Amazon VPC Architecture Assignment

Prepared by: Vikram

Problem Statement

You work for XYZ Corporation and have been asked to create and set up distinct Amazon VPCs for the production and development teams.

Production Network

1. Design and build a 4-tier architecture.
2. Create 5 subnets — 4 private (app1, app2, dbcache, db) and 1 public (web).
3. Launch instances in all subnets and name them as per subnet name.
4. Allow dbcache instance and app1 subnet to send internet requests.
5. Manage Security Groups and NACLs.

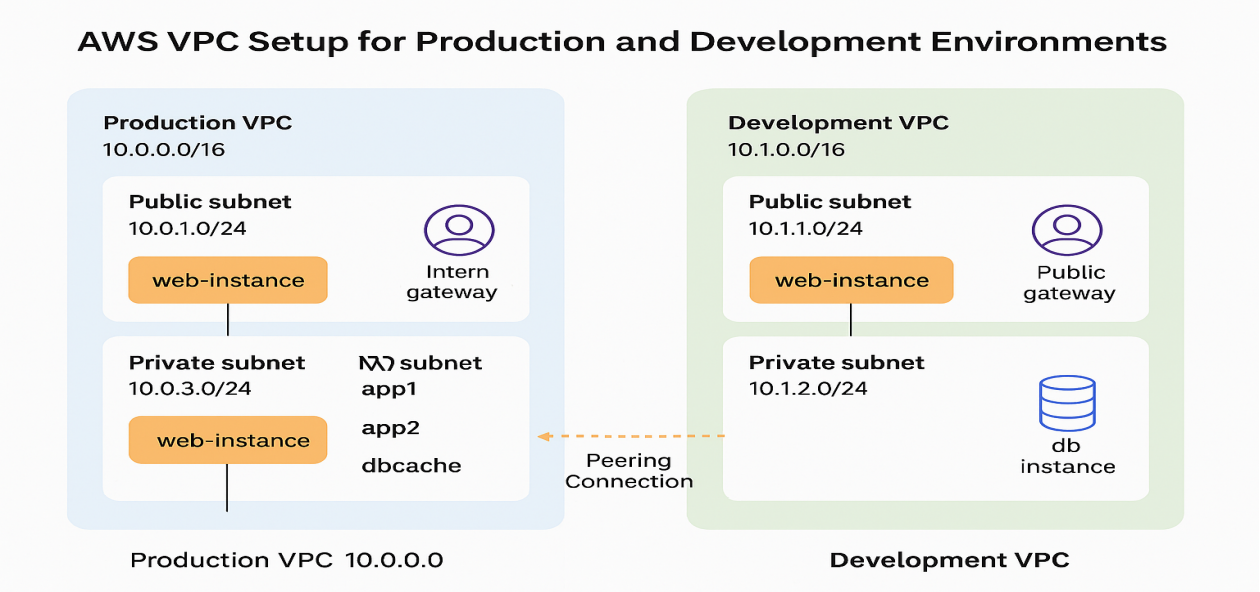
Development Network

1. Design and build a 2-tier architecture with subnets (web and db).
2. Allow only web subnet to send internet requests.
3. Create peering connection between production and development networks.
4. Setup connection between db subnets of both production and development networks.

Architecture Overview

Two isolated VPCs were created: - **Production VPC:** 10.0.0.0/16 (4-tier architecture) - **Development VPC:** 10.1.0.0/16 (2-tier architecture)

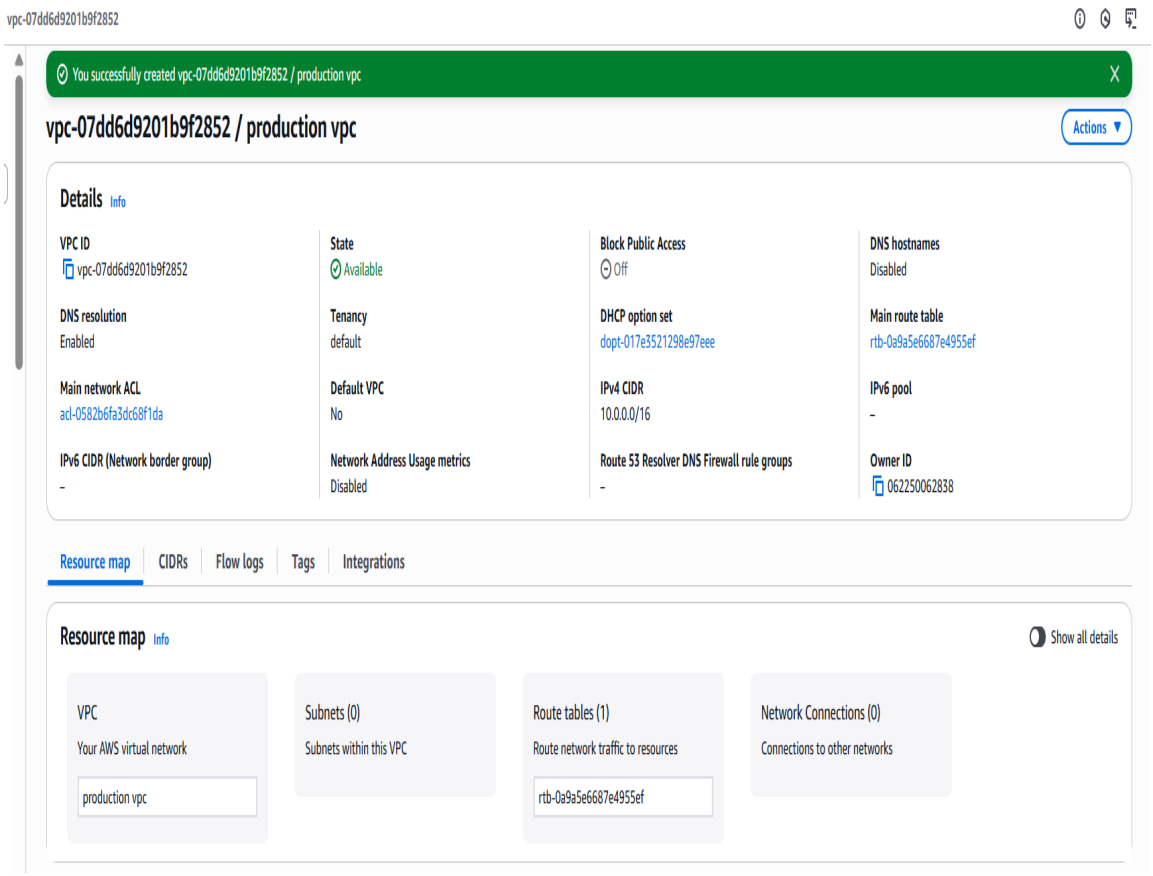
A VPC Peering connection was created between the two VPCs to allow private communication between their DB subnets. The Production VPC includes a NAT Gateway for private subnets, while the Development VPC allows only the web subnet to access the internet.

