Virtual Private Cloud...

PREPARED BY:

Abhilash Hasankar

OBJECTIVE:

To dermine working of two VPC's connected in two different regions and to develop a model which connects their private instances.

What is AWS VPC?

Amazon Virtual Private Cloud (VPC) provides us a logical isolated section of the Amazon Web Services (AWS) Cloud where we can launch AWS resources in a virtual network. We have complete control over virtual networking environment, which includes our own IP address range, configuring Internet gateway, creation of subnets, configuration of route tables and network gateways etc.

What is VPC Peering?

A VPC peering connection is a networking connection between two different VPCs in different AWS accounts/regions that enables you to route traffic between them using private IPv4/IPv6 addresses. With this configuration we can privately connect two different networks of two different VPC's and make them behave as a single network. **Note:** In order to form VPC peering both the network must not have overlapped CIDR's otherwise they won't connect, and VPC peering is not Transitive must be established for each VPC that needs to be communicated.

Flow Diagram:

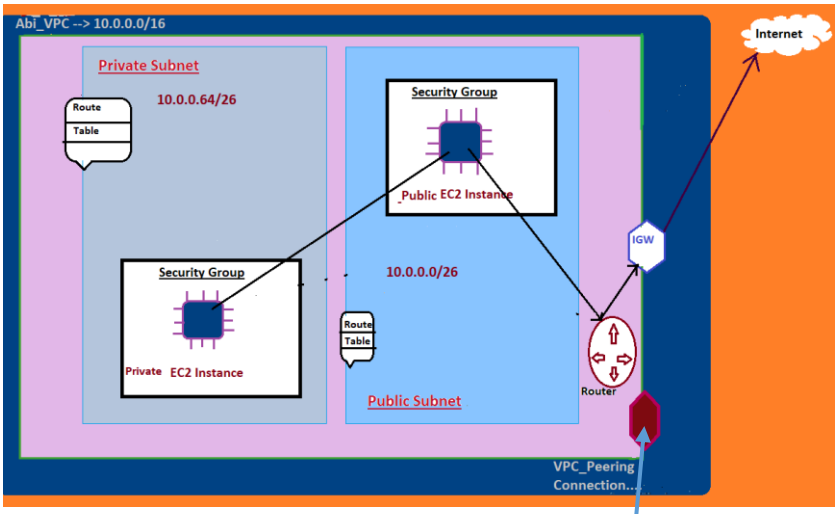


fig: 1 Abi_VPC

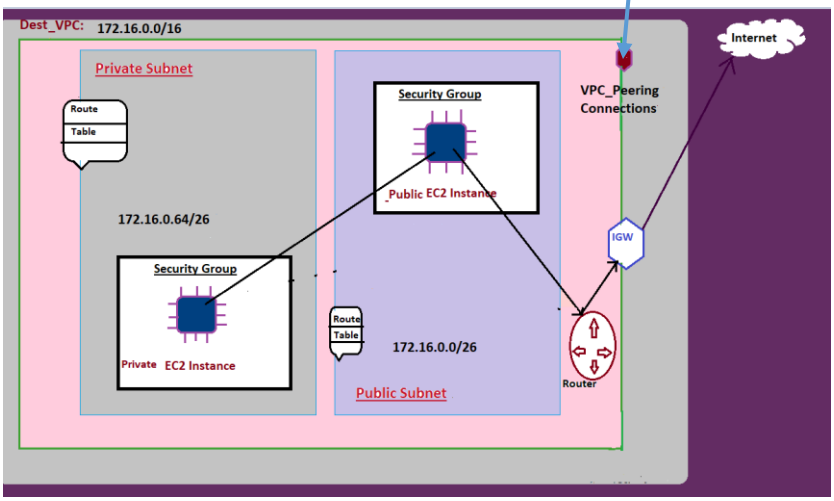


fig: 2 Dest_VPC

Explaination:

In this project We have two separate VPC's one in North Virginia (with name as Abi_VPC) with Ip address range 10.0.0.0/16 and more in Ohio (With name as Destination_VPC) with Ip address range 172.16.0.0/16. In Dest_VPC I've configured public subnet with IP range 172.16.0.0/26, and private subnet with IP range 172.16.0.64/26, attached an Internet Gateway IGW to the public subnet so that it can connect to the Internet. After this configuration two EC2 instances are launched one in public subnet which could be accessed from Internet and one more in private subnet. We have configured public instance such a way that it could be accessed (i-e SSH) from internet, but private instance is configured in such a way that it

could only be accessed (i-e SSH) through public instance and this public instance is also know as **Bastion Host.** We use Bastion host to ssh into our private EC2 instance. In order to achieve this configuration we need to edit the inbound rule of security group for private Instance to allow SSH from public Instance security group. And also we need add the ssh key pair of private instance in the public Instance in order to grant ssh key access. The same has been configured in Abi_VPC.

After this configuration, we need to form a VPC peering without this we cannot form connection between the instances. For this we need to send peering request from one vpc to another be it in same or cross region/account, later modify the route tables of both VPC's and the destination would be CIDR of other VPC. After peering we can now easily ping the other instances.

Results:

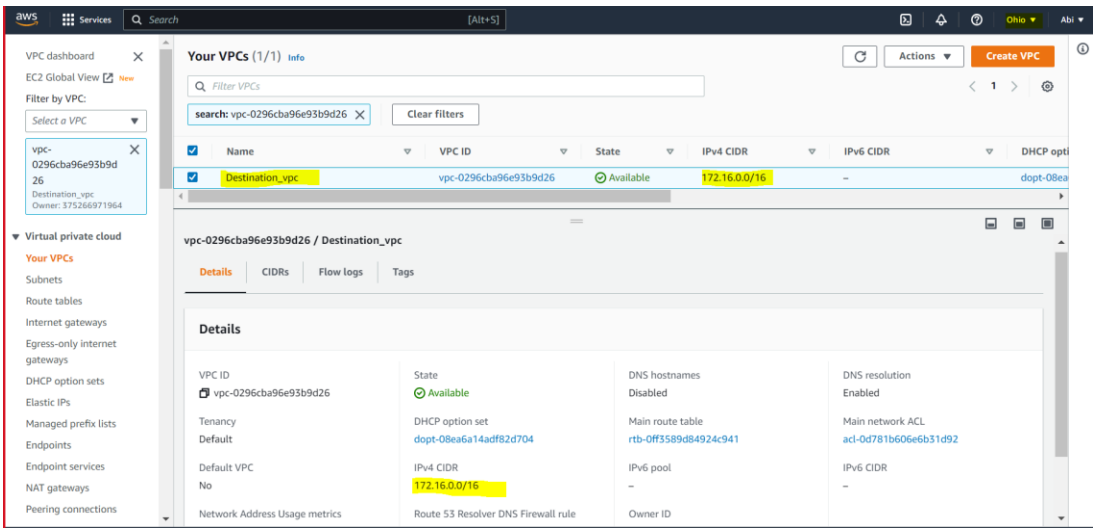


fig: 3 Dest_VPC with address range.

