

Problem Statement:

You work for XYZ Corporation and based on the expansion requirements of your corporation you have been asked to create and set up a distinct Amazon VPC for the production and development team. You are expected to perform the following tasks for the respective VPCs.

Production Network:

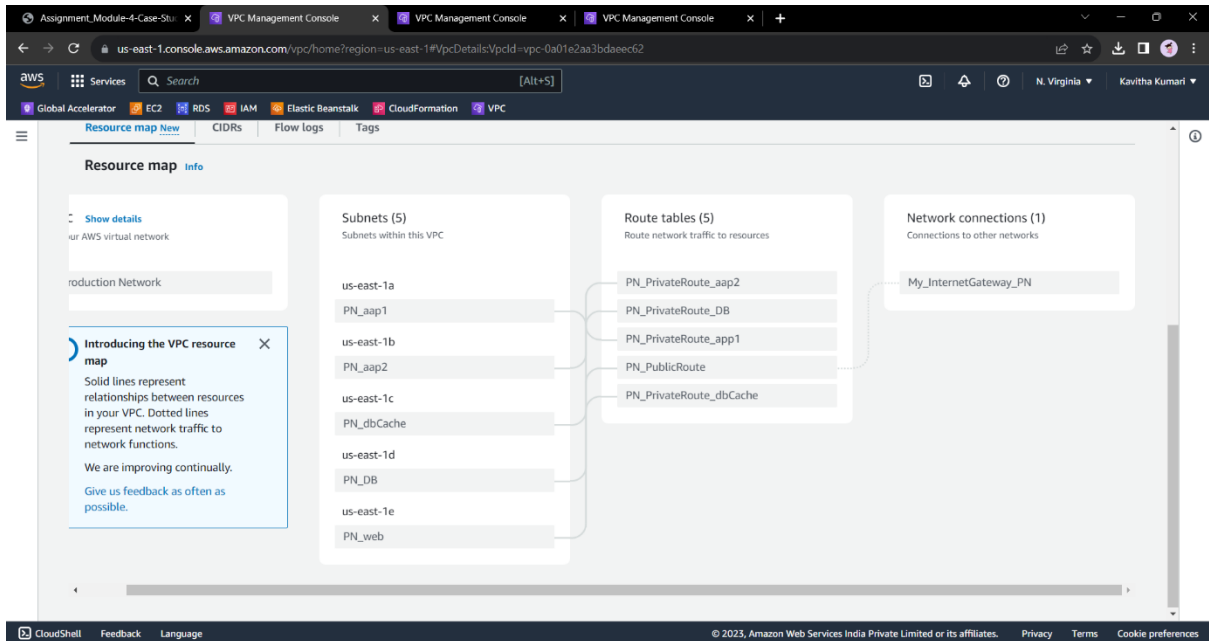
1. Design and build a 4-tier architecture.
2. Create 5 subnets out of which 4 should be private named app1, app2, dbcache and db and one should be public, named web.
3. Launch instances in all subnets and name them as per the subnet that they have been launched in.
4. Allow dbcache instance and app1 subnet to send internet requests.
5. Manage security groups and NACLs.
6. creating vpc end point for the s3 service and access the objects in any buckets from within the vpc

Development Network:

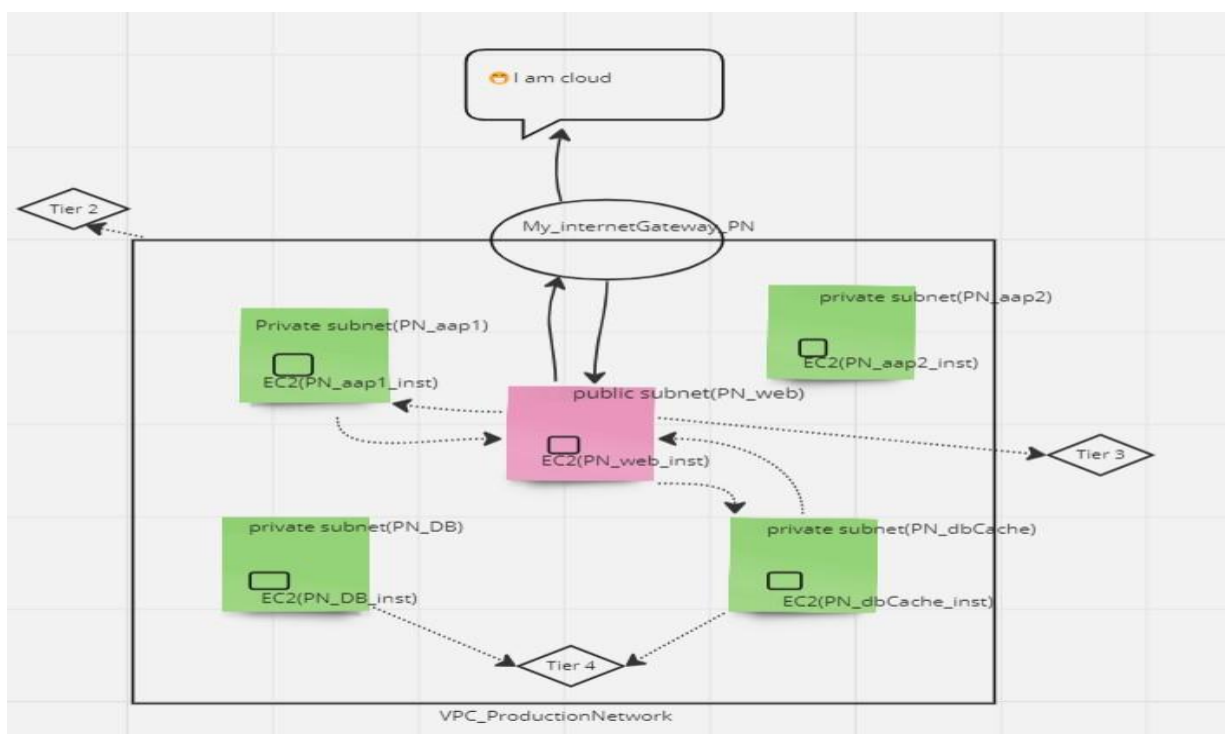
1. Design and build 2-tier architecture with two subnets named web and db and launch instances in both subnets and name them as per the subnet names
2. Make sure only the web subnet can send internet requests.
3. Create peering connection between production network and development network.
4. Setup connection between db subnets of both production network and development network respectively.

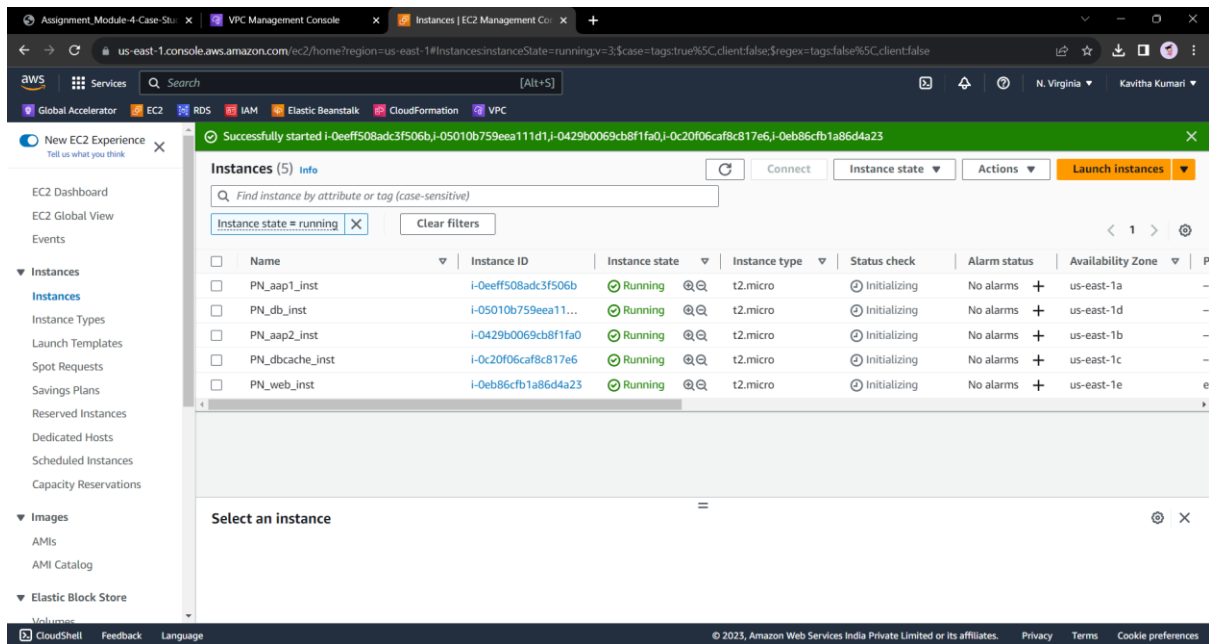
Procedure:

- Below is the 4-tier architecture.
- Create a VPC with the name Production Network. With the 5 subnets with the name as per given in the question.
- Create an internet gateway and attach it to the VPC.
- **Now we will create 5 Route table for each of the subnet. Note that for the public subnet that is web subnet we will give access to internet. Therefore, we will allow internet gateway in the PN_PublicRoute.**

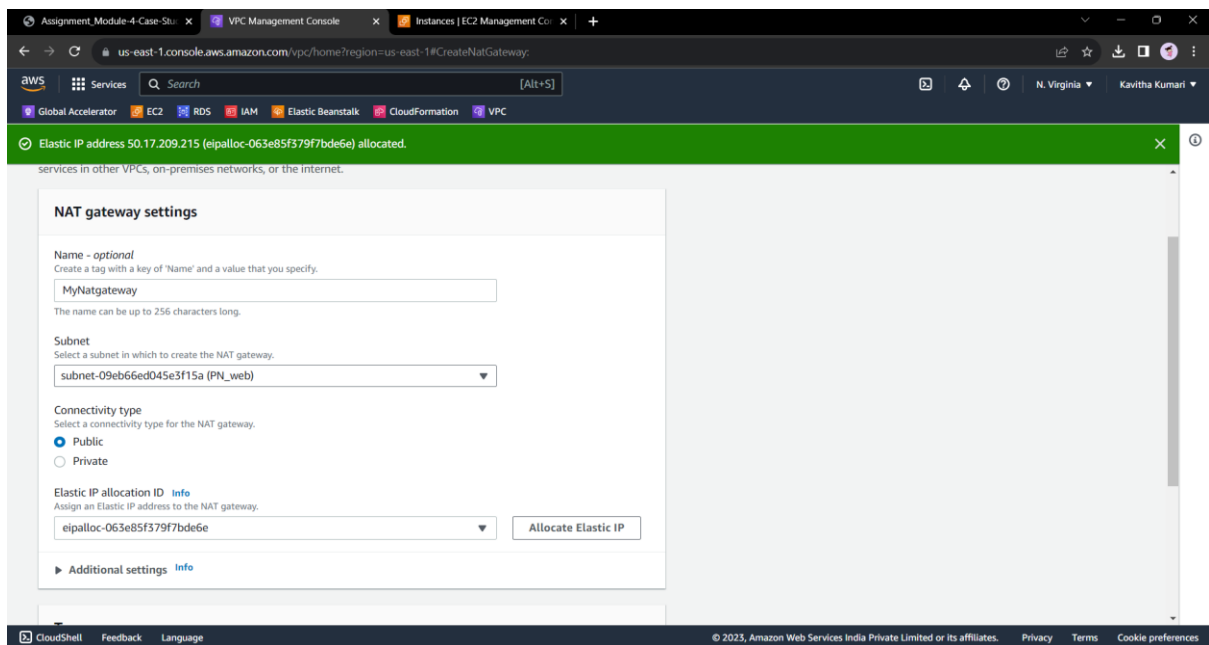


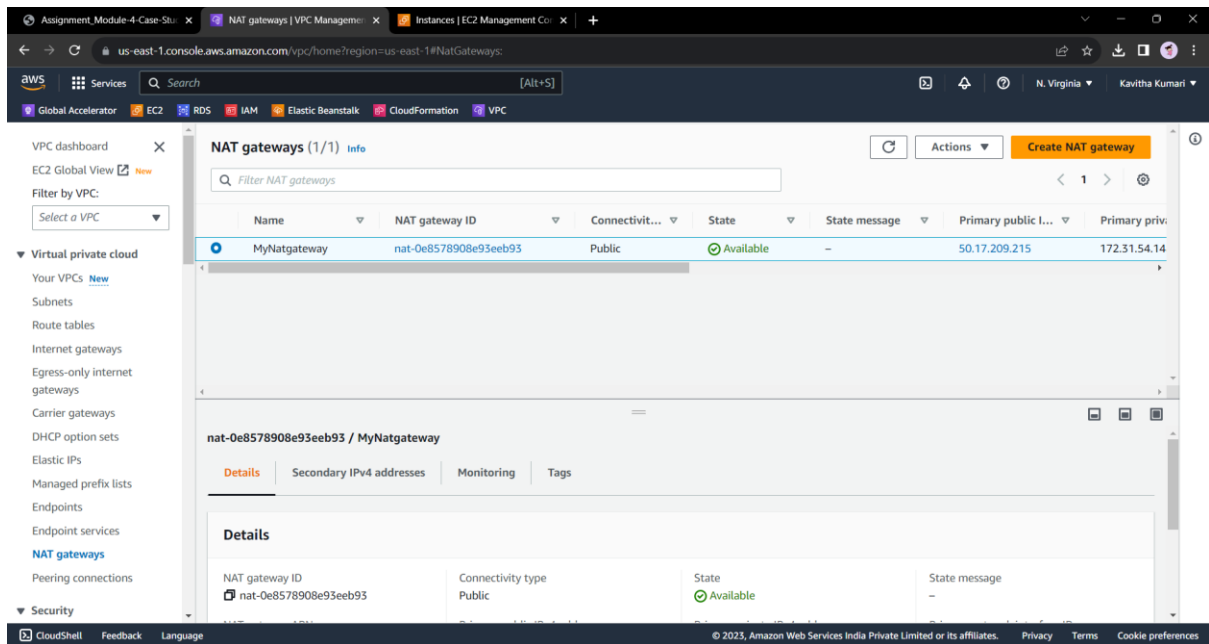
- Now we will create 4 Route table for the respective subnet.
- **Launch instances in all subnets and name them as per the subnet that they have been launched in.**