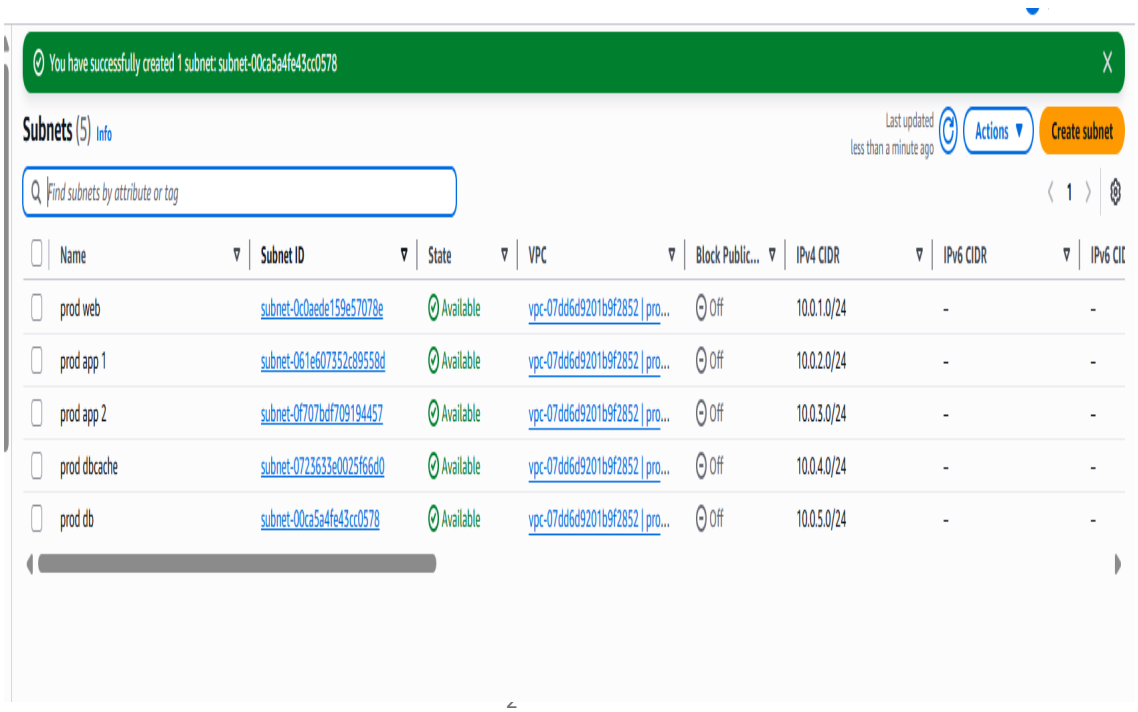


Step-by-Step Configuration

1. Create Production VPC (10.0.0.0/16)

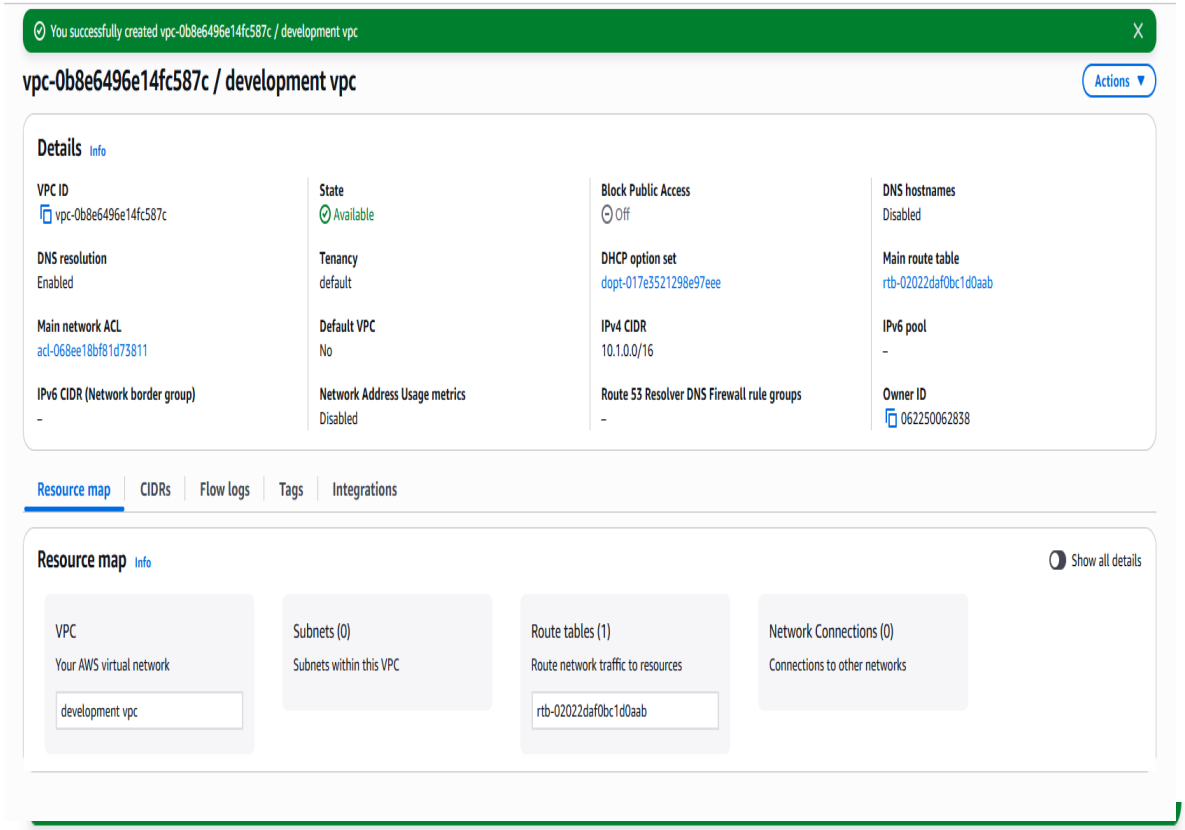
- Create the following subnets:
- web (public)
- app1, app2, dbcache, db (private)
- Assign subnets across different Availability Zones for high availability.

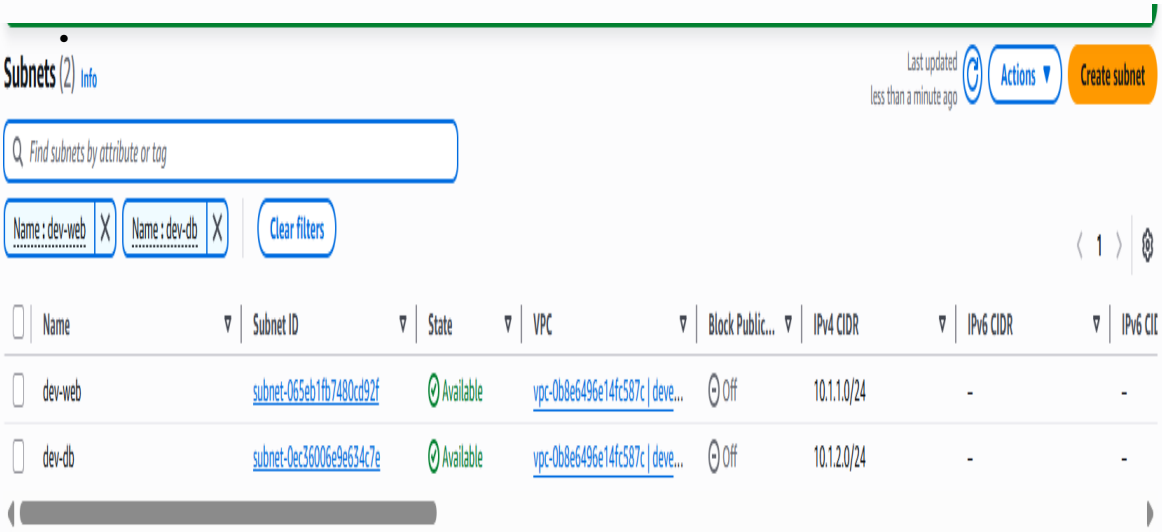




2. Create Development VPC (10.1.0.0/16)

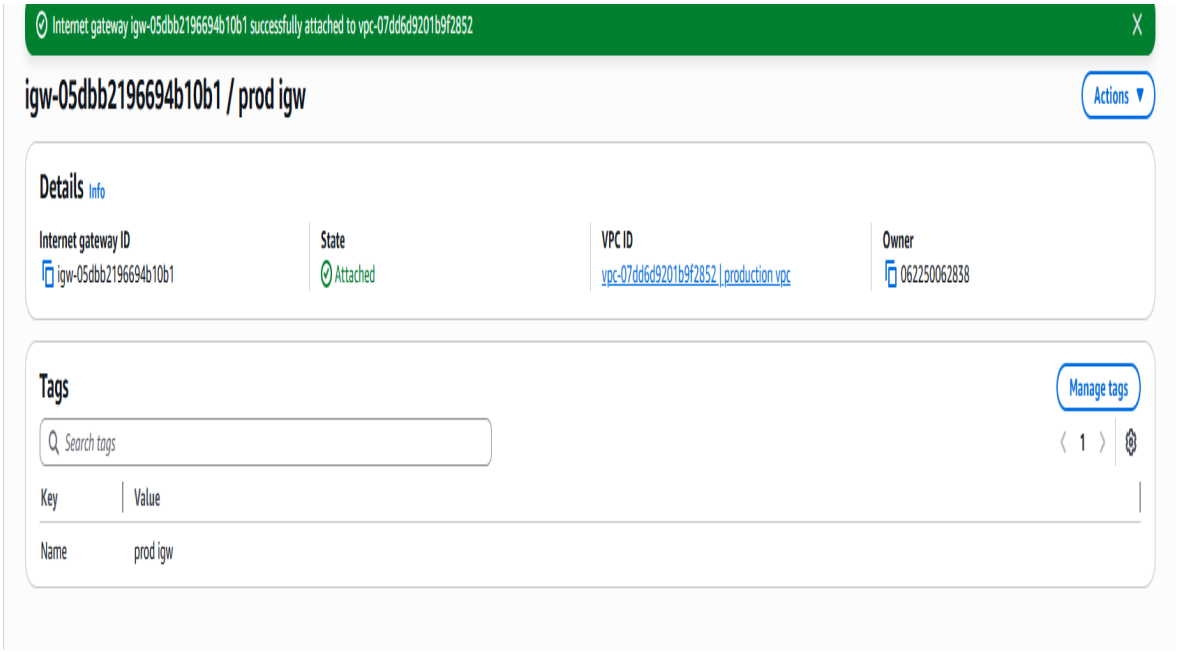
- Create subnets:
- web (public)
- db (private)

