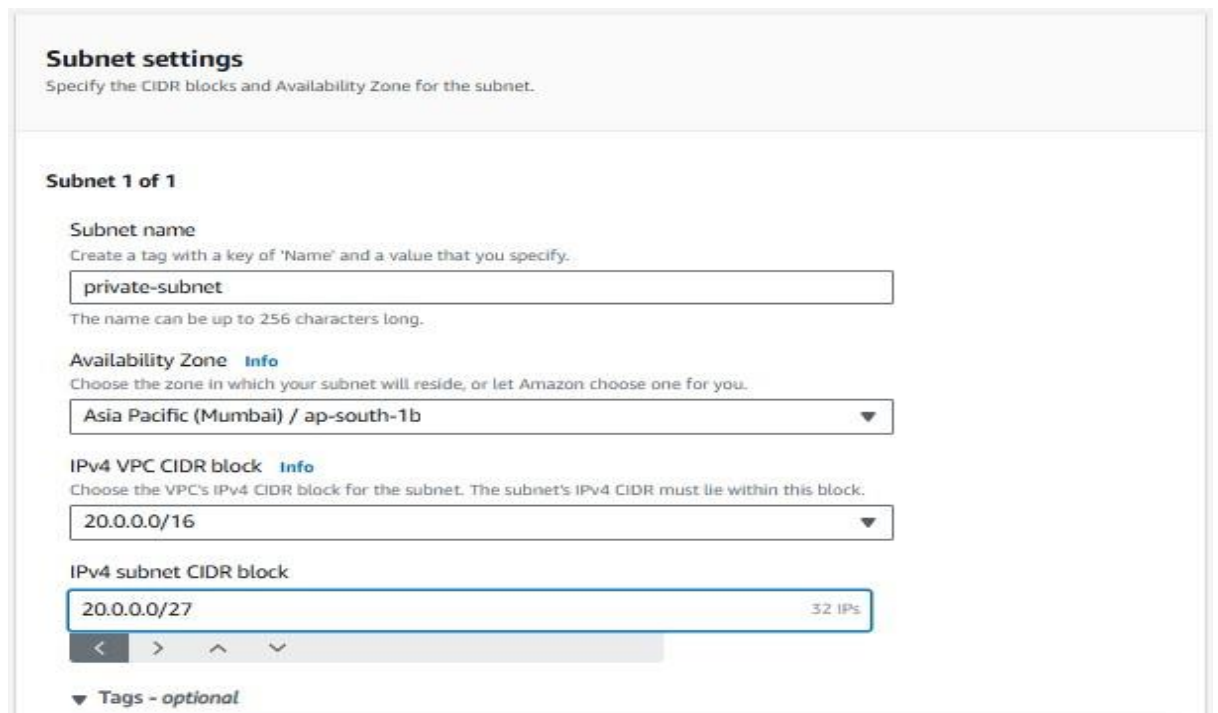
## Step 4:

1. Create second subnet
2. Click on create subnet
  - Select created VPC 2



The screenshot shows the 'VPC' configuration page. Under 'VPC ID', there is a dropdown menu with the value 'vpc-0a5e5c889de808043 (vpc2)'. Below this, under 'Associated VPC CIDRs', there is a table with one entry: 'IPv4 CIDRs' with the value '20.0.0.0/16'.

3. Edit subnet settings
  - Give the name for subnet as private subnet
  - Select the availability zone
  - Select subnet CIDR block range as (20.0.0.0/27)
  - Finally create the subnet as shown in below figure



The screenshot shows the 'Subnet settings' page. Under 'Subnet 1 of 1', there are four main sections: 'Subnet name' with a text input field containing 'private-subnet'; 'Availability Zone' with a dropdown menu showing 'Asia Pacific (Mumbai) / ap-south-1b'; 'IPv4 VPC CIDR block' with a dropdown menu showing '20.0.0.0/16'; and 'IPv4 subnet CIDR block' with a text input field containing '20.0.0.0/27' and a '32 IPs' indicator. At the bottom, there is a 'Tags - optional' section with a dropdown arrow.

## **Step 5:**

1. Go to route tables
2. Their already two route tables are created for created two VPC's
3. Give the names for two route tables as one is public route and another one is private route to avoid the confusions
4. Select the public-route and click on subnet associations and click on edit subnet associations and select public-subnet and click on save associations
5. Select the private-route and click on subnet associations and click on edit subnet associations and select private-subnet and click on save associations

## **Step 6:**

1. Select internet gateway
2. Click on create internet gateway
3. Give the name for internet gateway
4. Finally click on create internet gateway
5. Click on attach to a VPC
6. Select the created VPC 1
7. Finally click on attach internet gateway

## **Step 7:**

1. Go to route tables
2. Select the public-route
  - Click on routes
  - Click on edit routes
  - Click on add routes

- Select the internet gateway and click on save changes as shown in below figure

Destination: 10.0.0.0/16

Target: local

Status: Active

Internet Gateway

igw-0cc44df54f34d6041

Add route

## Step 8:

1. Select peering connections
2. Click on create peering connection
  - Give the name for peering
  - Select the VPC requester as VPC 1 and acceptor is VPC 2 as shown in below figure

