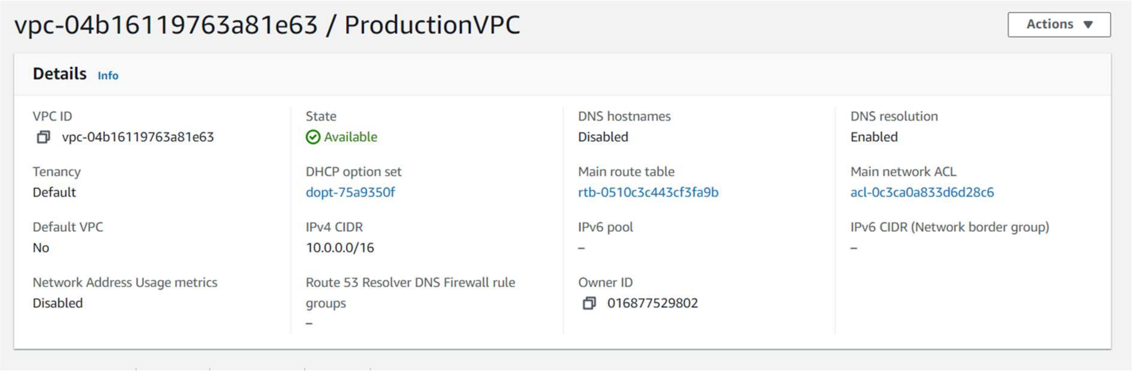
Production Network:

1. Design and Build a 4-Tier Architecture:

- **VPC Creation:**
  - Create a VPC named ProductionVPC.
  - Choose an appropriate CIDR block (e.g., 10.0.0.0/16).



vpc-04b16119763a81e63 / ProductionVPC

Details Info

VPC ID
vpc-04b16119763a81e63

State
✓ Available

DNS hostnames
Disabled

DNS resolution
Enabled

Tenancy
Default

DHCP option set
dopt-75a9350f

Main route table
rtb-0510c3c443cf3fa9b

Main network ACL
acl-0c3ca0a833d6d28c6

Default VPC
No

IPv4 CIDR
10.0.0.0/16

IPv6 pool
–

IPv6 CIDR (Network border group)
–

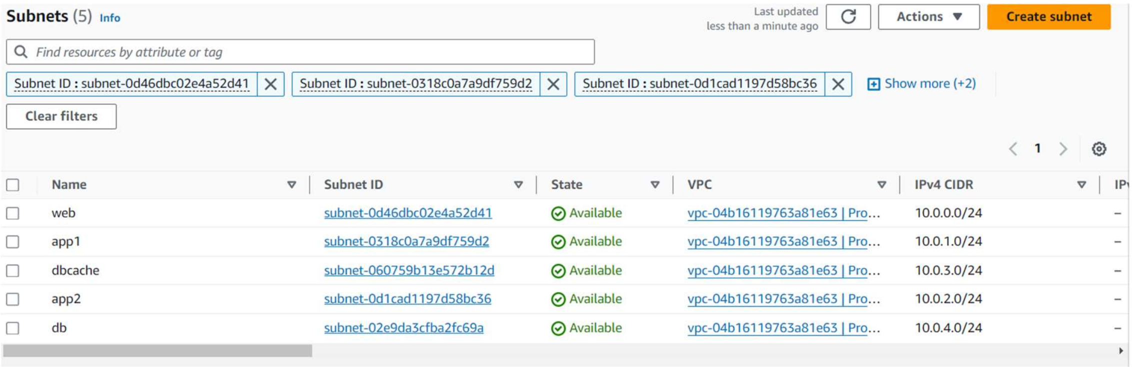
Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
–

Owner ID
016877529802

2. Create Subnets:

- **Public Subnet:**
  - Create a public subnet named web in ProductionVPC.
  - Example CIDR: 10.0.0.0/24.
- **Private Subnets:**
  - Create four private subnets:
    - app1 with CIDR 10.0.1.0/24.
    - app2 with CIDR 10.0.2.0/24.
    - dbcache with CIDR 10.0.3.0/24.
    - db with CIDR 10.0.4.0/24.



Subnets (5) Info

Subnet ID : subnet-0d46dbc02e4a52d41 ✕ Subnet ID : subnet-0318c0a7a9df759d2 ✕ Subnet ID : subnet-0d1cad1197d58bc36 ✕ Show more (+2)