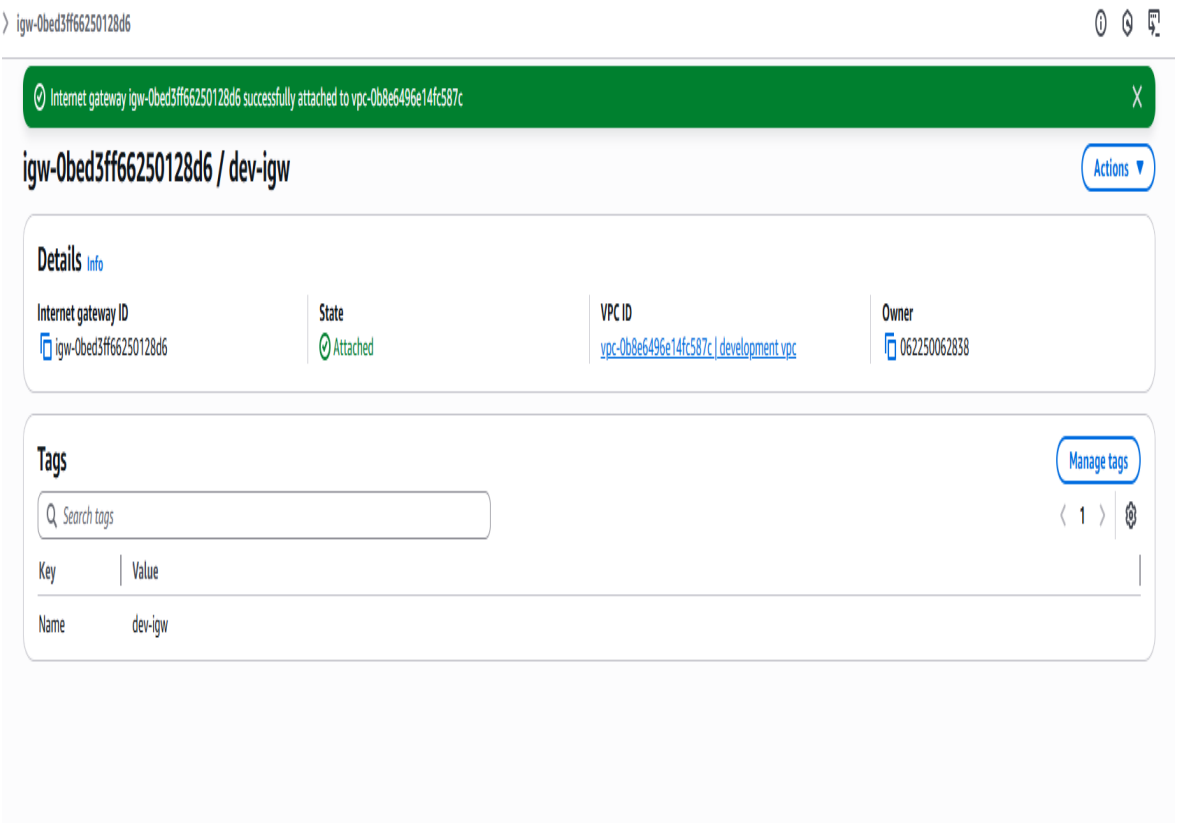




3. Attach Internet Gateways

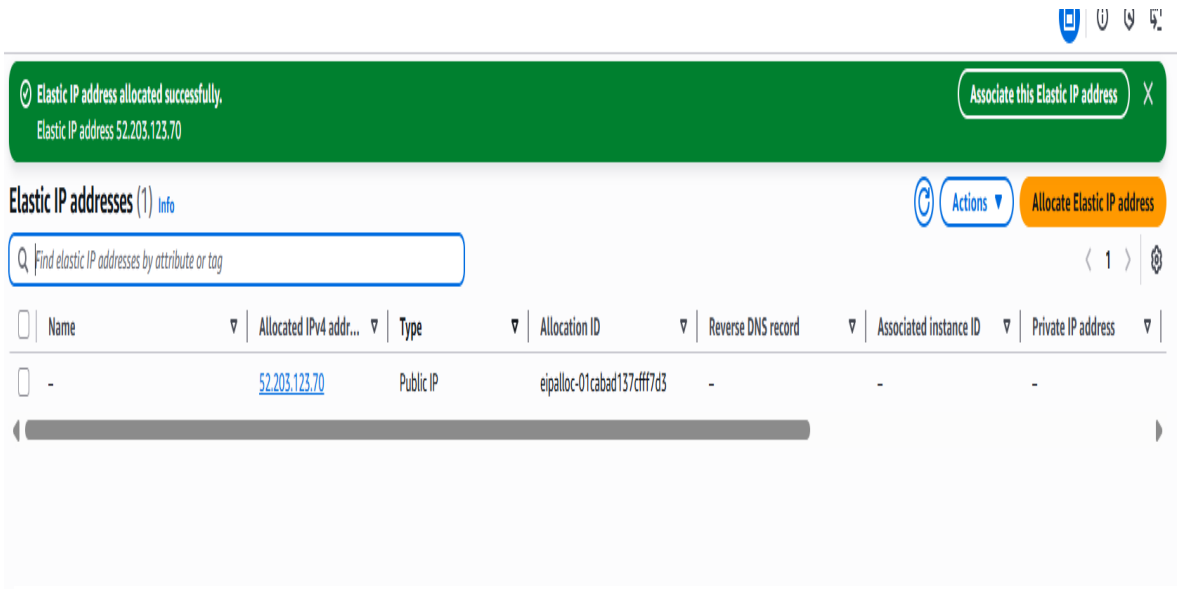
- Create and attach an Internet Gateway (IGW) to both VPCs.

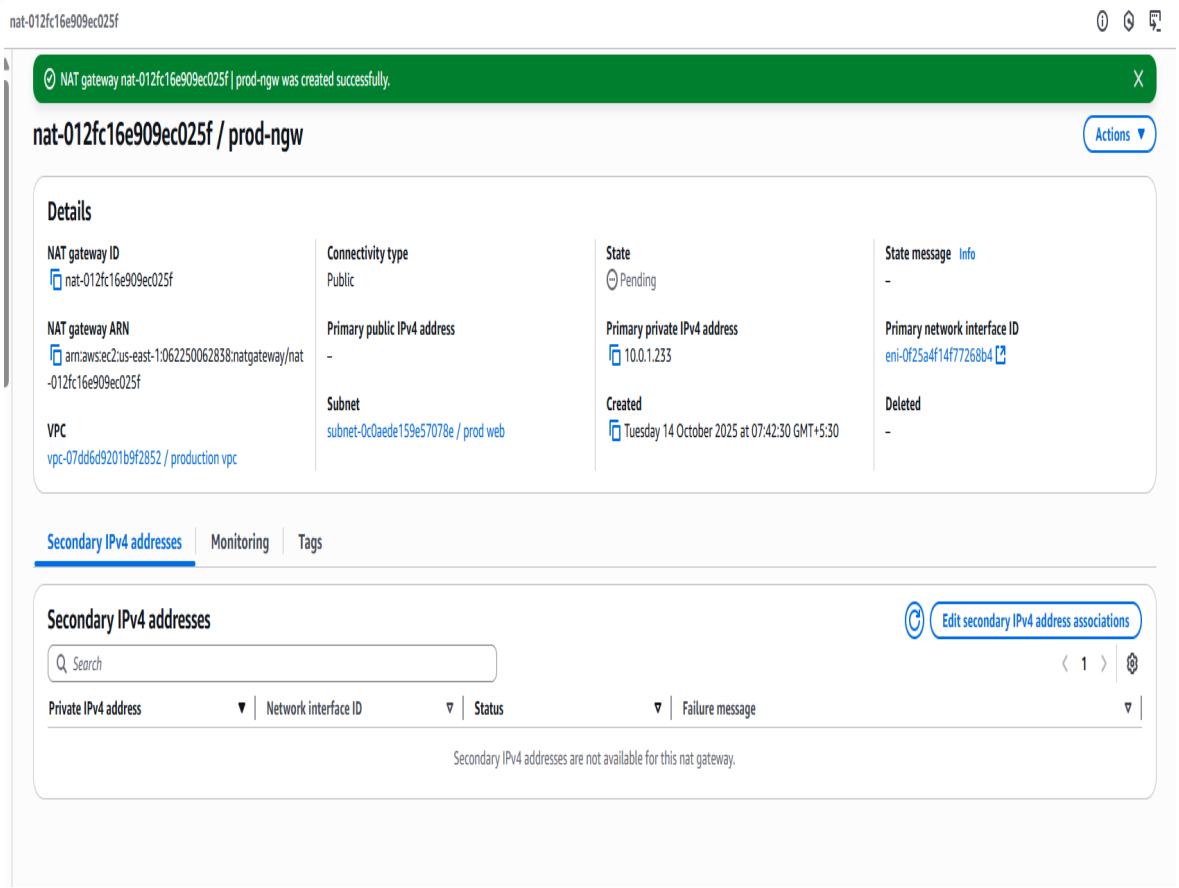




4. Create NAT Gateway (Production VPC only)

- Allocate a new **Elastic IP**.
- Create a **NAT Gateway** in the Production public subnet (web).
- Attach the allocated Elastic IP to the NAT Gateway.