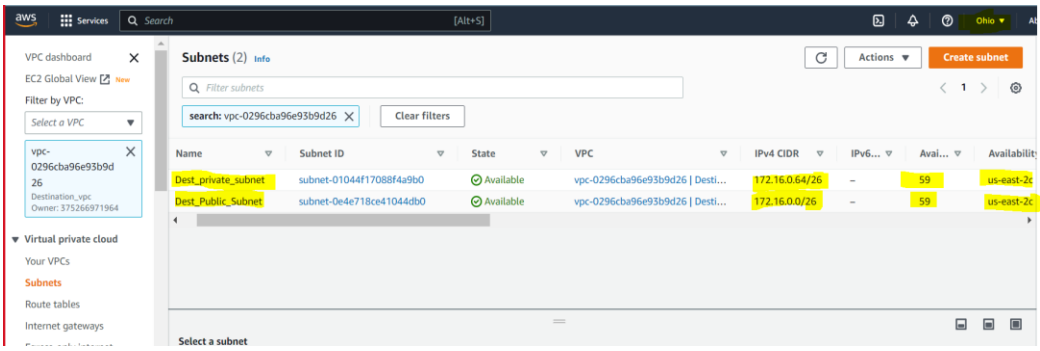


fig: 4 Public and Private Subnet range of Dest_VPC.

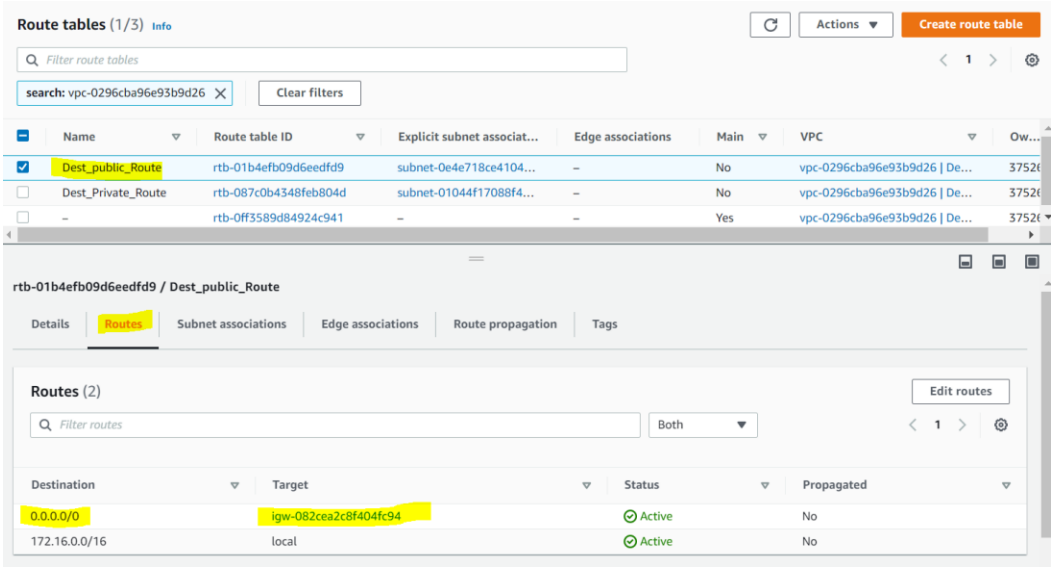


fig: 5 Public Route table of Dest_VPC with internet gateway(IGW) attached .

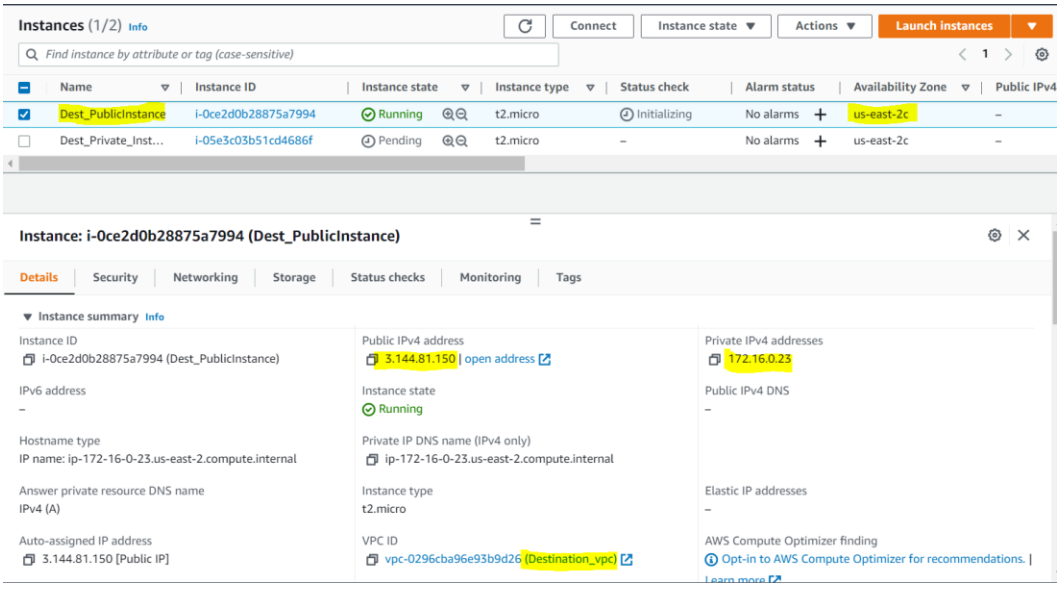


fig: 6 Instance created in Public_Subnet of Dest_VPC.

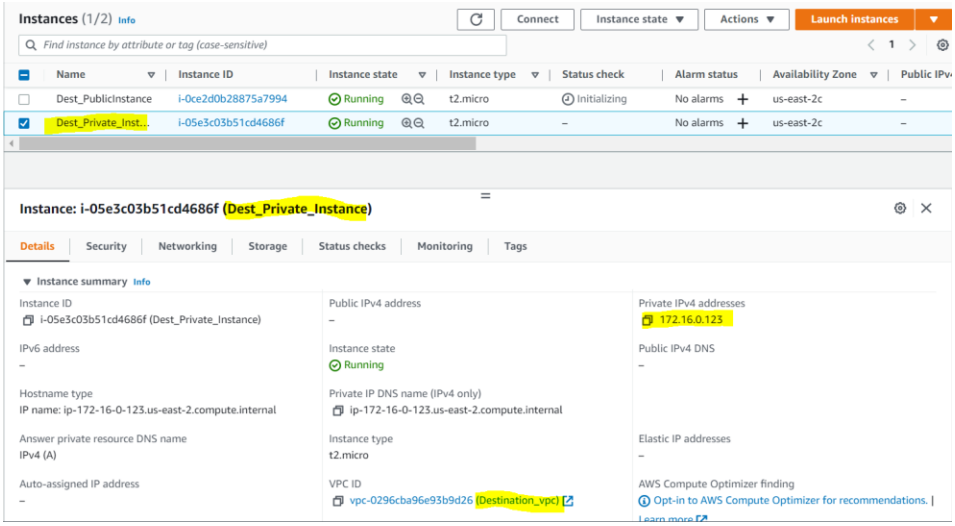


fig: 7 Instance created in Private_Subnet of Dest_VPC.