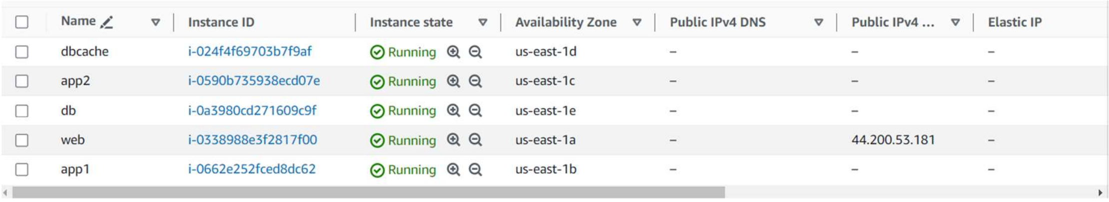
□	Name	Subnet ID	State	VPC	IPv4 CIDR	IP
□	web	subnet-0d46dbc02e4a52d41	✓ Available	vpc-04b16119763a81e63 | Pro...	10.0.0.0/24	–
□	app1	subnet-0318c0a7a9df759d2	✓ Available	vpc-04b16119763a81e63 | Pro...	10.0.1.0/24	–
□	dbcache	subnet-060759b13e572b12d	✓ Available	vpc-04b16119763a81e63 | Pro...	10.0.3.0/24	–
□	app2	subnet-0d1cad1197d58bc36	✓ Available	vpc-04b16119763a81e63 | Pro...	10.0.2.0/24	–
□	db	subnet-02e9da3cfba2fc69a	✓ Available	vpc-04b16119763a81e63 | Pro...	10.0.4.0/24	–

3. Launch Instances:

- Launch EC2 instances in each subnet:

  - Name them according to their respective subnets (web, app1, app2, dbcache, db).

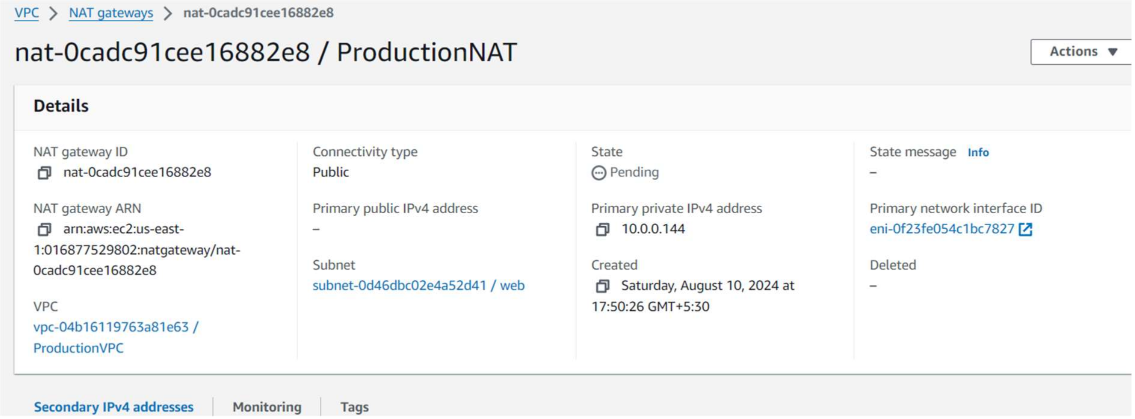
- Ensure that instances in private subnets do not have public IPs.



□	Name	Instance ID	Instance state	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
□	dbcache	i-024f4f69703b7f9af	Running	us-east-1d	–	–	–
□	app2	i-0590b735938ecd07e	Running	us-east-1c	–	–	–
□	db	i-0a3980cd271609c9f	Running	us-east-1e	–	–	–
□	web	i-0338988e3f2817f00	Running	us-east-1a	–	44.200.53.181	–
□	app1	i-0662e252fced8dc62	Running	us-east-1b	–	–	–

4. Internet Access:

- **NAT Gateway:**
  - Create a NAT Gateway in the web subnet.



VPC > NAT gateways > nat-0cadc91cee16882e8

nat-0cadc91cee16882e8 / ProductionNAT

Details

NAT gateway ID: nat-0cadc91cee16882e8

NAT gateway ARN: arn:aws:ec2:us-east-1:016877529802:natgateway/nat-0cadc91cee16882e8

VPC: vpc-04b16119763a81e63 / ProductionVPC

Connectivity type: Public

Primary public IPv4 address: –

Subnet: subnet-0d46dbc02e4a52d41 / web

State: Pending

Primary private IPv4 address: 10.0.0.144

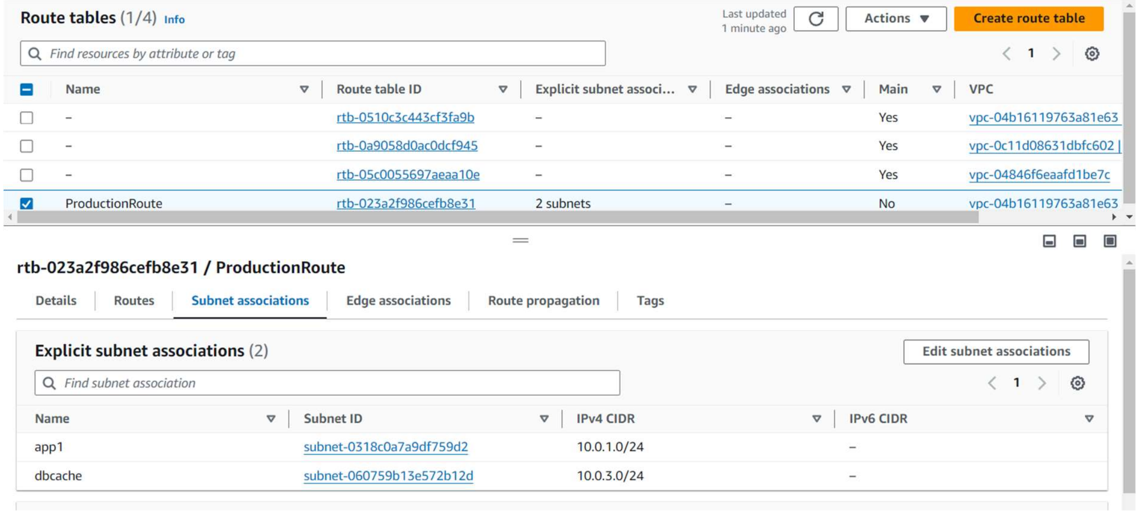
Created: Saturday, August 10, 2024 at 17:50:26 GMT+5:30

