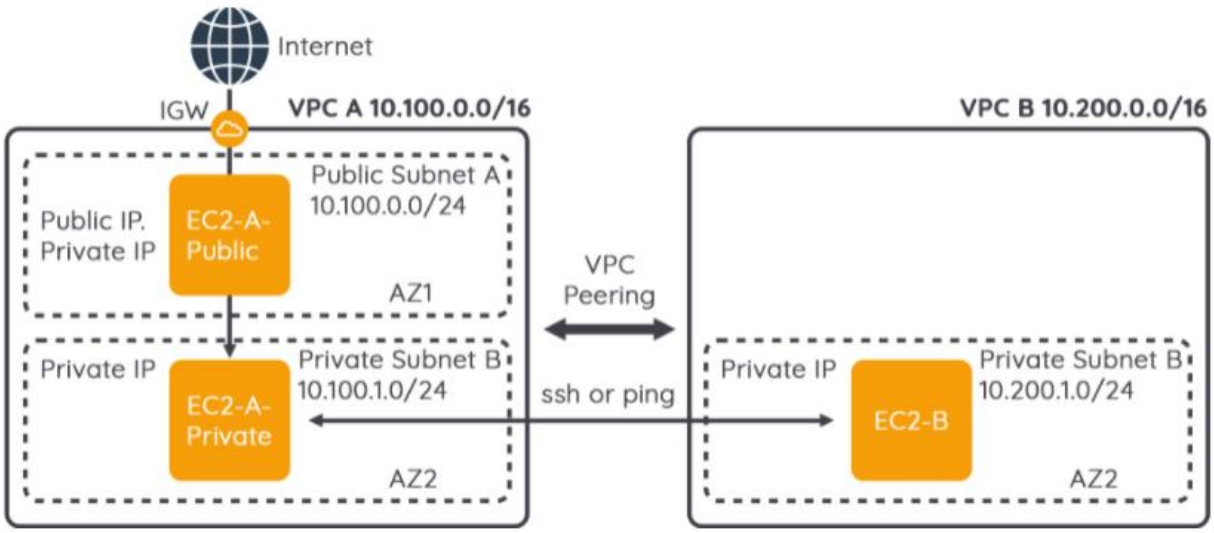
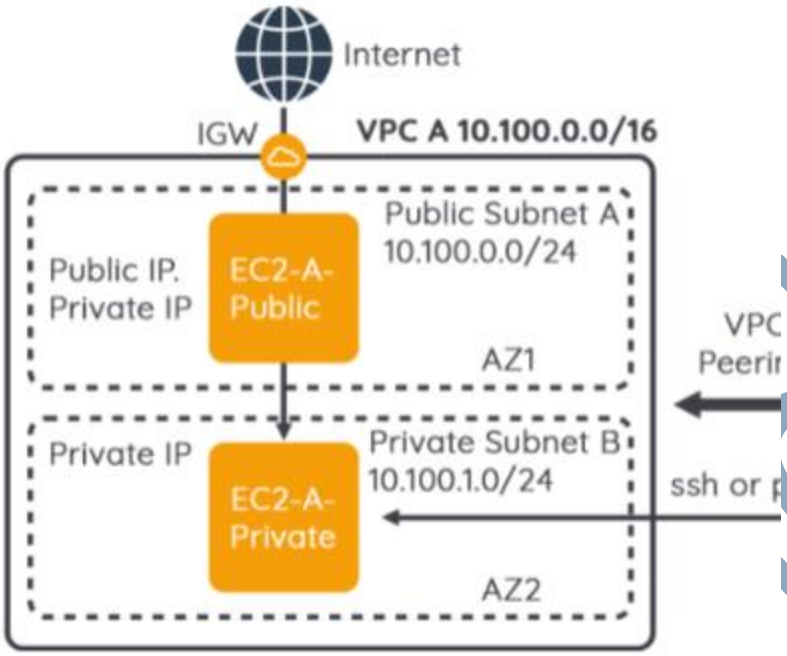
AWS VPC peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor an AWS Site-to-Site VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.



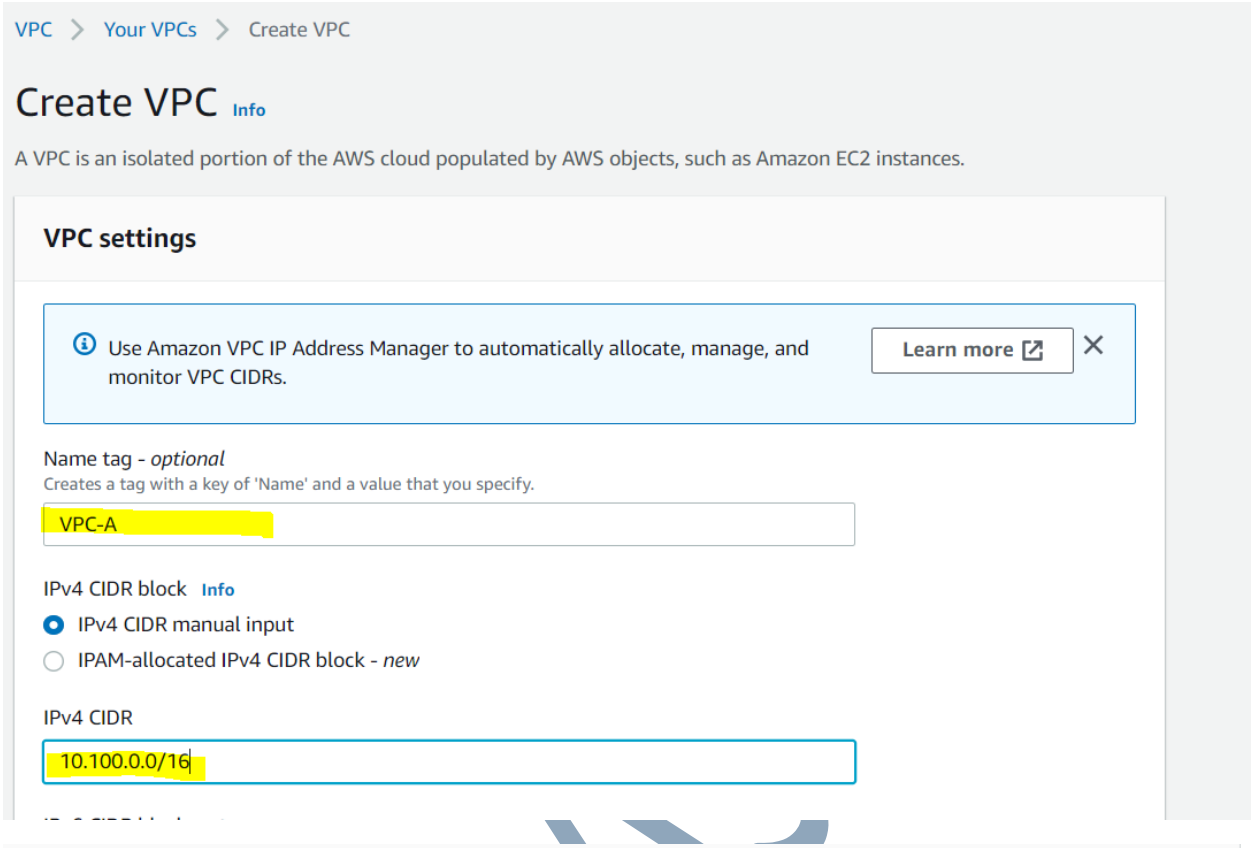
Steps:

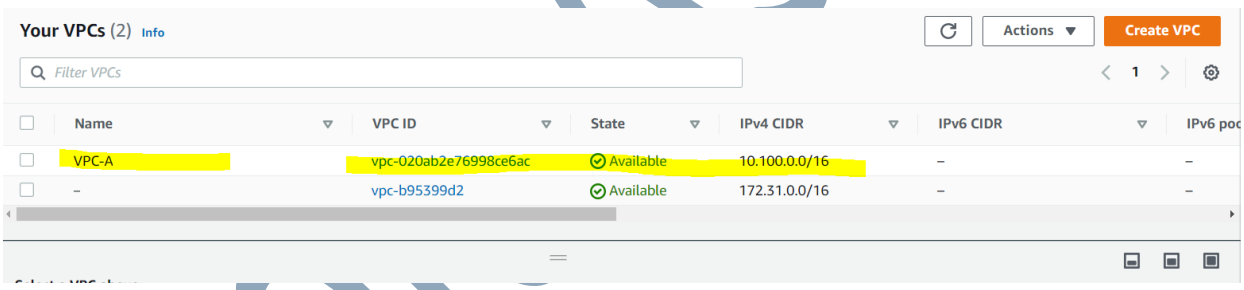


We are implementing above diagram public and private subnetes

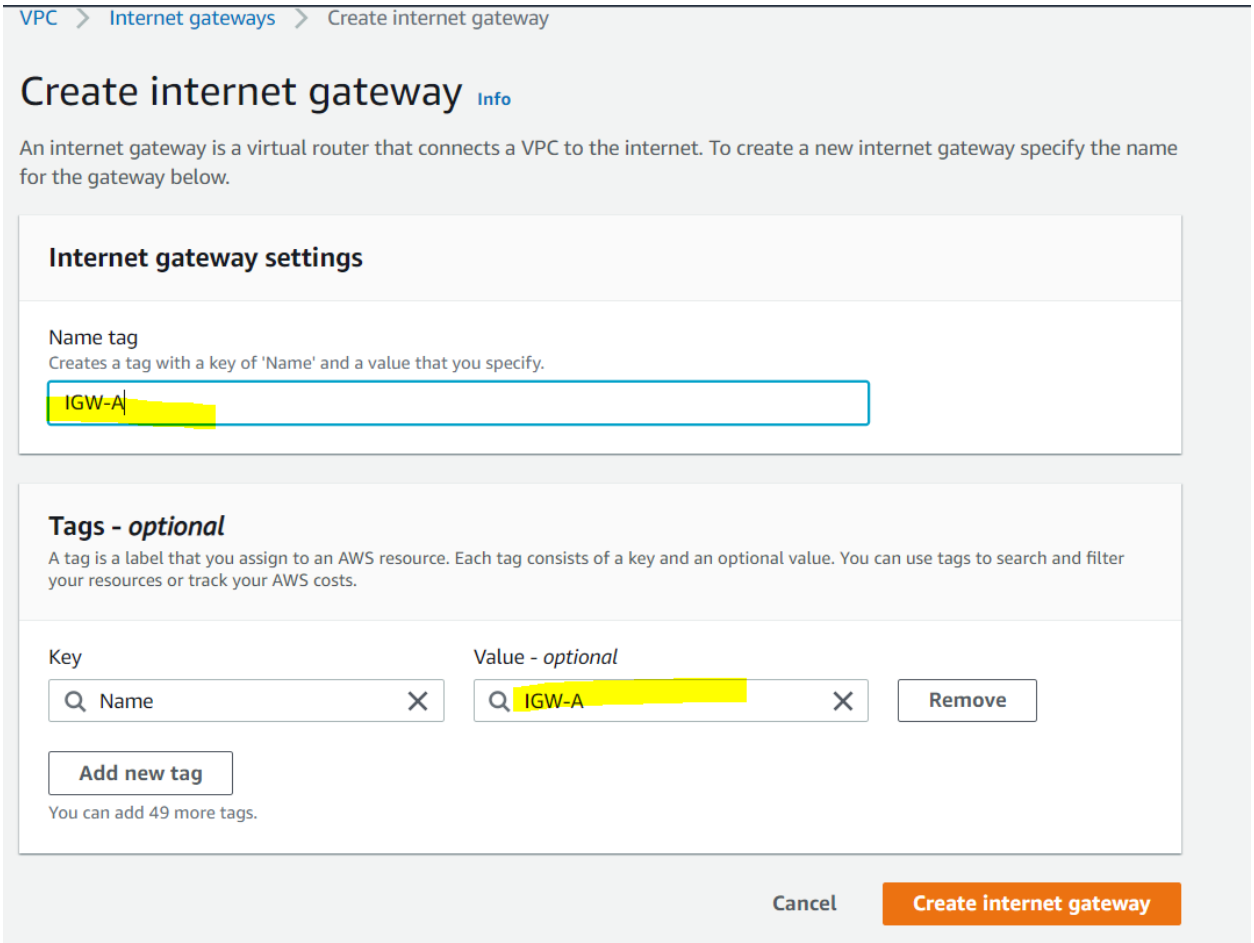
Creating a VPC A

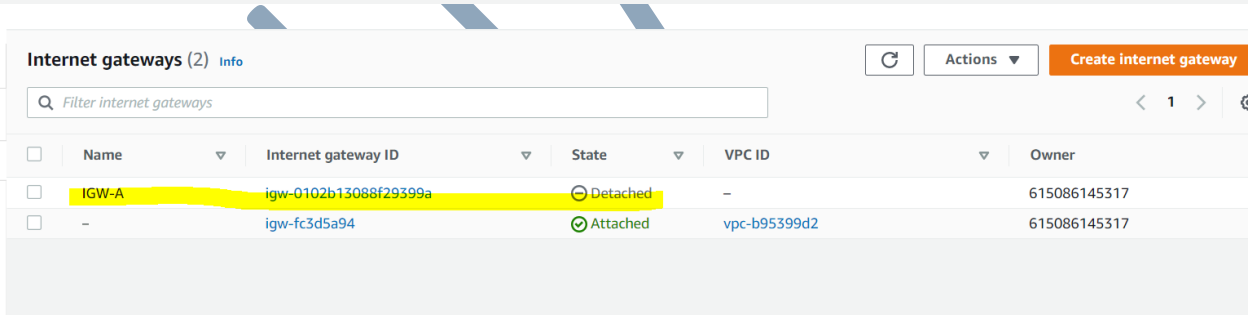
IP ADDRESS:10.100.0.0/16



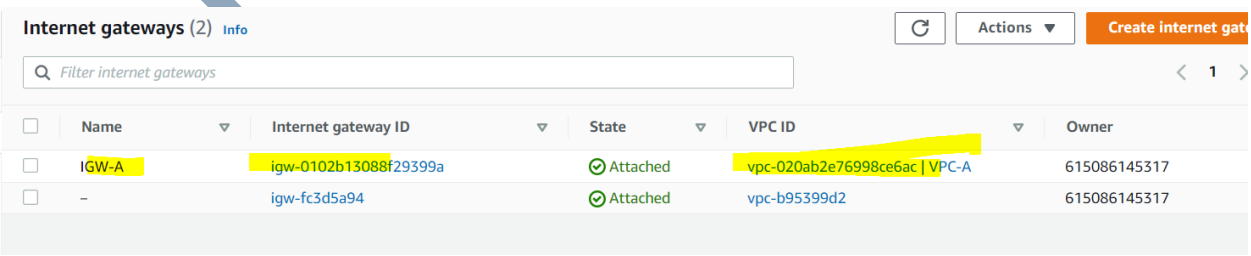


Step:2 Create a IGW for VPC-A





Attach to the VPC-A



Step:3 Creating a public and private subnets for VPC-A

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

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

VPC-A-SUBNET-PUBLIC

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference

IPv4 CIDR block Info

10.100.0.0/24

▼ Tags - *optional*

Key	Value - *optional*	
Name	VPC-A-SUBNET-PUBLIC	Remove

Add new tag

You can add 49 more tags.

