Case-Study- VPC-And-Peering

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.

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.

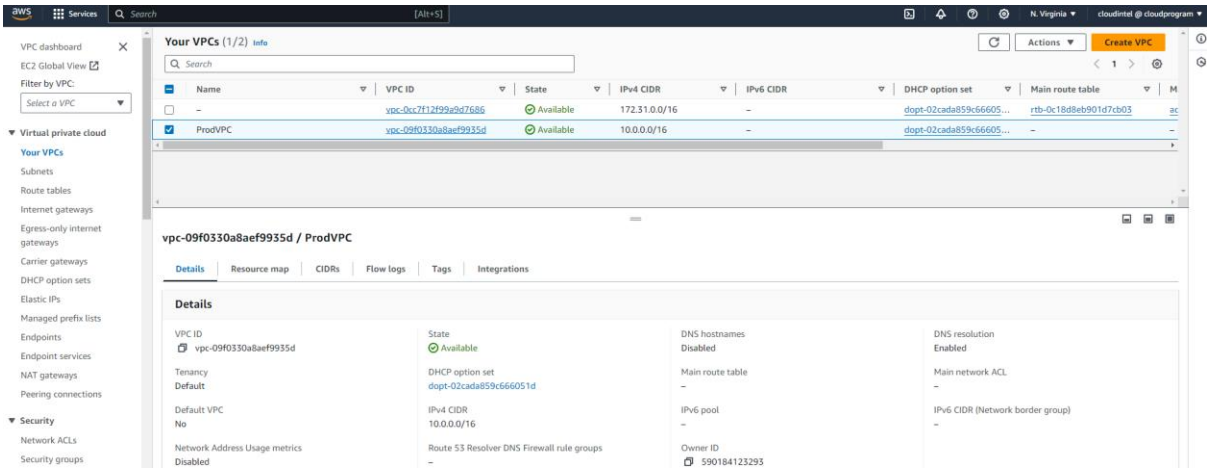
3. Create peering connection between production network and development network.

4. Setup connection between db subnets of both production network and development network respectively.

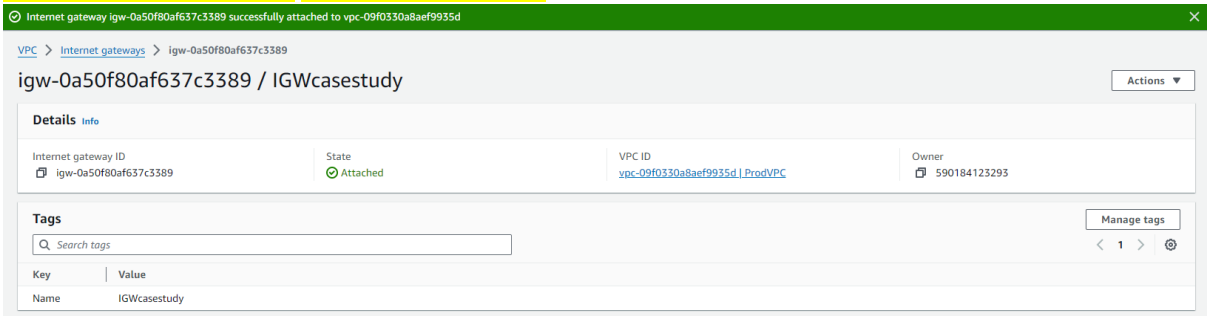
SOLUTION:

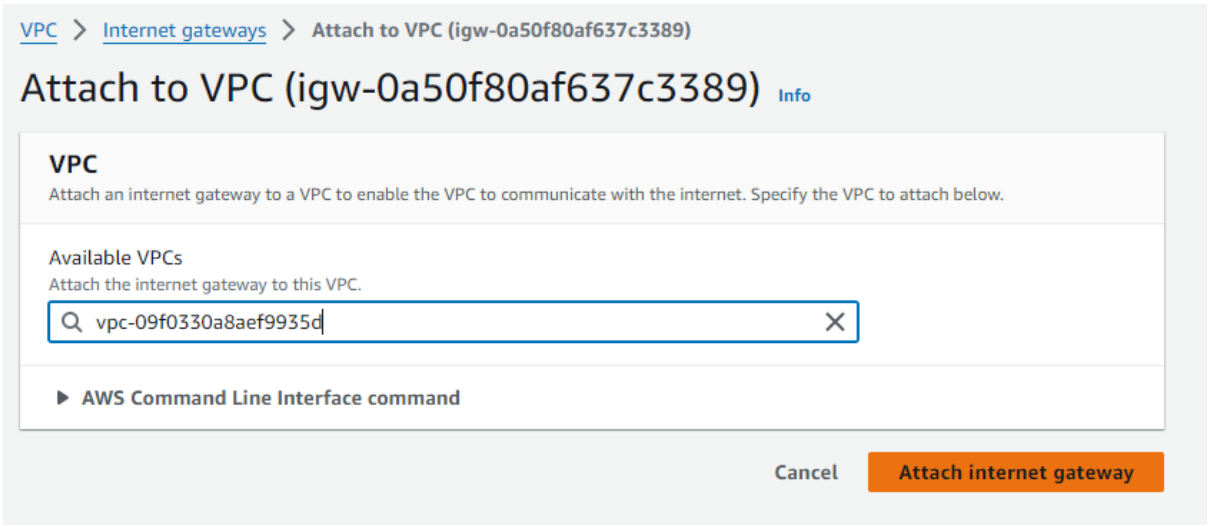
PRODUCTION NETWORK

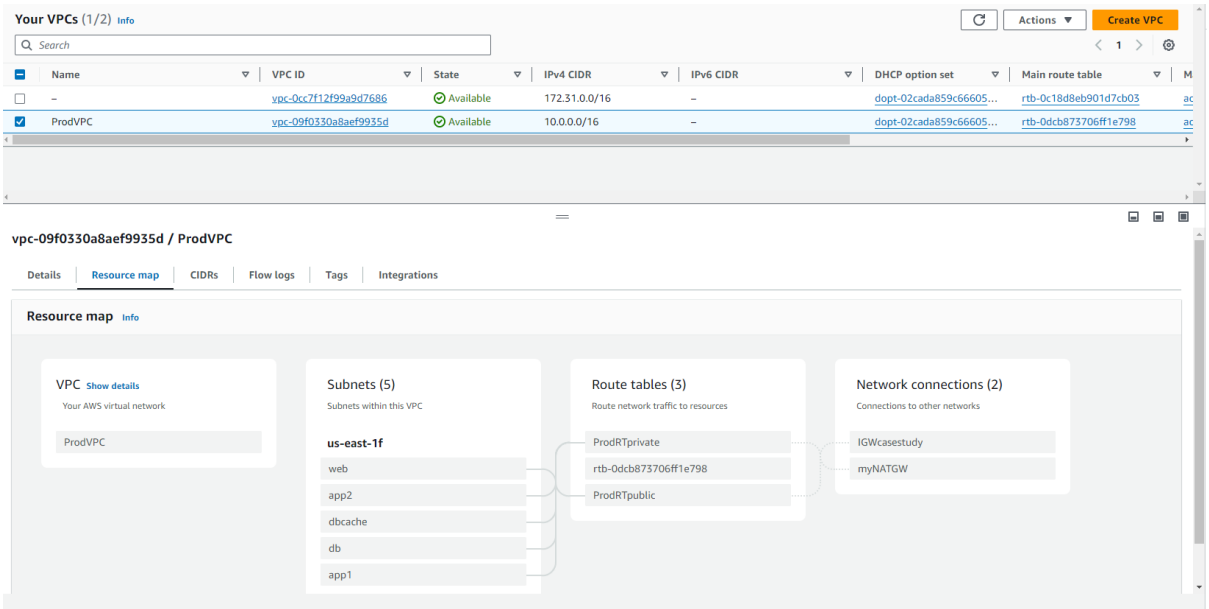
1. ProdVPC created



Create Internet Gateway & Attach to ProdVPC







Public Route Table

VPC > Route tables > rtb-0f17aaf6c99eef12f

rtb-0f17aaf6c99eef12f / ProdRTpublic

Actions

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0f17aaf6c99eef12f	No	–	–

VPC	Owner ID
vpc-09f0330a8aef9935d | ProdVPC	590184123293

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2)

Both | Edit routes

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0a50f80af637c3389	Active	No
10.0.0.0/16	local	Active	No

VPC > Route tables > rtb-0f17aaf6c99eef12f

rtb-0f17aaf6c99eef12f / ProdRTpublic

Actions

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0f17aaf6c99eef12f	No	–	–

VPC	Owner ID
vpc-09f0330a8aef9935d | ProdVPC	590184123293

Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (0)

Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR

No subnet associations

You do not have any subnet associations.