State message: –

Primary network interface ID: eni-0f23fe054c1bc7827

Deleted: –

  - Associate the NAT Gateway with the route tables of the app1 and dbcache subnets.



Route tables (1/4)

Last updated 1 minute ago

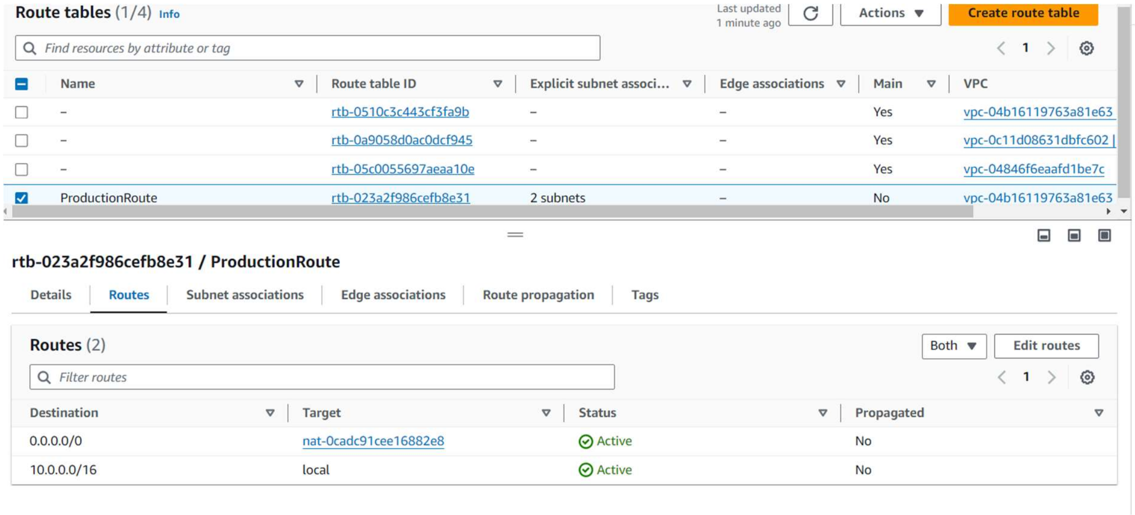
	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
□	–	rtb-0510c3c443cf3fa9b	–	–	Yes	vpc-04b16119763a81e63
□	–	rtb-0a9058d0ac0dcf945	–	–	Yes	vpc-0c11d08631dbfc602
□	–	rtb-05c0055697aeaa10e	–	–	Yes	vpc-04846f6eaafd1be7c
☑	ProductionRoute	rtb-023a2f986cefb8e31	2 subnets	–	No	vpc-04b16119763a81e63

rtb-023a2f986cefb8e31 / ProductionRoute

Explicit subnet associations (2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
app1	subnet-0318c0a7a9df759d2	10.0.1.0/24	–
dbcache	subnet-060759b13e572b12d	10.0.3.0/24	–

- **Route Tables:**
  - Update route tables:
    - app1 and dbcache should have a route to the NAT Gateway.


Route tables (1/4) Info

Last updated 1 minute ago

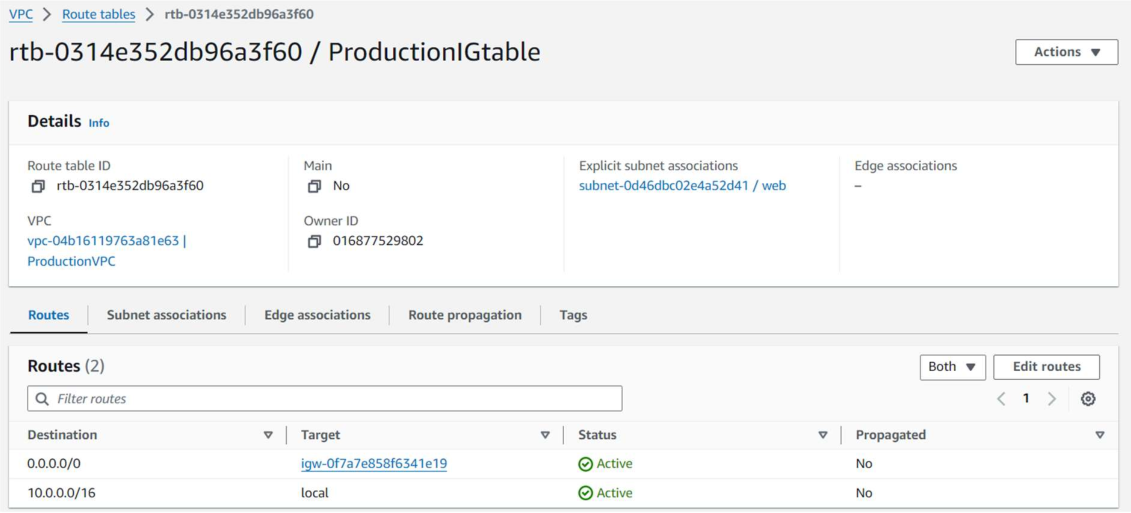
	Name	Route table ID	Explicit subnet associ…	Edge associations	Main	VPC
□	–	rtb-0510c3c443cf3fa9b	–	–	Yes	vpc-04b16119763a81e63
□	–	rtb-0a9058d0ac0dcf945	–	–	Yes	vpc-0c11d08631dbfc602 |
□	–	rtb-05c0055697aeaa10e	–	–	Yes	vpc-04846f6eaafd1be7c
☑	ProductionRoute	rtb-023a2f986cefb8e31	2 subnets	–	No	vpc-04b16119763a81e63