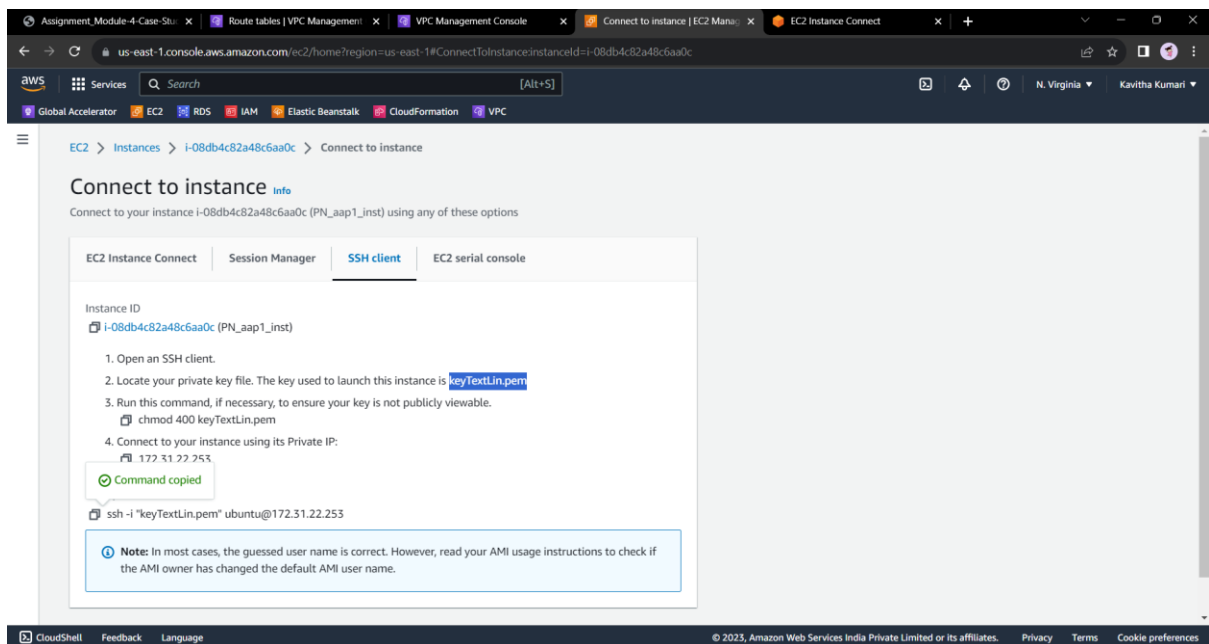


- Now we need to allow the dbcache inst and the app1 to send internet request.
- For this we need to create a NAT gateway so that our private instance can access the internet from the public instance in our network.
- In VPC goto Nat gateway and click on create NAT gateway.
- Enter the name of the NAT gateway and choose the public subnet and click on allocate the elastic IP and click on the create NAT gateway.





- Goto to the public instance and click on connect and there first we need to create the file with the name of the key which you have. Example we need to run the following command if I have the key ketTextLin.pem
- Sudo nano keyTextLin.pem
- Press ctrl + s and ctrl + x to save and exit.
- Now we need to change the access permission of the file. For this we will run the following command.
- Sudo chmod 400 ketTextLin.pem
- And then ssh in to private instance see the below steps:



Assignment_Module-4-Case-Stu... Route tables | VPC Management... VPC Management Console... Connect to instance | EC2 Manu... EC2 Instance Connect

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-021a2fee5a6bcd6be&osUser=ubuntu&sshPort=22#/?

System load: 0.0 Processes: 96
Usage of /: 20.6% of 7.57GB Users logged in: 0
Memory usage: 24% IPv4 address for eth0: 172.31.22.253
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See <https://ubuntu.com/esm> or run: `sudo pro status`

The list of available updates is more than a week old.
To check for new updates run: `sudo apt update`

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-22-253:~\$

i-021a2fee5a6bcd6be (PN_Web_inst)
PublicIPs: 54.160.70.16 PrivateIPs: 172.31.55.220

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

- Therefore, we can get the internet access to the private instance from the google.com with the help of NAT gateway.

Assignment_Module-4-Case-Stu... Route tables | VPC Management... VPC Management Console... Connect to instance | EC2 Manu... EC2 Instance Connect

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-021a2fee5a6bcd6be&osUser=ubuntu&sshPort=22#/?

Enable ESM Apps to receive additional future security updates.
See <https://ubuntu.com/esm> or run: `sudo pro status`

The list of available updates is more than a week old.
To check for new updates run: `sudo apt update`

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

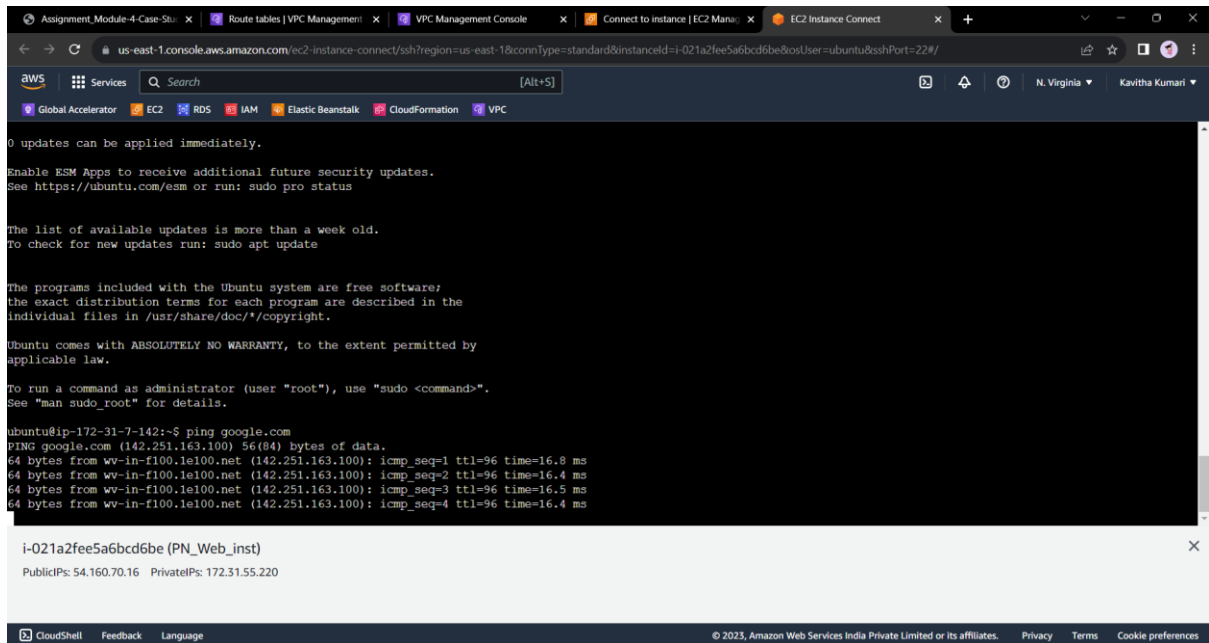
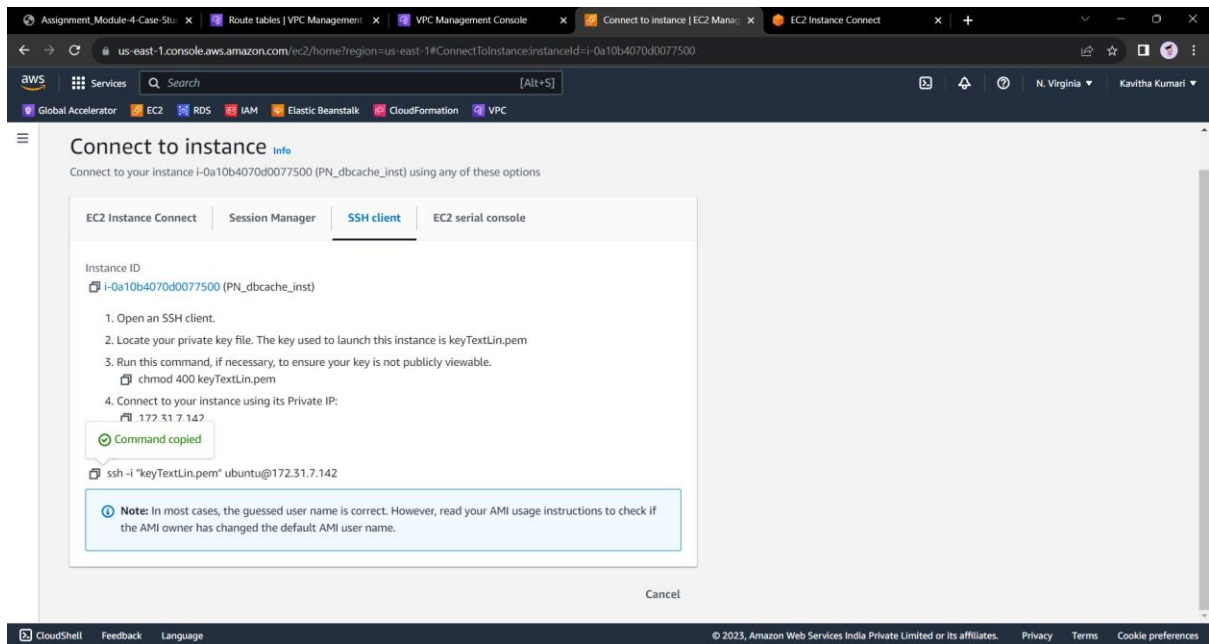
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