Subnets without explicit associations (1)

Edit subnet associations

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
web	subnet-0ad33aae12ca50adf	10.0.224.0/19	–

Private Route Table

VPC > Route tables > rtb-0bba2b25a5f589310

rtb-0bba2b25a5f589310 / ProdRTprivate

Actions

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0bba2b25a5f589310	No	4 subnets	–

VPC	Owner ID
vpc-09f0330a8aef9935d | ProdVPC	590184123293

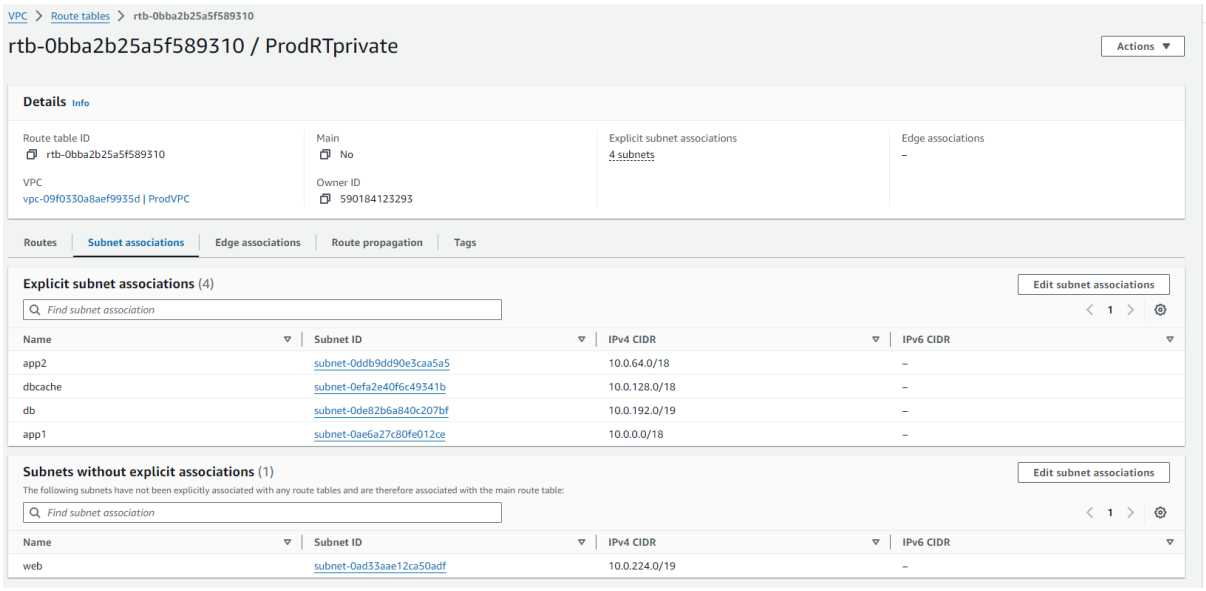
Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2)

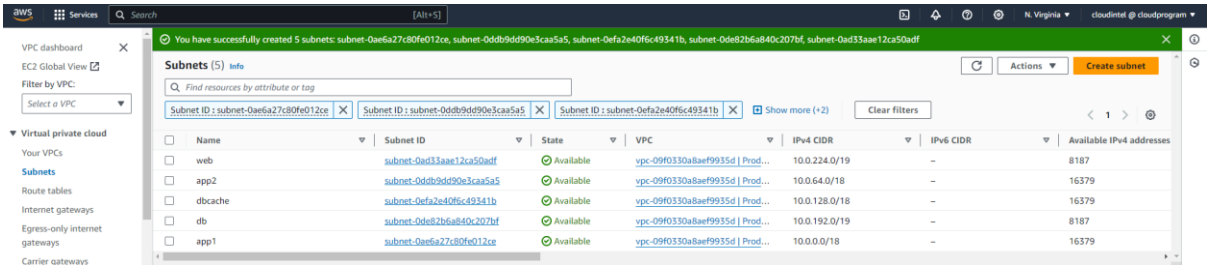
Both | Edit routes

Filter routes

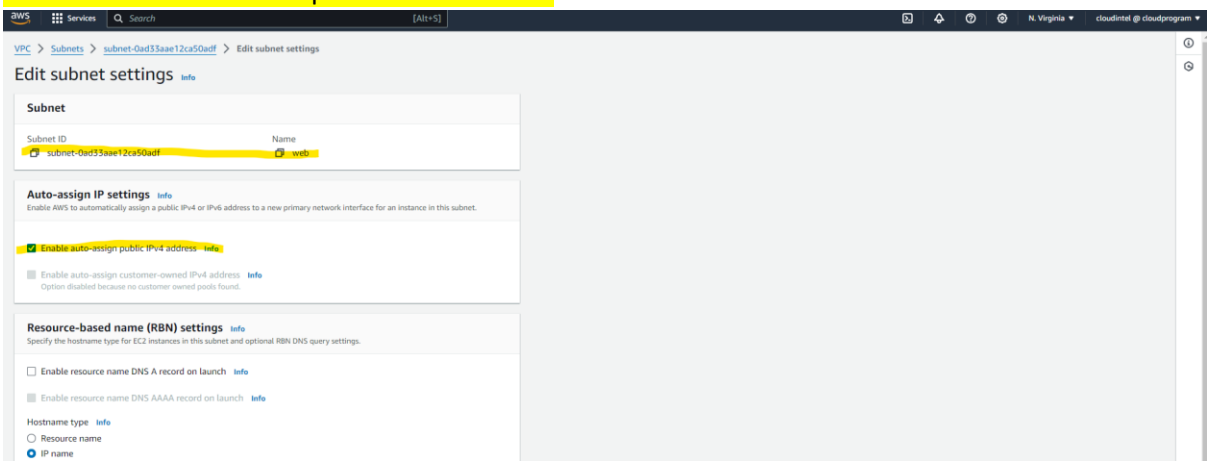
Destination	Target	Status	Propagated
0.0.0.0/0	nat-0f11caed550c9d5f7	Active	No
10.0.0.0/16	local	Active	No



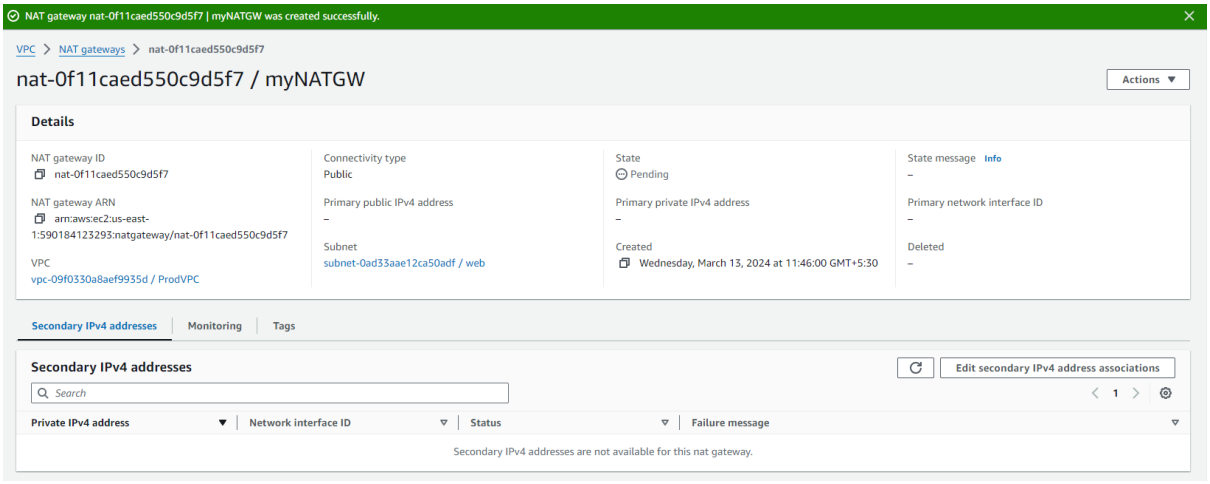
2. Subnets created



ENABLE PUBLIC IP for the public subnet “web”