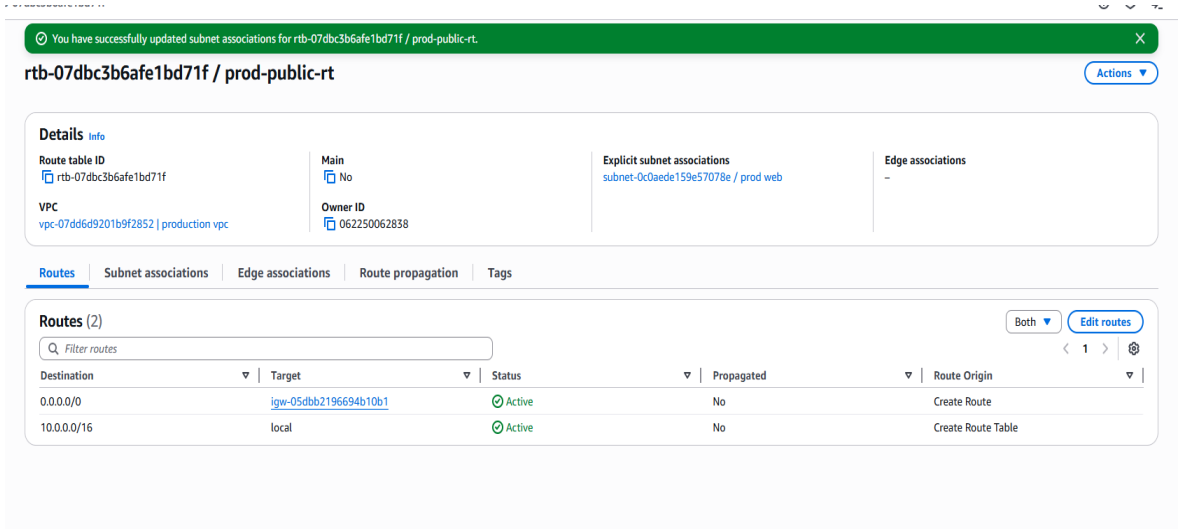


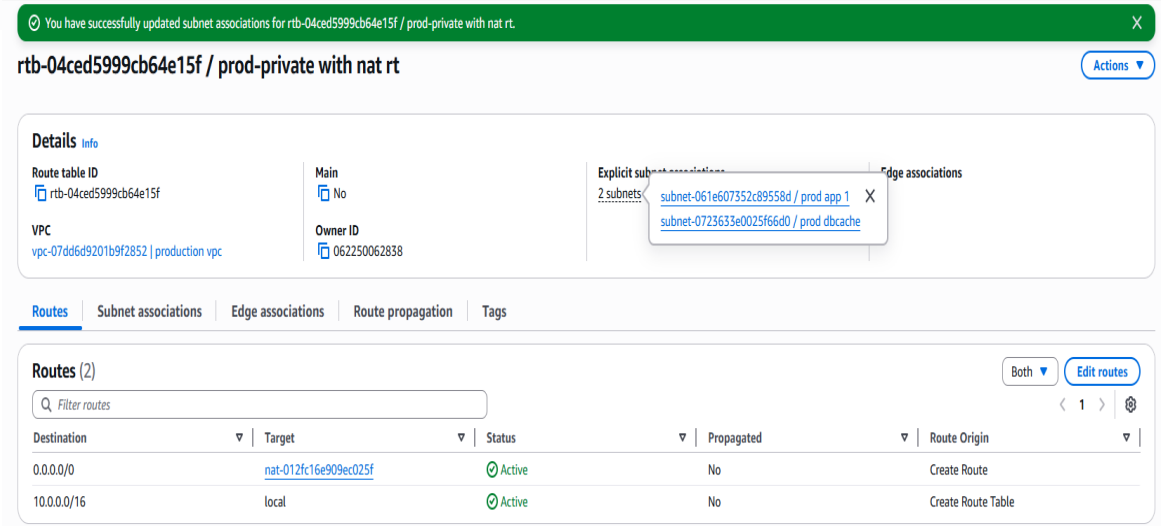


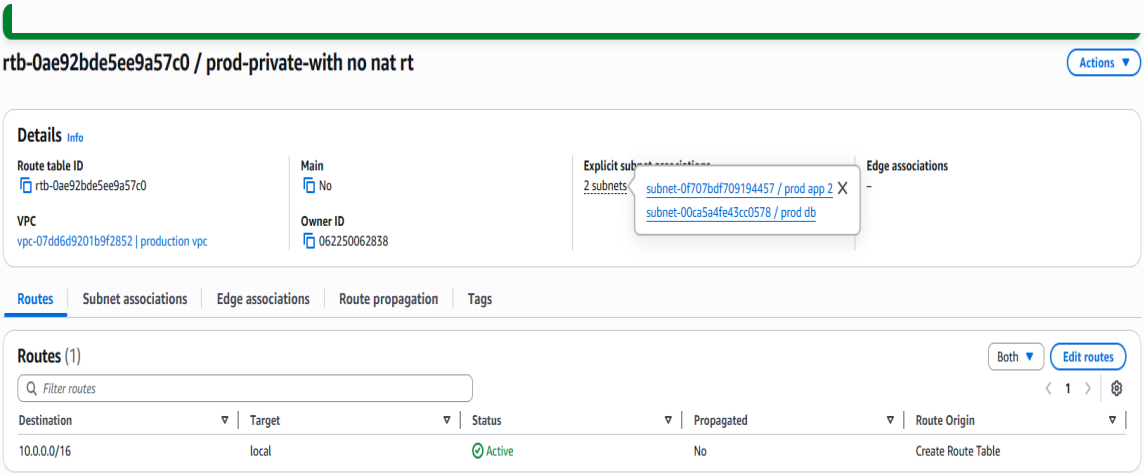
5. Configure Route Tables and Associations

- **Production VPC:**

- Public Route Table `web` subnet IGW (0.0.0.0/0)
- Private Route Table (with NAT) `app1` , `dbcache` subnets NAT Gateway (0.0.0.0/0)
- Private Route Table (no NAT) `app2` , `db` subnets No internet access