Remove

Subnets (5) Info

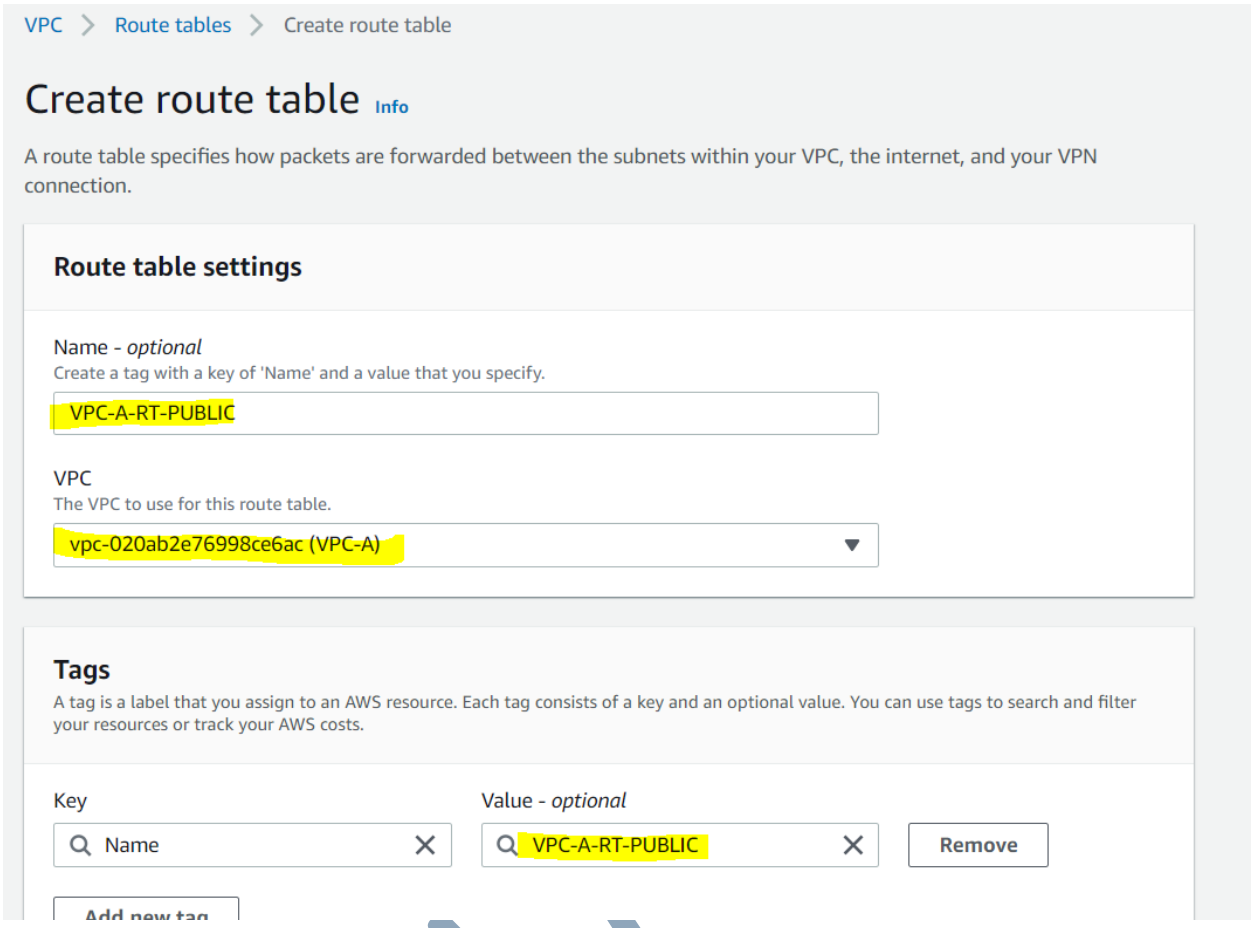
Actions ▼ | Create subnet

Filter subnets

1

Name	Subnet ID	State	VPC	IPv4 CIDR
VPC-A-SUBNET-PUBLIC	subnet-07a7107716841bc3b	Available	vpc-020ab2e76998ce6ac | VPC-A	10.100.0.0/24
VPC-A-SUBNET-PRIVATE	subnet-0c155bf5d3efa36a8	Available	vpc-020ab2e76998ce6ac | VPC-A	10.100.1.0/24
–	subnet-0e27d465	Available	vpc-b95399d2	172.31.32.0/20
–	subnet-1206265e	Available	vpc-b95399d2	172.31.0.0/20

Step: 3 Create a Route tables


VPC > Route tables > Create route table
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
VPC-A-RT-PUBLIC
VPC
The VPC to use for this route table.
vpc-020ab2e76998ce6ac (VPC-A)
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
VPC-A-RT-PUBLIC
Remove
Add new tag

VPC ID
Create subnets in this VPC.

vpc-020ab2e76998ce6ac (VPC-A)