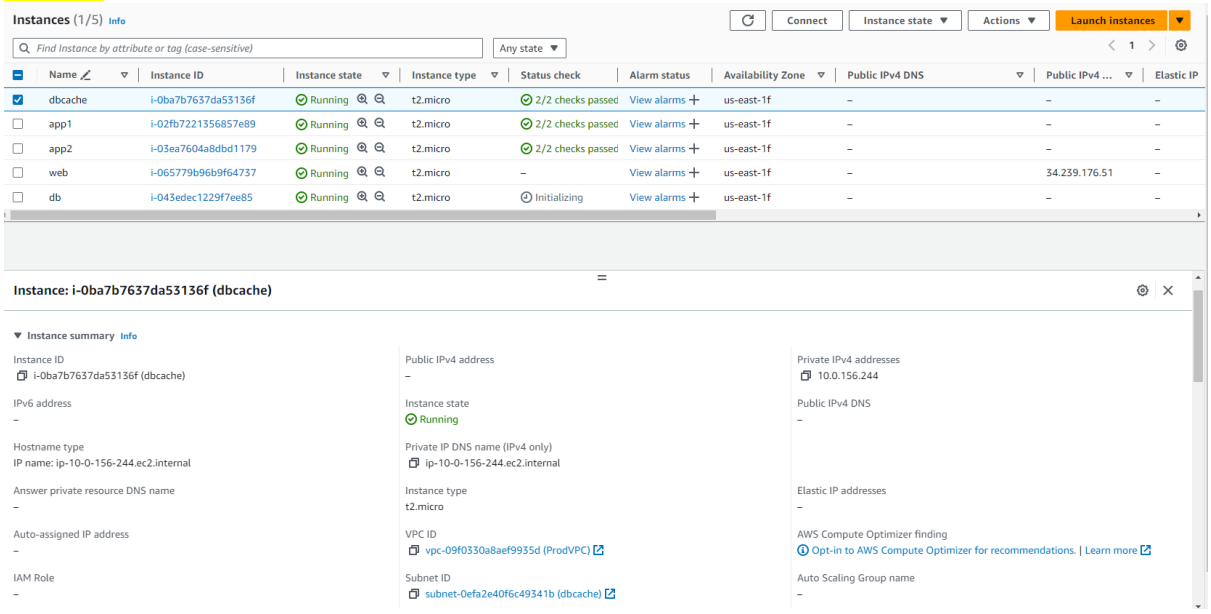


3. Setup NAT for instances in dbcache & app1 to send internet requests

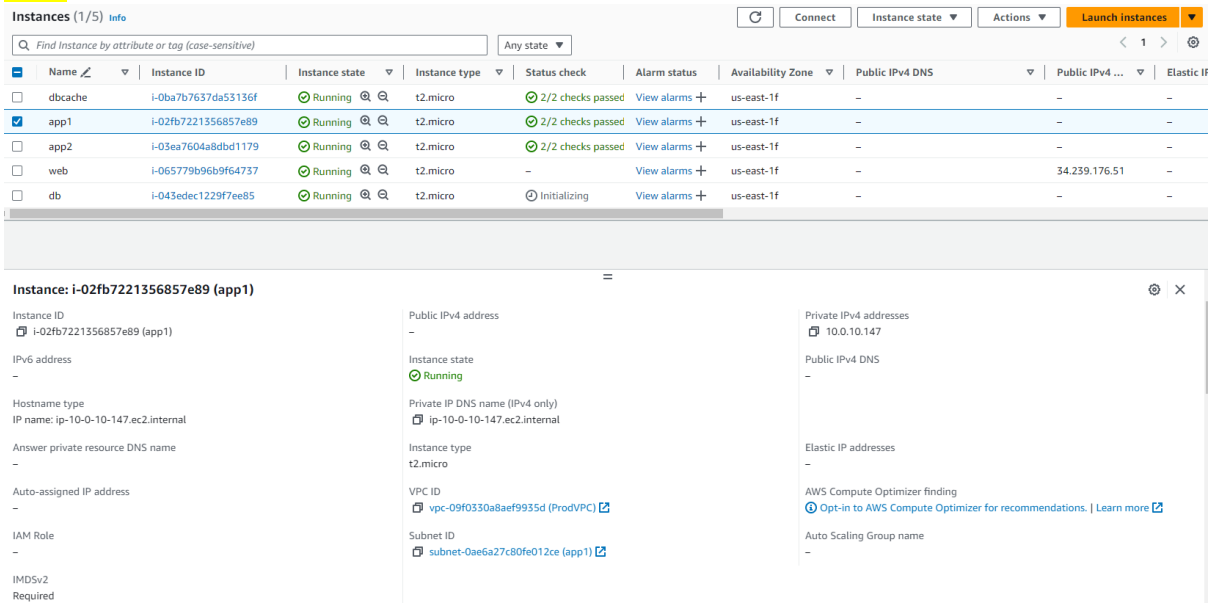


4. Launch EC2 instances in each subnet respectively

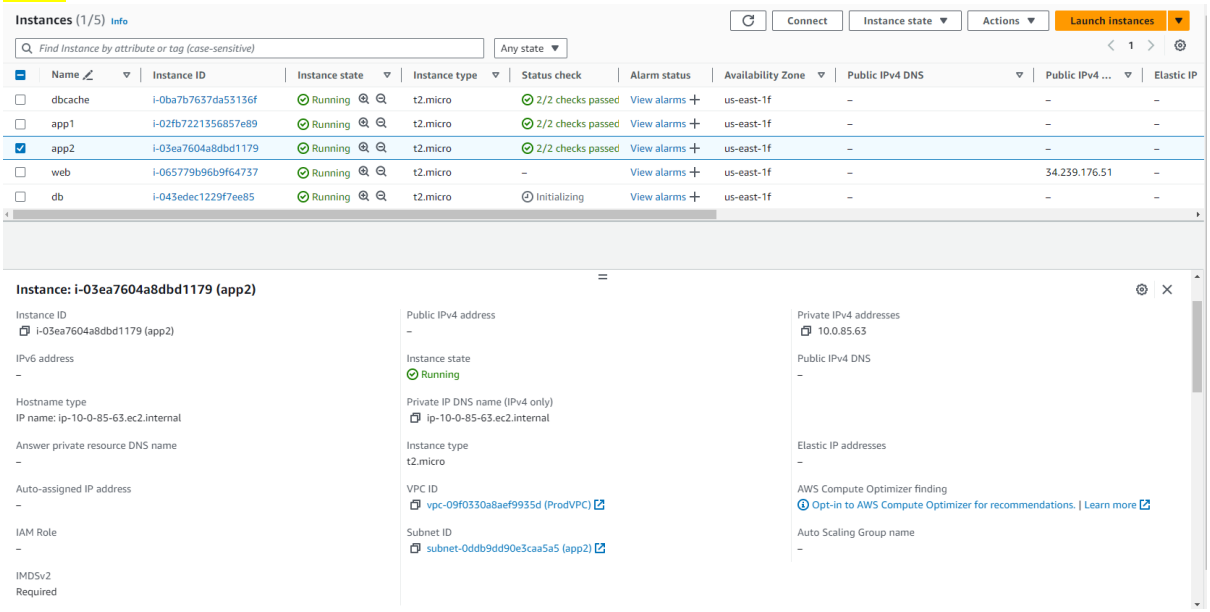
dbcache



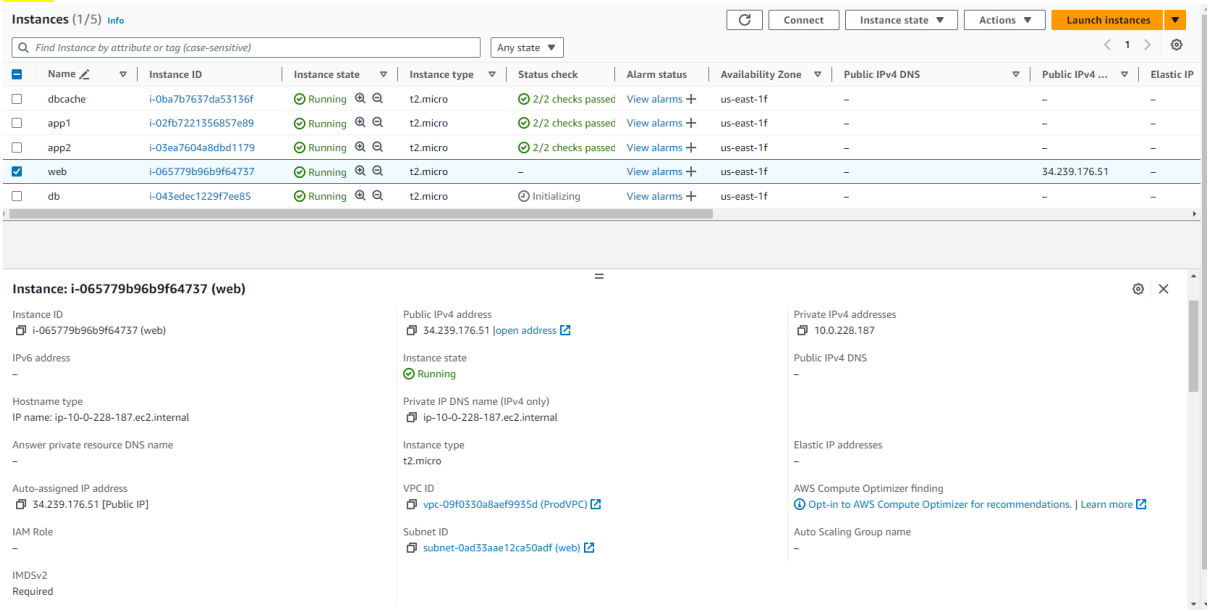
App1



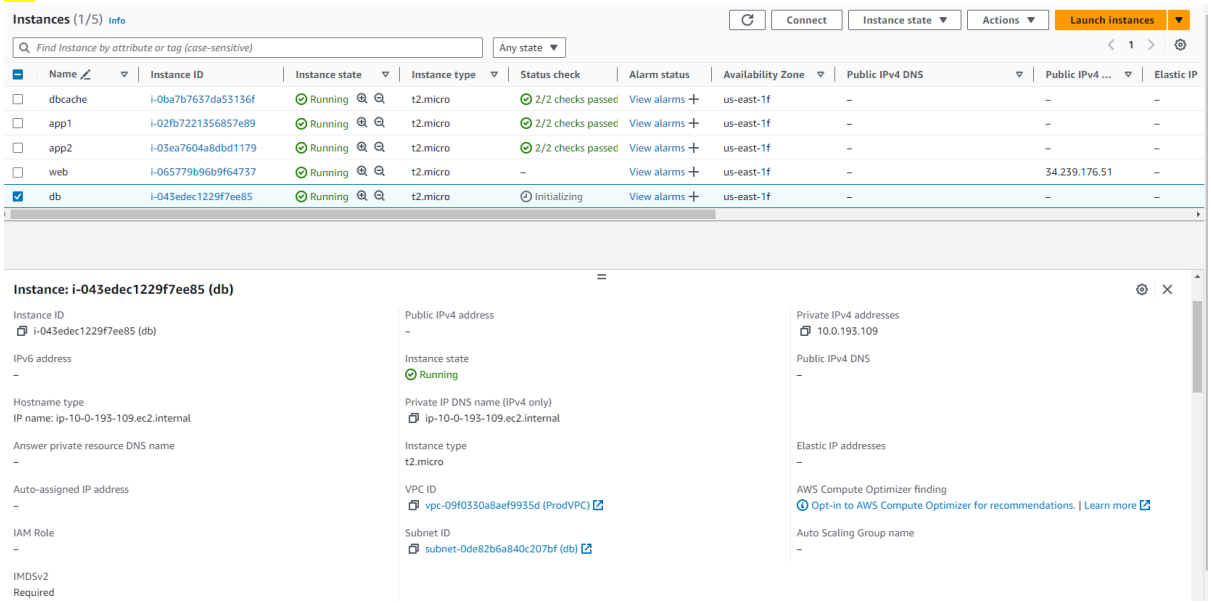
App2


Instances (1/5) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Any state
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
dbcache i-0ba7b7637da53136f Running t2.micro 2/2 checks passed View alarms us-east-1f
app1 i-02fb7221356857e89 Running t2.micro 2/2 checks passed View alarms us-east-1f
app2 i-03ea7604a8dbd1179 Running t2.micro 2/2 checks passed View alarms us-east-1f
web i-065779b96b9f64737 Running t2.micro View alarms us-east-1f 34.239.176.51
db i-043edec1229f7ee85 Running t2.micro Initializing View alarms us-east-1f
Instance: i-03ea7604a8dbd1179 (app2)
Instance ID
i-03ea7604a8dbd1179 (app2)
IPv6 address
Hostname type
IP name: ip-10-0-85-63.ec2.internal
Answer private resource DNS name
Auto-assigned IP address
IAM Role
IMDSv2
Required
Public IPv4 address
Instance state
Running
Private IP DNS name (IPv4 only)
ip-10-0-85-63.ec2.internal
Instance type
t2.micro
VPC ID
vpc-09f0330a8aef9935d (ProdVPC)
Subnet ID
subnet-0ddb9dd90e3caa5a5 (app2)
Private IPv4 addresses
10.0.85.63
Public IPv4 DNS
Elastic IP addresses
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
Auto Scaling Group name