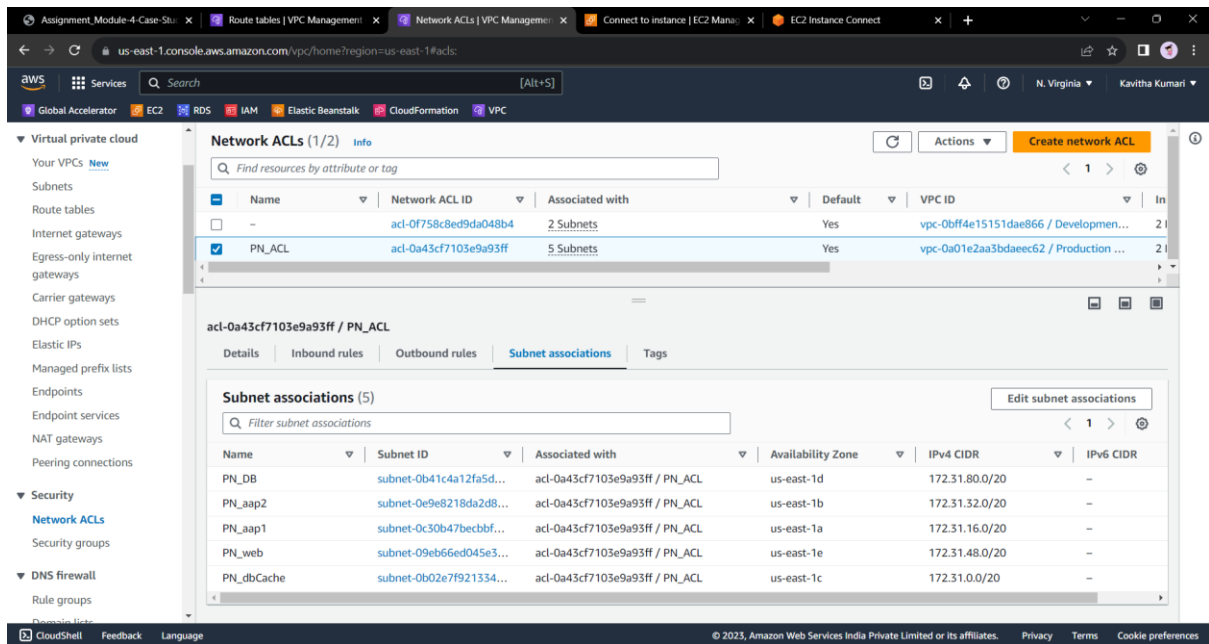
ubuntu@ip-172-31-22-253:~\$ ping google.com
PING google.com (142.250.31.101) 56(84) bytes of data:
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=1 ttl=49 time=2.96 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=2 ttl=49 time=2.49 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=3 ttl=49 time=2.48 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=4 ttl=49 time=2.47 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=5 ttl=49 time=2.49 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=6 ttl=49 time=2.48 ms
64 bytes from bj-in-f101.1e100.net (142.250.31.101): icmp_seq=7 ttl=49 time=2.53 ms

i-021a2fee5a6bcd6be (PN_Web_inst)
PublicIPs: 54.160.70.16 PrivateIPs: 172.31.55.220

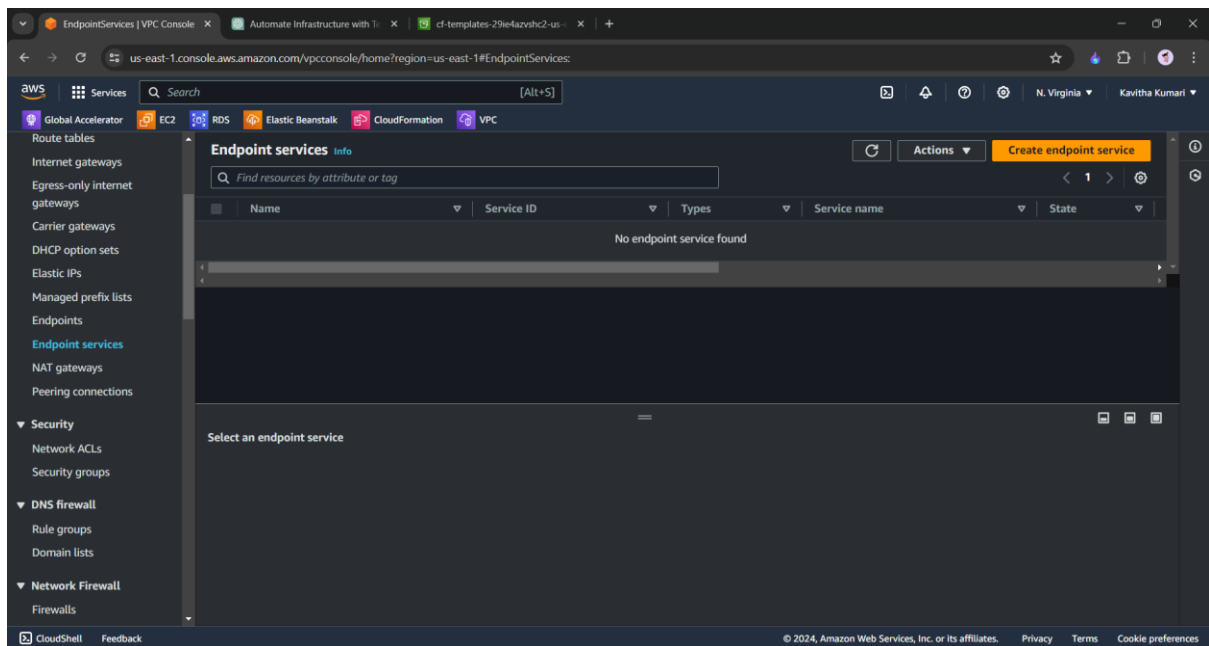
CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences



- Below is how we managing the security groups and NACLs

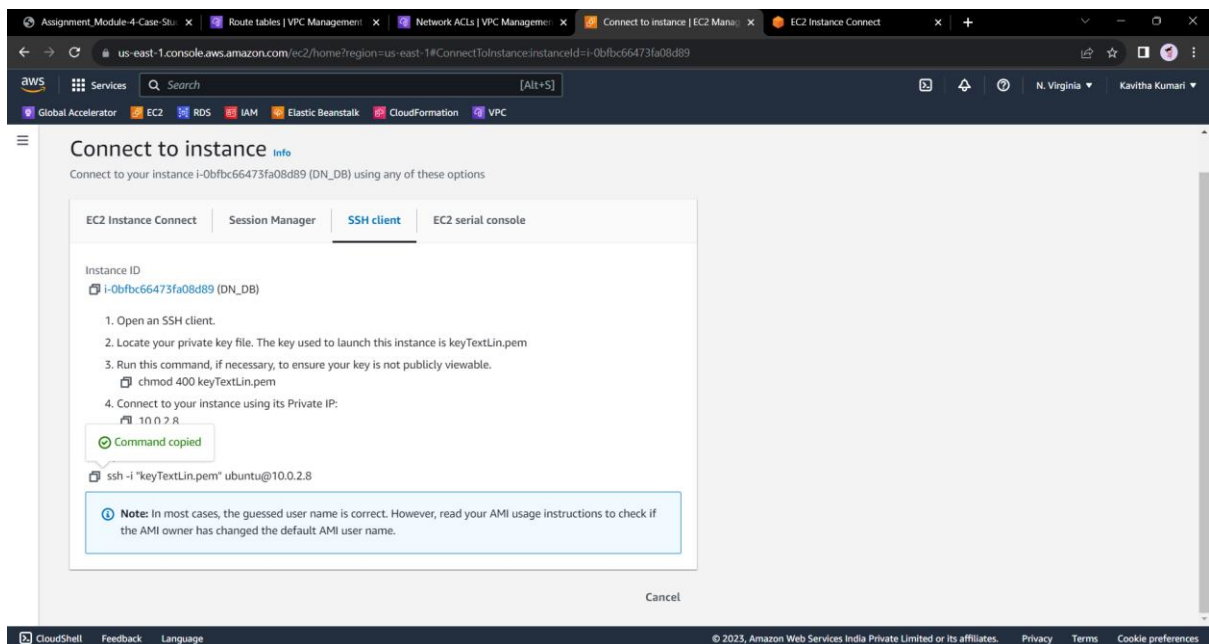
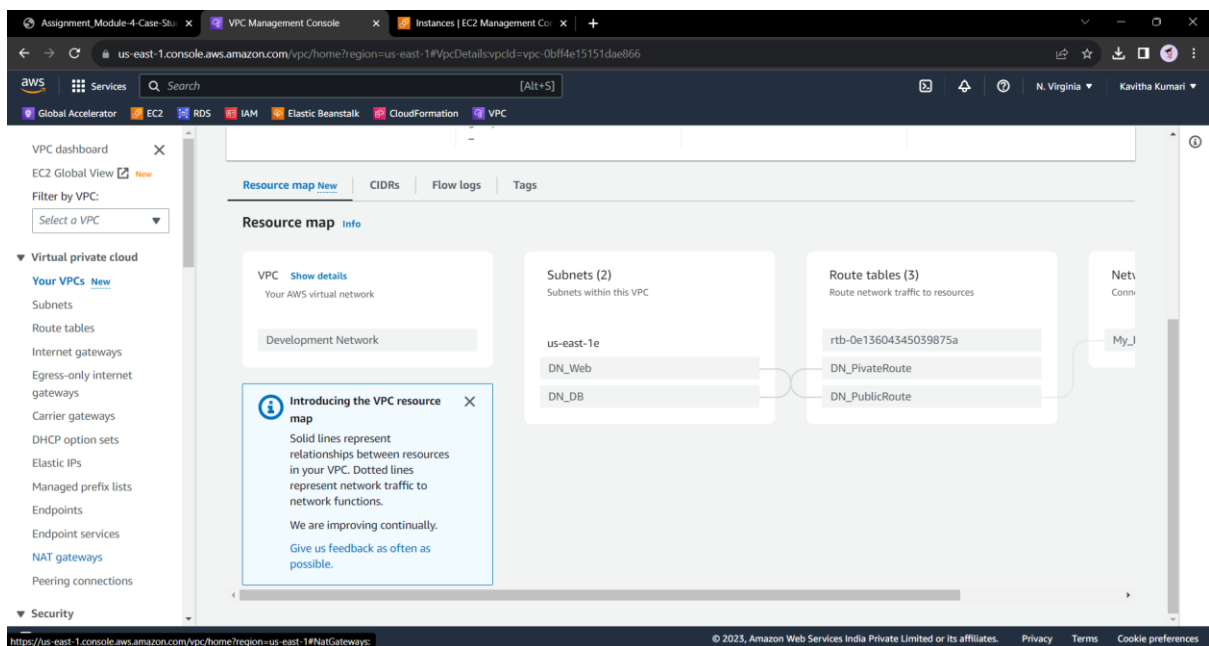


- creating vpc end point for the s3 service and access the objects in any buckets from within the vpc: -
- **Go to the Amazon VPC console.**
- **In the navigation pane, choose "Endpoints" and then "Create Endpoint."**



- **Select "AWS services" as the service category.**
- **Choose "com.amazonaws.region.s3" as the service name.**
- **Select the VPC and specify the route table for the endpoint.**
- **Optionally, you can restrict access to specific S3 buckets by specifying the bucket policy.**
- **Update Route Tables:**

- Ensure that the route tables associated with your VPC have a route for the Amazon S3 endpoint to direct traffic destined for the S3 service to the VPC endpoint.
- Update Route Tables:
- Ensure that the route tables associated with your VPC have a route for the Amazon S3 endpoint to direct traffic destined for the S3 service to the VPC endpoint.
- Update Route Tables:
- Ensure that the route tables associated with your VPC have a route for the Amazon S3 endpoint to direct traffic destined for the S3 service to the VPC endpoint.
- -----
- Design and build 2-tier architecture with two subnets named web and db and launch instances in both subnets and name them as per the subnet names



- Make sure only the web subnet can send internet requests.

```

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

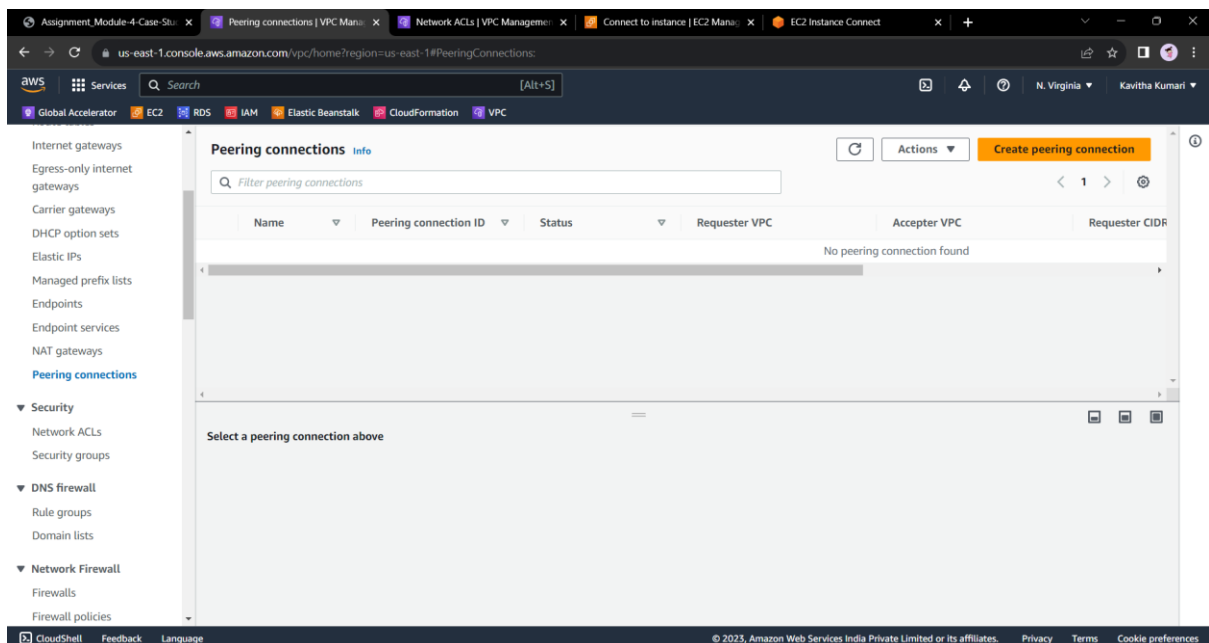
ubuntu@ip-10-0-2-8:~$ ping google.com
PING google.com (142.251.16.113) 56(84) bytes of data.
^C
--- google.com ping statistics ---
31 packets transmitted, 0 received, 100% packet loss, time 30705ms

ubuntu@ip-10-0-2-8:~$ exit
logout
Connection to 10.0.2.8 closed.
ubuntu@ip-10-0-1-182:~$ ping google.com
PING google.com (142.251.16.138) 56(84) bytes of data.
64 bytes from bl-in-fl38.1e100.net (142.251.16.138): icmp_seq=1 ttl=96 time=2.09 ms
64 bytes from bl-in-fl38.1e100.net (142.251.16.138): icmp_seq=2 ttl=96 time=2.18 ms
64 bytes from bl-in-fl38.1e100.net (142.251.16.138): icmp_seq=3 ttl=96 time=2.21 ms
64 bytes from bl-in-fl38.1e100.net (142.251.16.138): icmp_seq=4 ttl=96 time=2.14 ms

```

i-049e05676cf528163 (DN_Web_inst)
PublicIPs: 54.88.204.24 PrivateIPs: 10.0.1.182

- Here we can see that we are able to ping google.com from the public instance.
- **Create peering connection between production network and development network**
- Here, we need to connect the ProductionNetwork VPC to DevelopmentNetwork through the VPC Peering.
- Click on **create peering connection**.