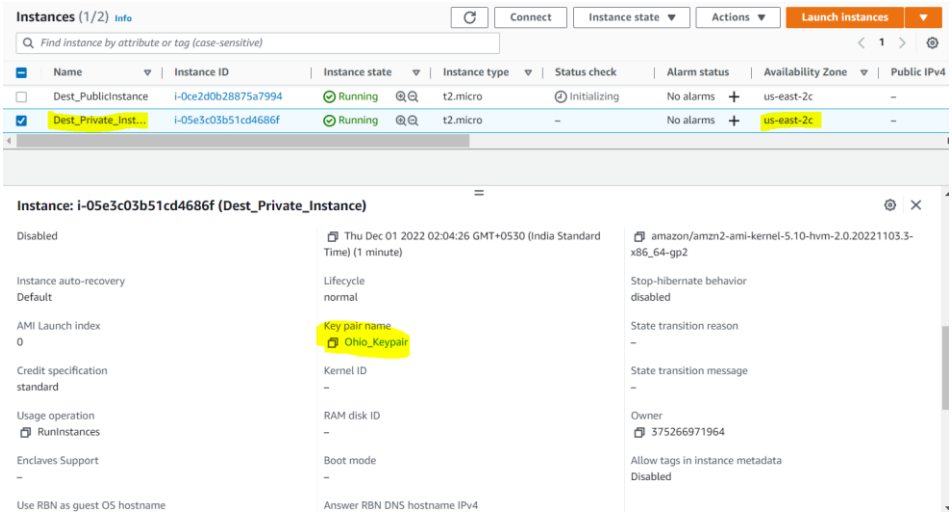


fig: 8 Private Instance with SSH key pair.

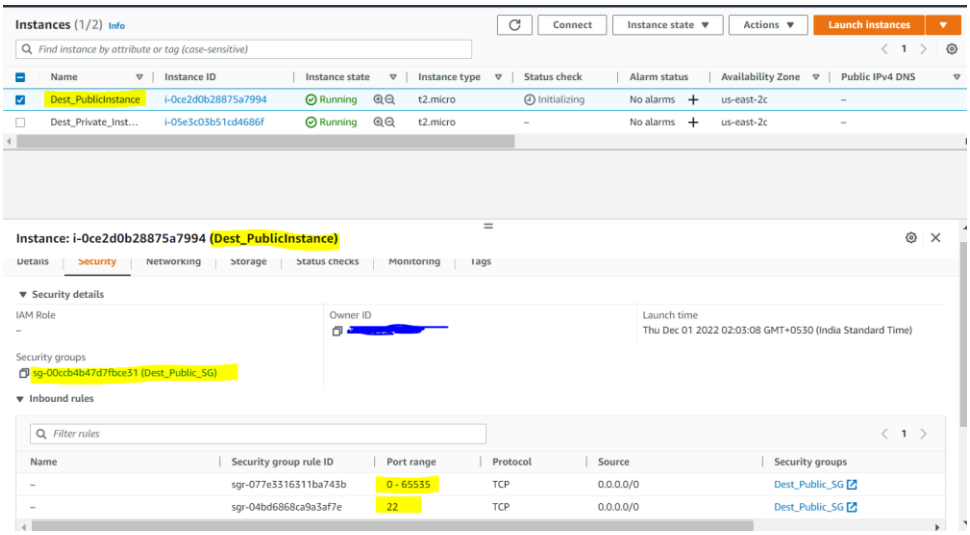


fig: 9 Public Instance's Inbound Security Group.

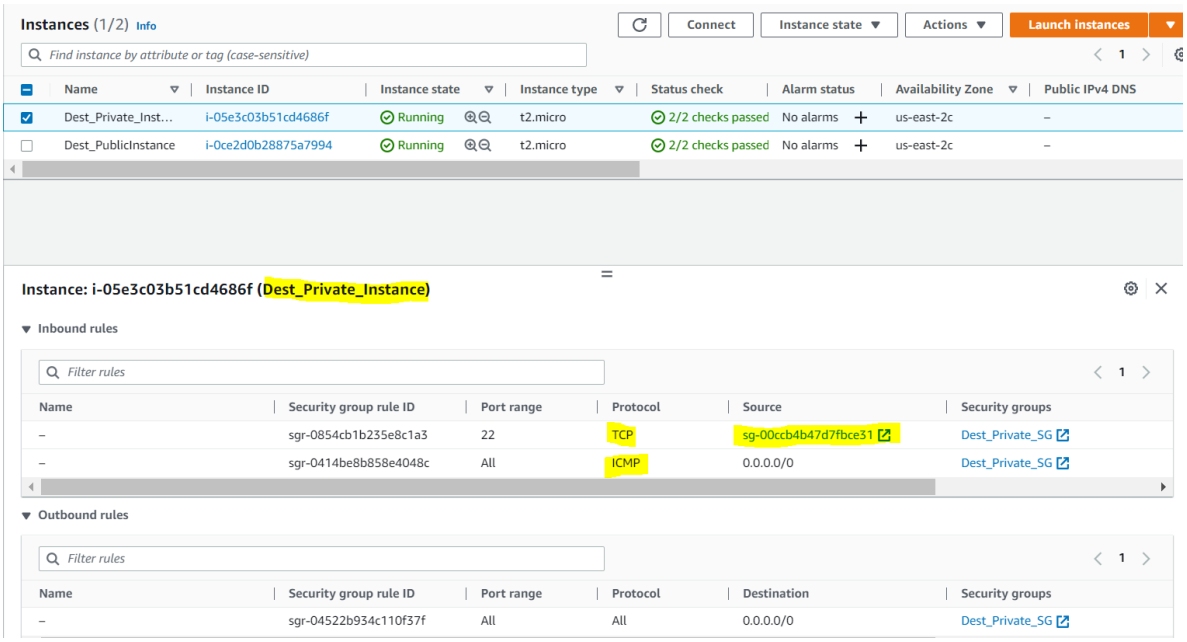


fig: 10 Private Instance's Inbound Security Group with allowed SSH from public instance.