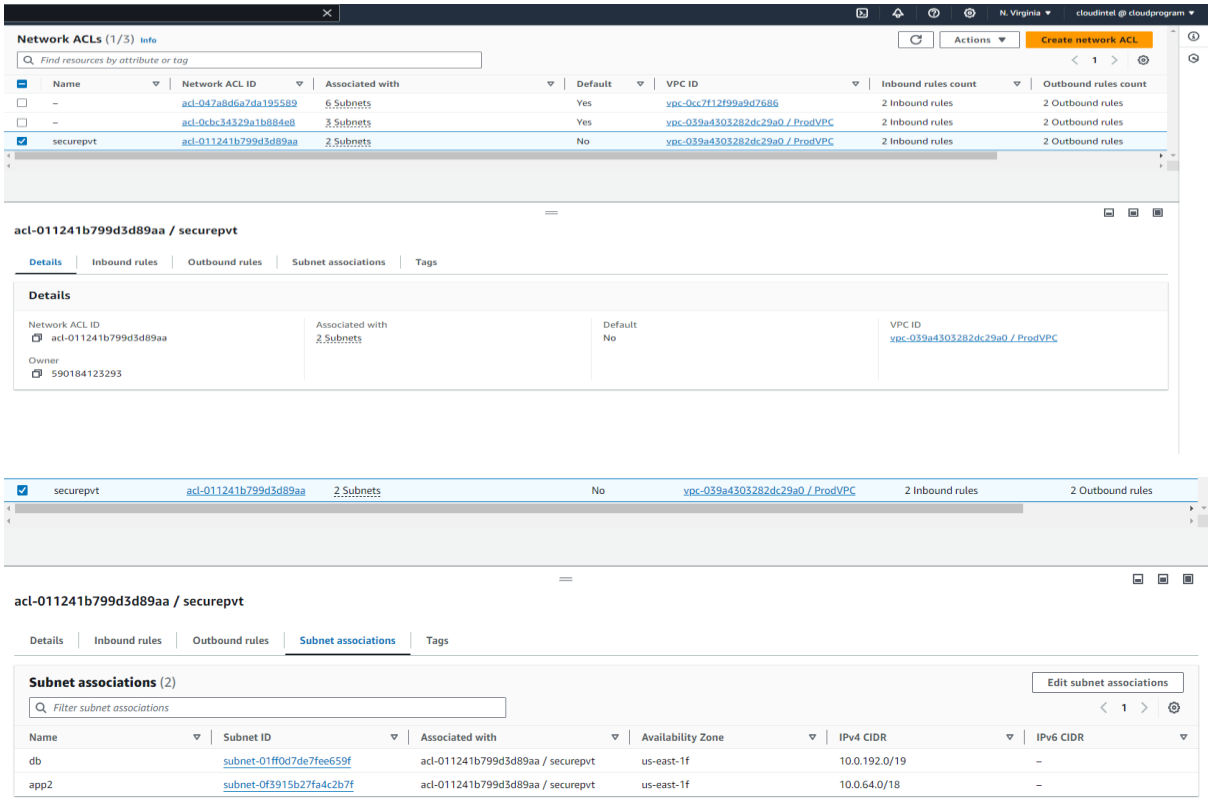
web


Instances (1/5) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Any state
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
dbcache i-0ba7b7637da53136f Running t2.micro 2/2 checks passed View alarms us-east-1f
app1 i-02fb7221356857e89 Running t2.micro 2/2 checks passed View alarms us-east-1f
app2 i-03ea7604a8dbd1179 Running t2.micro 2/2 checks passed View alarms us-east-1f
web i-065779b96b9f64737 Running t2.micro View alarms us-east-1f 34.239.176.51
db i-043edec1229f7ee85 Running t2.micro Initializing View alarms us-east-1f
Instance: i-065779b96b9f64737 (web)
Instance ID
i-065779b96b9f64737 (web)
IPv6 address
Hostname type
IP name: ip-10-0-228-187.ec2.internal
Answer private resource DNS name
Auto-assigned IP address
34.239.176.51 [Public IP]
IAM Role
IMDSv2
Required
Public IPv4 address
34.239.176.51 |open address
Instance state
Running
Private IP DNS name (IPv4 only)
ip-10-0-228-187.ec2.internal
Instance type
t2.micro
VPC ID
vpc-09f0330a8aef9935d (ProdVPC)
Subnet ID
subnet-0ad33aae12ca50adf (web)
Private IPv4 addresses
10.0.228.187
Public IPv4 DNS
Elastic IP addresses
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
Auto Scaling Group name

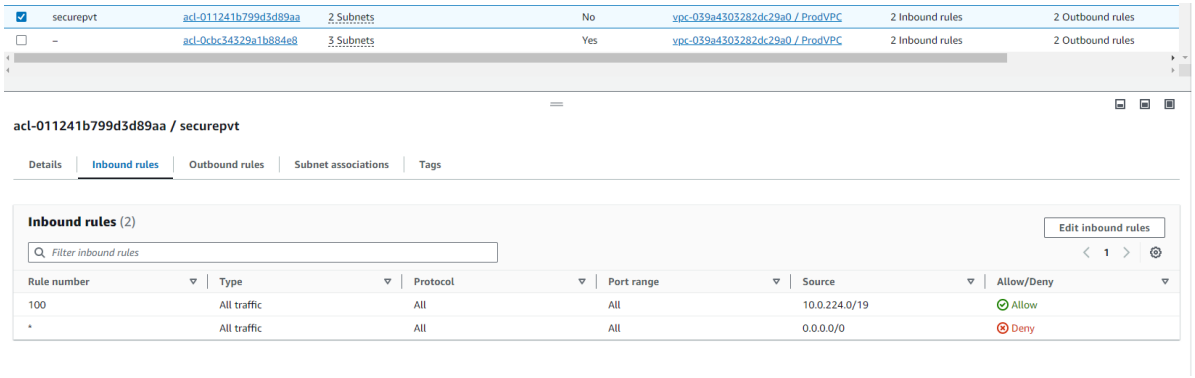
db



NACL created for db & app2 subnet that does not require internet access



INBOUND – SSH allowed within VPC



securepvt	acl-011241b799d3d89aa	2 Subnets	No	vpc-039a4303282dc29a0 / ProdVPC	2 Inbound rules	2 Outbound rules
–	acl-0cbc34329a1b884e8	3 Subnets	Yes	vpc-039a4303282dc29a0 / ProdVPC	2 Inbound rules	2 Outbound rules

acl-011241b799d3d89aa / securepvt

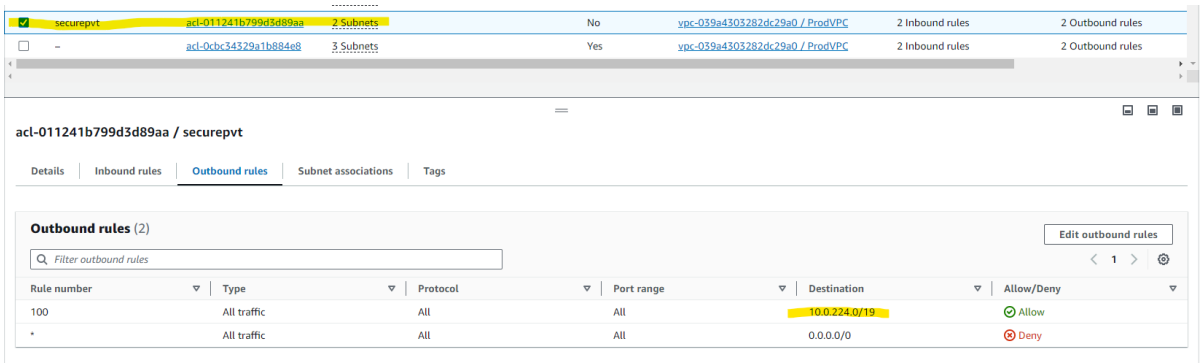
Details | Inbound rules | Outbound rules | Subnet associations | Tags

Inbound rules (2) — Edit inbound rules

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	10.0.224.0/19	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Outbound



securepvt	acl-011241b799d3d89aa	2 Subnets	No	vpc-039a4303282dc29a0 / ProdVPC	2 Inbound rules	2 Outbound rules
–	acl-0cbc34329a1b884e8	3 Subnets	Yes	vpc-039a4303282dc29a0 / ProdVPC	2 Inbound rules	2 Outbound rules

acl-011241b799d3d89aa / securepvt

Details | Inbound rules | Outbound rules | Subnet associations | Tags

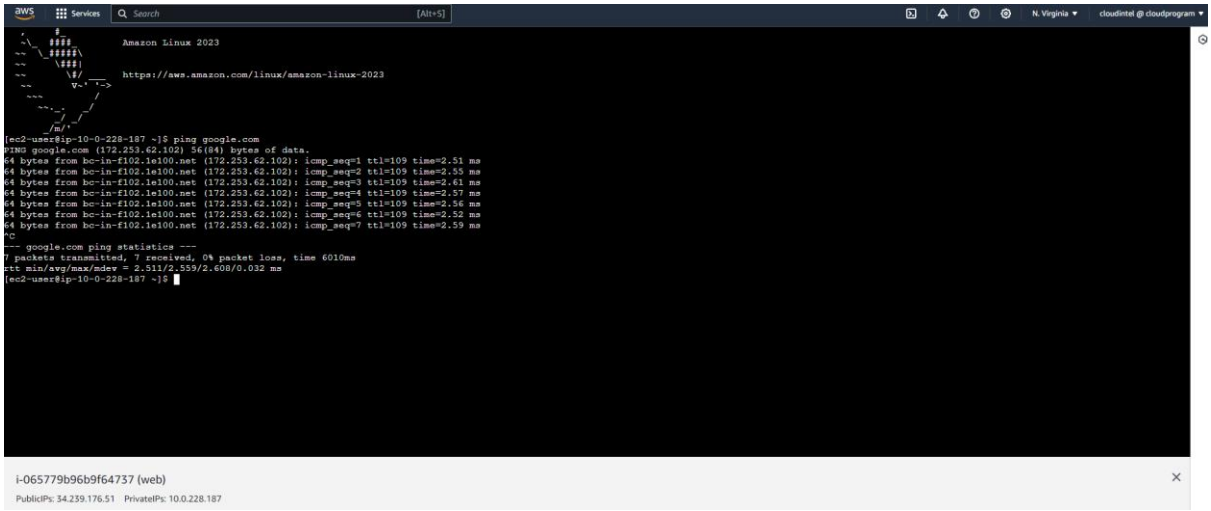
Outbound rules (2) — Edit outbound rules

