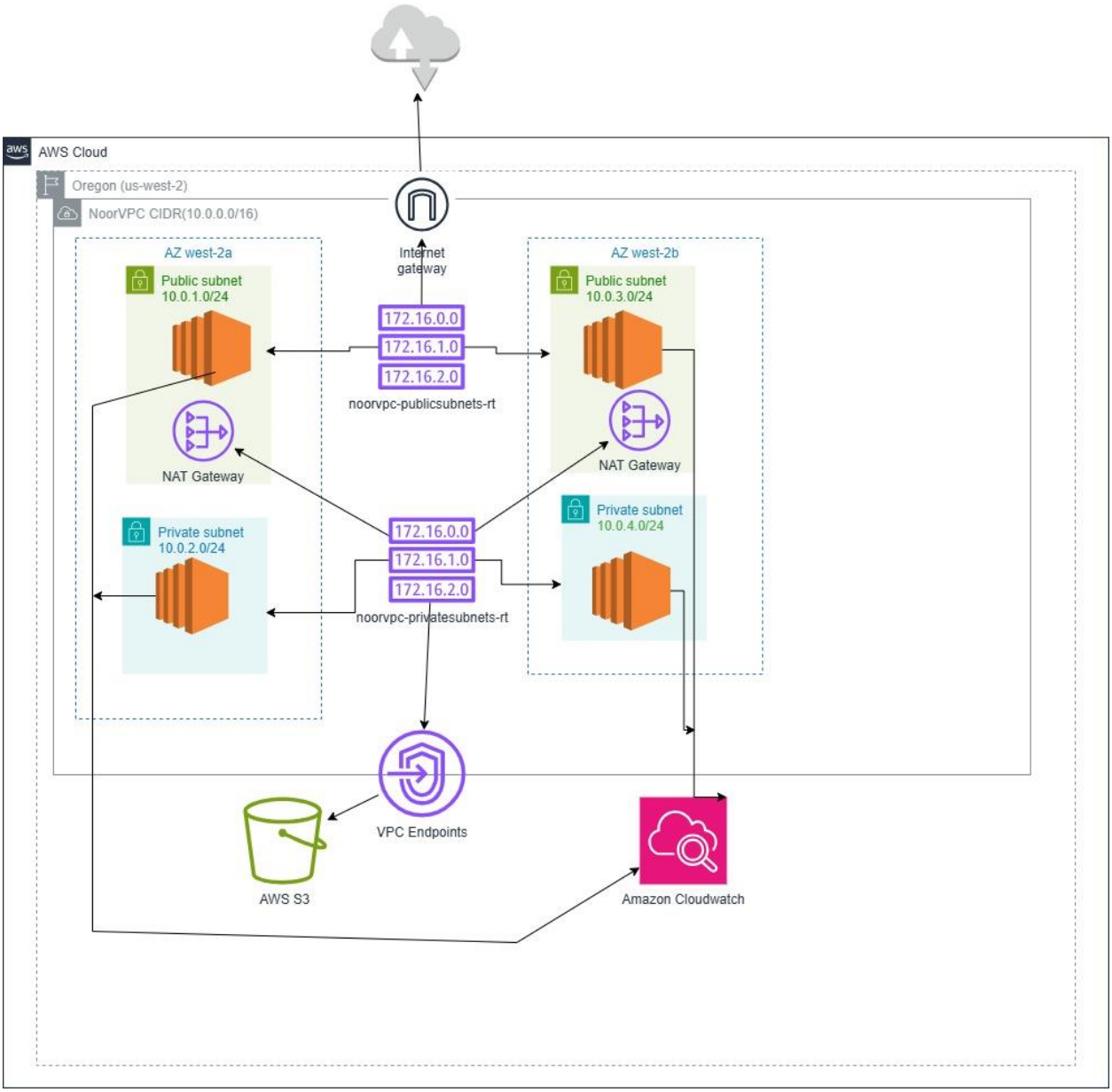
AWS VPC Architecture Implementation Documentation