rtb-023a2f986cefb8e31 / ProductionRoute

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	nat-0cadc91cee16882e8	✓ Active	No
10.0.0.0/16	local	✓ Active	No

- web should have a route to the Internet Gateway.


VPC > Route tables > rtb-0314e352db96a3f60

rtb-0314e352db96a3f60 / ProductionIGtable

Details Info

Route table ID: rtb-0314e352db96a3f60

Main: No

Explicit subnet associations: subnet-0d46dbc02e4a52d41 / web

Edge associations: –

VPC: vpc-04b16119763a81e63 | ProductionVPC

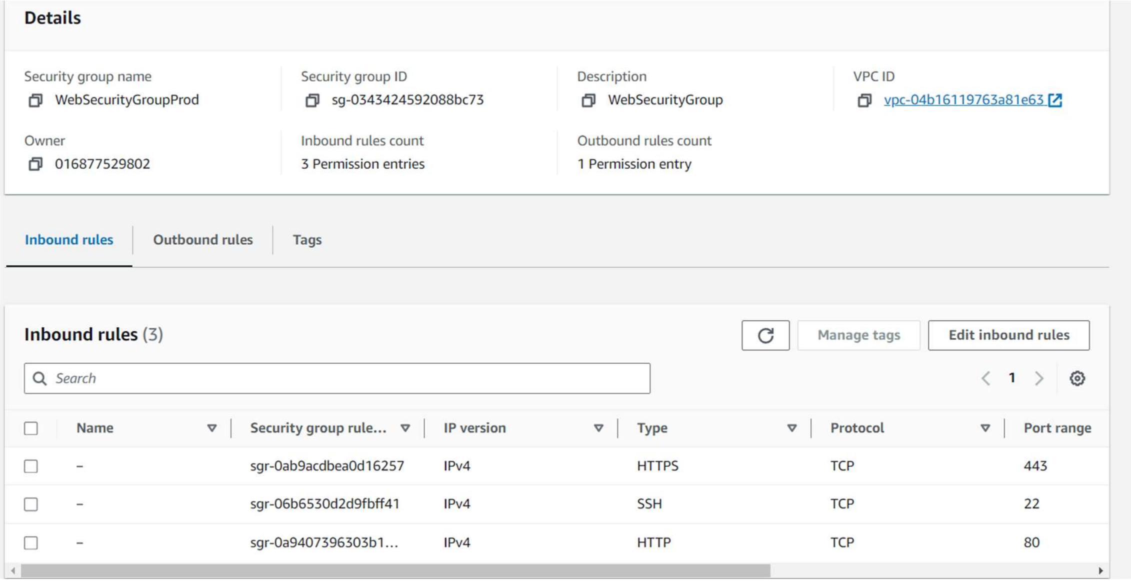
Owner ID: 016877529802

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f7a7e858f6341e19	✓ Active	No
10.0.0.0/16	local	✓ Active	No

5. Manage Security Groups and NACLs:

- **Security Groups:**
  - web: Allow inbound HTTP/HTTPS, and SSH access. Restrict outbound to necessary ports.