Associated VPC CIDRs

IPv4 CIDRs

10.100.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

VPC-A-SUBNET-PRIVATE

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference

IPv4 CIDR block Info

10.100.1.0/24

▶ Tags - *optional*

Create a route table for public subnet Add route for internet

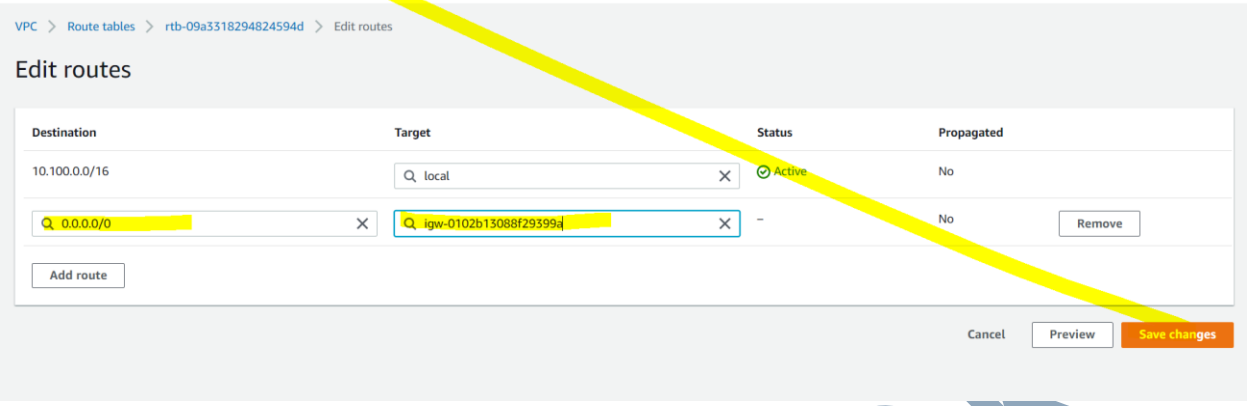
Route tables (1/3) Info

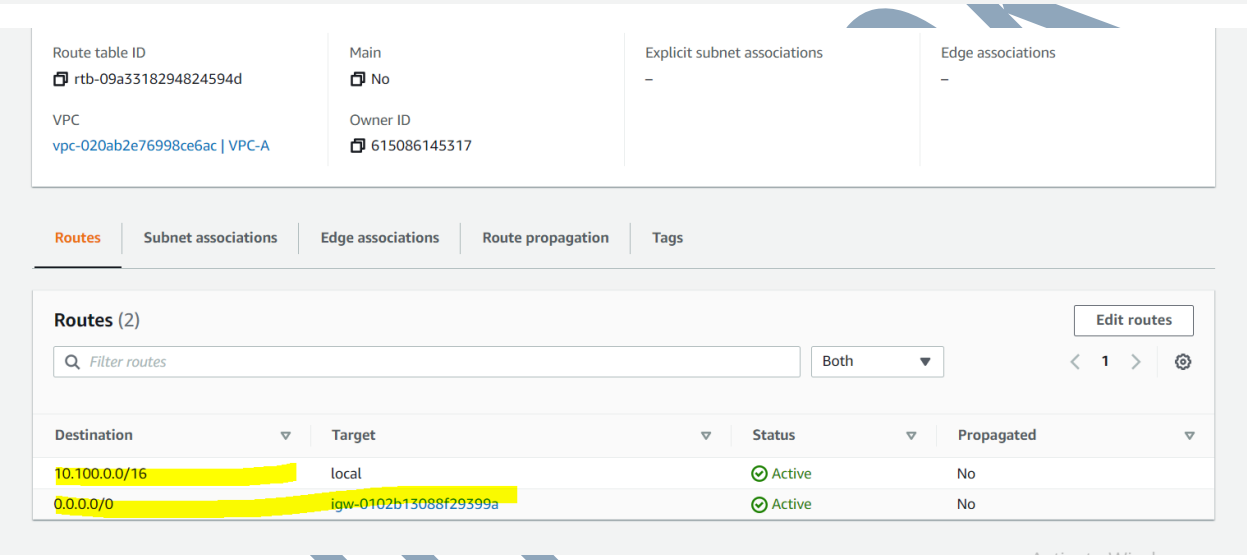
Actions | Create route table

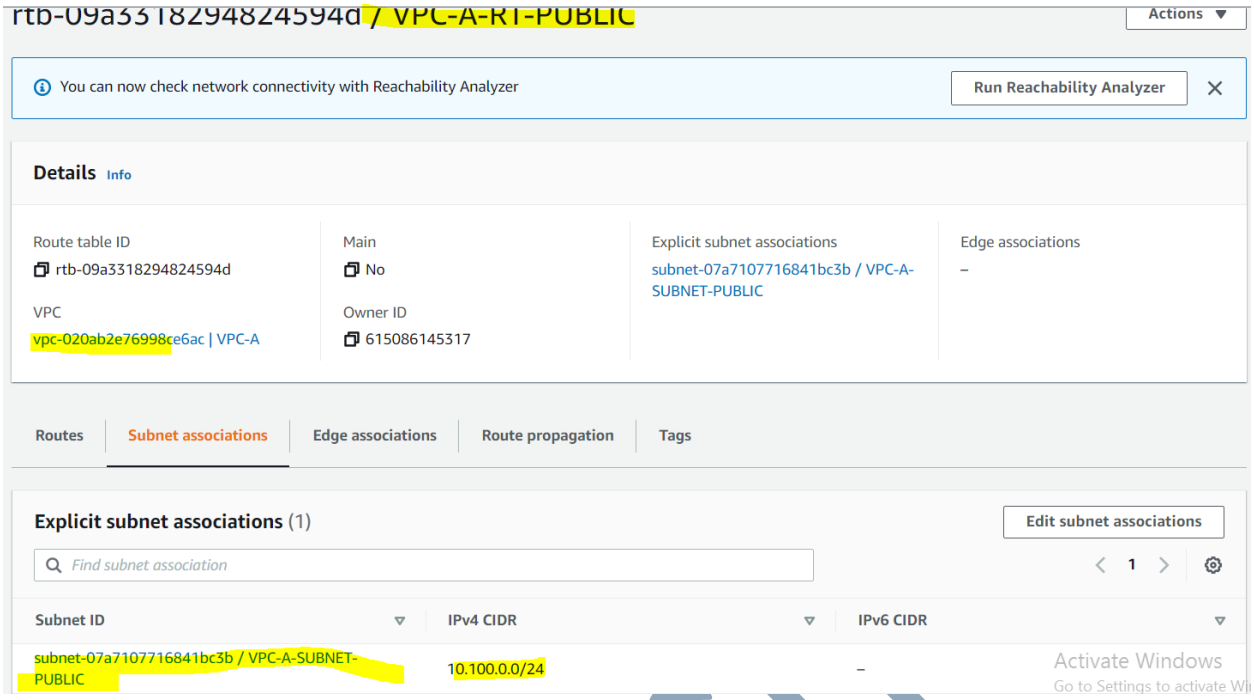
Filter route tables

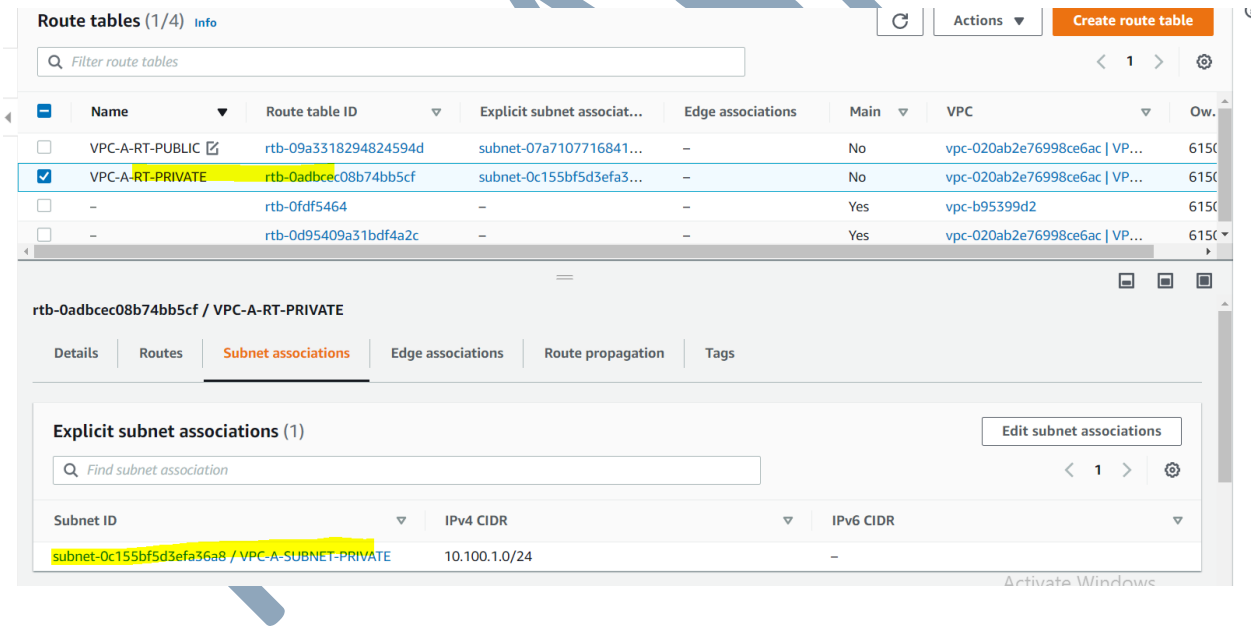
1

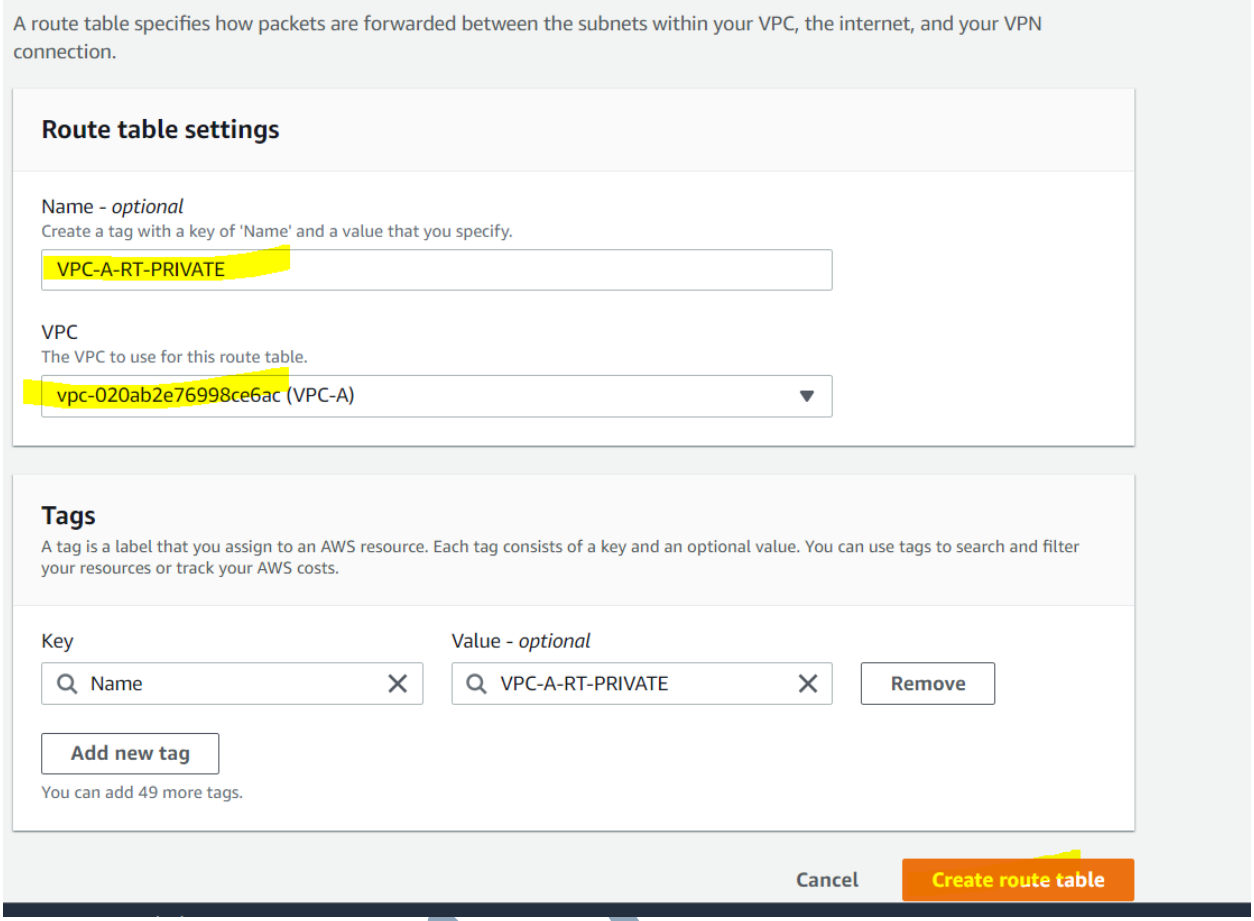
Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Ow
VPC-A-RT-PUBLIC	rtb-09a3318294824594d	–	–	No	vpc-020ab2e76998ce6ac | VP...	615
–	rtb-0fdf5464	–	–	Yes	vpc-b95399d2	615
–	rtb-0d95409a31bdf4a2c	–	–	Yes	vpc-020ab2e76998ce6ac | VP...	615