**Peering connection settings**

Name - *optional*  
Create a tag with a key of 'Name' and a value that you specify.

peering

**Select a local VPC to peer with**

VPC ID (Requester)  
vpc-0b2a44ef00cd67c2b (vpc1)

VPC CIDRs for vpc-0b2a44ef00cd67c2b (vpc1)

CIDR	Status	Status reason
10.0.0.0/16	Associated	-

**Select another VPC to peer with**

Account  
☒ My account  
☐ Another account

Region  
☒ This Region (ap-south-1)  
☐ Another Region

VPC ID (Acceptor)  
vpc-0a5e5c889de808043 (vpc2)

VPC CIDRs for vpc-0a5e5c889de808043 (vpc2)

CIDR	Status	Status reason
20.0.0.0/16	Associated	-

## Step 9:

1. Go to route tables
2. Select the public-route
  - Click on routes
  - Click on edit routes
  - Click on add routes
  - Give created VPC 2 IP address and select peering connection and select created peering connection ID and click on save changes as shown in below figure

Destination	Target	Status
10.0.0.0/16	local	Active
<input type="text" value="Q 0.0.0.0/0"/>	<input type="text" value="Q local"/>	
	Internet Gateway	Active
<input type="text" value="Q 20.0.0.0/16"/>	<input type="text" value="Q igw-0cc44df54f34d6041"/>	
	Peering Connection	-
	<input type="text" value="Q pcx-09179c82ac2ba022d"/>	

3. Select the private-route
  - Click on routes
  - Click on edit routes
  - Click on add routes
  - Give created VPC 1 IP address and select peering connection and select created peering connection ID and click on save changes as shown in below figure

Destination	Target	Status
20.0.0.0/16	local	Active
<input type="text" value="Q 10.0.0.0/16"/>	<input type="text" value="Q local"/>	
	Peering Connection	-
	<input type="text" value="Q pcx-09179c82ac2ba022d"/>	

## Step 10:

1. Go to EC2 services
2. Create two instances
3. One instance with VPC 1 and another instance with VPC 2
4. Click on launch instance
  - Give the name for instance
  - Select the AMI as amazon Linux
  - Select the key pair
  - Edit the network settings
  - Select the VPC as VPC 1
  - Select the subnet as public subnet
  - Enable the auto-assign public IP as shown in below figure

The screenshot shows the 'Network settings' section of the AWS Management Console during an EC2 instance launch. The 'VPC' is set to 'vpc-0b2a44ef00cd67c2b (vpc1)' with a CIDR of '10.0.0.0/16'. The 'Subnet' is 'subnet-0d5f00cfc9bdf2625' (public-subnet) with a CIDR of '10.0.0.0/27'. The 'Auto-assign public IP' is set to 'Enable'. Under 'Firewall (security groups)', the 'Create security group' button is selected. The 'Security group name' is 'launch-wizard-17'. The 'Description' is 'launch-wizard-17 created 2024-09-22T15:29:09.647Z'. Under 'Inbound Security Group Rules', there is one rule for 'SSH' (TCP) on port '22' from 'Anywhere' (0.0.0.0/0).

**Network settings** [Info](#)

VPC - required [Info](#)

vpc-0b2a44ef00cd67c2b (vpc1)  
10.0.0.0/16

Subnet [Info](#)

subnet-0d5f00cfc9bdf2625 public-subnet  
VPC: vpc-0b2a44ef00cd67c2b Owner: 0540571099018  
Availability Zone: ap-south-1a Zone type: Availability Zone  
IP addresses available: 27 CIDR: 10.0.0.0/27

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - required

launch-wizard-17

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./()@[]+=&:[]!\$\*

Description - required [Info](#)

launch-wizard-17 created 2024-09-22T15:29:09.647Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP) 22, 0.0.0.0/0 [Remove](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh	TCP	22
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere	<a href="#">Add CIDR, prefix list or security</a> 0.0.0.0/0 X	e.g. SSH for admin desktop

- Finally click on launch instance



## 5. Create another instance

- Give the name for instance
- Select the AMI as amazon Linux
- Select the key pair
- Edit the network settings
- Select the VPC as VPC 2
- Select the subnet as private subnet
- Disable the auto-assign public IP as shown in below figure

The screenshot shows the 'Network settings' section of the AWS console. It includes the following fields and options:

- VPC - required:** A dropdown menu showing 'vpc-0a5e5c889de808043 (vpc2)' with a refresh icon.
- Subnet:** A dropdown menu showing 'subnet-012308116e41bac88' with a refresh icon and a 'Create new subnet' link.
- Auto-assign public IP:** A dropdown menu set to 'Disable'.
- Firewall (security groups):** Two buttons: 'Create security group' (selected) and 'Select existing security group'.
- Security group name - required:** A text input field containing 'launch-wizard-18'.
- Description - required:** A text input field containing 'launch-wizard-18 created 2024-09-22T15:55:58.720Z'.
- Inbound Security Group Rules:** A section with a 'Remove' button and a table of rules.