- Fill the details as shown in the following picture.

Assignment_Module-4-Case-Stu... VPC Management Console Network ACLs | VPC Manage... Connect to instance | EC2 Mana... EC2 Instance Connect

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreatePeeringConnection

Services Search [Alt+S]

Global Accelerator EC2 RDS IAM Elastic Beanstalk CloudFormation VPC

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.

Peeringconnect_Pro

Select a local VPC to peer with

VPC ID (Requester)

vpc-0a01e2aa3bdaec62 (Production Network)

VPC CIDRs for vpc-0a01e2aa3bdaec62 (Production Network)

CIDR	Status	Status reason
172.31.0.0/16	Associated	-

Select another VPC to peer with

Account

☒ My account

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Assignment_Module-4-Case-Stu... VPC Management Console Network ACLs | VPC Manage... Connect to instance | EC2 Mana... EC2 Instance Connect

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreatePeeringConnection

Services Search [Alt+S]

Global Accelerator EC2 RDS IAM Elastic Beanstalk CloudFormation VPC

Select a local VPC to peer with

VPC ID (Requester)

vpc-0a01e2aa3bdaec62 (Production Network)

VPC CIDRs for vpc-0a01e2aa3bdaec62 (Production Network)

CIDR	Status	Status reason
172.31.0.0/16	Associated	-

Select another VPC to peer with

Account

☒ My account

☐ Another account

Region

☒ This Region (us-east-1)

☐ Another Region

VPC ID (Acceptor)

vpc-0bff4e15151dae866 (Development Network)

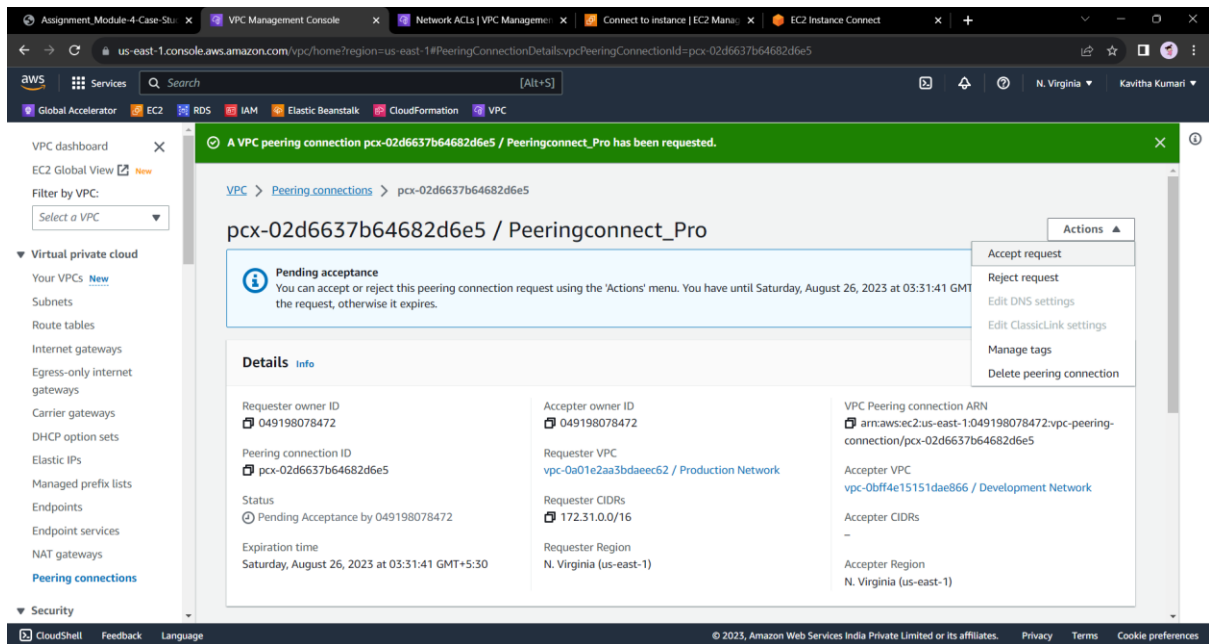
VPC CIDRs for vpc-0bff4e15151dae866 (Development Network)

CIDR	Status	Status reason
10.0.0.0/16	Associated	-

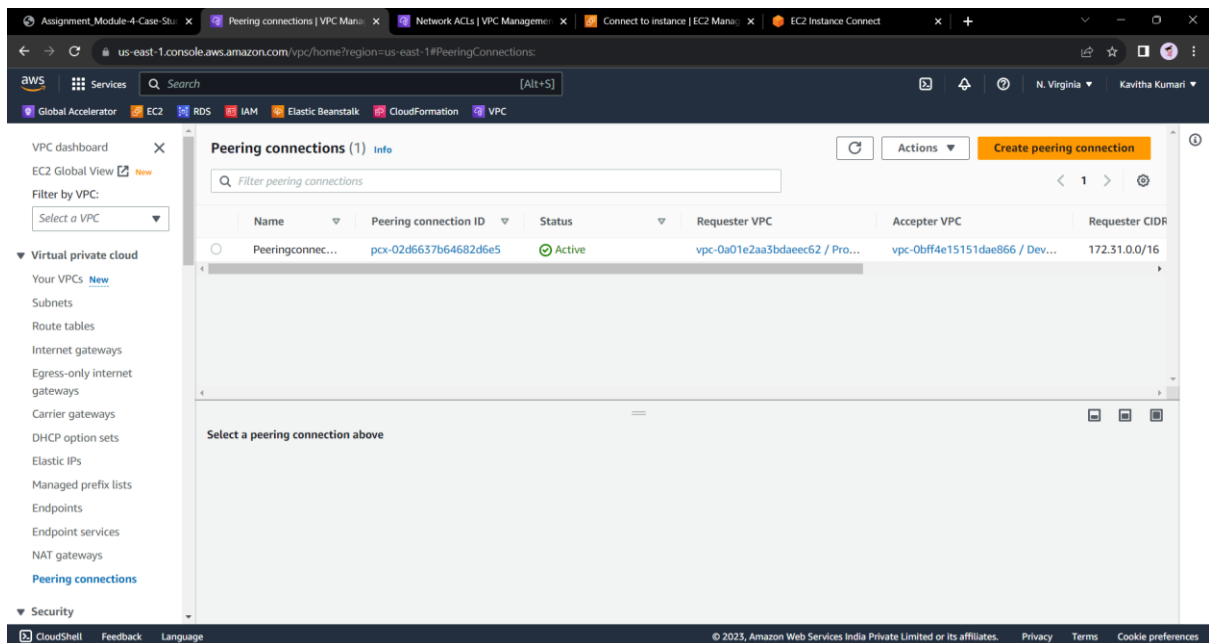
CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

- Click on submit and then it will be created. To establish the connection, we also need to accept the request as shown below.



- Once we accept the request, we will see the status as Active as shown in the following picture.



- Setup connection between db subnets of both production network and development network respectively.**
- In the below figure we are adding the subnet ip address of the DB instance of the DevelopmentNetwork to the DB instance route table of the ProductionNetwork and target is set as peering connection which we have made now.