Sardar Noor Ul Hassan

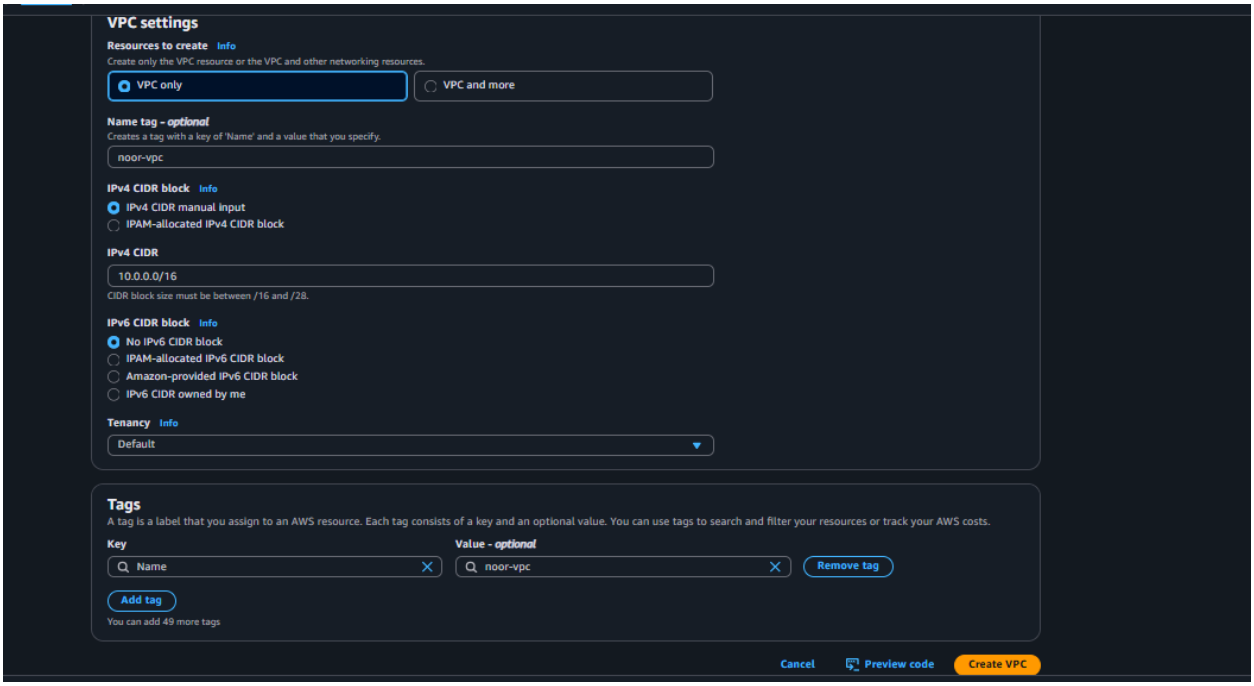
VPC Architecture Diagram

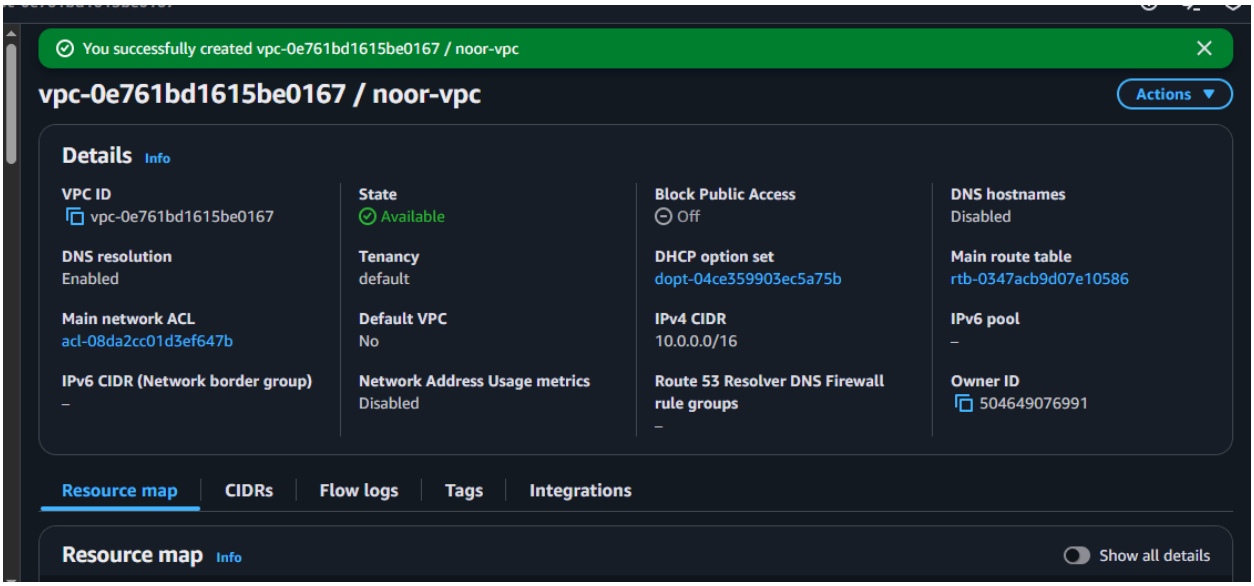


1. Create a Custom VPC

Steps Performed:

1. Opened the **VPC Dashboard** → selected **Create VPC**.
2. Selected **VPC only** option.
3. Defined the **CIDR block:** 10.0.0.0/16 (allows 65,536 IP addresses).
4. Named the VPC as **NoorVPC**.
5. Verified VPC creation in the console.