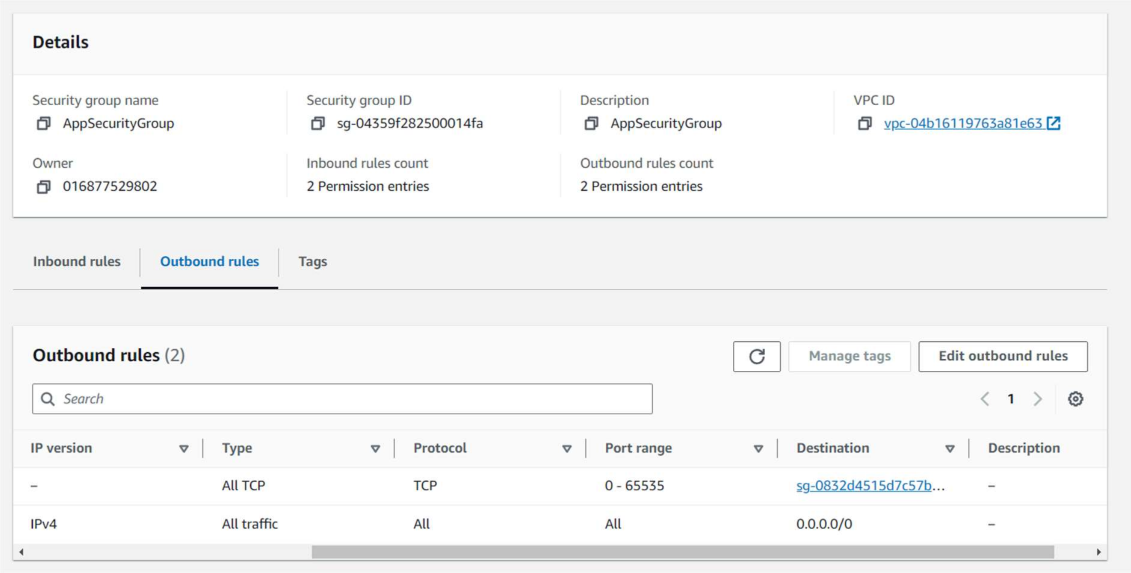
Details

Security group name WebSecurityGroupProd	Security group ID sg-0343424592088bc73	Description WebSecurityGroup	VPC ID vpc-04b16119763a81e63
Owner 016877529802	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules (3)

□	Name	Security group rule...	IP version	Type	Protocol	Port range
□	–	sgr-0ab9acdbea0d16257	IPv4	HTTPS	TCP	443
□	–	sgr-06b6530d2d9fbff41	IPv4	SSH	TCP	22
□	–	sgr-0a9407396303b1...	IPv4	HTTP	TCP	80

- ○ app1 and app2: Allow inbound traffic only from web and between themselves. Allow outbound to dbcache.



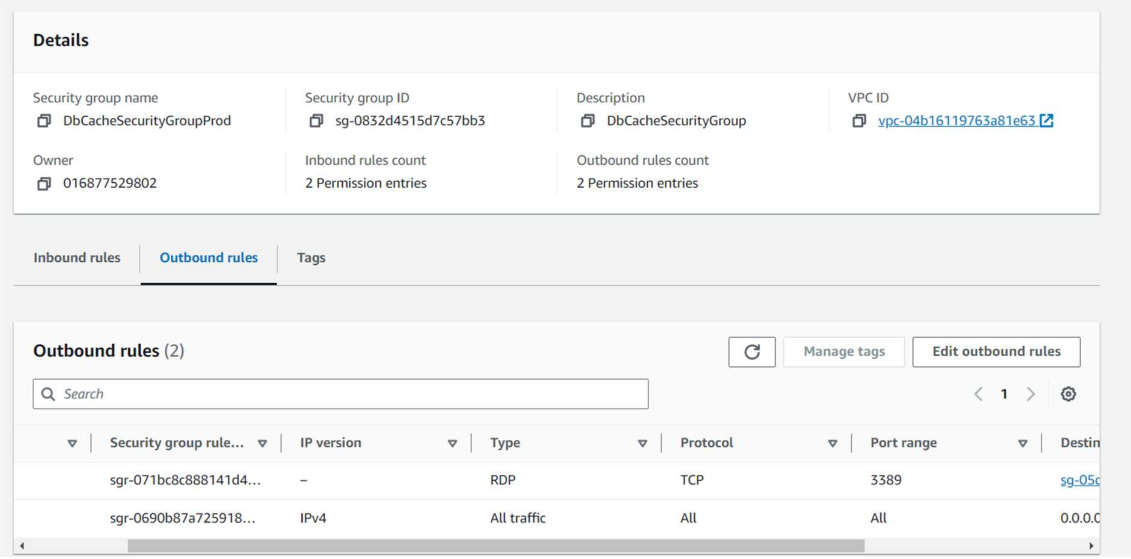
Details

Security group name AppSecurityGroup	Security group ID sg-04359f282500014fa	Description AppSecurityGroup	VPC ID vpc-04b16119763a81e63
Owner 016877529802	Inbound rules count 2 Permission entries	Outbound rules count 2 Permission entries	

Outbound rules (2)

IP version	Type	Protocol	Port range	Destination	Description
–	All TCP	TCP	0 - 65535	sg-0832d4515d7c57b...	–
IPv4	All traffic	All	All	0.0.0.0/0	–

- ○ dbcache: Allow inbound traffic from app1 and app2. Allow outbound to the internet and db.