Assignment_Mo... x Peering connect... x Network ACLs | V x VPC Manage... x Subnets | VPC M... x Instance details | x VPC Manage... x EC2 Instance Co... x +

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes:RouteTableId=rtb-0c80009bc1c93c340

Services Search [Alt+S]

Global Accelerator EC2 RDS IAM Elastic Beanstalk CloudFormation VPC

N. Virginia Kavitha Kumari

VPC > Route tables > rtb-0c80009bc1c93c340 > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
10.0.2.0/24	pcx-02d6637b64682d6e5	-	No

Add route

Cancel Preview Save changes

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Assignment_Mo... x Peering connect... x Network ACLs | V x VPC Manage... x Subnets | VPC M... x Instance details | x VPC Manage... x EC2 Instance Co... x +

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-0abd8ca4fc2347bbf

Services Search [Alt+S]

Global Accelerator EC2 RDS IAM Elastic Beanstalk CloudFormation VPC

N. Virginia Kavitha Kumari

VPC dashboard x

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

- Your VPCs New
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

Security

VPC > Route tables > rtb-0abd8ca4fc2347bbf

rtb-0abd8ca4fc2347bbf / DN_PivateRoute

Actions

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

Details info

Route table ID rtb-0abd8ca4fc2347bbf	Main No	Explicit subnet associations subnet-0dd2a83dfa90fe44 / DN_DB	Edge associations -
VPC vpc-0bff4e15151dae866 Development Network	Owner ID O49198078472		

Routes Subnet associations Edge associations Route propagation Tags

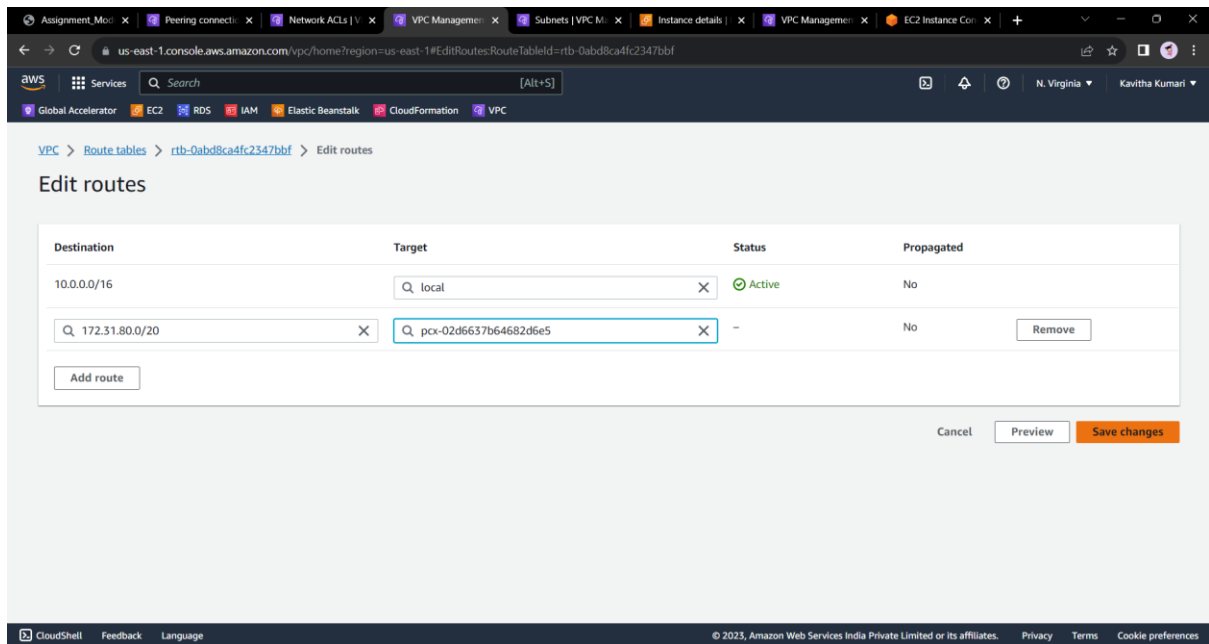
Routes (1)

Filter routes Both

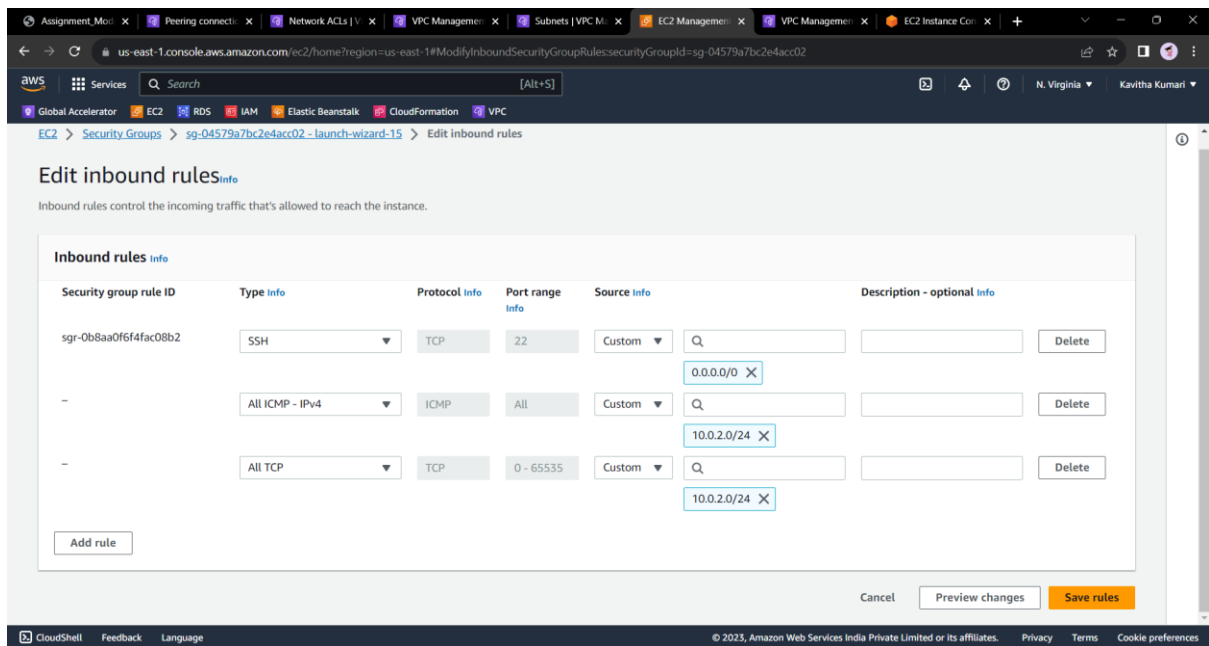
Destination	Target	Status	Propagated
-------------	--------	--------	------------