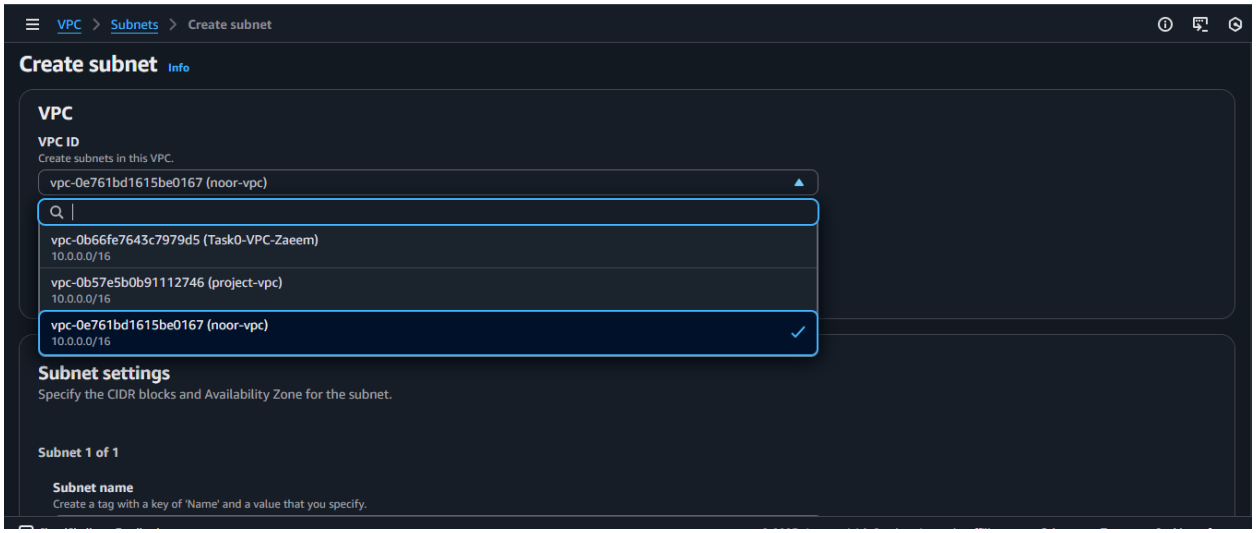


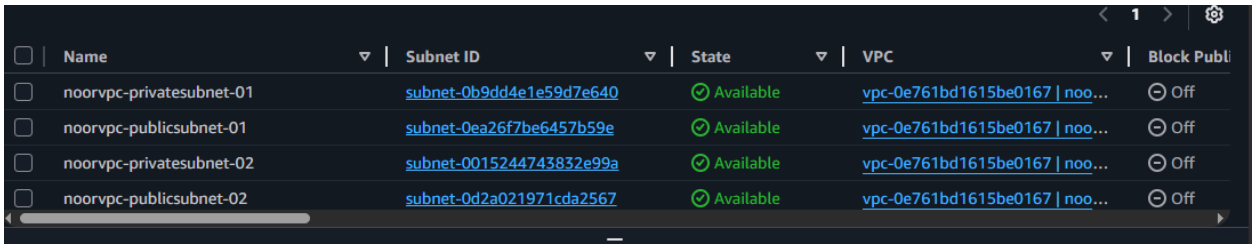


2. Define Public and Private Subnets (Multi-AZ)

Steps Performed:

1. Created **4 subnets** under the VPC:
    - **Noorvpc-publicsubnet-01:** 10.0.1.0/24 (AZ-1)
    - **Noorvpc-privatesubnet-01:** 10.0.2.0/24 (AZ-1)
    - **Noorvpc-publicsubnet-02:** 10.0.3.0/24 (AZ-2)
    - **Noorvpc-privatesubnet-02:** 10.0.4.0/24 (AZ-2)
2. Enabled **Auto-assign Public IP** for both public subnets.
3. Verified subnets are correctly mapped to different Availability Zones.