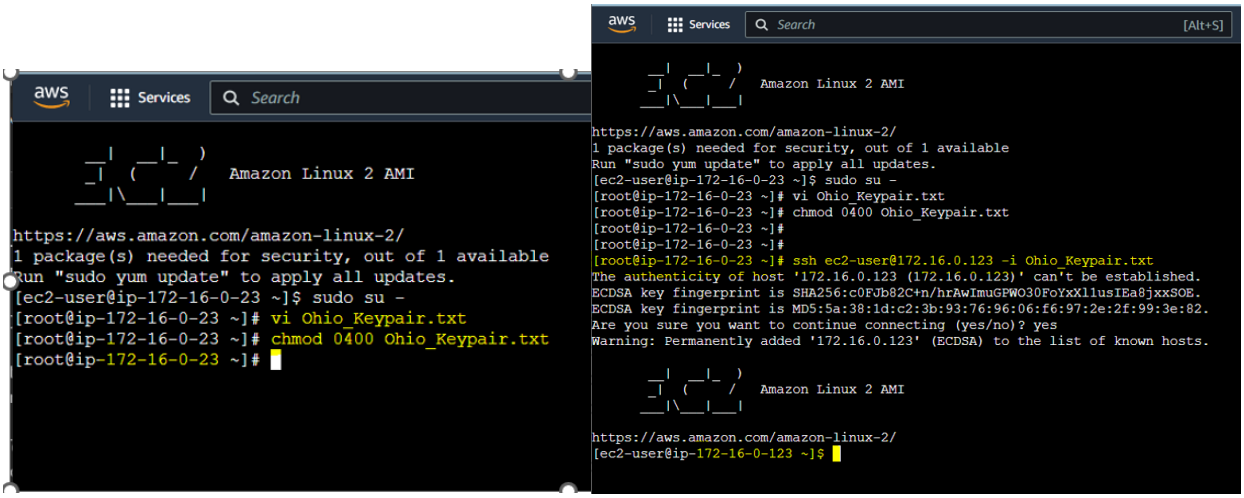
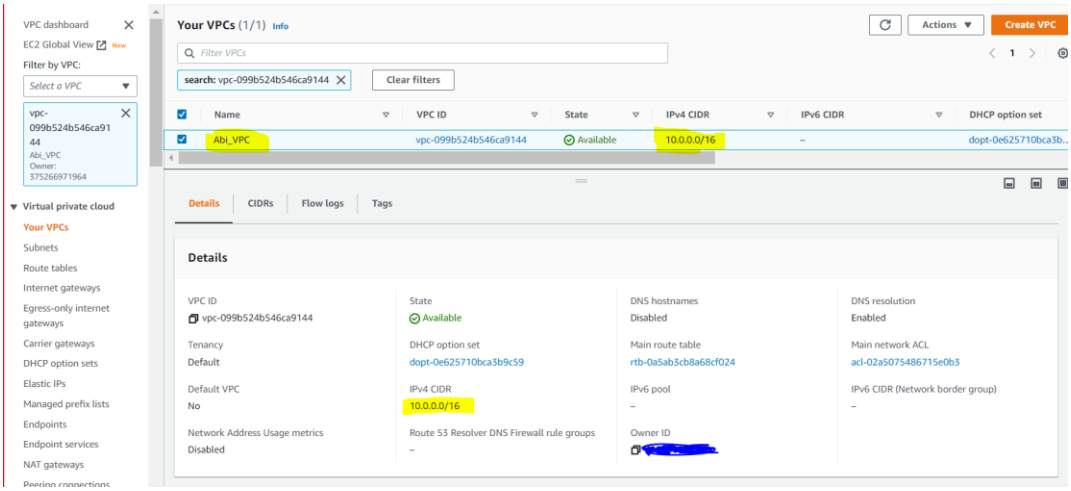


fig: 11 Bansion Host Configuration of Dest_VPC



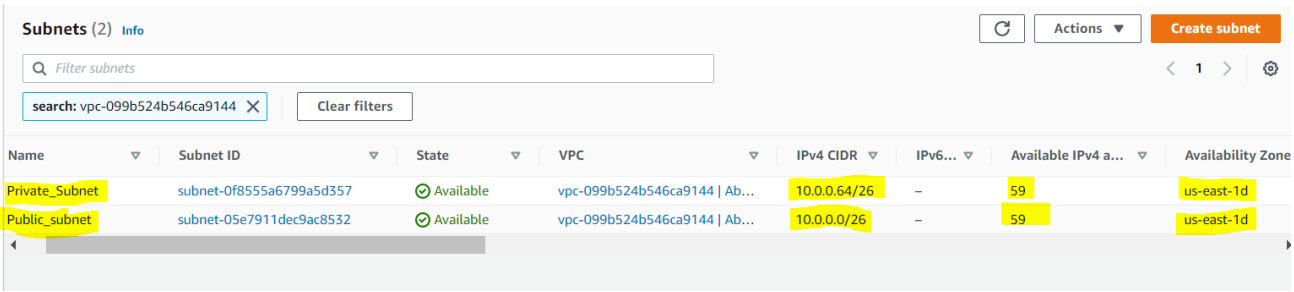


fig: 12 Abi_VPC with its public and private subnets and ranges

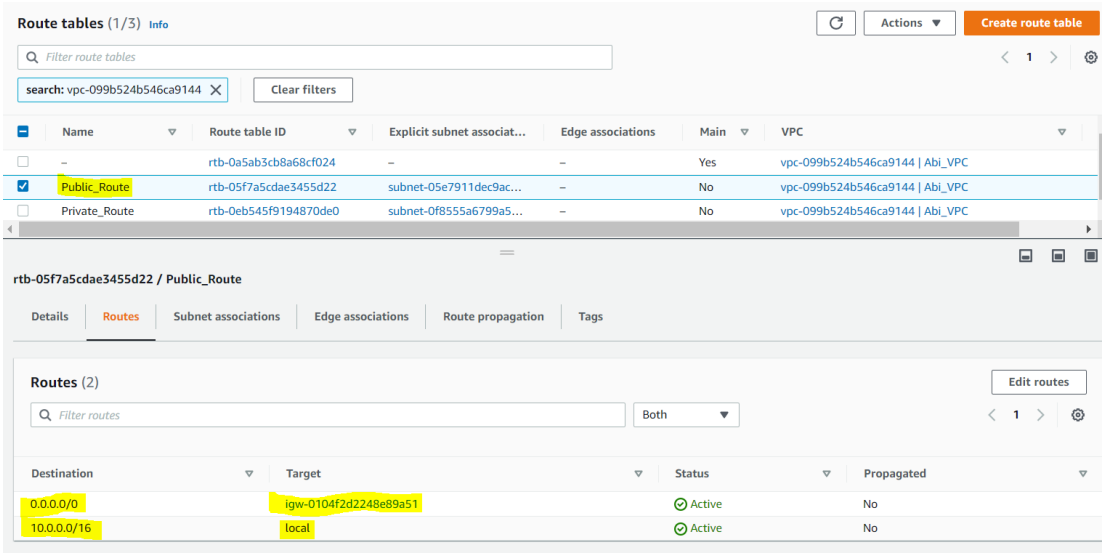


fig: 13 Public Route and its route table of Abi_VPC.