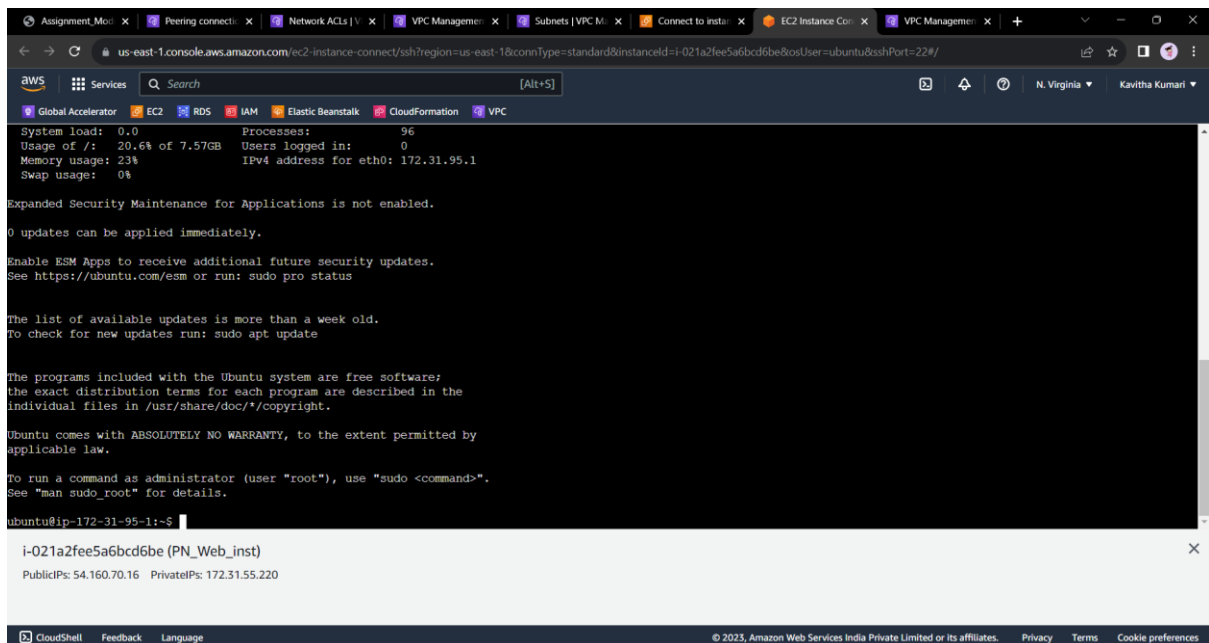
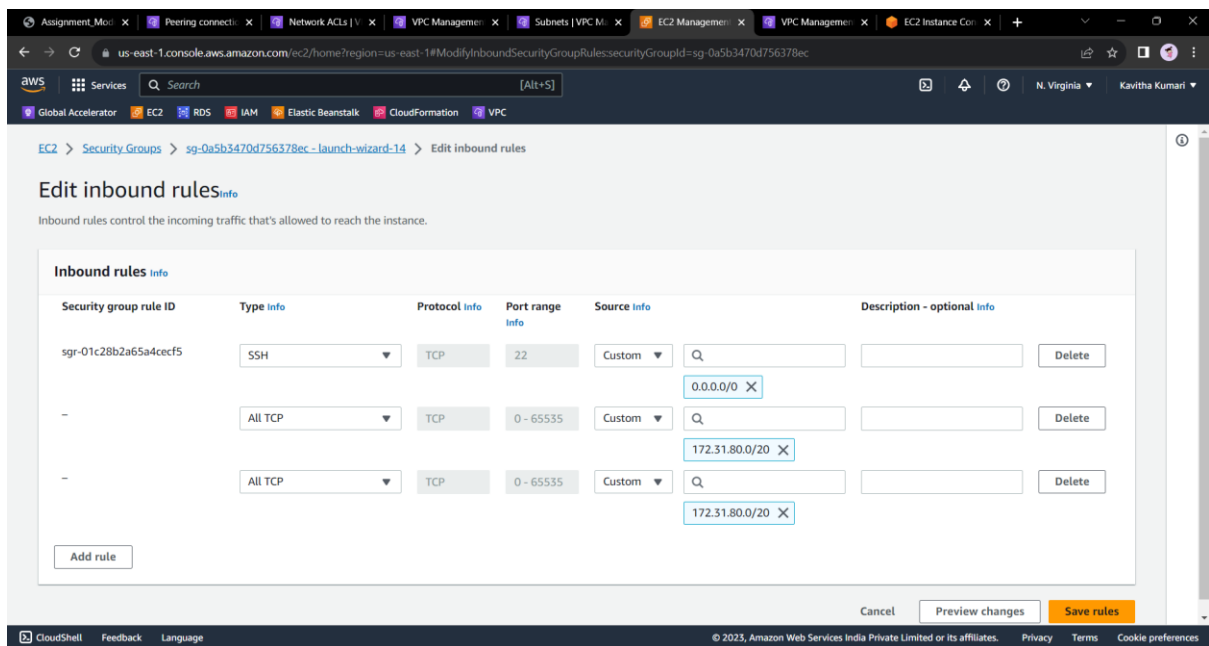
Edit routes

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

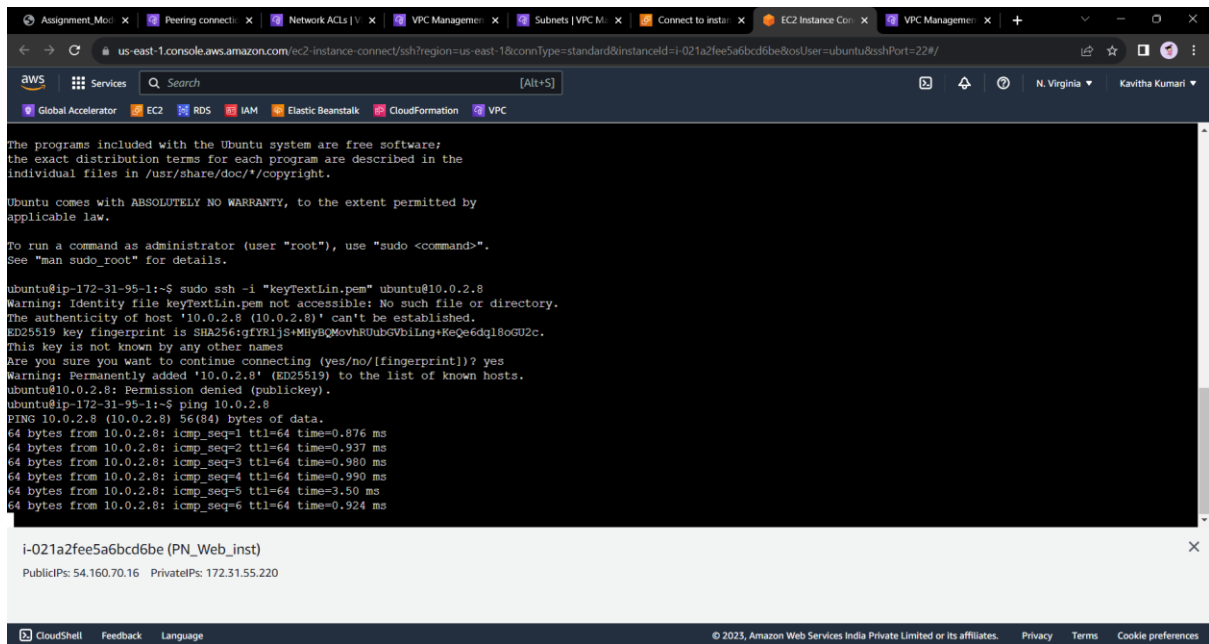


- Now edited the Security Group's inbound rule for both of these instances as per the following screenshot:





Now I am in my PN_DB instance. Let me try to ssh into my DN_DB



The screenshot displays the AWS Management Console interface. The top navigation bar shows the user is logged in as 'Kavitha Kumari' in the 'N. Virginia' region. The main content area shows a terminal window for an EC2 instance. The terminal output is as follows:

```
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-95-1:~$ sudo ssh -i "keyTextLin.pem" ubuntu@10.0.2.8  
Warning: Identity file keyTextLin.pem not accessible: No such file or directory.  
The authenticity of host '10.0.2.8 (10.0.2.8)' can't be established.  
ED25519 key fingerprint is SHA256:gYfYRljs+MBYBQMovhRUubGVbILng+ReQe6dql8oGU2c.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.2.8' (ED25519) to the list of known hosts.  
ubuntu@10.0.2.8: Permission denied (publickey).  
ubuntu@ip-172-31-95-1:~$ ping 10.0.2.8  
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data.  
64 bytes from 10.0.2.8: icmp_seq=1 ttl=64 time=0.876 ms  
64 bytes from 10.0.2.8: icmp_seq=2 ttl=64 time=0.937 ms  
64 bytes from 10.0.2.8: icmp_seq=3 ttl=64 time=0.980 ms  
64 bytes from 10.0.2.8: icmp_seq=4 ttl=64 time=0.990 ms  
64 bytes from 10.0.2.8: icmp_seq=5 ttl=64 time=3.50 ms  
64 bytes from 10.0.2.8: icmp_seq=6 ttl=64 time=0.924 ms
```

Below the terminal window, a metadata box for the instance 'i-021a2fee5a6bcd6be (PN_Web_inst)' is visible, showing PublicIPs: 54.160.70.16 and PrivateIPs: 172.31.55.220.

From here I can ping into my DN_DB instance.

-----End-----