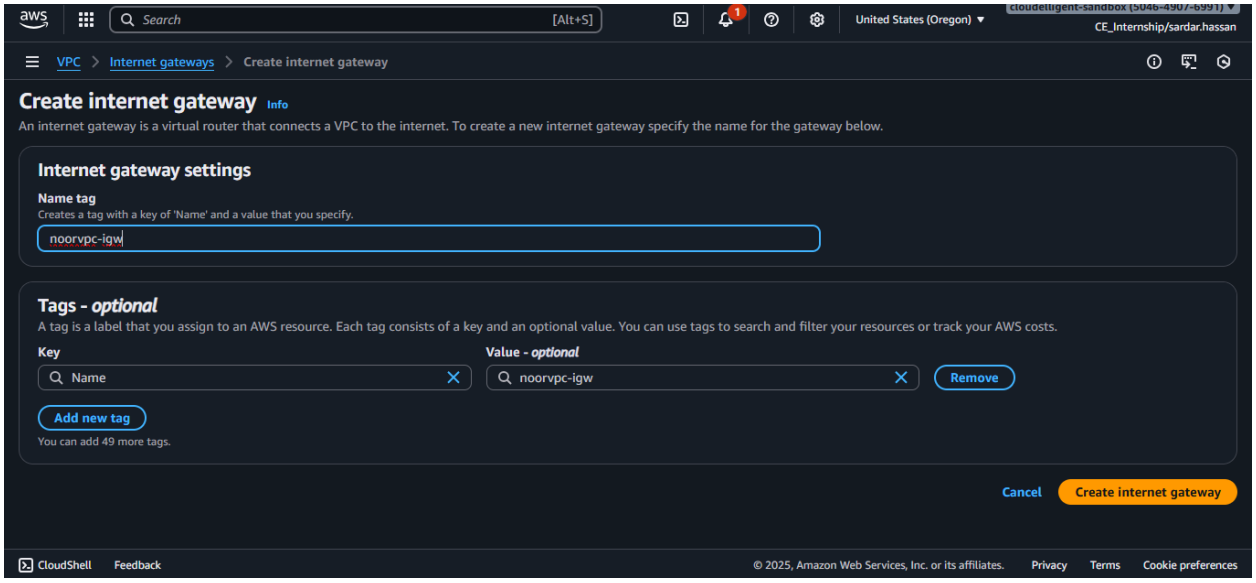


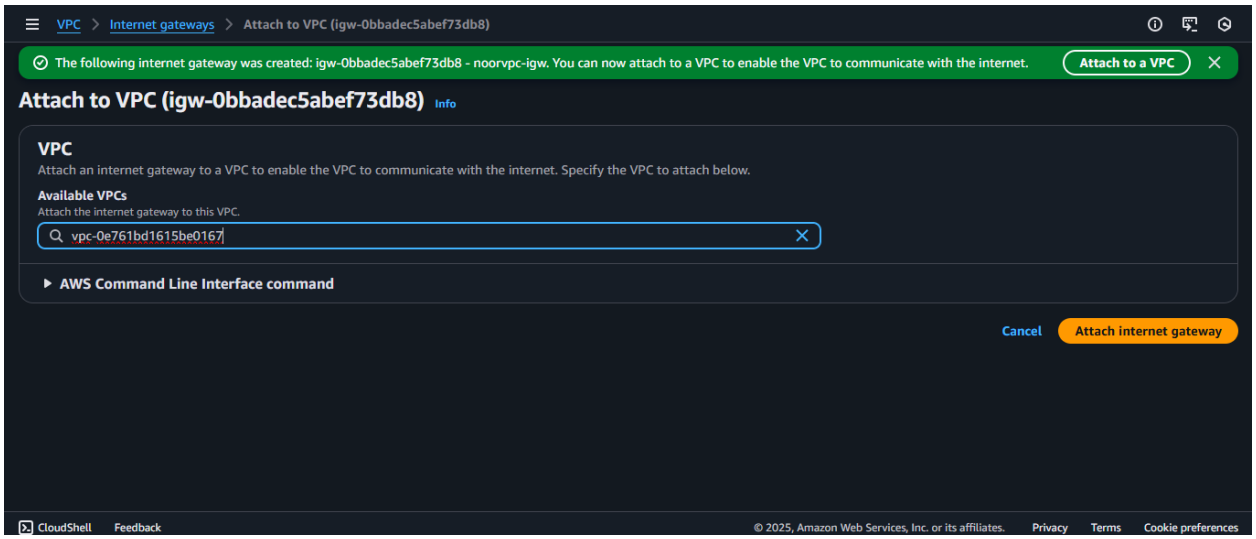


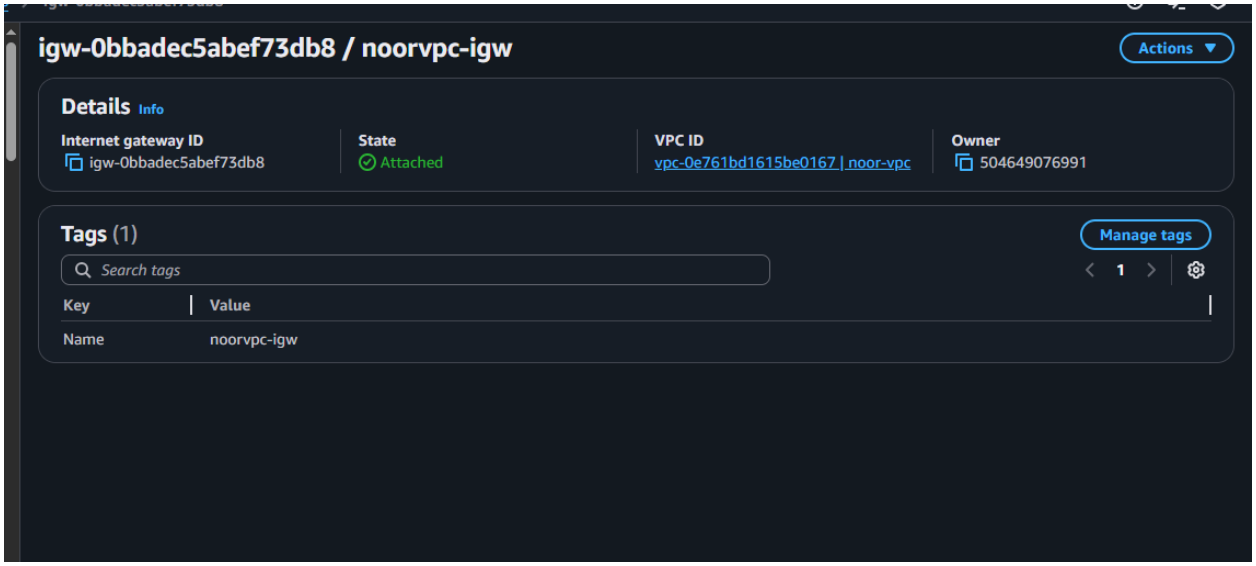
3. Set Up Internet Gateway

Steps Performed:

1. Created an **Internet Gateway (IGW)** named NoorVPC-IGW.
2. Attached the IGW to **NoorVPC**.
3. Confirmed attachment under **VPC → Internet Gateways**.