VPC > Route tables > rtb-09a3318294824594d > Edit routes
Edit routes
Destination
Target
Status
Propagated
10.100.0.0/16
local
Active
No
0.0.0.0/0
igw-0102b13088f29399a
–
No
Remove
Add route
Cancel
Preview
Save changes


Route table ID
rtb-09a3318294824594d
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-020ab2e76998ce6ac | VPC-A
Owner ID
615086145317
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Edit routes
Filter routes
Both
1
Destination
Target
Status
Propagated
10.100.0.0/16
local
Active
No
0.0.0.0/0
igw-0102b13088f29399a
Active
No


rtb-09a3318294824594d / VPC-A-RT-PUBLIC
Actions
You can now check network connectivity with Reachability Analyzer
Run Reachability Analyzer
Details Info
Route table ID
rtb-09a3318294824594d
Main
No
Explicit subnet associations
subnet-07a7107716841bc3b / VPC-A-SUBNET-PUBLIC
Edge associations
–
VPC
vpc-020ab2e76998ce6ac | VPC-A
Owner ID
615086145317
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (1)
Edit subnet associations
Find subnet association
Subnet ID
IPv4 CIDR
IPv6 CIDR
subnet-07a7107716841bc3b / VPC-A-SUBNET-PUBLIC
10.100.0.0/24
–
Activate Windows


Route tables (1/4) Info
Actions
Create route table
Filter route tables
Name
Route table ID
Explicit subnet associat...
Edge associations
Main
VPC
VPC-A-RT-PUBLIC
rtb-09a3318294824594d
subnet-07a7107716841...
–
No
vpc-020ab2e76998ce6ac | VP...
VPC-A-RT-PRIVATE
rtb-0adbcec08b74bb5cf
subnet-0c155bf5d3efa3...
–
No
vpc-020ab2e76998ce6ac | VP...
–
rtb-0fdf5464
–
–
Yes
vpc-b95399d2
–
rtb-0d95409a31bdf4a2c
–
–
Yes
vpc-020ab2e76998ce6ac | VP...
rtb-0adbcec08b74bb5cf / VPC-A-RT-PRIVATE
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (1)
Edit subnet associations
Find subnet association
Subnet ID
IPv4 CIDR
IPv6 CIDR
subnet-0c155bf5d3efa36a8 / VPC-A-SUBNET-PRIVATE
10.100.1.0/24
–



Create a ec2-instances for public and private subnets like below

1. Choose AMI | 2. Choose Instance Type | **3. Configure Instance** | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

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 lower pricing, assign an

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	Request Spot instances
Network	vpc-020ab2e76998ce6ac | VPC-A Create new VPC
Subnet	subnet-07a7107716841bc3b | VPC-A-SUBNET-PUB Create new subnet 251 IP Addresses available
Auto-assign Public IP	Enable
Hostname type	Use subnet setting (IP name)
DNS Hostname	Enable IP name IPv4 (A record) DNS requests Enable resource-based IPv4 (A record) DNS requests Enable resource-based IPv6 (AAAA record) DNS requests
Placement group	Add instance to placement group
Capacity Reservation	Open

Instances (2) Info

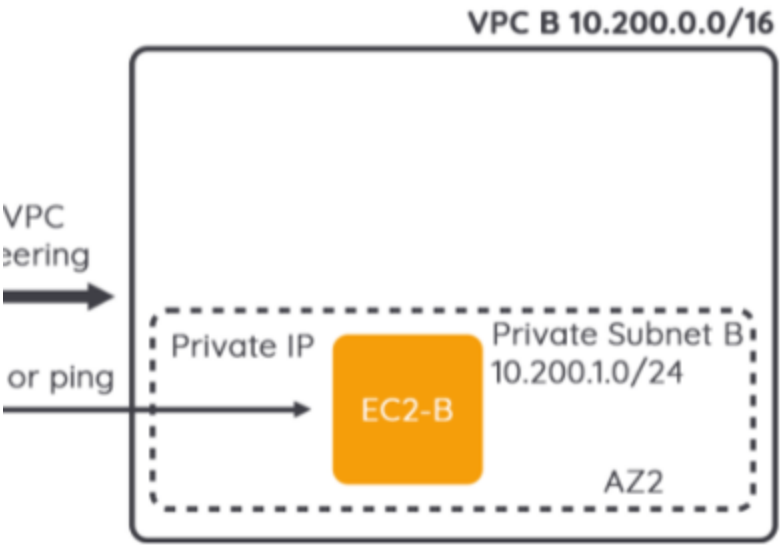
Connect | Instance state | Actions | Launch instances