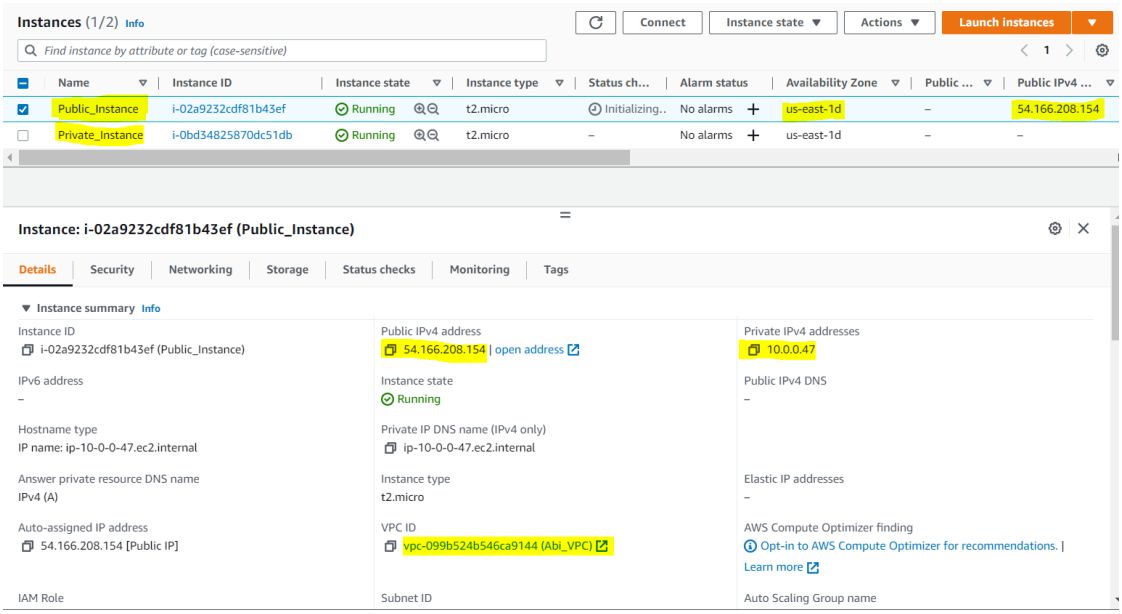


fig: 14 Public and Private Instance created in Abi_VPC.

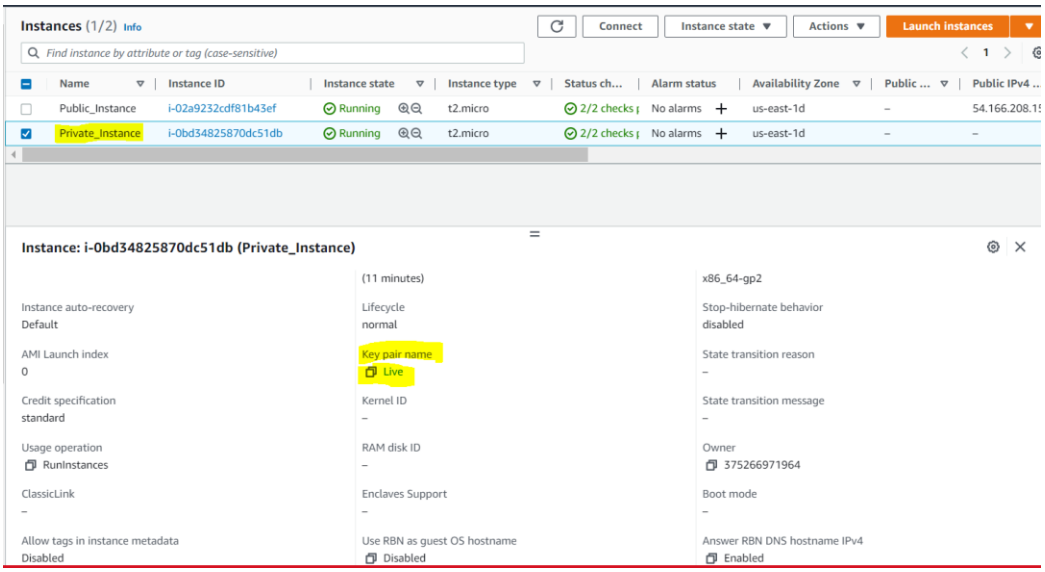


fig: 15 Private Instance with its key pair attached.

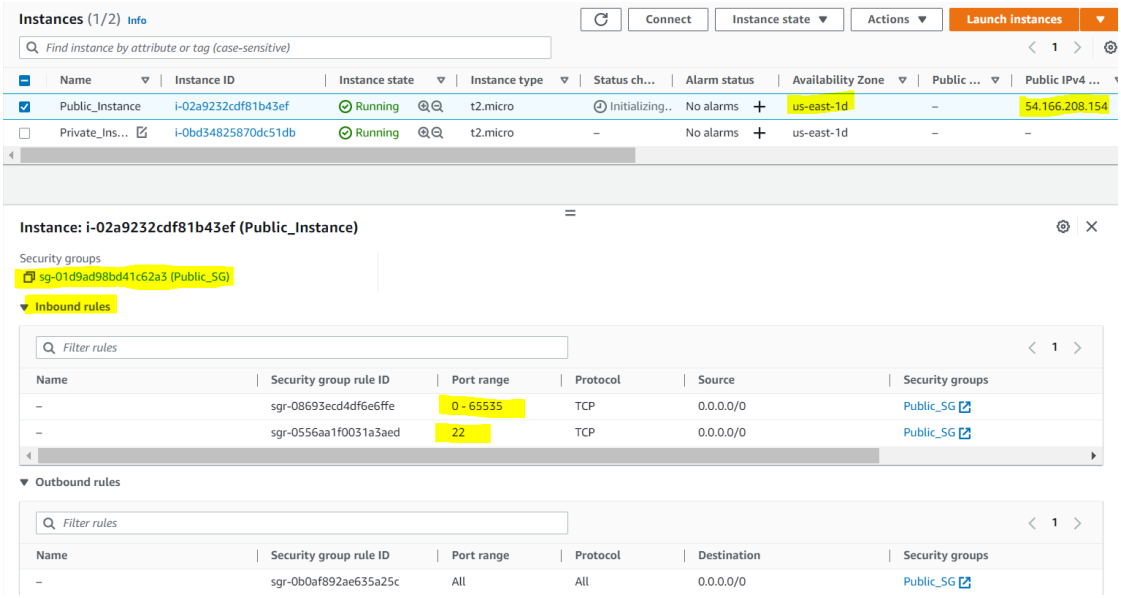


fig: 16 Public Instance with its Inbound Security group of Abi_VPC

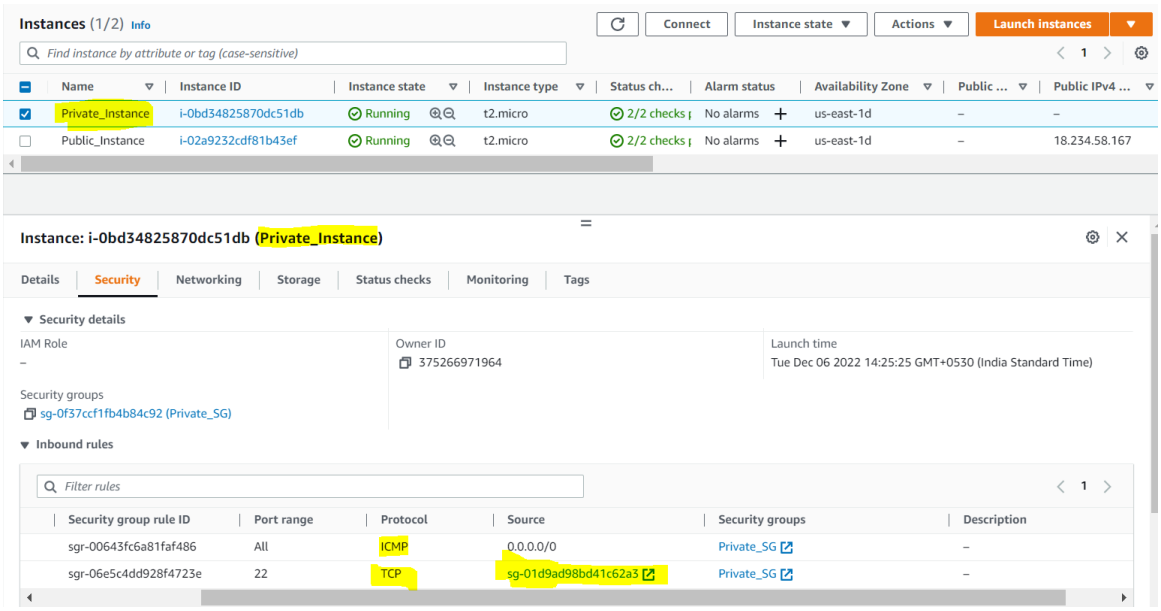


fig: 17 Private Instance with allowed SSH from Public Instance.