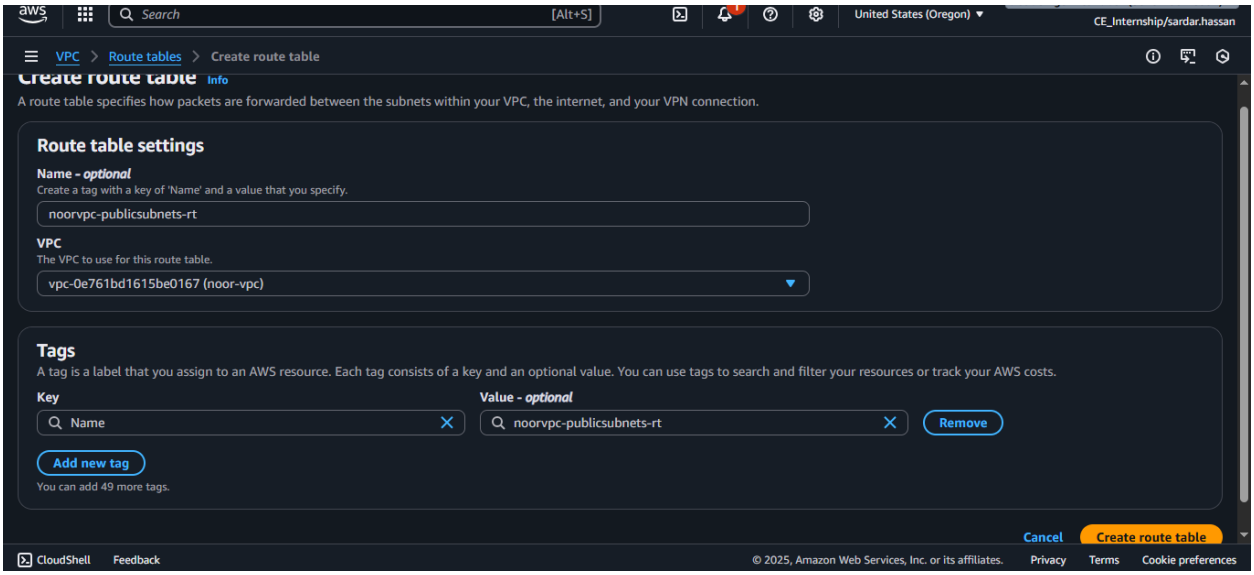


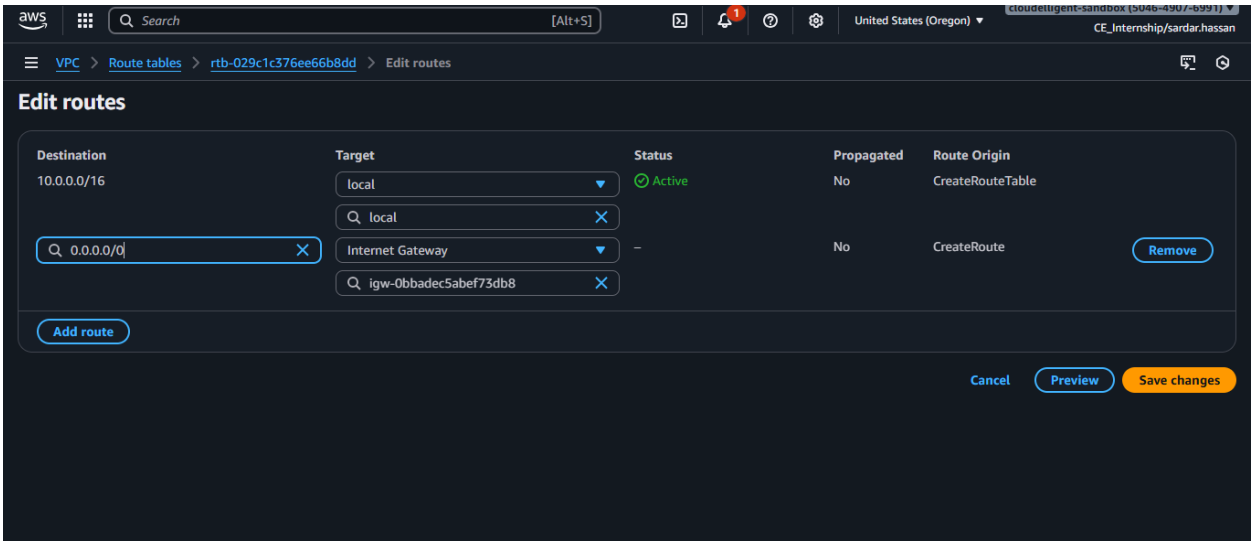
---