Details

Security group name
DbCacheSecurityGroupProd

Security group ID
sg-0832d4515d7c57bb3

Description
DbCacheSecurityGroup

VPC ID
vpc-04b16119763a81e63

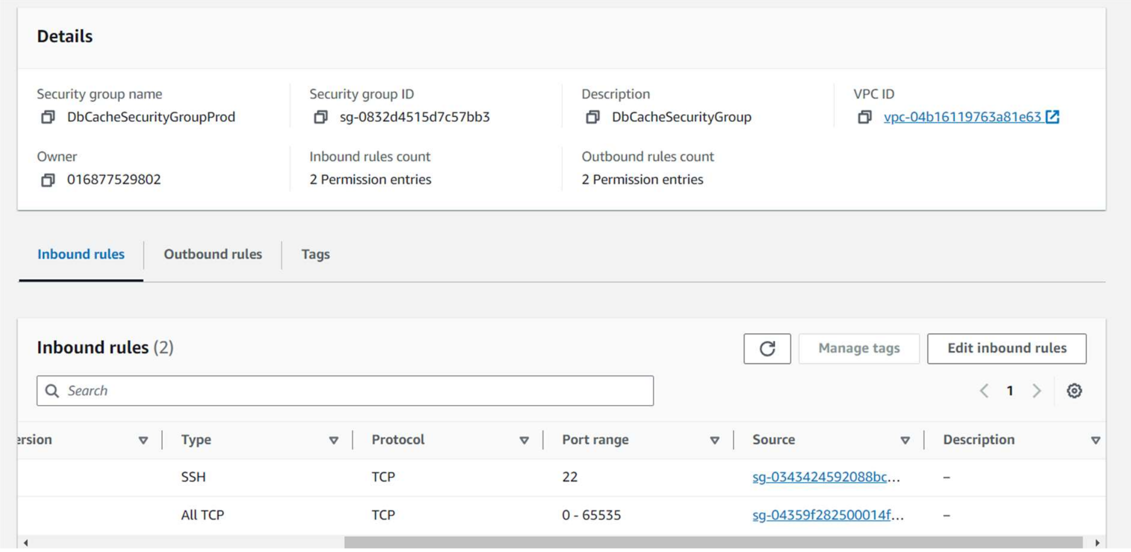
Owner
016877529802

Inbound rules count
2 Permission entries

Outbound rules count
2 Permission entries

Outbound rules (2)

	Security group rule...	IP version	Type	Protocol	Port range	Destin
	sgr-071bc8c888141d4...	–	RDP	TCP	3389	sg-05c
	sgr-0690b87a725918...	IPv4	All traffic	All	All	0.0.0.0



Details

Security group name
DbCacheSecurityGroupProd

Security group ID
sg-0832d4515d7c57bb3

Description
DbCacheSecurityGroup

VPC ID
vpc-04b16119763a81e63

Owner
016877529802

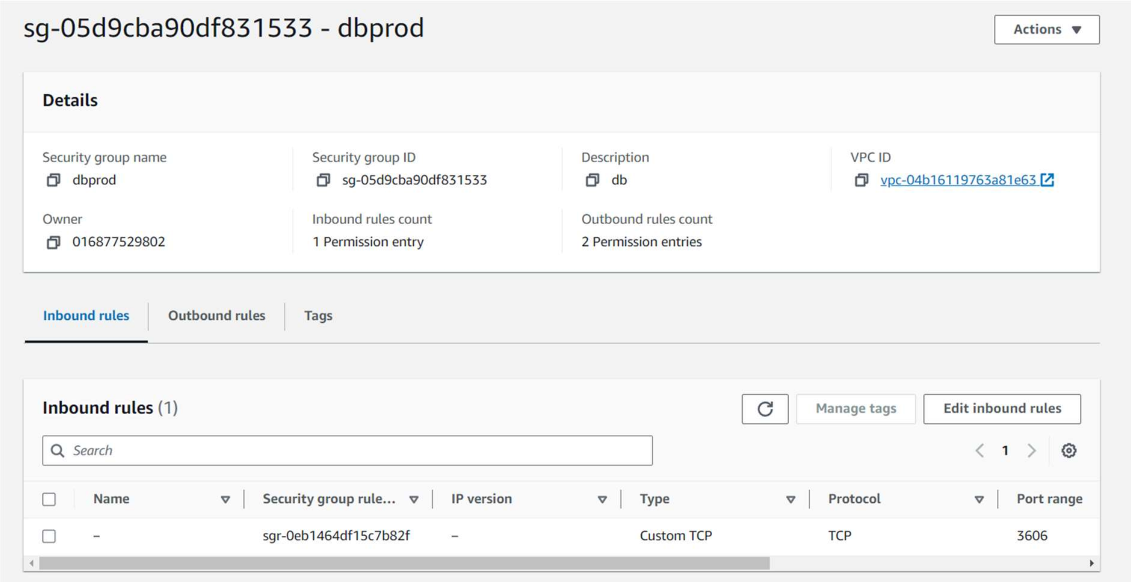
Inbound rules count
2 Permission entries

Outbound rules count
2 Permission entries

Inbound rules (2)

ersion	Type	Protocol	Port range	Source	Description
	SSH	TCP	22	sg-0343424592088bc...	–
	All TCP	TCP	0 - 65535	sg-04359f282500014f...	–

- db: Allow inbound traffic only from dbcache. Restrict outbound as needed.



sg-05d9cba90df831533 - dbprod

Details

Security group name	Security group ID	Description	VPC ID
dbprod	sg-05d9cba90df831533	db	vpc-04b16119763a81e63
Owner	**Inbound rules count**	**Outbound rules count**	
016877529802	1 Permission entry	2 Permission entries	

Inbound rules (1)

□	Name	Security group rule...	IP version	Type	Protocol	Port range
□	–	sgr-0eb1464df15c7b82f	–	Custom TCP	TCP	3606

- **NACLs:**
    - Implement network ACLs to provide an additional layer of security, restricting inbound/outbound traffic according to your architecture.