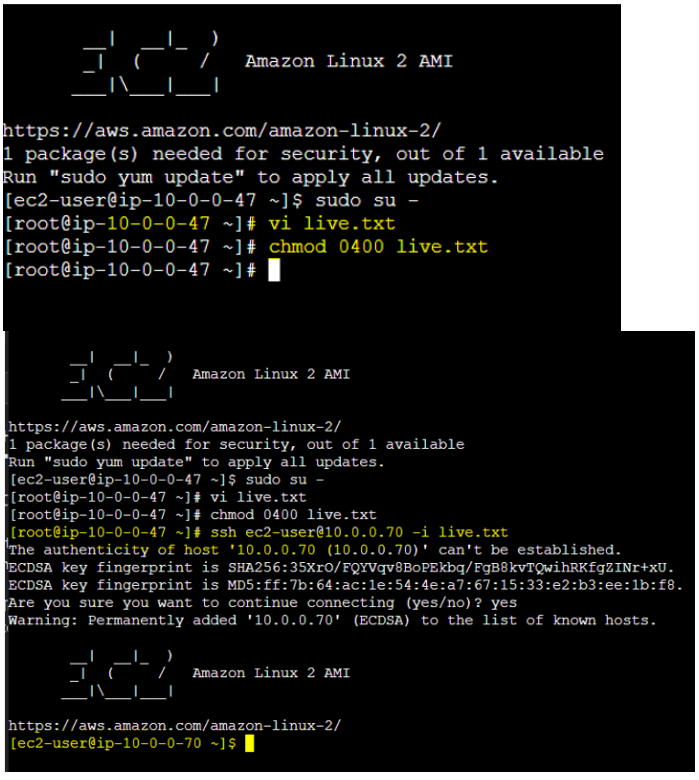


fig: 18 Bansion Host Configuration of Abi_VPC

Pinging from Dest_VPC to Abi_VPC: …

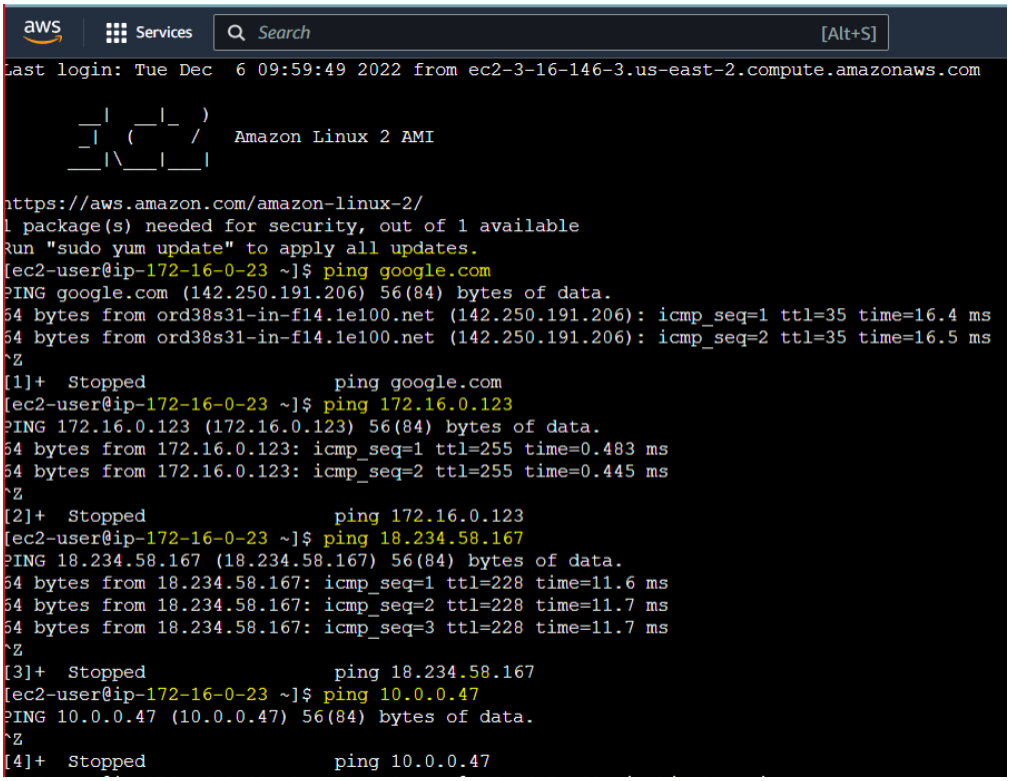


fig: 19 Connection Results from Public Instance of Dest_VPC before VPC_Peering ..

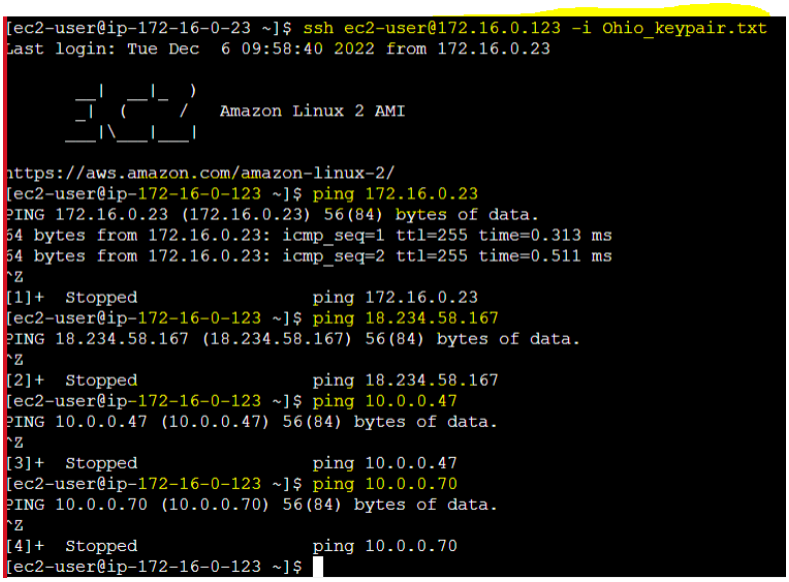


fig: 20 Connection Results from Private Instance of Dest_VPC before VPC_Peering..