Filter outbound rules

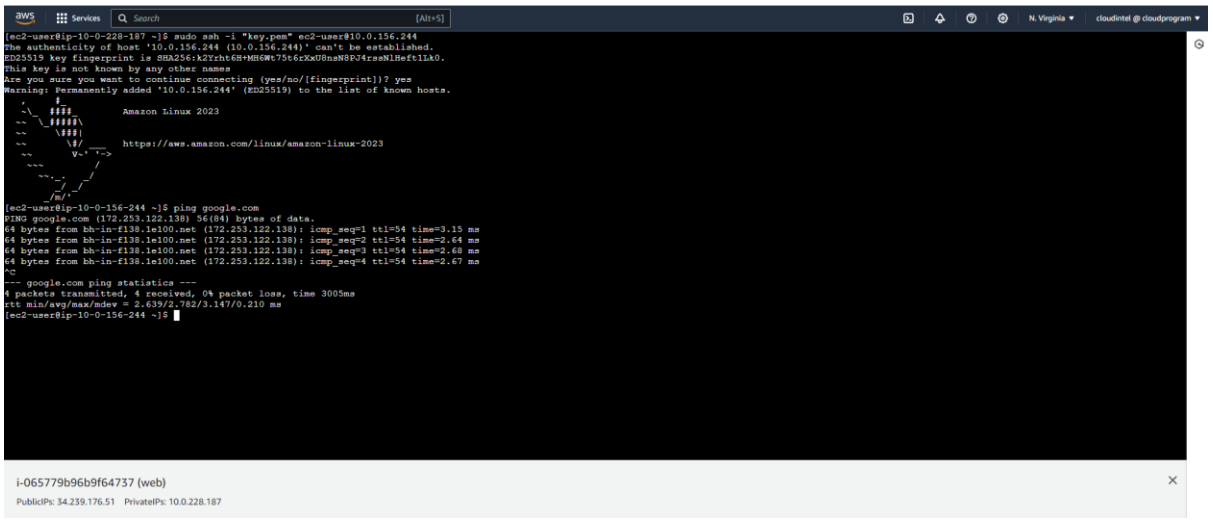
Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	10.0.224.0/19	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

VERIFICATION

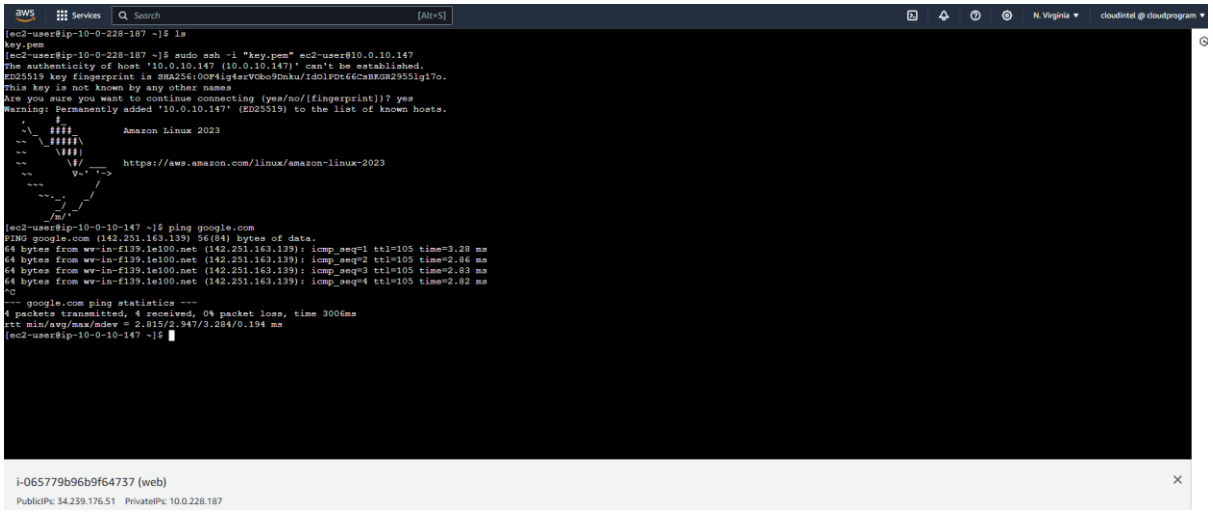
Web Instance internet connectivity



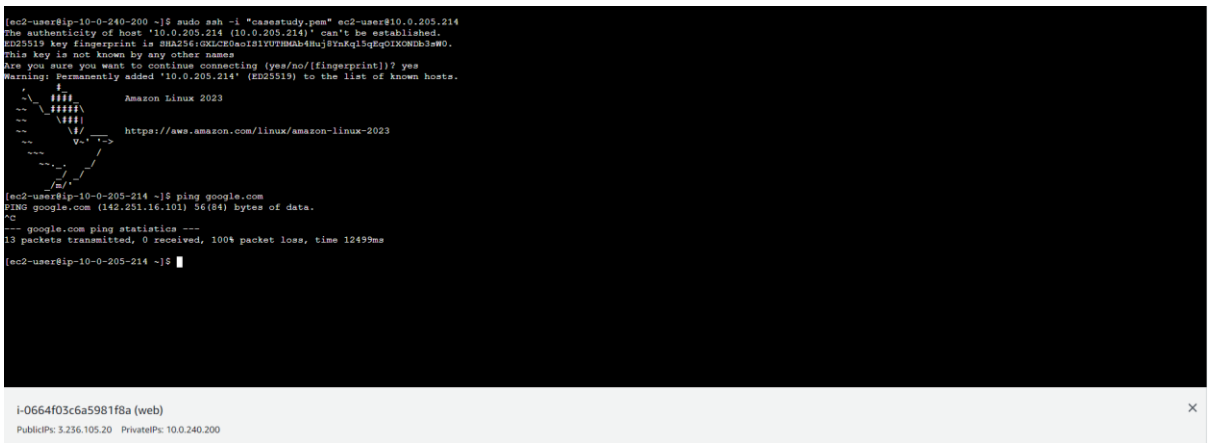
Dbcache private instance connected via web instance (SSH) and internet verified