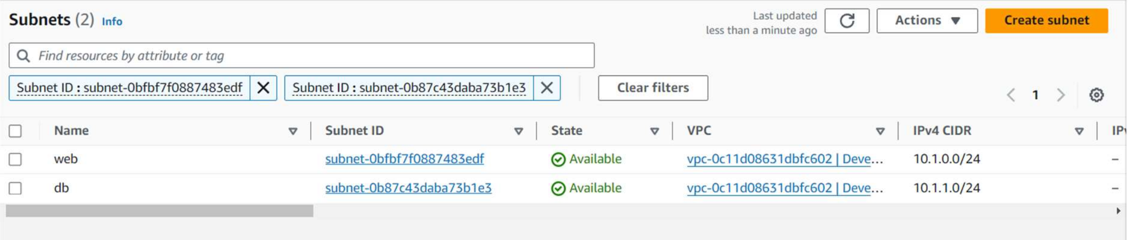
Development Network:

1. Design and Build a 2-Tier Architecture:

- **VPC Creation:**
    - Create a VPC named DevelopmentVPC.
    - Choose an appropriate CIDR block (e.g., 10.1.0.0/16).

2. Create Subnets:

- **Web Subnet:**
    - Create a public subnet named web with CIDR 10.1.0.0/24.
- **DB Subnet:**
    - Create a private subnet named db with CIDR 10.1.1.0/24.

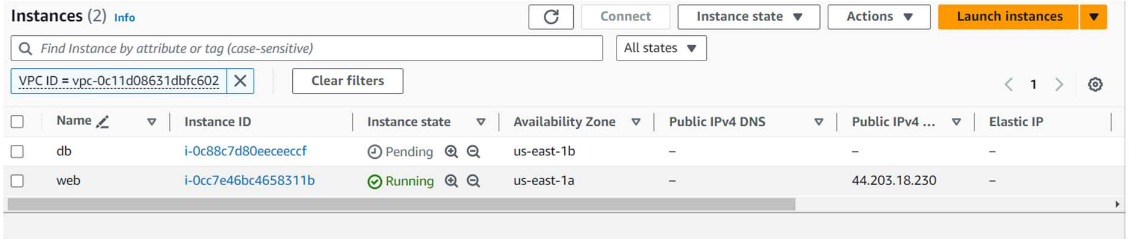

Subnets (2) Info

Subnet ID : subnet-0bfbf7f0887483edf ✕ Subnet ID : subnet-0b87c43daba73b1e3 ✕

□	Name	Subnet ID	State	VPC	IPv4 CIDR	IP
□	web	subnet-0bfbf7f0887483edf	✓ Available	vpc-0c11d08631dbfc602 | Deve...	10.1.0.0/24	–
□	db	subnet-0b87c43daba73b1e3	✓ Available	vpc-0c11d08631dbfc602 | Deve...	10.1.1.0/24	–

3. Launch Instances:

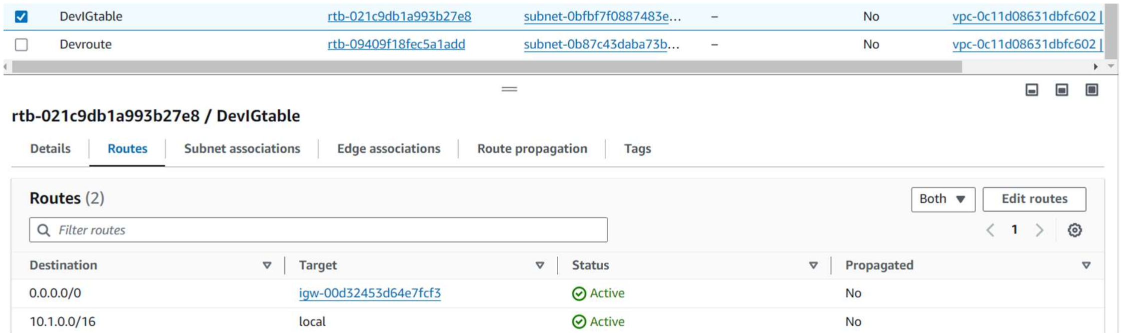
- Launch EC2 instances in both subnets and name them web and db.



☐	Name	Instance ID	Instance state	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☐	db	i-0c88c7d80eeceeccf	Pending	us-east-1b	–	–	–
☐	web	i-0cc7e46bc4658311b	Running	us-east-1a	–	44.203.18.230	–

4. Internet Access:

- **NAT Gateway:**
  - ○ Create a NAT Gateway in the web subnet.
  - ○ Associate the NAT Gateway with the route table of the db subnet.
- **Route Tables:**
  - ○ Update route tables:
    - ▪ web should have a route to the Internet Gateway.