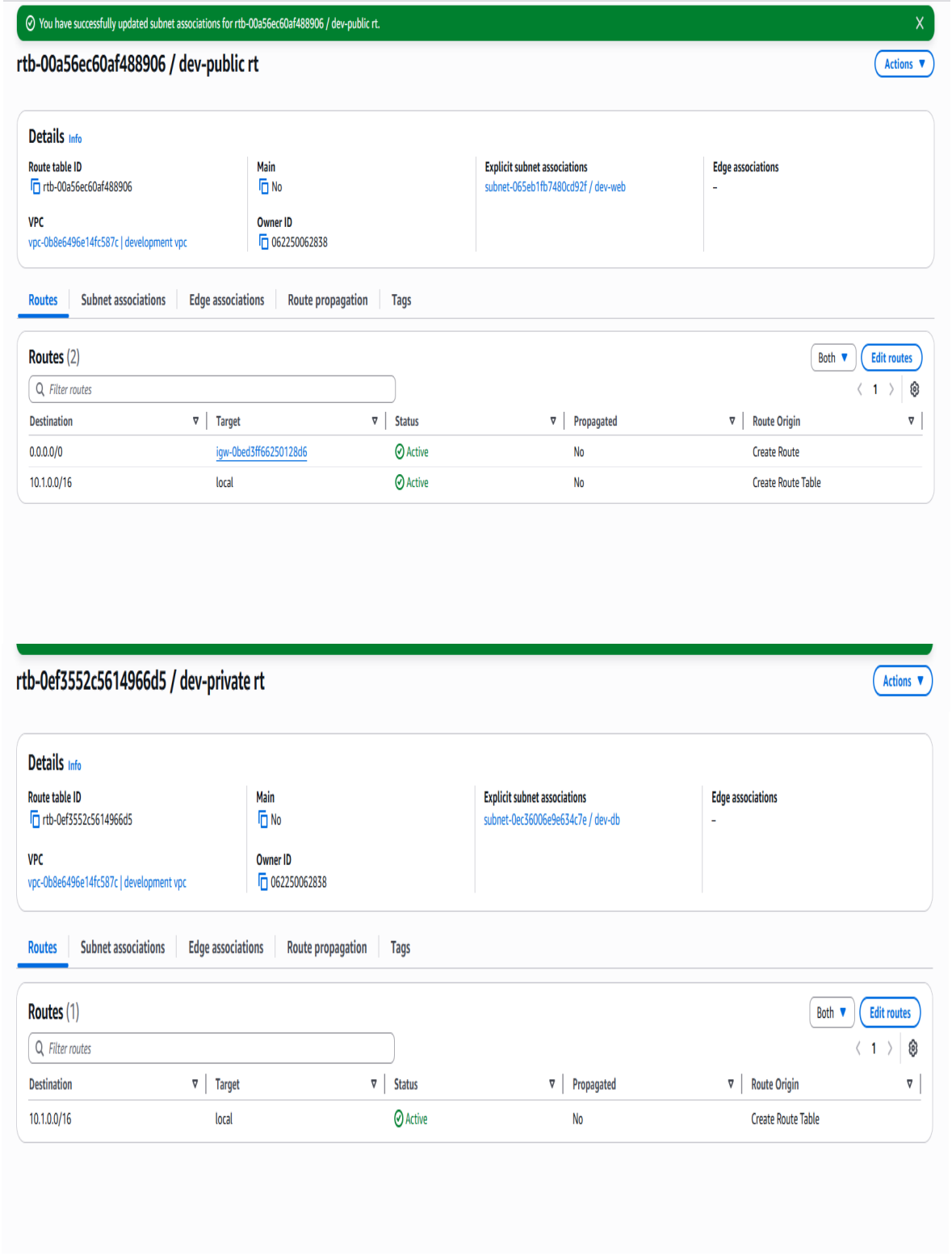






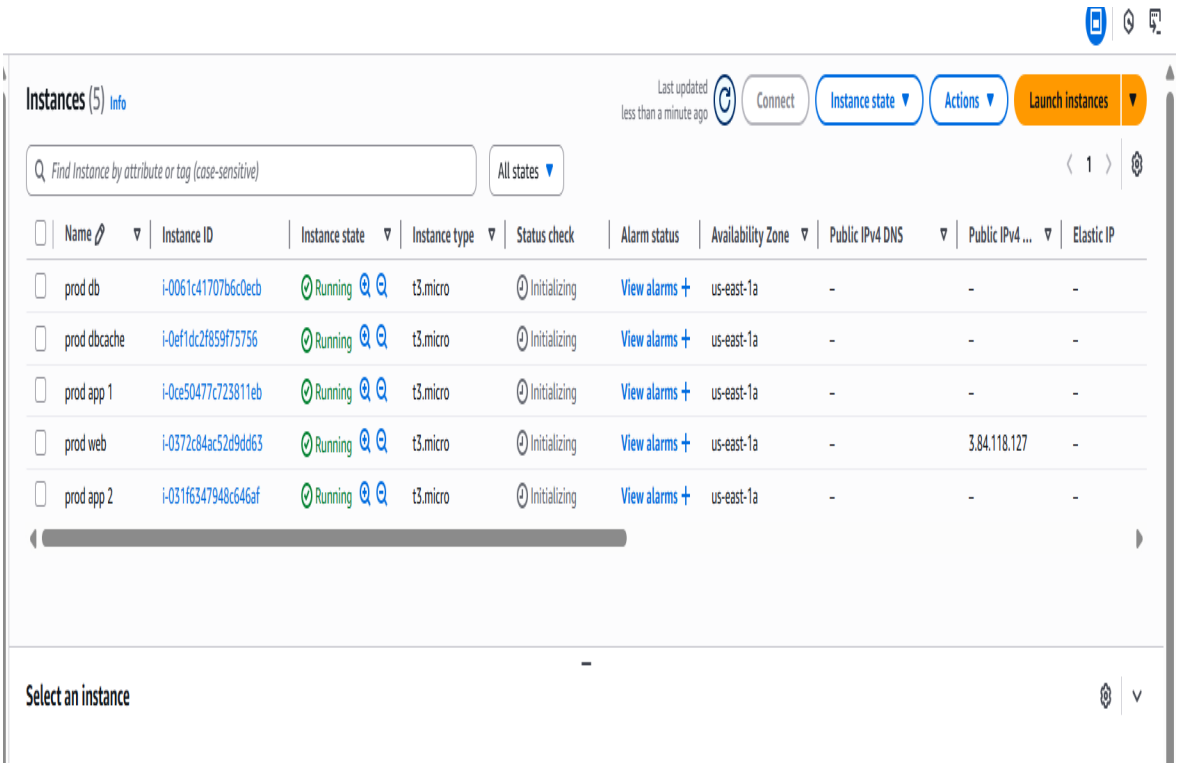
- **Development VPC:**

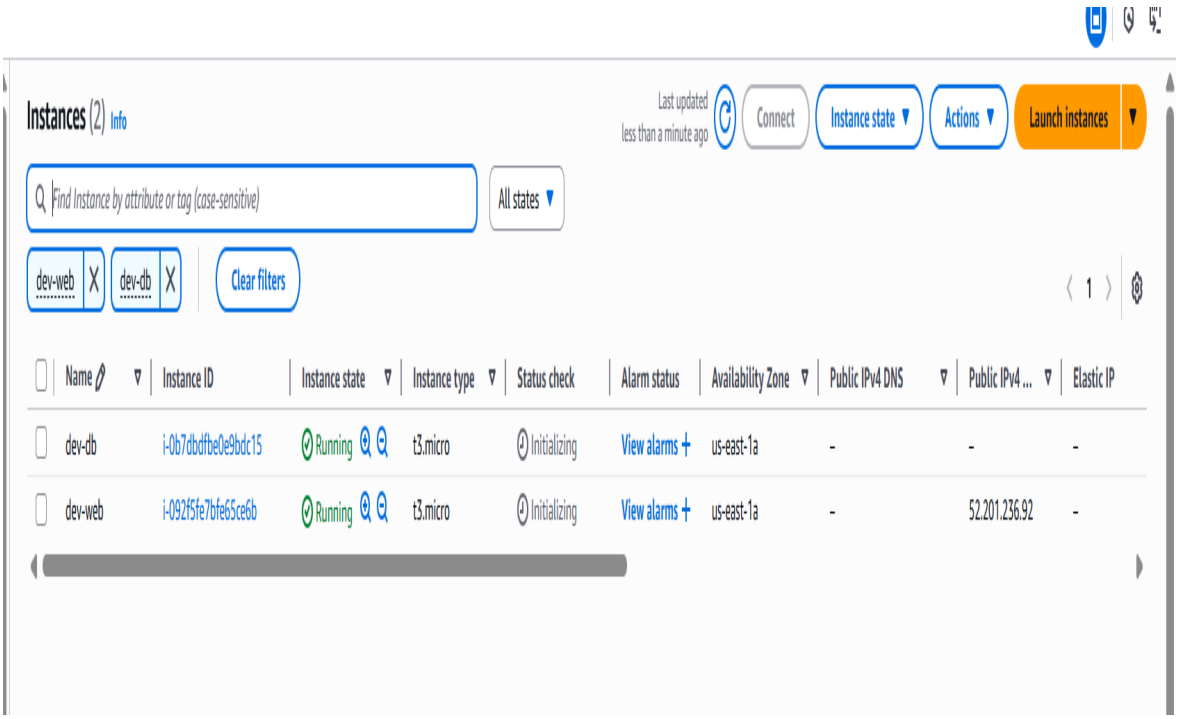
- Public Route Table web subnet IGW (0.0.0.0/0)
- Private Route Table db subnet No internet access



6. Launch EC2 Instances

- Use **Amazon Linux 2** AMI.
- Assign **key pairs** for SSH access.
- Public instances (web) Enable Auto-assign Public IP.
- Private instances (app1, app2, dbcache, db) Disable Public IP.
- Assign correct **Security Groups** and **Subnets**.



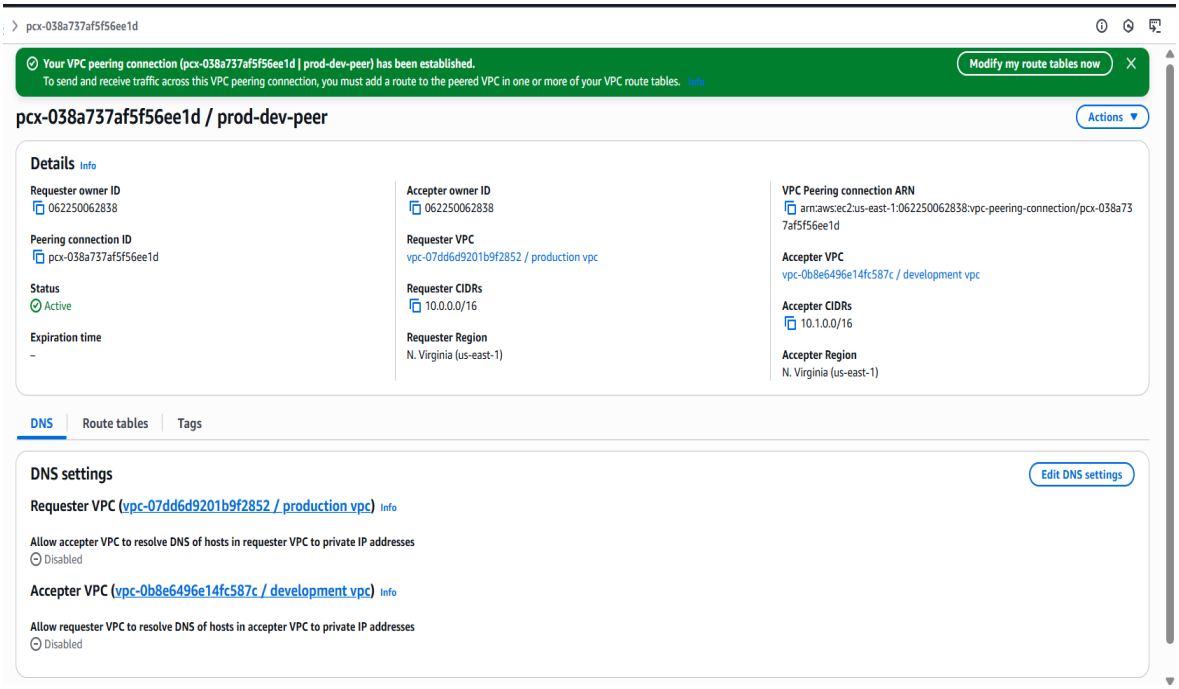


VPC Peering Connection & Routing Configuration

Step 1 — Create and Accept Peering Connection

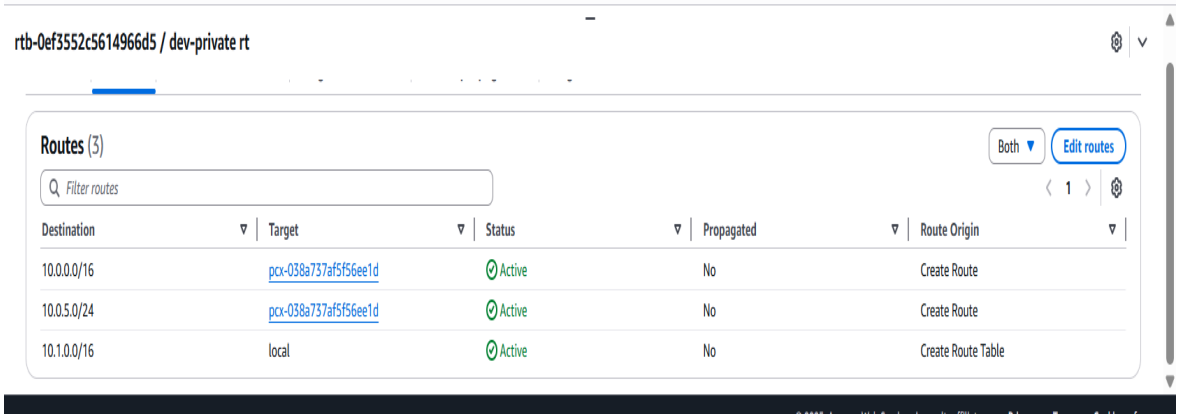
- Go to VPC Console Peering Connections Create Peering Connection.
- Requester: Production VPC
- Accepter: Development VPC

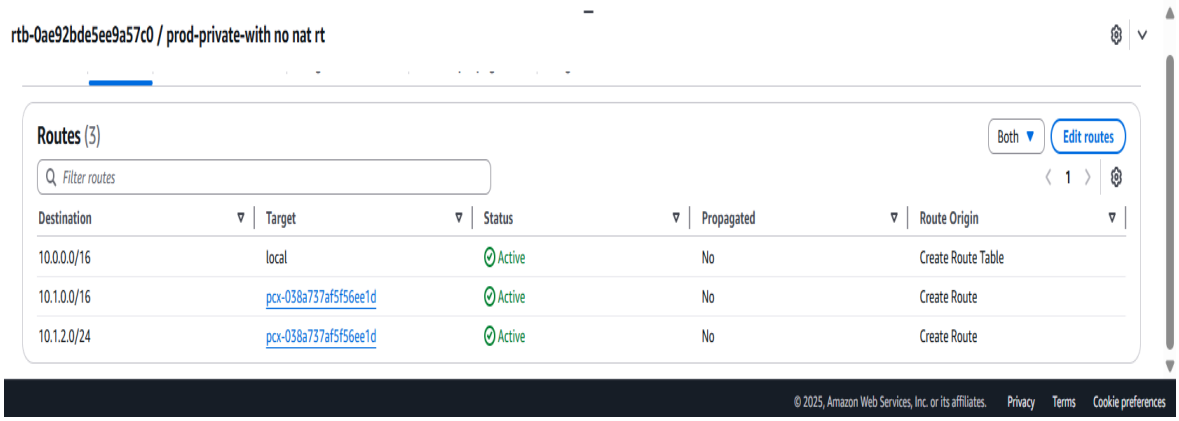
- Accept request after creation.