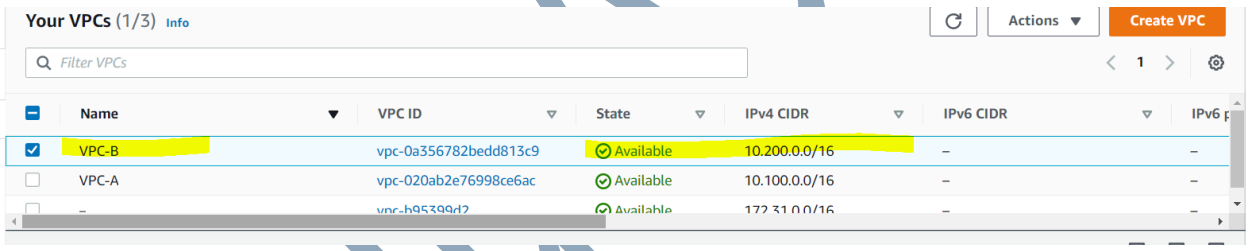
Search

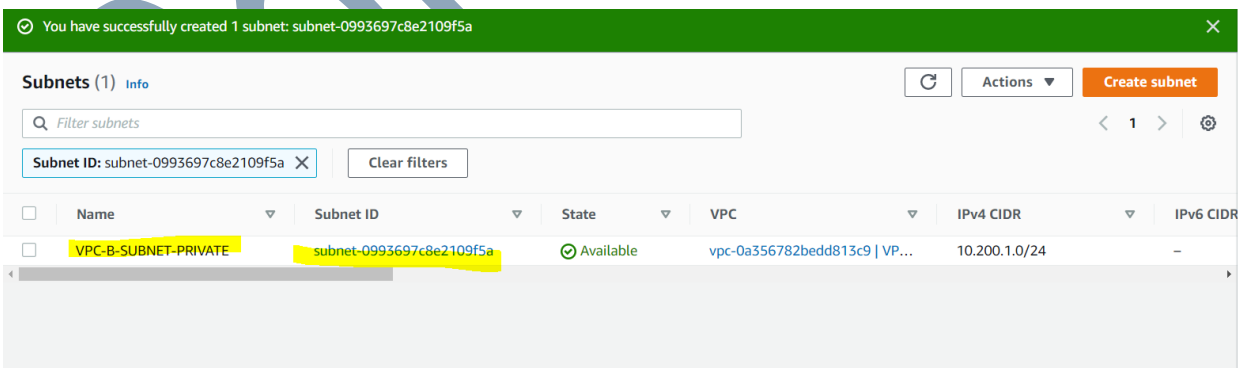
1

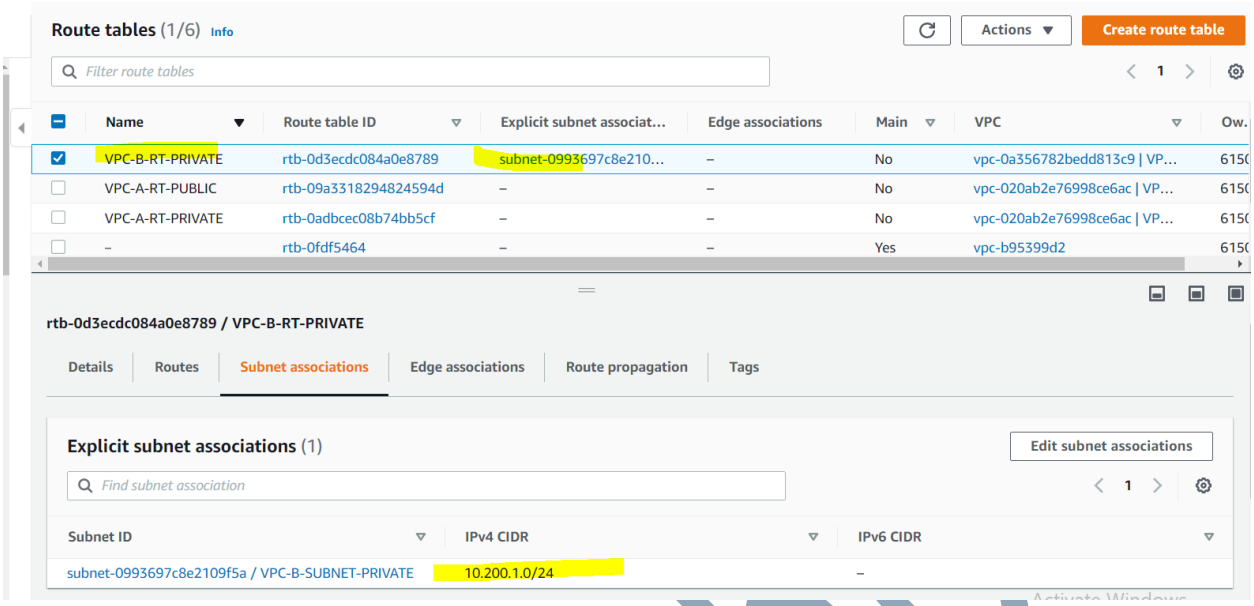
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv
VPC-A-ec2-private	i-0e519688f55f80cc0	Running	t2.micro	–	No alarms	ap-south-1b	–
VPC-A-ec2-pubilc	i-0e8b871cdd76db753	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b	–

Now we are creating VPC-B for vpc pering

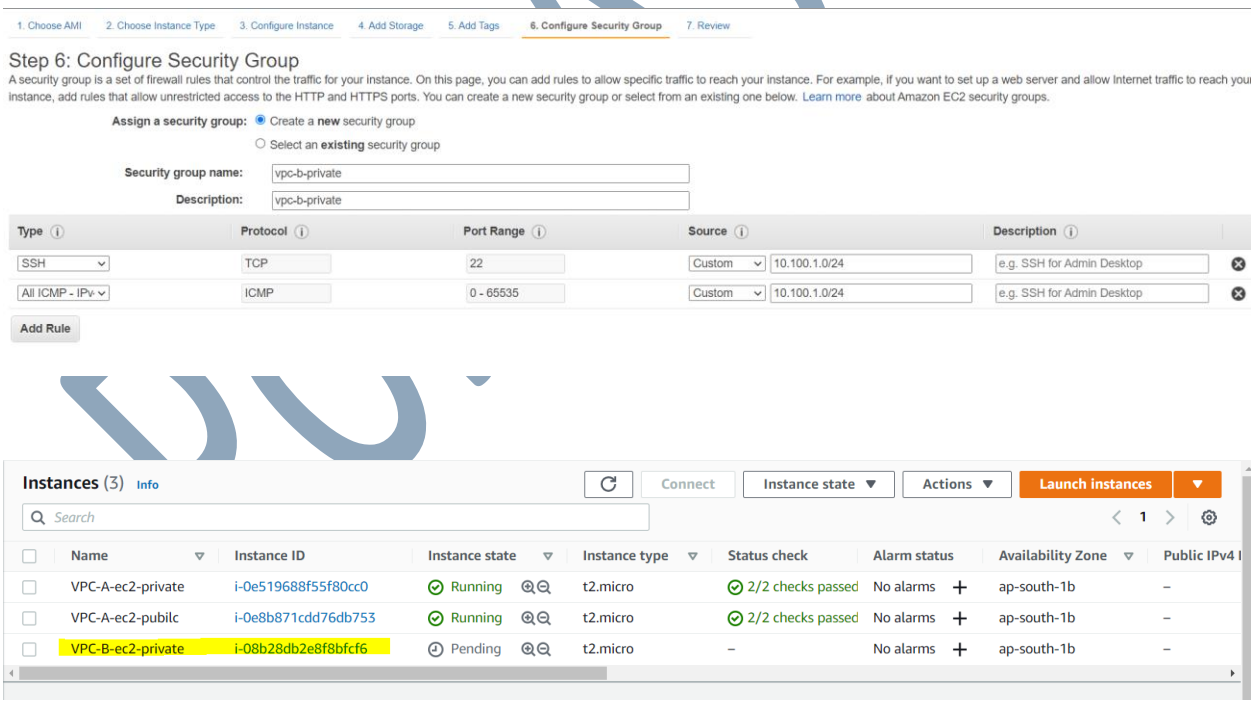

VPC B 10.200.0.0/16
VPC
eering
or ping
Private IP
EC2-B
Private Subnet B
10.200.1.0/24
AZ2


Your VPCs (1/3) Info
Actions
Create VPC
Filter VPCs
1
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
VPC-B
vpc-0a356782bedd813c9
Available
10.200.0.0/16
VPC-A
vpc-020ab2e76998ce6ac
Available
10.100.0.0/16


You have successfully created 1 subnet: subnet-0993697c8e2109f5a
Subnets (1) Info
Actions
Create subnet
Filter subnets
1
Subnet ID: subnet-0993697c8e2109f5a
Clear filters
Name
Subnet ID
State
VPC
IPv4 CIDR
IPv6 CIDR
VPC-B-SUBNET-PRIVATE
subnet-0993697c8e2109f5a
Available
vpc-0a356782bedd813c9 | VP...
10.200.1.0/24



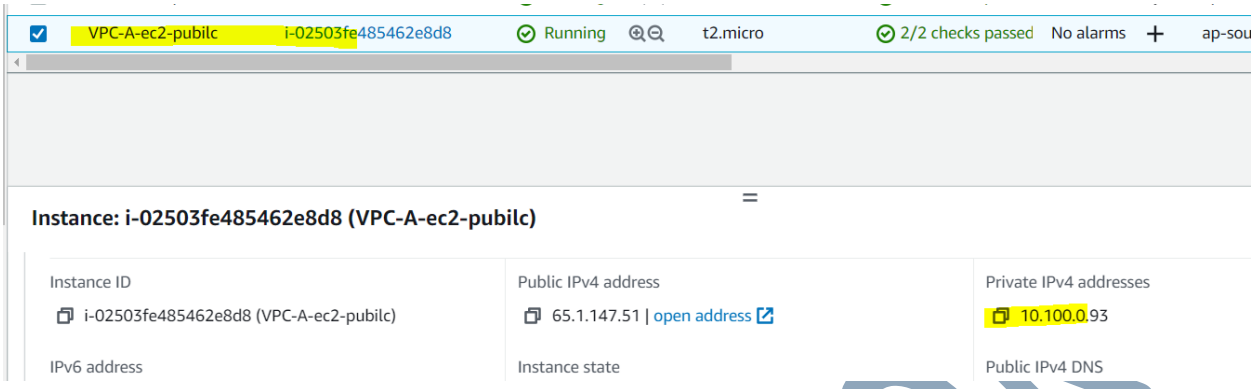
Now lunch the ec2 instance on VPC-B Region