App1 private instance connected via web instance (SSH) and internet verified

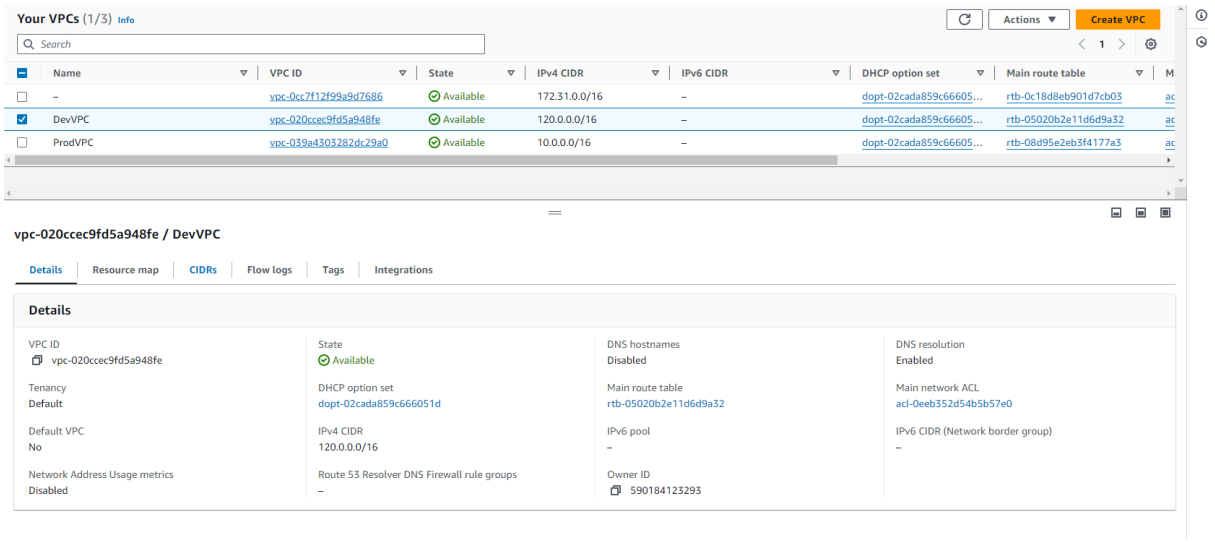


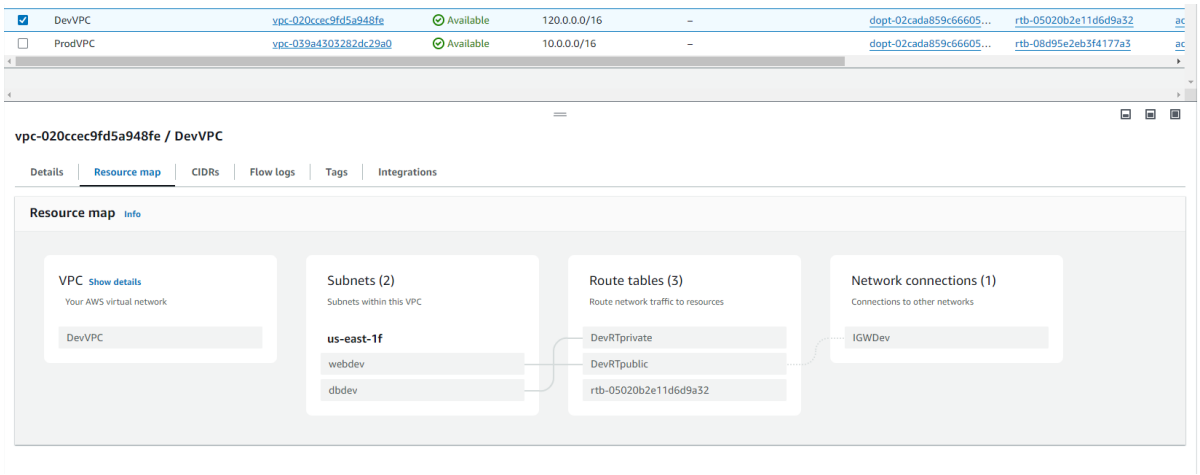
db private instance connected via web instance (SSH) and internet connection failed as expected