Pinging from Abi_VPC to Dest_VPC: …

```
Last login: Tue Dec  6 10:04:34 2022 from ec2-18-206-107-27.compute-1.amazonaws.com

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

https://aws.amazon.com/amazon-linux-2/
1 package(s) needed for security, out of 1 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-47 ~]$ ping google.com
PING google.com (142.251.16.102) 56(84) bytes of data.
64 bytes from bl-in-f102.1e100.net (142.251.16.102): icmp_seq=1 ttl=95 time=1.94 ms
64 bytes from bl-in-f102.1e100.net (142.251.16.102): icmp_seq=2 ttl=95 time=1.93 ms
^Z
[1]+  Stopped                 ping google.com
[ec2-user@ip-10-0-0-47 ~]$ ping 10.0.0.70
PING 10.0.0.70 (10.0.0.70) 56(84) bytes of data.
64 bytes from 10.0.0.70: icmp_seq=1 ttl=255 time=0.582 ms
64 bytes from 10.0.0.70: icmp_seq=2 ttl=255 time=0.589 ms
^Z
[2]+  Stopped                 ping 10.0.0.70
[ec2-user@ip-10-0-0-47 ~]$ ping 3.139.95.136
PING 3.139.95.136 (3.139.95.136) 56(84) bytes of data.
64 bytes from 3.139.95.136: icmp_seq=1 ttl=228 time=11.5 ms
64 bytes from 3.139.95.136: icmp_seq=2 ttl=228 time=11.6 ms
^Z
[3]+  Stopped                 ping 3.139.95.136
[ec2-user@ip-10-0-0-47 ~]$ ping 172.16.0.23
PING 172.16.0.23 (172.16.0.23) 56(84) bytes of data.
^Z
[4]+  Stopped                 ping 172.16.0.23
```

fig: 21 Connection Results from Public Instance of Abi_VPC before VPC_Peering.

```
[ec2-user@ip-10-0-0-47 ~]$ ssh ec2-user@10.0.0.70 -i live.txt
Last login: Tue Dec  6 10:05:28 2022 from 10.0.0.47

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-70 ~]$ ping 10.0.0.47
PING 10.0.0.47 (10.0.0.47) 56(84) bytes of data.
64 bytes from 10.0.0.47: icmp_seq=1 ttl=255 time=0.466 ms
64 bytes from 10.0.0.47: icmp_seq=2 ttl=255 time=0.600 ms
^Z
[1]+  Stopped                 ping 10.0.0.47
[ec2-user@ip-10-0-0-70 ~]$ ping 3.139.95.136
PING 3.139.95.136 (3.139.95.136) 56(84) bytes of data.
^Z
[2]+  Stopped                 ping 3.139.95.136
[ec2-user@ip-10-0-0-70 ~]$ ping 172.16.0.23
PING 172.16.0.23 (172.16.0.23) 56(84) bytes of data.
^Z
[3]+  Stopped                 ping 172.16.0.23
[ec2-user@ip-10-0-0-70 ~]$ ping 172.16.0.123
PING 172.16.0.123 (172.16.0.123) 56(84) bytes of data.
^Z
[4]+  Stopped                 ping 172.16.0.123
[ec2-user@ip-10-0-0-70 ~]$
```

fig: 22 Connection Results from Private Instance of Abi_VPC before VPC_Peering.

Peering:

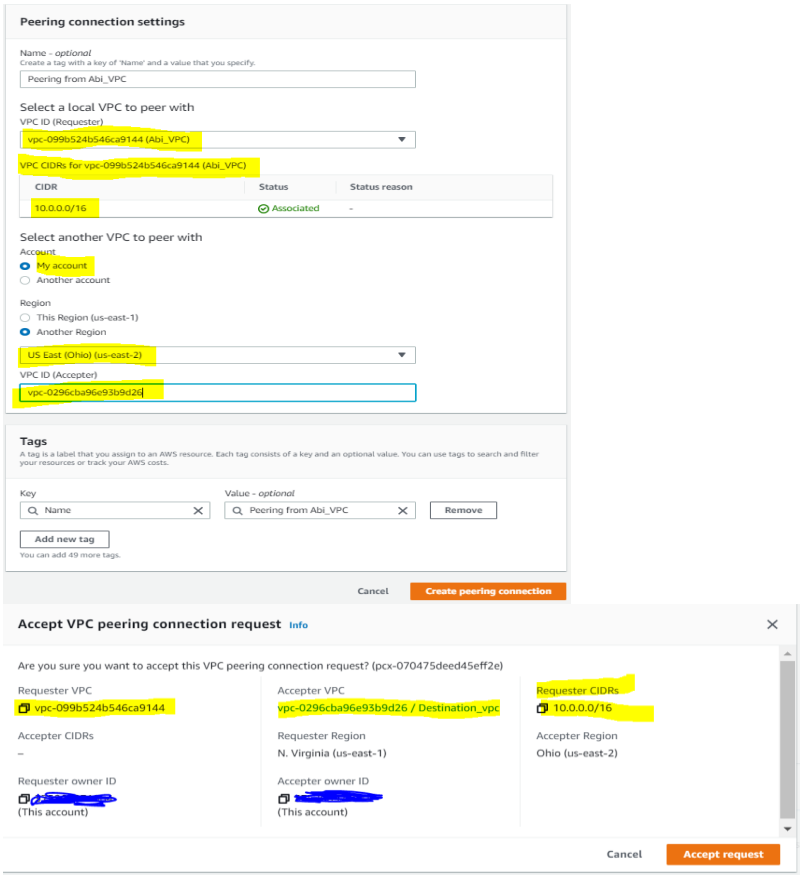


fig: 23 Sending and accepting Peering request

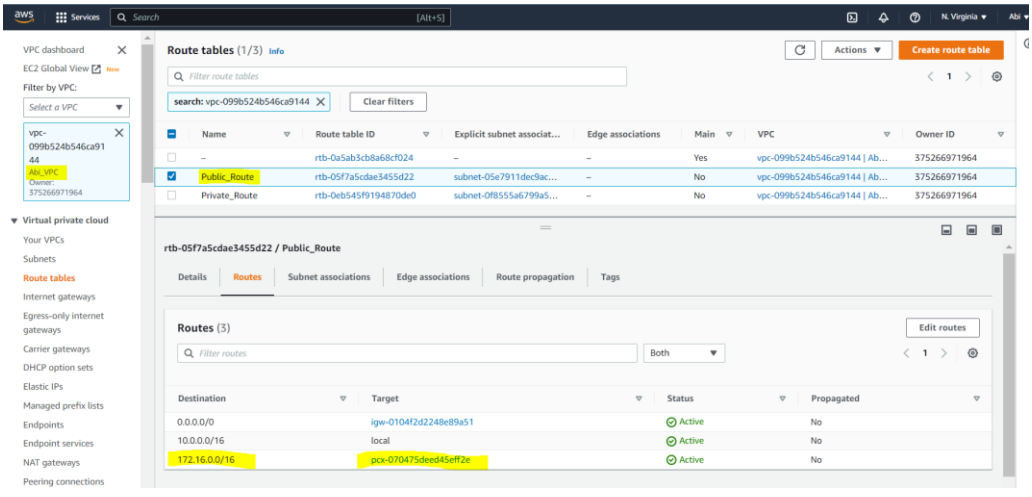


fig: 24 Updated route table with CIDR of peered VPC.