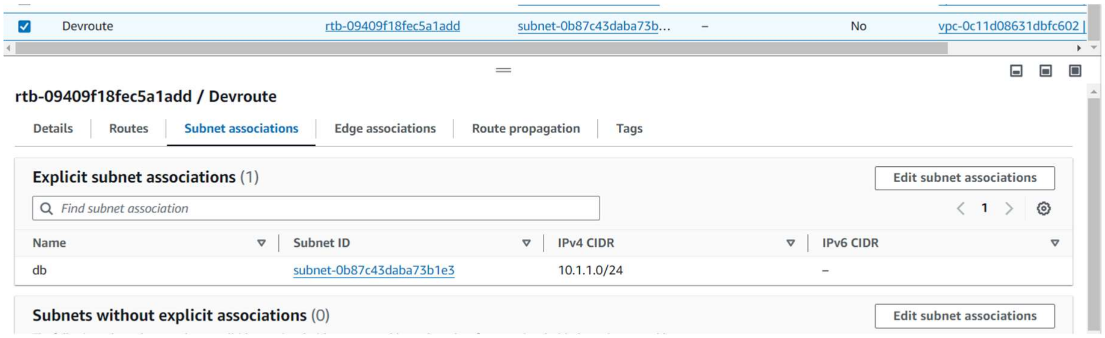


☐						
☑	DevIGtable	rtb-021c9db1a993b27e8	subnet-0bfbf7f0887483e...	–	No	vpc-0c11d08631dbfc602 |
☐	Devroute	rtb-09409f18fec5a1add	subnet-0b87c43daba73b...	–	No	vpc-0c11d08631dbfc602 |

rtb-021c9db1a993b27e8 / DevIGtable

Destination	Target	Status	Propagated
0.0.0.0/0	igw-00d32453d64e7fcf3	Active	No
10.1.0.0/16	local	Active	No

- ▪ db should have a route to the NAT Gateway.



☑	Devroute	rtb-09409f18fec5a1add	subnet-0b87c43daba73b...	–	No	vpc-0c11d08631dbfc602 |

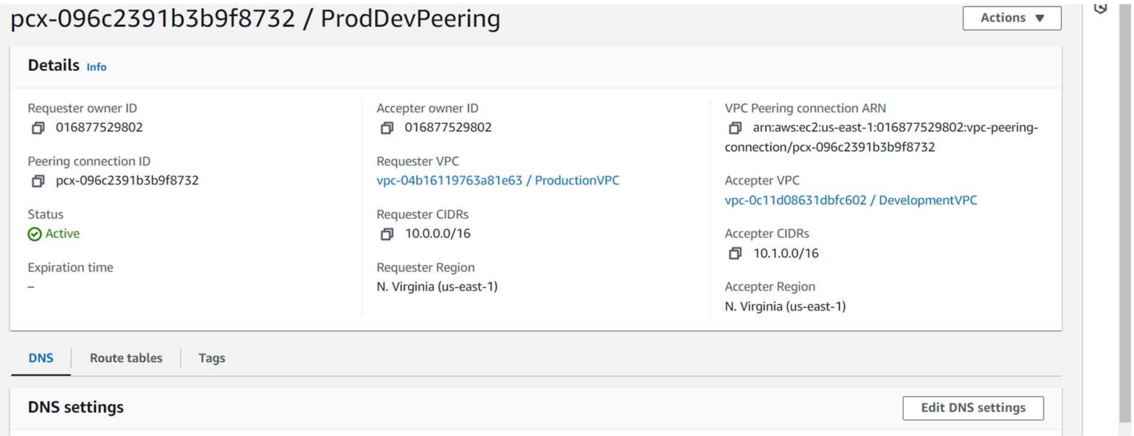
rtb-09409f18fec5a1add / Devroute

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
db	subnet-0b87c43daba73b1e3	10.1.1.0/24	–

VPC Peering and Interconnectivity:

1. Peering Connection:

- Create a VPC peering connection between ProductionVPC and DevelopmentVPC.
- Update the route tables in both VPCs to allow traffic between them.



pcx-096c2391b3b9f8732 / ProdDevPeering

Details

Requester owner ID
016877529802

Peering connection ID
pcx-096c2391b3b9f8732

Status
Active

Expiration time
–

Accepter owner ID
016877529802

Requester VPC
vpc-04b16119763a81e63 / ProductionVPC

Requester CIDRs
10.0.0.0/16

Requester Region
N. Virginia (us-east-1)

VPC Peering connection ARN
arn:aws:ec2:us-east-1:016877529802:vpc-peering-connection/pcx-096c2391b3b9f8732

Accepter VPC
vpc-0c11d08631dbfc602 / DevelopmentVPC

Accepter CIDRs
10.1.0.0/16

Accepter Region
N. Virginia (us-east-1)

DNS settings

2. DB Subnets Interconnection:

- Configure the security groups and route tables to allow communication between the db subnets in both VPCs.
- Ensure that traffic is restricted to only the required ports for database communication.