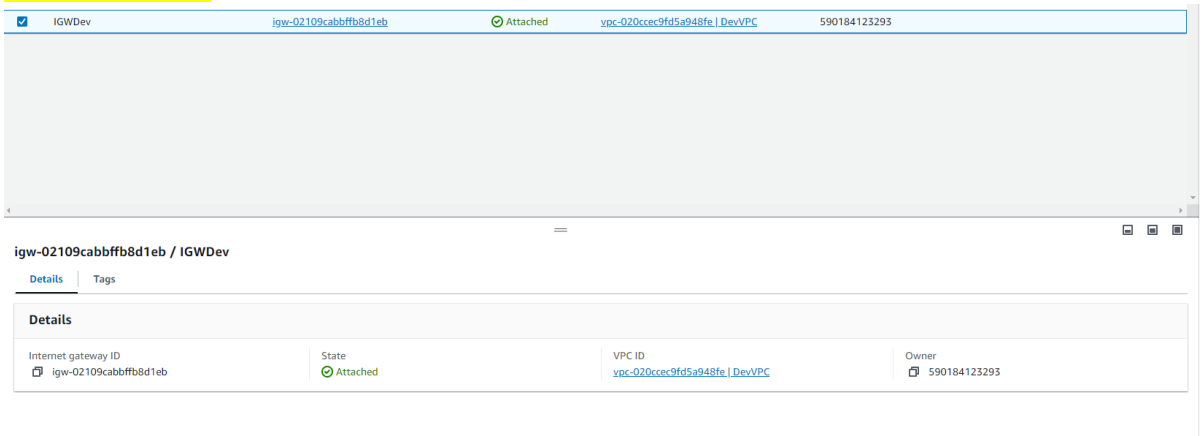
DEVELOPMENT NETWORK

1. DevVPC created



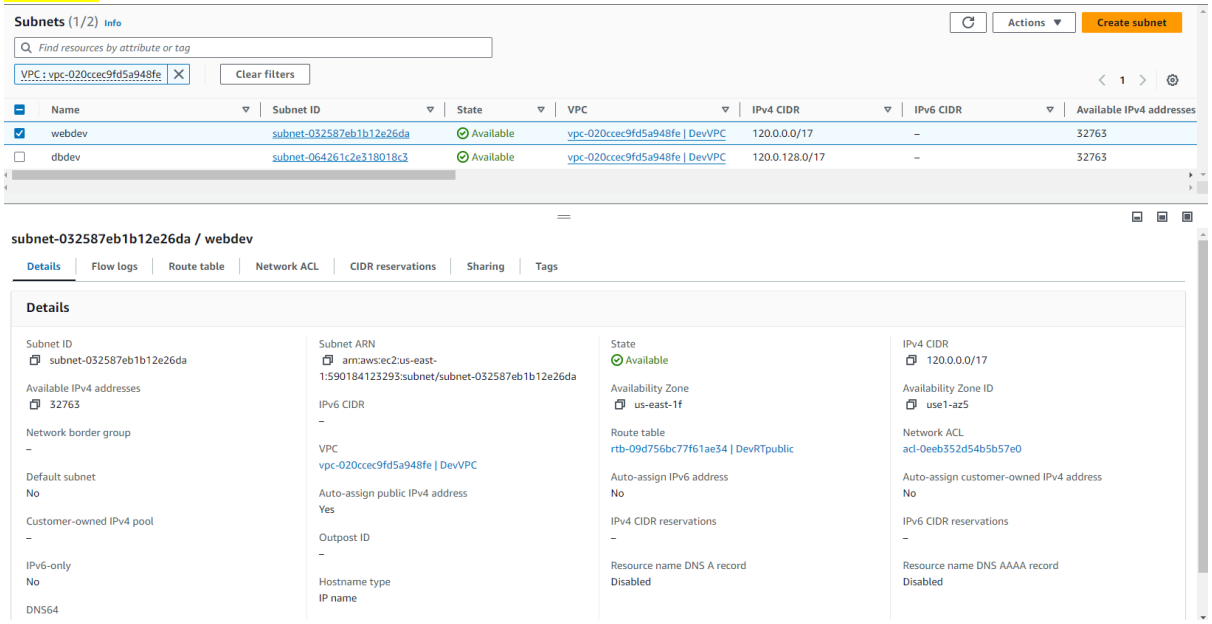


Internet Gateway

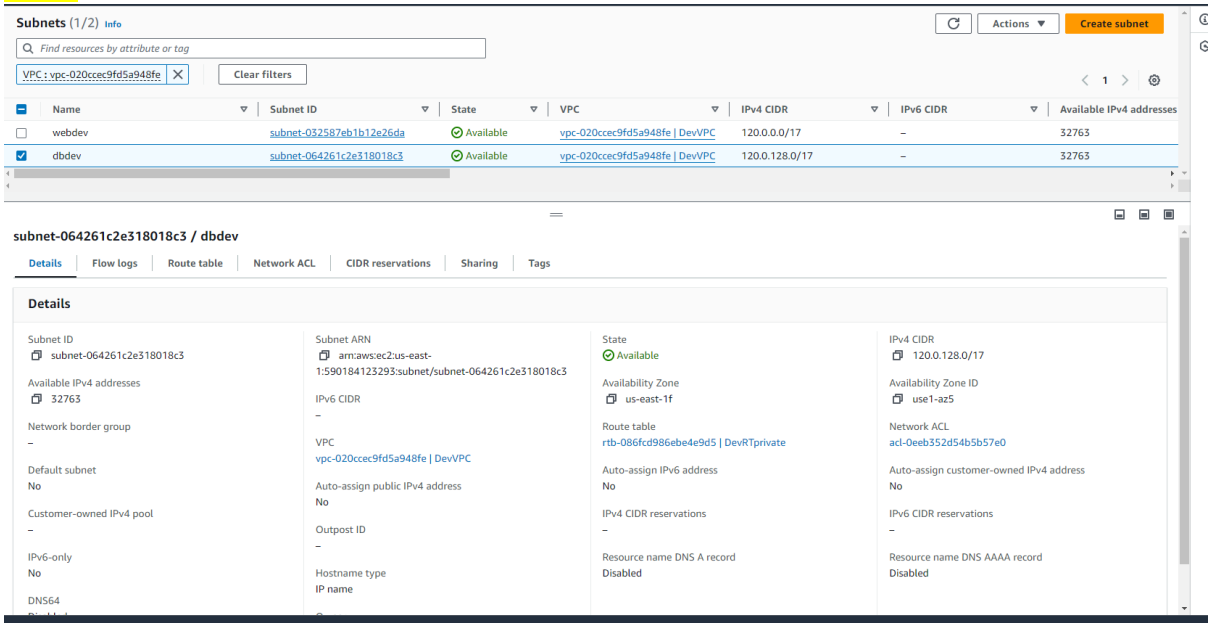


2. Subnets created

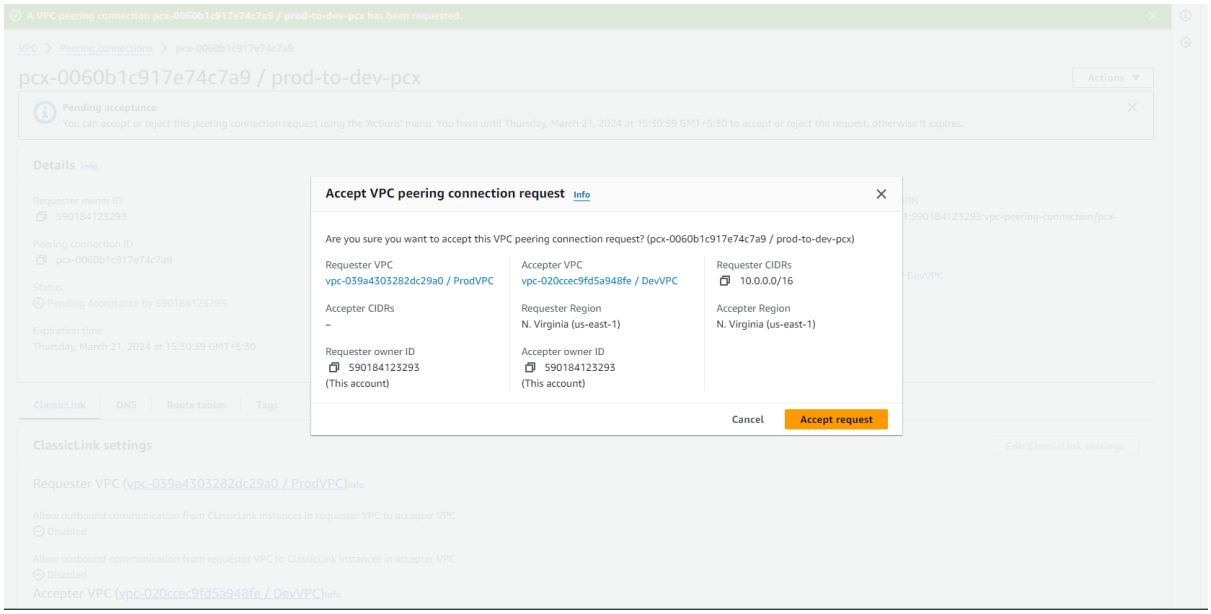
webdev

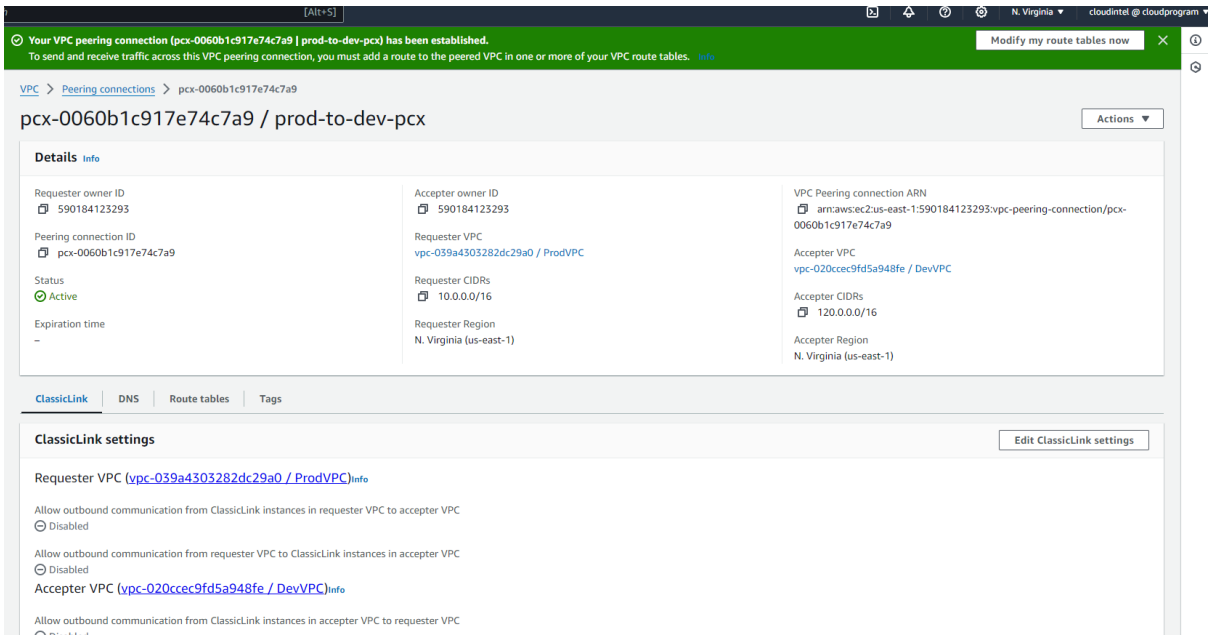


dbdev

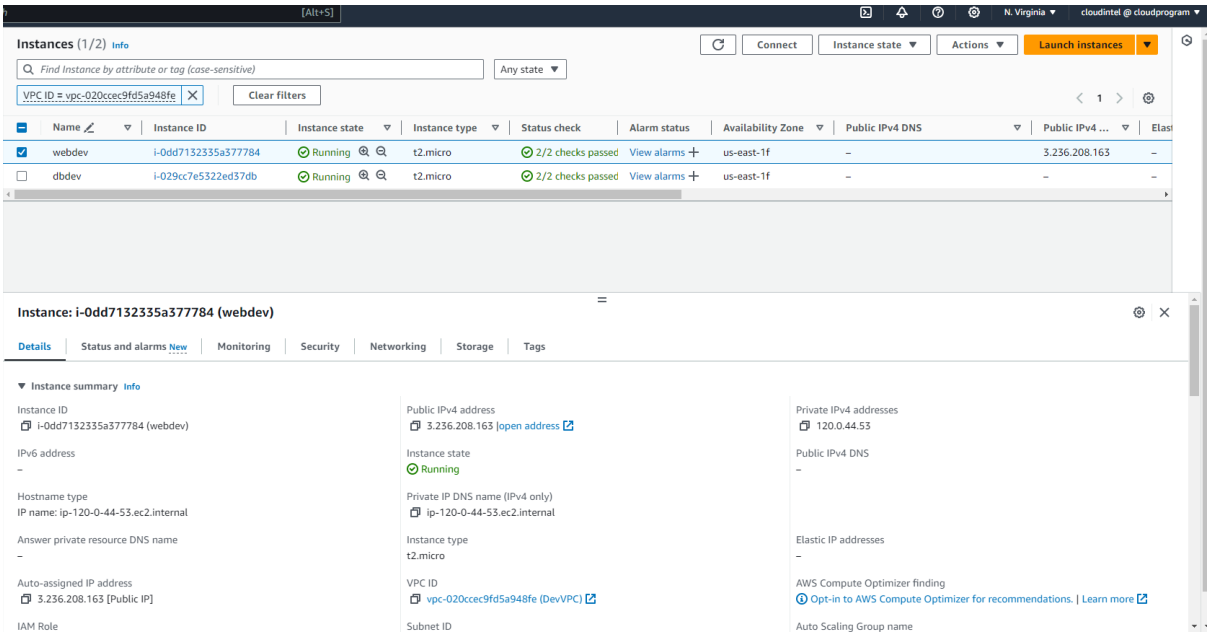


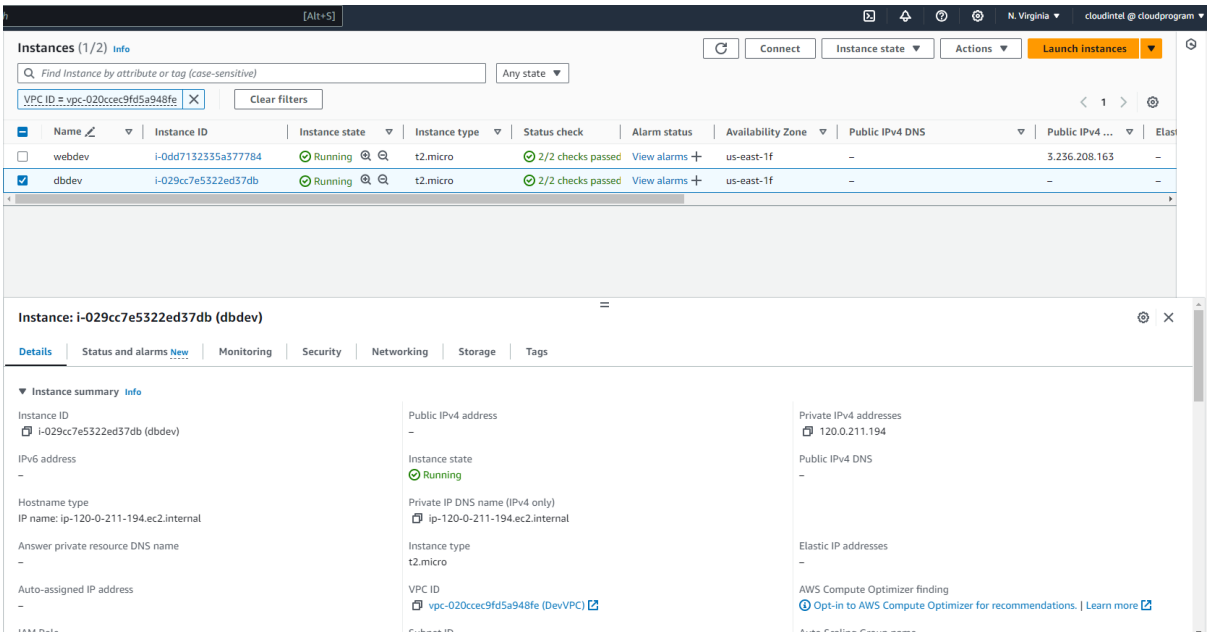
3. Setup peering connection



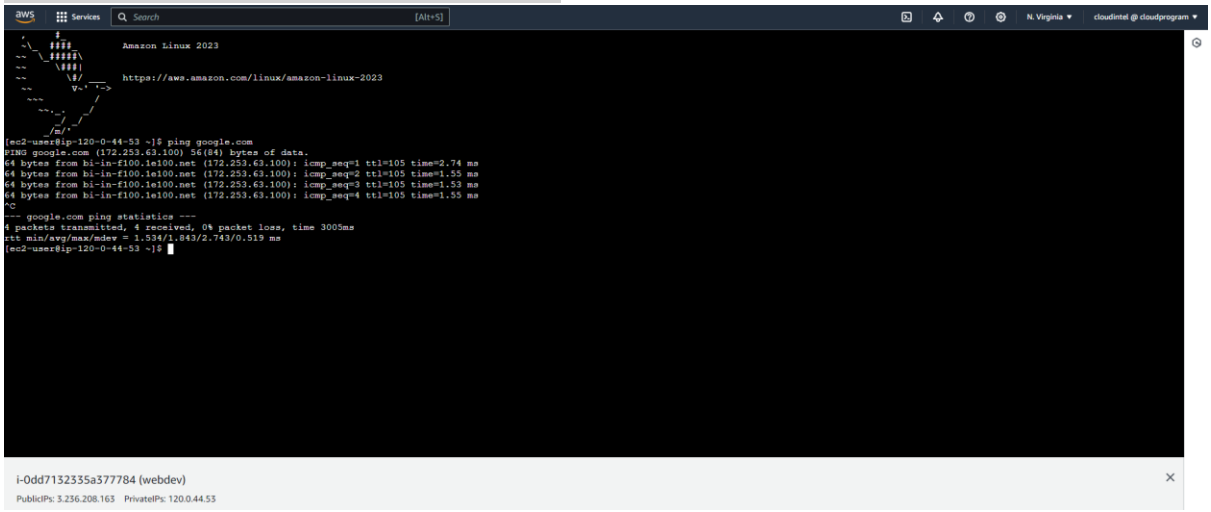


4. Create EC2 instances webdev & dbdev

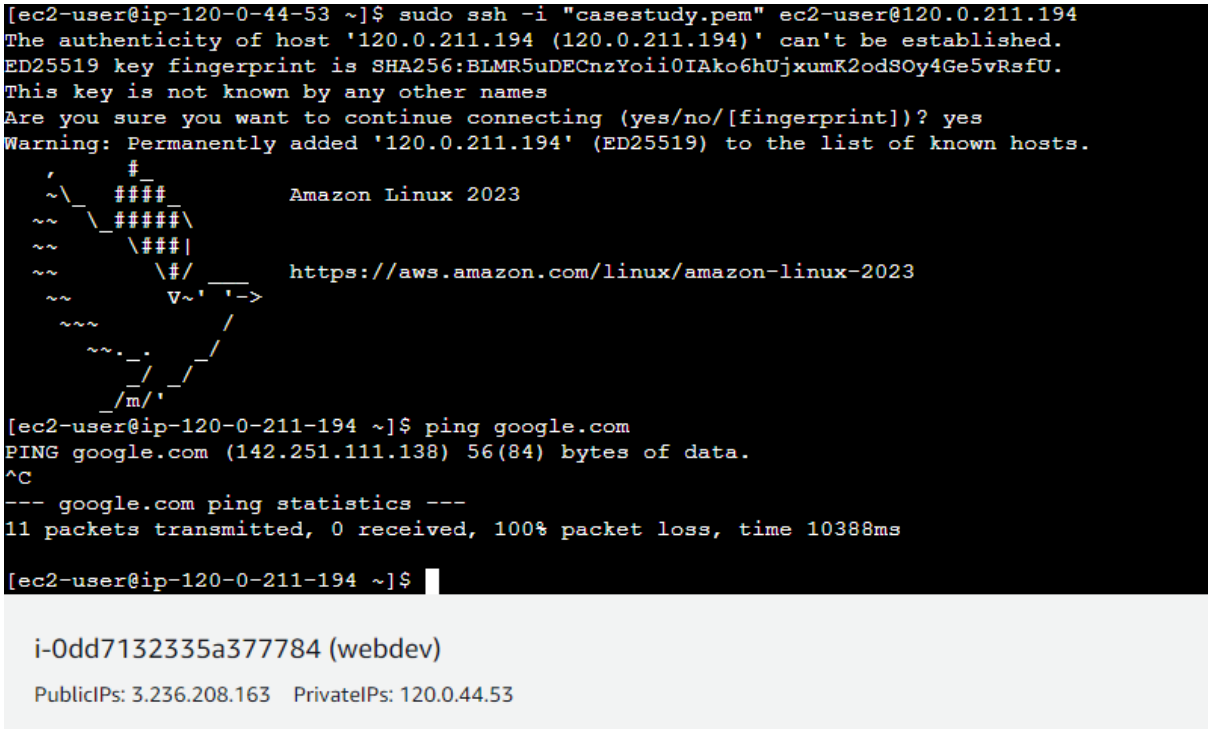