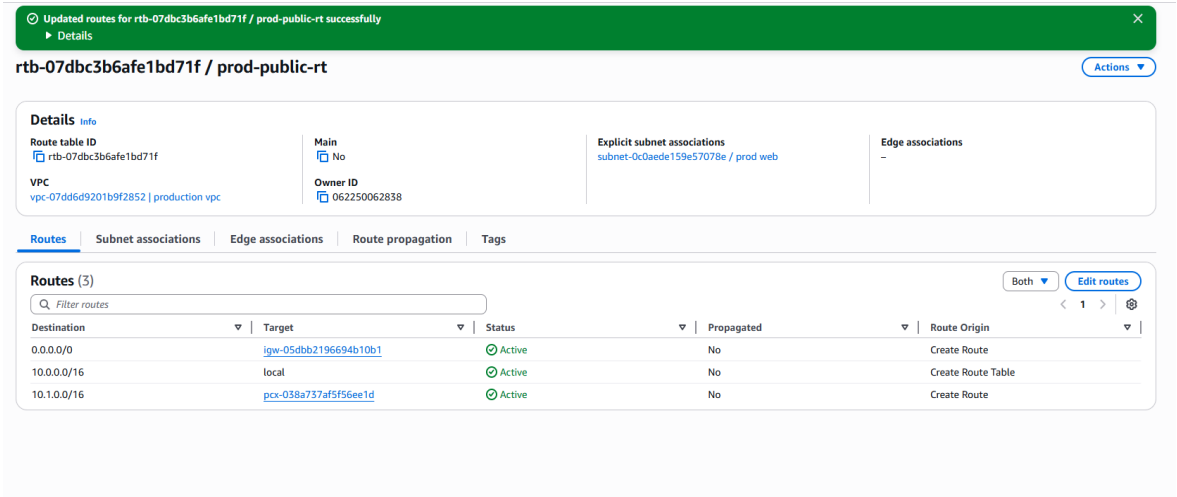


Step 2 — Edit Route Tables for Peering

- **Production Private (db subnet):** Route 10.1.0.0/16 Peering Connection ID
- **Development Private (db subnet):** Route 10.0.0.0/16 Peering Connection ID
- **Optional:** Add same route in `prod-public-rt` for testing.


rtb-0ef3552c5614966d5 / dev-private rt
Routes (3)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
pcx-038a737af5f56ee1d
Active
No
Create Route
10.0.5.0/24
pcx-038a737af5f56ee1d
Active
No
Create Route
10.1.0.0/16
local
Active
No
Create Route Table

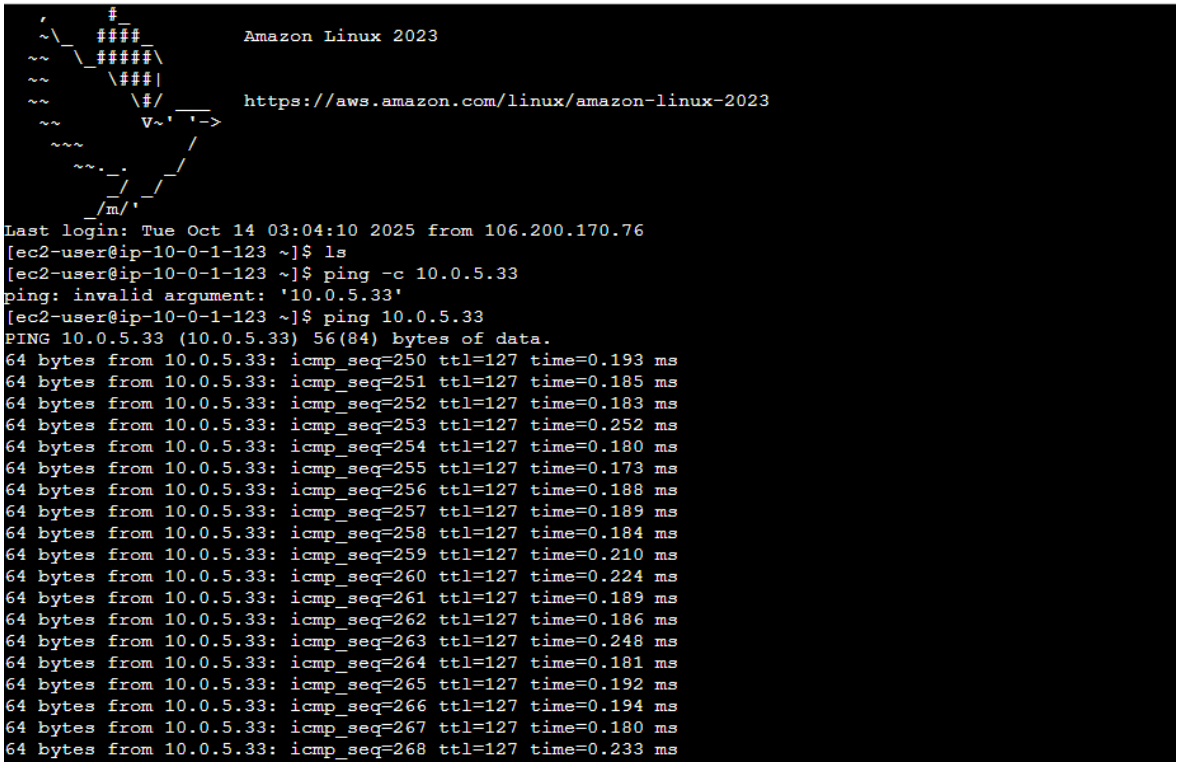

rtb-0ae92bde5ee9a57c0 / prod-private-with no nat rt
Routes (3)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
Create Route Table
10.1.0.0/16
pcx-038a737af5f56ee1d
Active
No
Create Route
10.1.2.0/24
pcx-038a737af5f56ee1d
Active
No
Create Route
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

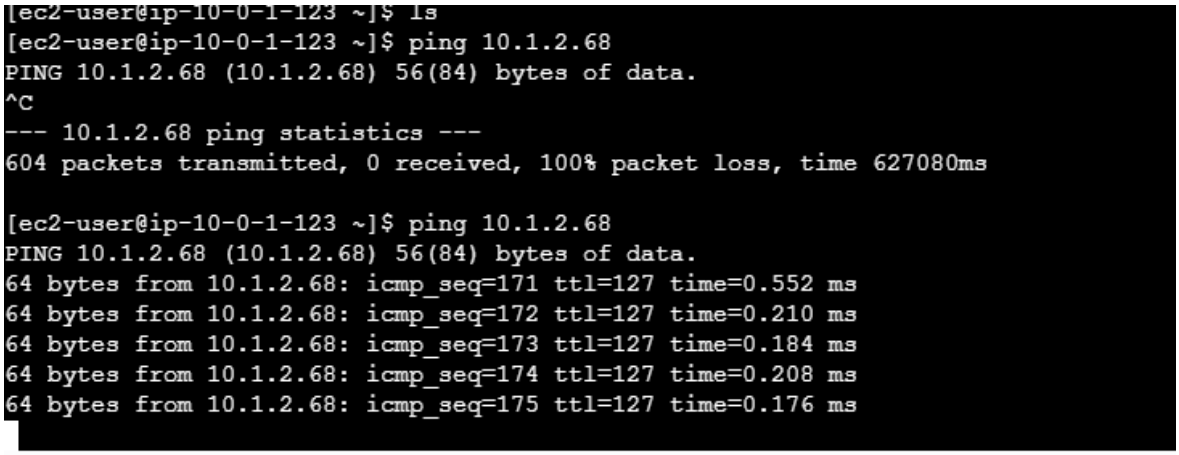

Updated routes for rtb-07dbc3b6afe1bd71f / prod-public-rt successfully
Details
rtb-07dbc3b6afe1bd71f / prod-public-rt
Actions
Details
Info
Route table ID
rtb-07dbc3b6afe1bd71f
Main
No
Explicit subnet associations
subnet-0c0aede159e57078e / prod web
Edge associations
–
VPC
vpc-07dd6d9201b9f2852 | production vpc
Owner ID
062250062838
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (3)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
Route Origin
0.0.0.0/0
igw-05dbb2196694b10b1
Active
No
Create Route
10.0.0.0/16
local
Active
No
Create Route Table
10.1.0.0/16
pcx-038a737af5f56ee1d
Active
No
Create Route

Connectivity Testing

1. SSH into **Production Web** instance.
2. Ping Production DB private IP: `ping 10.0.x.x`
3. Ping Development DB private IP: `ping 10.1.x.x`
4. SSH into **Development Web** instance.
5. Ping Development DB private IP to confirm internal connectivity.