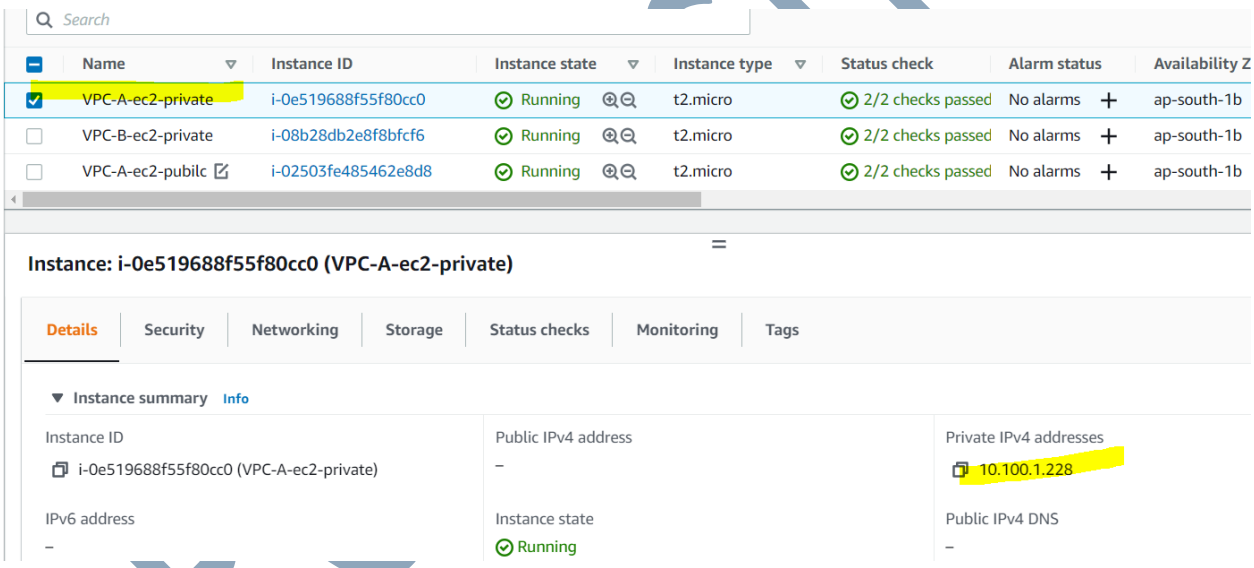
VPC peering checking:

Step:1 login to the public ip

EC2 Public Instance VPC A



EC2 Private Instance VPC A



EC2 Private Instance VPC B

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zon
VPC-A-ec2-private	i-0e519688f55f80cc0	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b
VPC-B-ec2-private	i-08b28db2e8f8bfcf6	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b
VPC-A-ec2-pubilc	i-02503fe485462e8d8	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b

Instance: i-08b28db2e8f8bfcf6 (VPC-B-ec2-private)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-08b28db2e8f8bfcf6 (VPC-B-ec2-private)	–	10.200.1.145
IPv6 address	**Instance state**	**Public IPv4 DNS**
–	Running	–

Private instance IP

ec2-user@ip-10-100-0-93:~

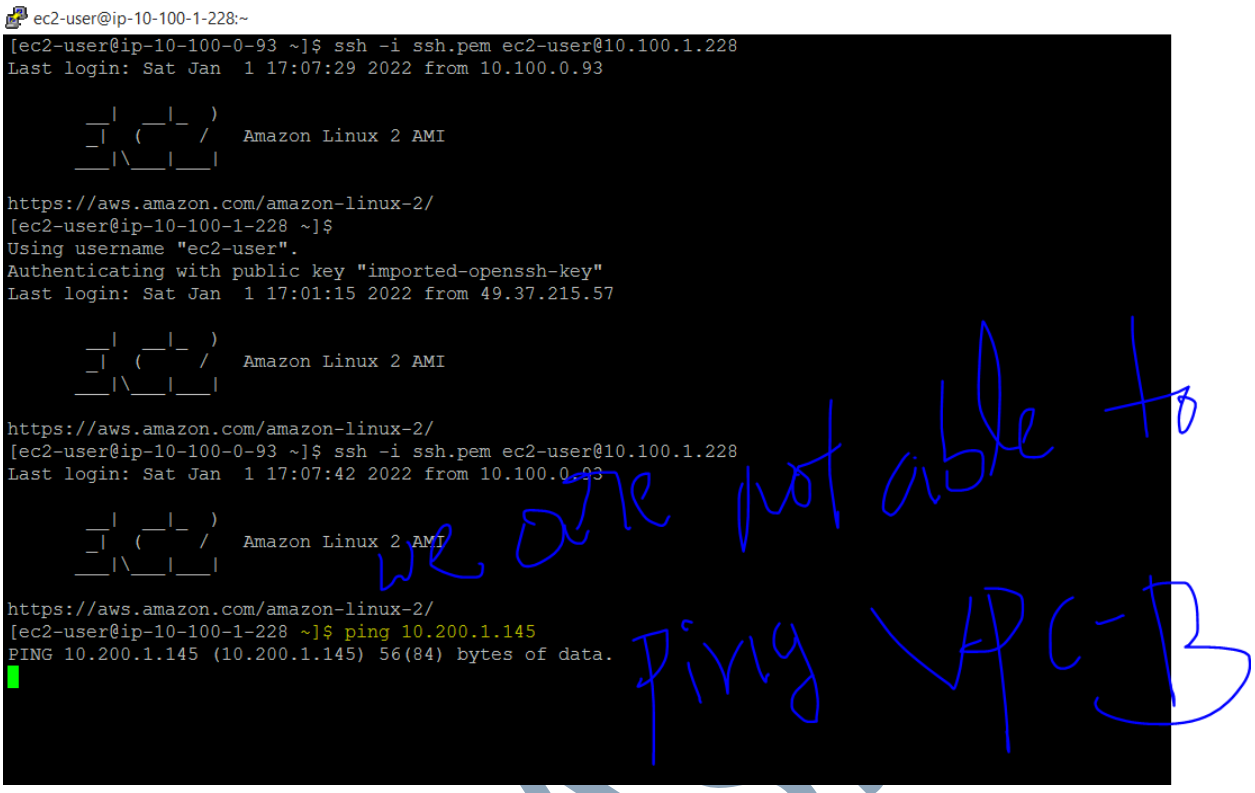
```
[ec2-user@ip-10-100-0-93 ~]$ ssh ec2-user@10.100.1.228
The authenticity of host '10.100.1.228 (10.100.1.228)' can't be established.
ECDSA key fingerprint is SHA256:WaqHqpXRbnB56+7QRbbyGNzSqPHkG2VGvJ4Lv+HMkw8.
ECDSA key fingerprint is MD5:ee:18:de:da:30:01:ed:fe:a7:9b:5e:b4:c1:91:4b:5f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.100.1.228' (ECDSA) to the list of known hosts.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-100-0-93 ~]$
```