Internet connectivity setup in webdev instance

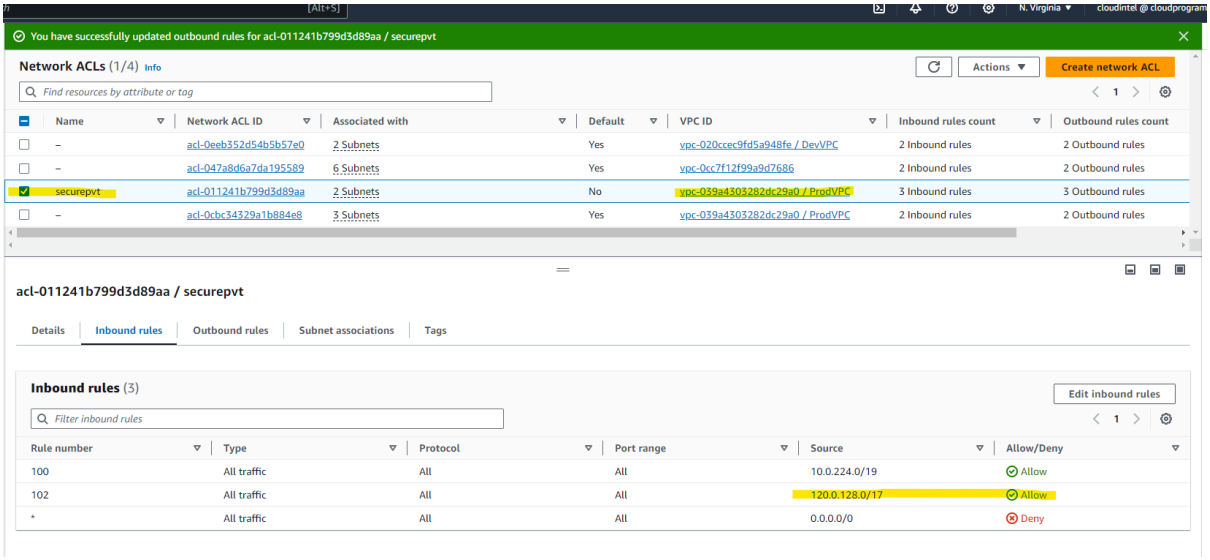


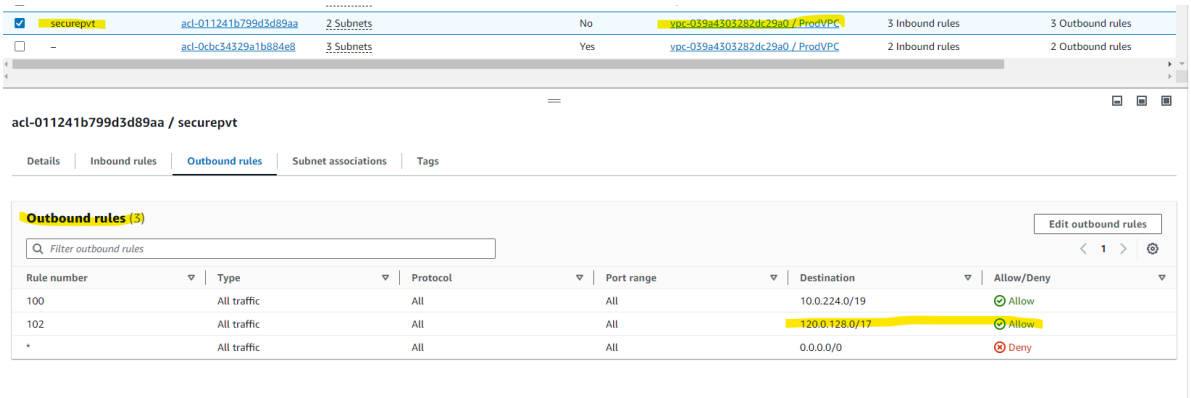
No Internet connectivity setup in dbdev instance



5. Setup connection between db subnets of PROD and DEV network

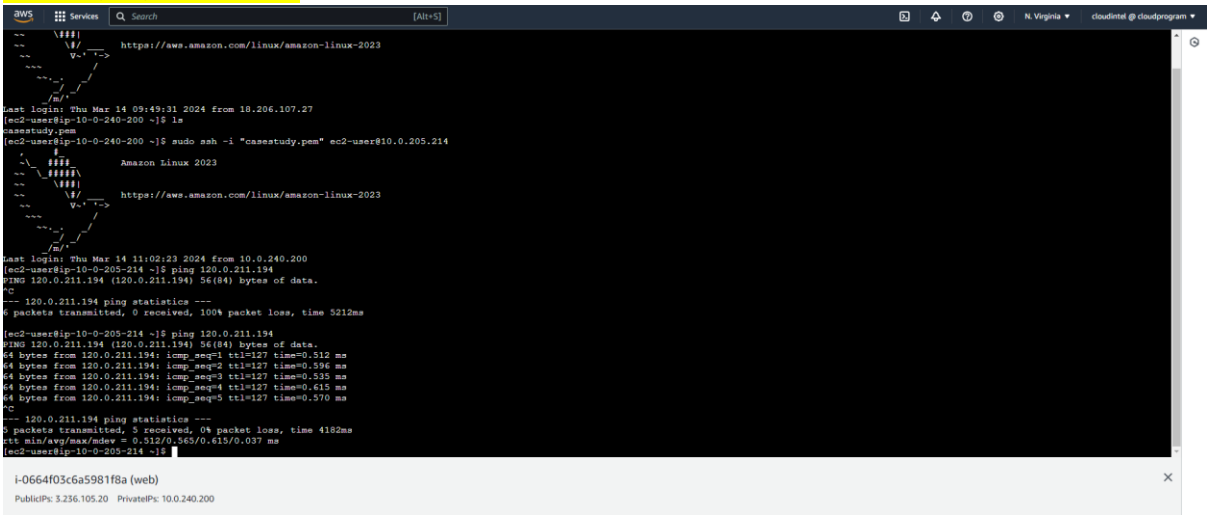
Updated NACL in PROD VPC to allow connectivity





Connection verified from ProdVPC -db instance TO DevVPC -dbdev instance

Web -> (ssh) db -> dbdev



Connection verified from DevVPC -dbdev instance TO ProdVPC -db instance

Webdev -> (ssh) dbdev -> db