Pinging from Dest_VPC to Abi_VPC:

```
Last login: Tue Dec  6 13:03:04 2022 from ec2-3-16-146-4.us-east-2.compute.amazonaws.com

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

https://aws.amazon.com/amazon-linux-2/
1 package(s) needed for security, out of 1 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-16-0-23 ~]$ ping 10.0.0.47
PING 10.0.0.47 (10.0.0.47) 56(84) bytes of data.
64 bytes from 10.0.0.47: icmp_seq=1 ttl=255 time=11.7 ms
64 bytes from 10.0.0.47: icmp_seq=2 ttl=255 time=11.7 ms
64 bytes from 10.0.0.47: icmp_seq=3 ttl=255 time=11.7 ms
^Z
[1]+  Stopped                 ping 10.0.0.47
[ec2-user@ip-172-16-0-23 ~]$ ping 10.0.0.70
PING 10.0.0.70 (10.0.0.70) 56(84) bytes of data.
64 bytes from 10.0.0.70: icmp_seq=1 ttl=255 time=11.7 ms
64 bytes from 10.0.0.70: icmp_seq=2 ttl=255 time=11.7 ms
^Z
[2]+  Stopped                 ping 10.0.0.70
```

fig: 25 Connection Results from Public Instance of Dest_VPC After VPC_Peering.

```
[ec2-user@ip-172-16-0-23 ~]$ ssh ec2-user@172.16.0.123 -i Ohio_keypair.txt
Last login: Tue Dec  6 10:09:25 2022 from 172.16.0.23

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-16-0-123 ~]$ ping 10.0.0.47
PING 10.0.0.47 (10.0.0.47) 56(84) bytes of data.
64 bytes from 10.0.0.47: icmp_seq=1 ttl=255 time=11.8 ms
64 bytes from 10.0.0.47: icmp_seq=2 ttl=255 time=11.8 ms
^Z
[1]+  Stopped                 ping 10.0.0.47
[ec2-user@ip-172-16-0-123 ~]$ ping 10.0.0.70
PING 10.0.0.70 (10.0.0.70) 56(84) bytes of data.
64 bytes from 10.0.0.70: icmp_seq=1 ttl=255 time=11.5 ms
64 bytes from 10.0.0.70: icmp_seq=2 ttl=255 time=11.7 ms
64 bytes from 10.0.0.70: icmp_seq=3 ttl=255 time=11.7 ms
^Z
[2]+  Stopped                 ping 10.0.0.70
[ec2-user@ip-172-16-0-123 ~]$
```

fig: 26 Connection Results from Private Instance of Dest_VPC After VPC_Peering.

Pinging from Abi_VPC to Dest_VPC: …

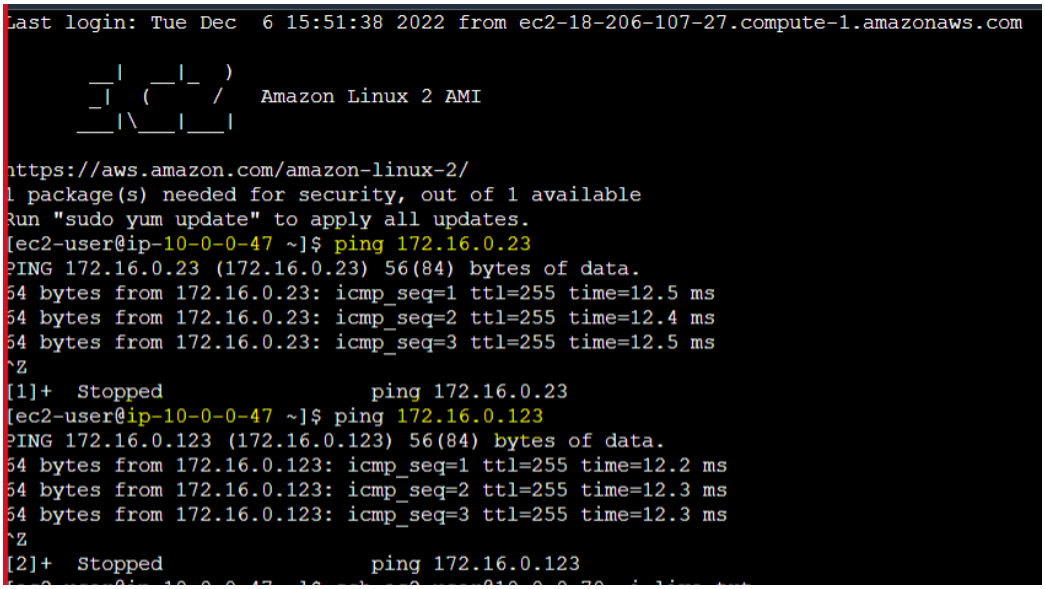


fig: 27 Connection Results from Public Instance of Abi_VPC After VPC_Peering.

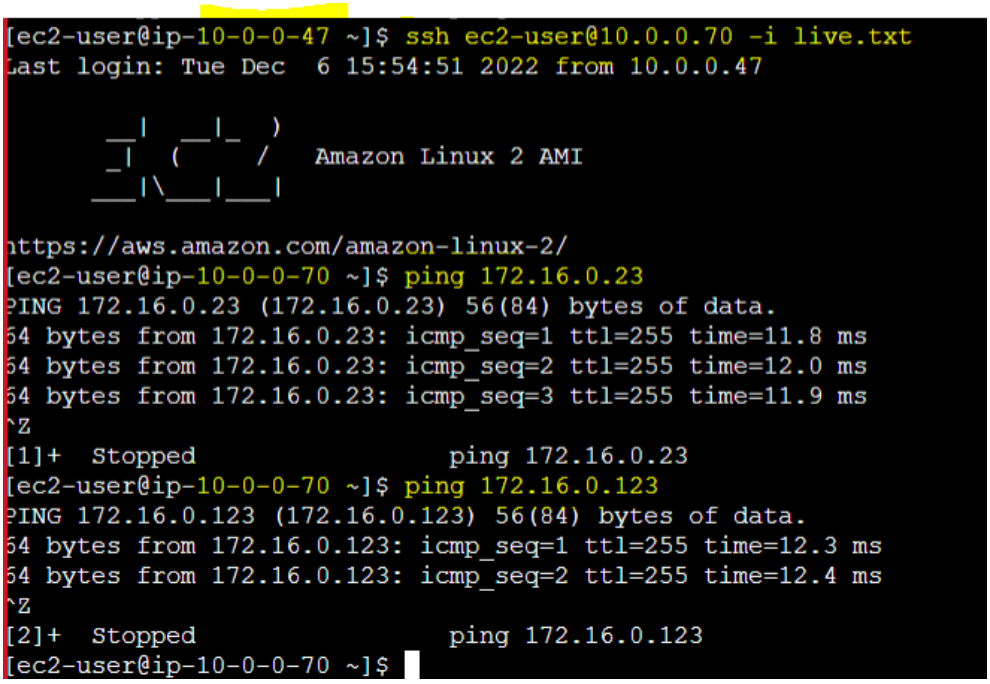


fig: 28 Connection Results from Private Instance of Abi_VPC After VPC_Peering.