Expected Results: - Prod web Internet access - Prod app1/dbcache Internet via NAT - Dev web Internet access - Private DBs No internet access





```
 \    #
  \   ###       Amazon Linux 2023
   \  ###i
       #/        https://aws.amazon.com/linux/amazon-linux-2023
        _/  _
 _       /
  _ _   /
    / ,  _/
    _/ ᵀ
[ec2-user@ip-10-1-1-123 ~]$ ping 10.1.2.68
PING 10.1.2.68 (10.1.2.68) 56(84) bytes of data.
64 bytes from 10.1.2.68 (16.1.26) itmp=seq=1 ttl=200 ms
64 bytes from 10.1.2.68 (16.1.26) icmp-seq=2 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp-seq=3 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp-seq=4 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp-seq=5 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp-seq=6 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp-seq=7 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp-seq=8 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp-seq=9 ttl=127 ms
--- ping statistics -iP6
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 0.171/0.193/0.233/0.019 ms
```

Security Groups

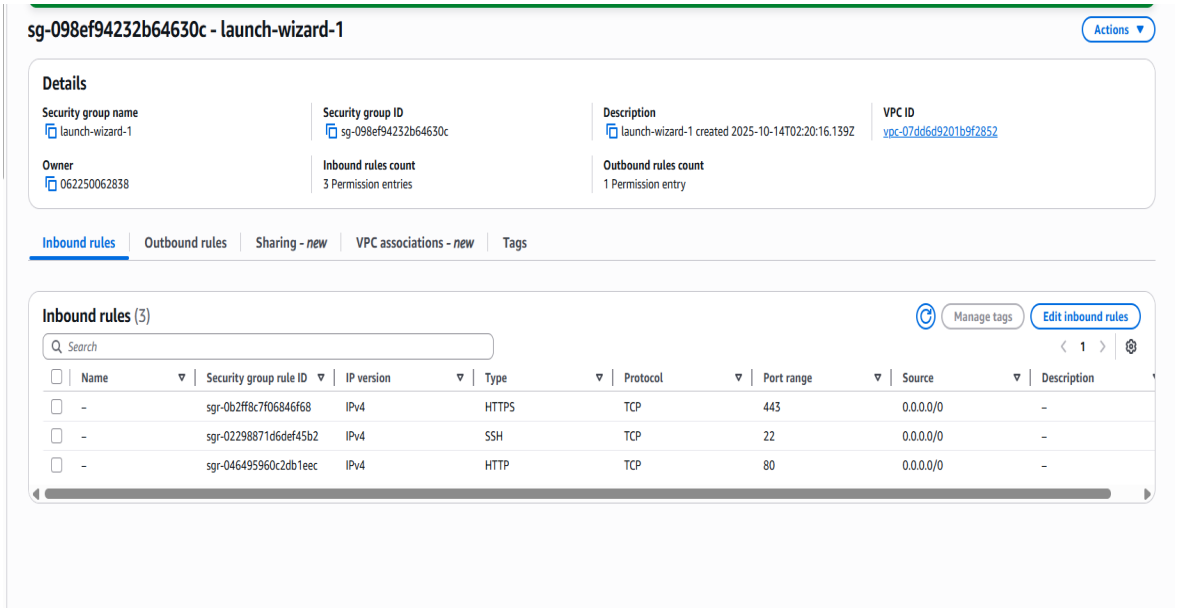
Security Groups work like firewalls for EC2 instances. They control what kind of traffic is allowed **in and out**.

Production VPC

Security Group	Purpose	Inbound Rules	Outbound Rules
web-sg	Web server	Allow SSH (22) & HTTP (80) from anywhere	Allow all traffic
app1-sg	Application tier	Allow HTTP (80) from web-sg	Allow all traffic (for NAT)
app2-sg	Internal tier	Allow internal traffic only from app1/app2	Allow all traffic
dbcache-sg	Cache server	Allow 3306 (MySQL) from app1/app2	Allow all traffic (via NAT)
db-sg	Database	Allow 3306 (MySQL) from app1/app2; ICMP from dev-db-sg	Allow all traffic

Development VPC

Security Group	Purpose	Inbound Rules	Outbound Rules
dev-web-sg	Web server	Allow SSH (22) & HTTP (80) from anywhere	Allow all traffic
dev-db-sg	Database	Allow 3306 (MySQL) & ICMP from Production DB SG	Allow all traffic



sg-03bcf2601140c346c - launch-wizard-2

Actions

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-2	sg-03bcf2601140c346c	launch-wizard-2 created 2025-10-14T02:23:04.582Z	vpc-07dd6d9201b9f2852

Owner	Inbound rules count	Outbound rules count
062250062838	2 Permission entries	1 Permission entry

Inbound rules | Outbound rules | Sharing - *new* | VPC associations - *new* | Tags

Inbound rules (2)

Manage tags | Edit inbound rules

Search

1

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0c90b5cf6a56490fb	-	HTTP	TCP	80	sg-098ef94232b64630c...	-
-	sgr-0a26b1823af425f51	IPv4	SSH	TCP	22	0.0.0.0/0	-

sg-0d97d7a7e8773fe96 - launch-wizard-4

Actions

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-4	sg-0d97d7a7e8773fe96	launch-wizard-4 created 2025-10-14T02:24:05.201Z	vpc-07dd6d9201b9f2852

Owner	Inbound rules count	Outbound rules count
062250062838	2 Permission entries	1 Permission entry

Inbound rules | Outbound rules | Sharing - *new* | VPC associations - *new* | Tags

Inbound rules (2)

Manage tags | Edit inbound rules

Search

1

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0291c72d3faf0f0fb	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sgr-0fbb5d9b5cf60d847	-	MYSQL/Aurora	TCP	3306	sg-03bcf2601140c346c...	-

sg-0727c38521ba07a1b - launch-wizard-5

Actions

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-5	sg-0727c38521ba07a1b	launch-wizard-5 created 2025-10-14T02:24:46.198Z	vpc-07dd6d9201b9f2852

Owner	Inbound rules count	Outbound rules count
062250062838	2 Permission entries	1 Permission entry

Inbound rules | Outbound rules | Sharing - *new* | VPC associations - *new* | Tags

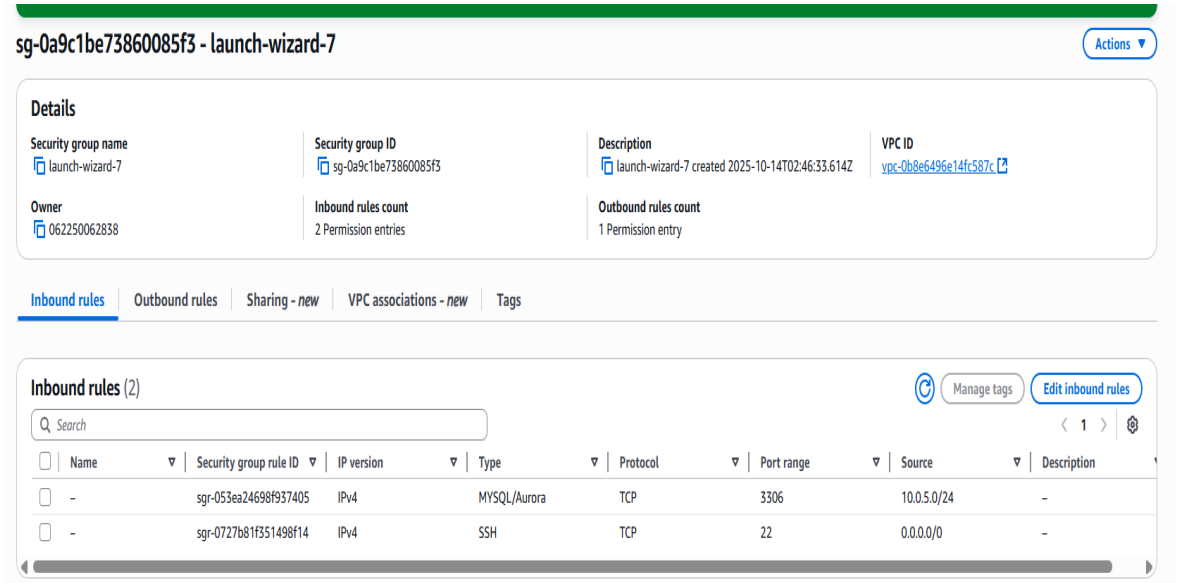
Inbound rules (2)