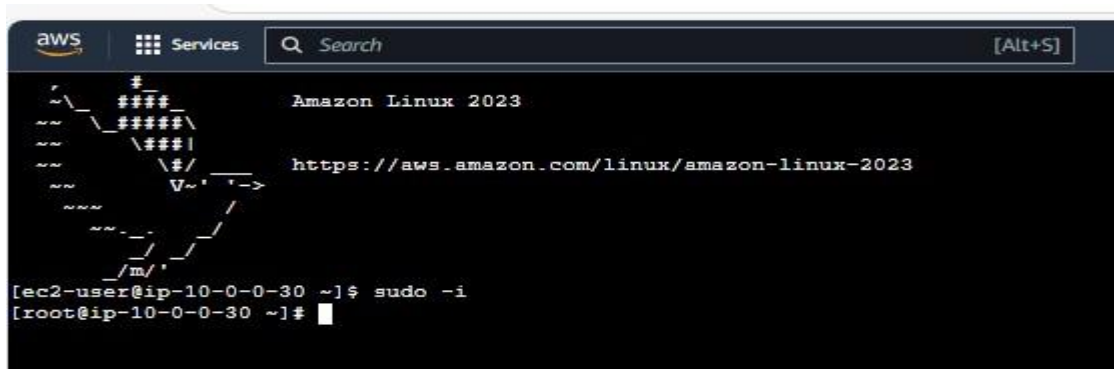
Type	Protocol	Port range	Source type	Source	Description - optional
ssh	TCP	22	Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

- Finally click on launch instance

## Step 11:

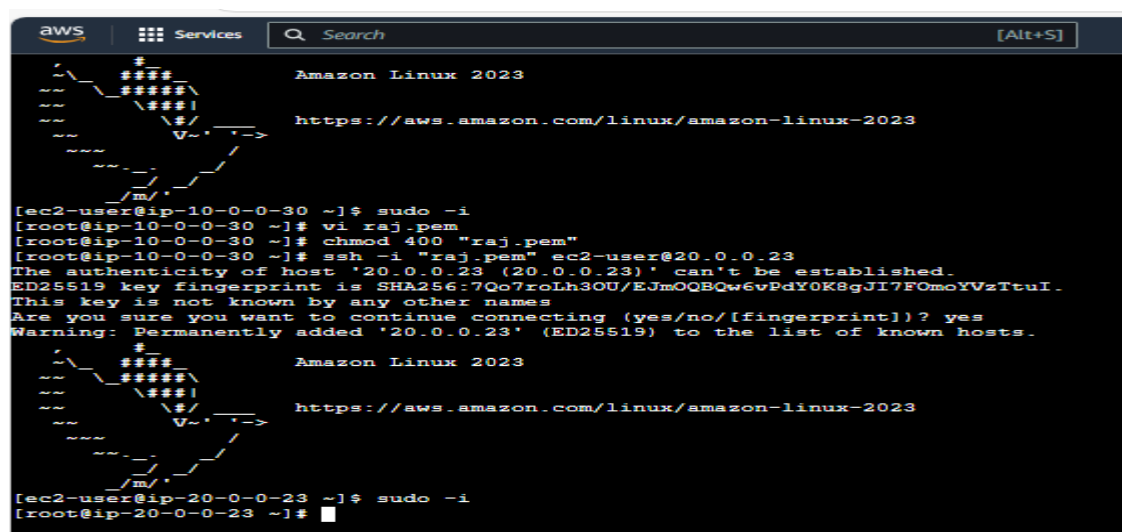
1. Select public-instance or instance 1
2. Click on connect option

3. Click on EC2 instance connect and click on connect option then EC2 instance is connected to the server and type `sudo -i` to switch root user as shown in below figure



```
aws Services Search [Alt+S]
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-0-30 ~]$ sudo -i
[root@ip-10-0-0-30 ~]#
```

4. Select private instance or instance 2
- Click on connect option
  - Select ssh client
  - Copy the key pair and go to server and type `vi` space then paste the copied key pair
  - Then `vi` editor is opened and copy the key pair content and paste in `vi` editor then save and quit
  - Go to `ssh` client and copy the `chmod 400 "raj.pem"` and paste in server
  - Copy the example URL and paste in server then server is switched from instance 1 to instance 2 server as shown in below figure



```
aws Services Search [Alt+S]
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-0-30 ~]$ sudo -i
[root@ip-10-0-0-30 ~]# vi raj.pem
[root@ip-10-0-0-30 ~]# chmod 400 "raj.pem"
[root@ip-10-0-0-30 ~]# ssh -i "raj.pem" ec2-user@20.0.0.23
The authenticity of host '20.0.0.23 (20.0.0.23)' can't be established.
ED25519 key fingerprint is SHA256:7Qo7roLh3OU/EJmOQBQw6vPdYOK8gJI7FOmoYVzTtuI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.0.0.23' (ED25519) to the list of known hosts.
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-20-0-0-23 ~]$ sudo -i
[root@ip-20-0-0-23 ~]#
```