ec2-user@ip-10-100-1-228:~

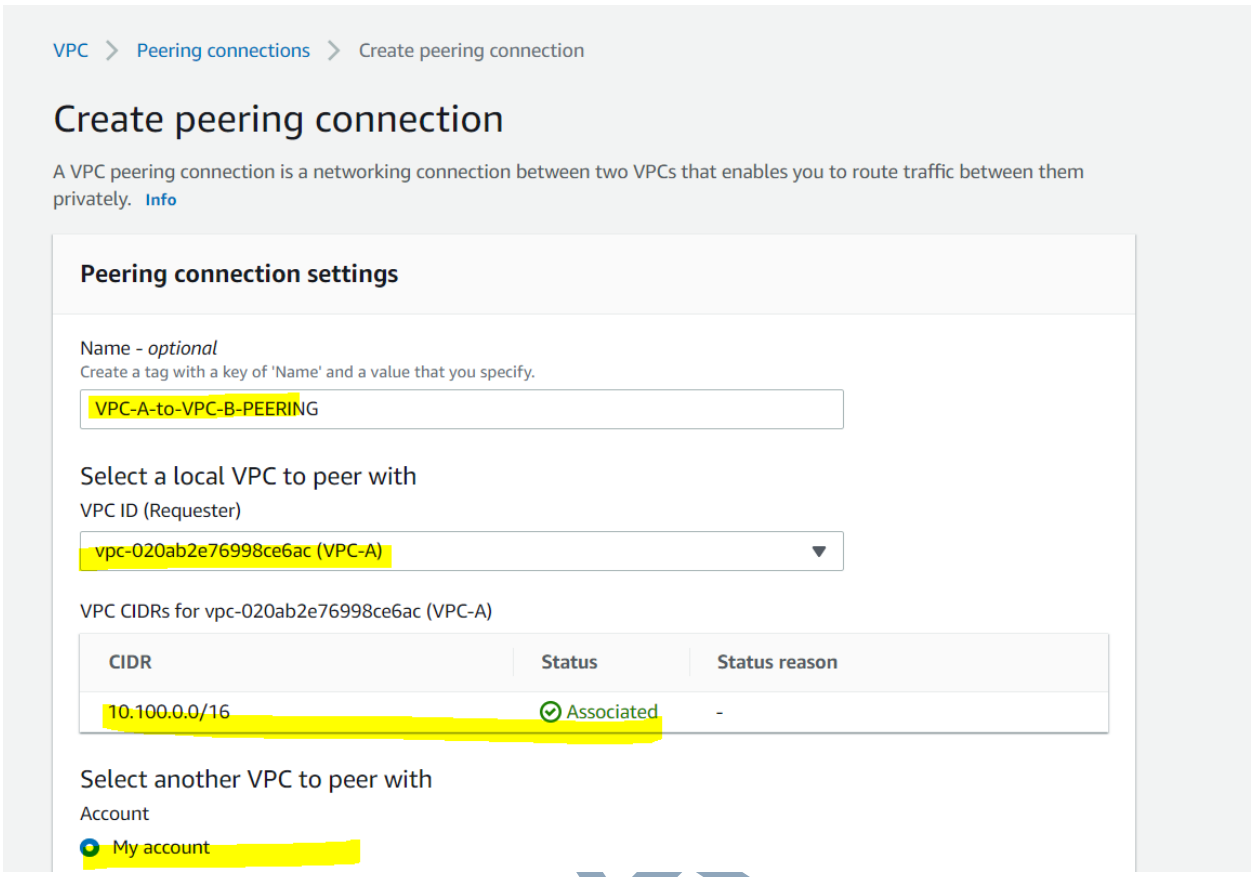
```
[ec2-user@ip-10-100-0-93 ~]$ ssh -i ssh.pem ec2-user@10.100.1.228
Last login: Sat Jan  1 17:07:29 2022 from 10.100.0.93

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-100-1-228 ~]$
```



Finally now we need to create vpc peering connection


VPC > Peering connections > Create peering connection
Create peering connection
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Info
Peering connection settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
VPC-A-to-VPC-B-PEERING
Select a local VPC to peer with
VPC ID (Requester)
vpc-020ab2e76998ce6ac (VPC-A)
VPC CIDRs for vpc-020ab2e76998ce6ac (VPC-A)
CIDR
Status
Status reason
10.100.0.0/16
Associated
-
Select another VPC to peer with
Account
My account

Region

This Region (ap-south-1)

Another Region

VPC ID (Accepter)

vpc-09ca2460884e6a22c (VPC-B)

VPC CIDRs for vpc-09ca2460884e6a22c (VPC-B)

CIDR	Status	Status reason
10.200.0.0/16	Associated	-

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	VPC-A-to-VPC-B-PEERING	Remove

Add new tag

You can add 49 more tags.

Cancel | Create peering connection

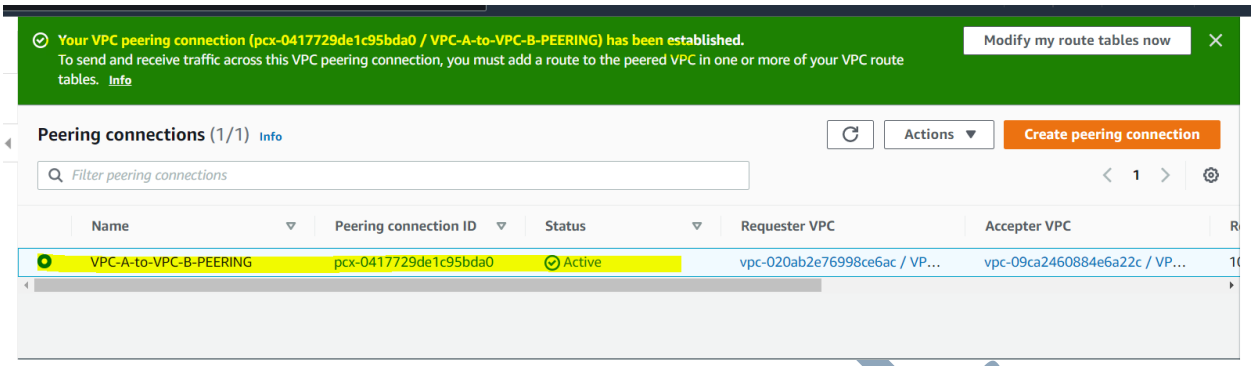
Peering connections (1) Info

Actions | Create peering connection

Filter peering connections

1

Name	Peering connection ID	Status	Requester VPC	Accepter VPC
VPC-A-to-VPC-B-PEERING	pcx-0417729de1c95bda0	Pending acceptance	vpc-020ab2e76998ce6ac / VP…	vpc-09ca2460884e6a22c / VP…




```
[ec2-user@ip-10-100-0-93 ~]$ ssh -i ssh.pem ec2-user@10.100.1.228
Last login: Sat Jan  1 17:07:42 2022 from 10.100.0.93

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-100-1-228 ~]$ ping 10.200.1.145
PING 10.200.1.145 (10.200.1.145) 56(84) bytes of data.
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Sat Jan  1 17:13:11 2022 from 49.37.215.57

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-100-0-93 ~]$ ssh -i ssh.pem ec2-user@10.100.1.228
Last login: Sat Jan  1 17:13:13 2022 from 10.100.0.93

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-100-1-228 ~]$ ping 10.200.1.145
PING 10.200.1.145 (10.200.1.145) 56(84) bytes of data.
64 bytes from 10.200.1.145: icmp_seq=1 ttl=64 time=0.403 ms
64 bytes from 10.200.1.145: icmp_seq=2 ttl=64 time=0.508 ms
64 bytes from 10.200.1.145: icmp_seq=3 ttl=64 time=0.423 ms
64 bytes from 10.200.1.145: icmp_seq=4 ttl=64 time=0.496 ms
64 bytes from 10.200.1.145: icmp_seq=5 ttl=64 time=0.407 ms
64 bytes from 10.200.1.145: icmp_seq=6 ttl=64 time=0.458 ms
64 bytes from 10.200.1.145: icmp_seq=7 ttl=64 time=0.417 ms
64 bytes from 10.200.1.145: icmp_seq=8 ttl=64 time=0.437 ms
64 bytes from 10.200.1.145: icmp_seq=9 ttl=64 time=0.424 ms
^C
--- 10.200.1.145 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8168ms
rtt min/avg/max/mdev = 0.403/0.441/0.508/0.041 ms
[ec2-user@ip-10-100-1-228 ~]$
```