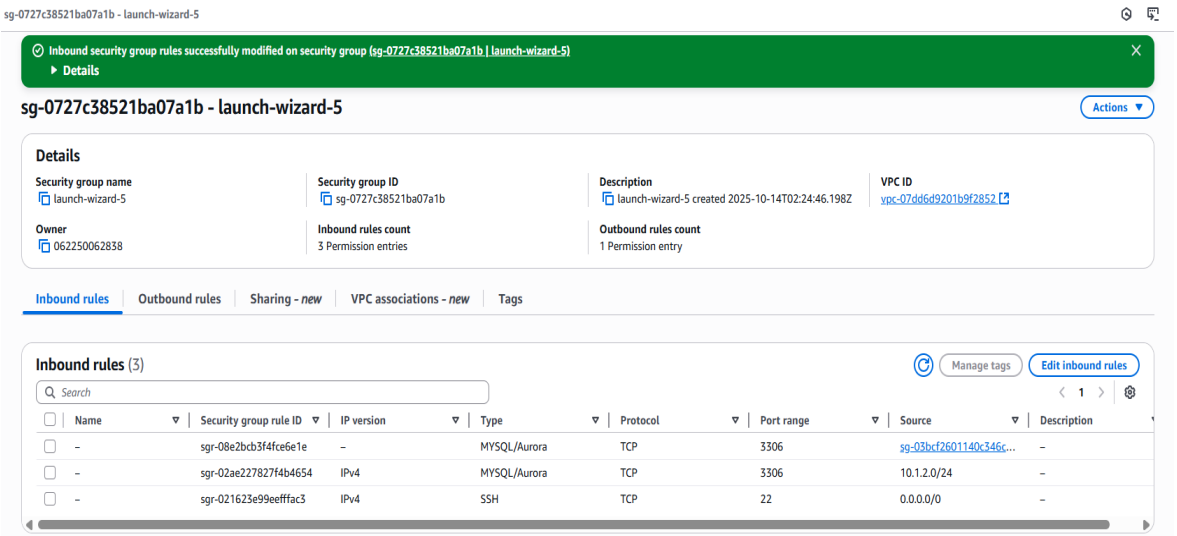
Manage tags | Edit inbound rules

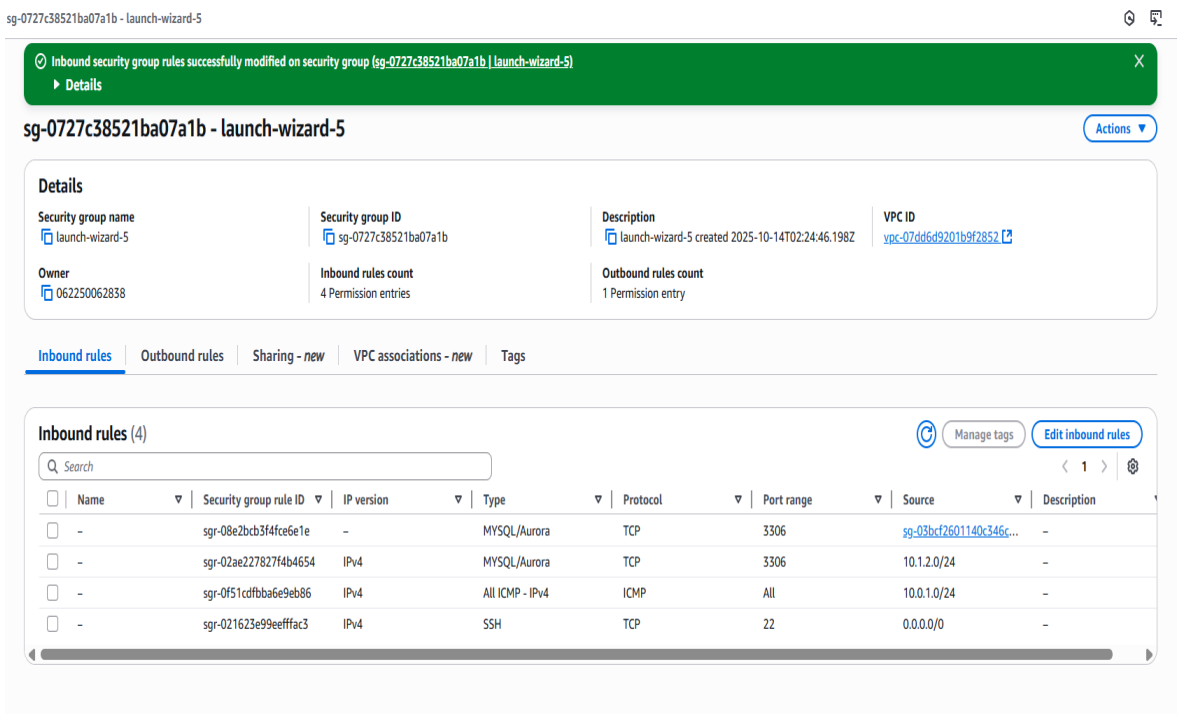
Search

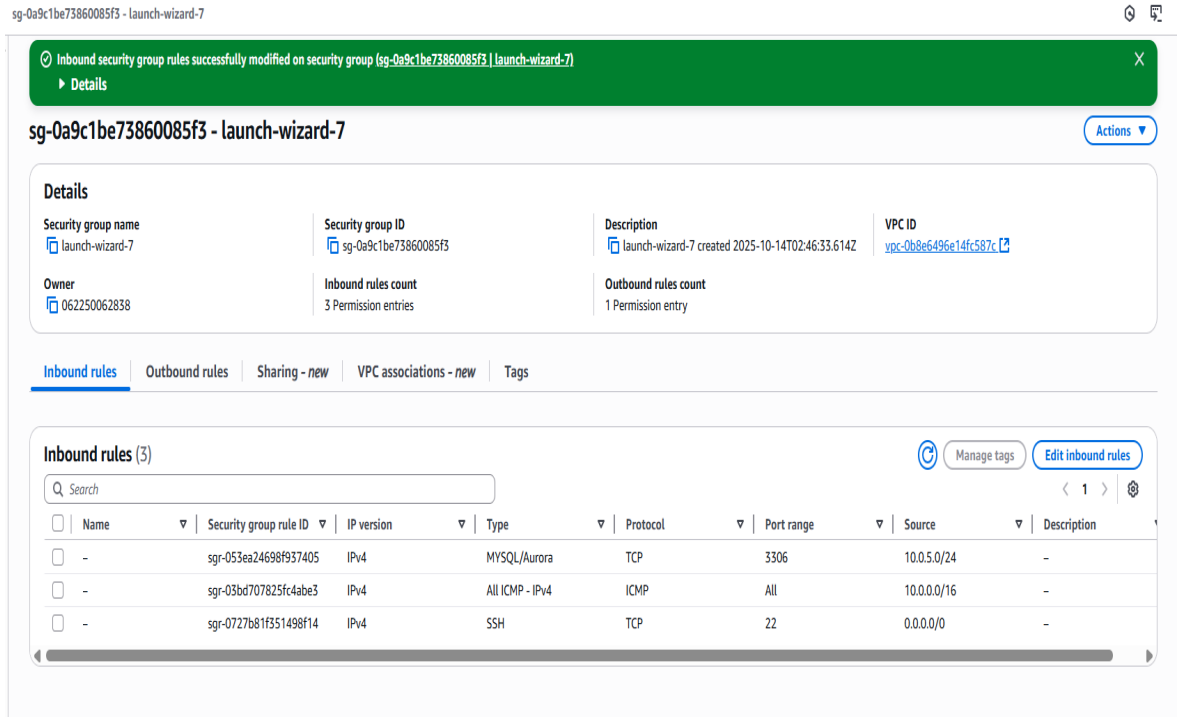
1

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
-	sgr-08e2bcb3f4fce6e1e	-	MYSQL/Aurora	TCP	3306	sg-03bcf2601140c346c...	-
-	sgr-021623e99eefffac3	IPv4	SSH	TCP	22	0.0.0.0/0	-


sg-0a9c1be73860085f3 - launch-wizard-7
Actions
Details
Security group name
launch-wizard-7
Security group ID
sg-0a9c1be73860085f3
Description
launch-wizard-7 created 2025-10-14T02:46:33.614Z
VPC ID
vpc-0b8e6496e14fc587c
Owner
062250062838
Inbound rules count
2 Permission entries
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (2)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
Type
Protocol
Port range
Source
Description
- sgr-053ea24698f937405 IPv4 MYSQL/Aurora TCP 3306 10.0.5.0/24 -
- sgr-0727b81f351498f14 IPv4 SSH TCP 22 0.0.0.0/0 -


sg-0727c38521ba07a1b - launch-wizard-5
Inbound security group rules successfully modified on security group (sg-0727c38521ba07a1b | launch-wizard-5)
Details
sg-0727c38521ba07a1b - launch-wizard-5
Actions
Details
Security group name
launch-wizard-5
Security group ID
sg-0727c38521ba07a1b
Description
launch-wizard-5 created 2025-10-14T02:24:46.198Z
VPC ID
vpc-07dd6d9201b9f2852
Owner
062250062838
Inbound rules count
3 Permission entries
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (3)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
Type
Protocol
Port range
Source
Description
- sgr-08e2bcb3f4fce6e1e - MYSQL/Aurora TCP 3306 sg-03bcf2601140c346c... -
- sgr-02ae227827f4b4654 IPv4 MYSQL/Aurora TCP 3306 10.1.2.0/24 -
- sgr-021623e99eefffac3 IPv4 SSH TCP 22 0.0.0.0/0 -


sg-0727c38521ba07a1b - launch-wizard-5
Inbound security group rules successfully modified on security group (sg-0727c38521ba07a1b | launch-wizard-5)
Details
sg-0727c38521ba07a1b - launch-wizard-5
Actions
Details
Security group name
launch-wizard-5
Security group ID
sg-0727c38521ba07a1b
Description
launch-wizard-5 created 2025-10-14T02:24:46.198Z
VPC ID
vpc-07dd6d9201b9f2852
Owner
062250062838
Inbound rules count
4 Permission entries
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (4)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
Type
Protocol
Port range
Source
Description
- sgr-08e2bcb3f4fce6e1e - MYSQL/Aurora TCP 3306 sg-03bcf2601140c346c... -
- sgr-02ae227827f4b4654 IPv4 MYSQL/Aurora TCP 3306 10.1.2.0/24 -
- sgr-0f51cdfbba6e9eb86 IPv4 All ICMP - IPv4 ICMP All 10.0.1.0/24 -
- sgr-021623e99eefffac3 IPv4 SSH TCP 22 0.0.0.0/0 -


sg-0a9c1be73860085f3 - launch-wizard-7
Inbound security group rules successfully modified on security group (sg-0a9c1be73860085f3 | launch-wizard-7)
Details
sg-0a9c1be73860085f3 - launch-wizard-7
Actions
Details
Security group name
launch-wizard-7
Security group ID
sg-0a9c1be73860085f3
Description
launch-wizard-7 created 2025-10-14T02:46:33.614Z
VPC ID
vpc-0b8e6496e14fc587c
Owner
062250062838
Inbound rules count
3 Permission entries
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (3)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
Type
Protocol
Port range
Source
Description
- sgr-053ea24698f937405 IPv4 MYSQL/Aurora TCP 3306 10.0.5.0/24 -
- sgr-03bd707825fc4abe3 IPv4 All ICMP - IPv4 ICMP All 10.0.0.0/16 -
- sgr-0727b81f351498f14 IPv4 SSH TCP 22 0.0.0.0/0 -

Network ACLs (Simplified)

NACLs are an extra layer of security at the **subnet level**. Think of them as “rules for the entire street,” while security groups are “rules for each house.”

Public Subnet NACL

- **Inbound:** Allow 22 (SSH), 80 (HTTP), 443 (HTTPS) from 0.0.0.0/0
- **Outbound:** Allow all (0.0.0.0/0)

Private Subnet NACL

- **Inbound:** Allow traffic only from internal subnets (10.0.0.0/8, 10.1.0.0/8)
- **Outbound:** Allow response traffic (1024–65535)

Verification & Validation

- Check instance reachability per subnet.
- Confirm NAT Gateway traffic for app1 and dbcache.
- Confirm peering communication between DBs.
- Verify route associations and security rules.

Final Result: All configurations function as expected. Production and Development networks are isolated yet securely connected via peering, with controlled internet access and validated routing.

Conclusion

The setup successfully demonstrates two independent VPCs (Production and Development) with secure, tiered design and controlled communication through peering. Internet access policies, NAT configuration, and private routing were validated through connectivity tests and audits.