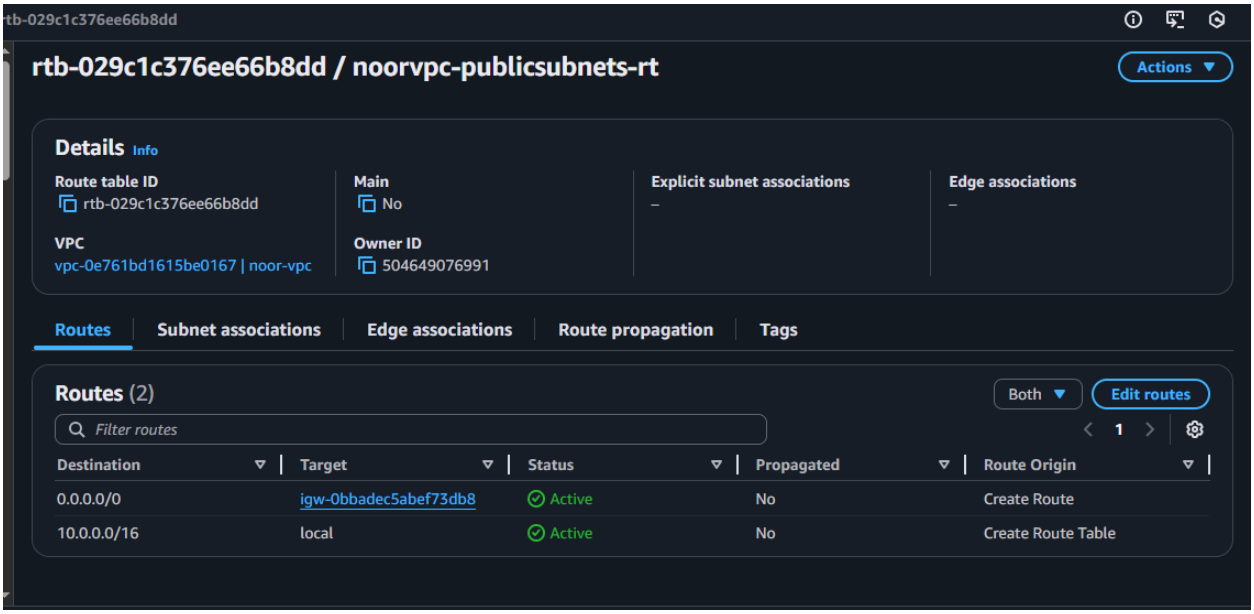
4. Create Route Tables

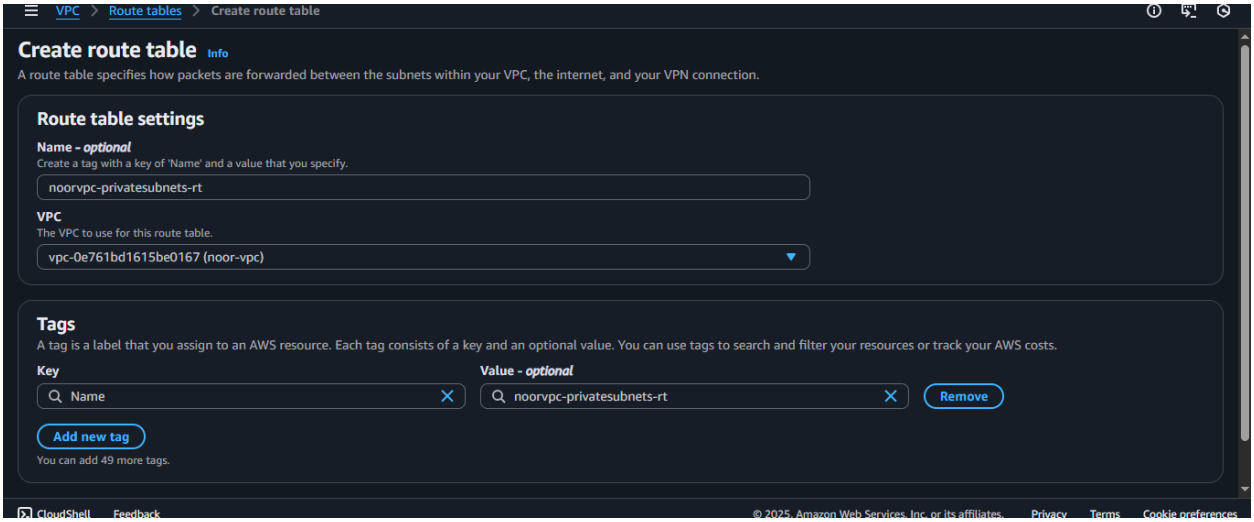
Steps Performed:

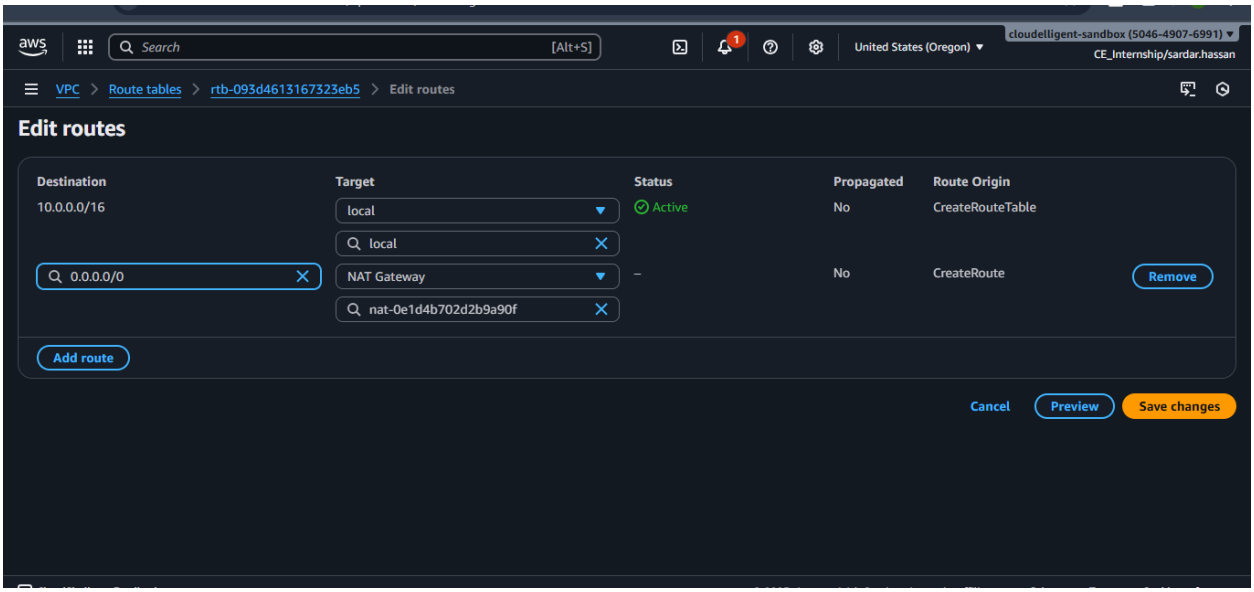
1. Created two route tables: (i.e **noorvpc-publicsubnets-rt** and **noorvpc-privatesubnets-rt**
    - **Public Route Table**
        - Added route: 0.0.0.0/0 → Internet Gateway (NoorVPC-IGW).
        - Associated with both public subnets.
    - **Private Route Table**
        - Initially, only local route 10.0.0.0/16 was present.
        - Later updated to include **NAT Gateway** route (see below).

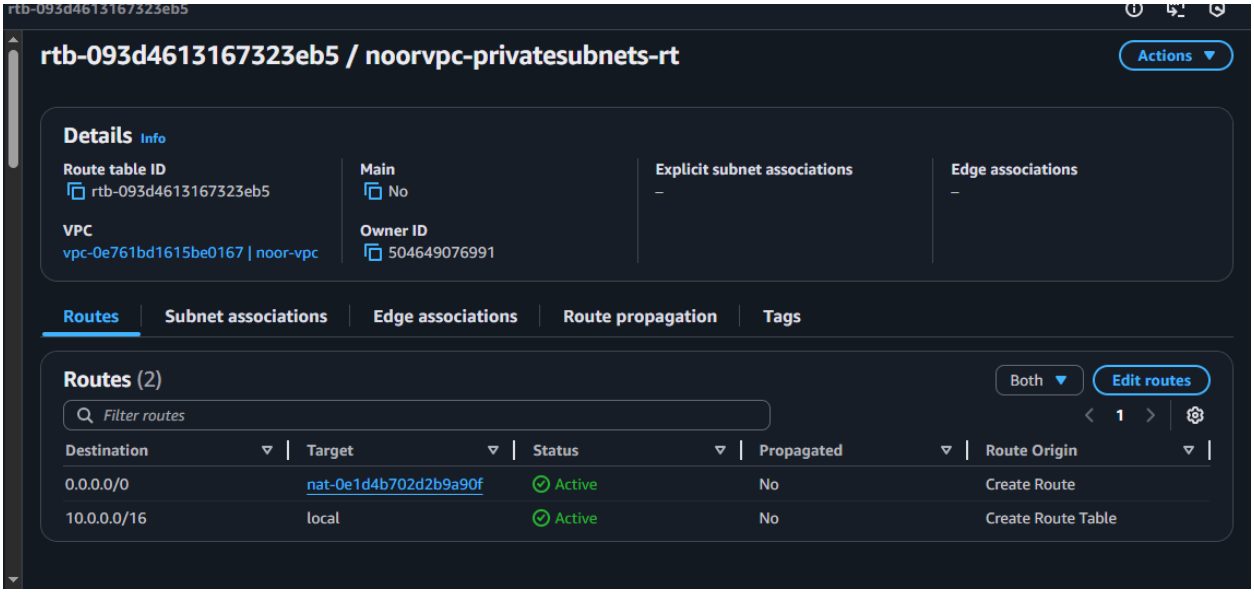

Search
[Alt+S]
United States (Oregon)
CE_Internship/sardar.hassan
VPC
Route tables
Create route table
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
noorvpc-publicsubnets-rt
VPC
The VPC to use for this route table.
vpc-0e761bd1615be0167 (noor-vpc)
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
noorvpc-publicsubnets-rt
Remove
Add new tag
You can add 49 more tags.
Cancel
Create route table
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

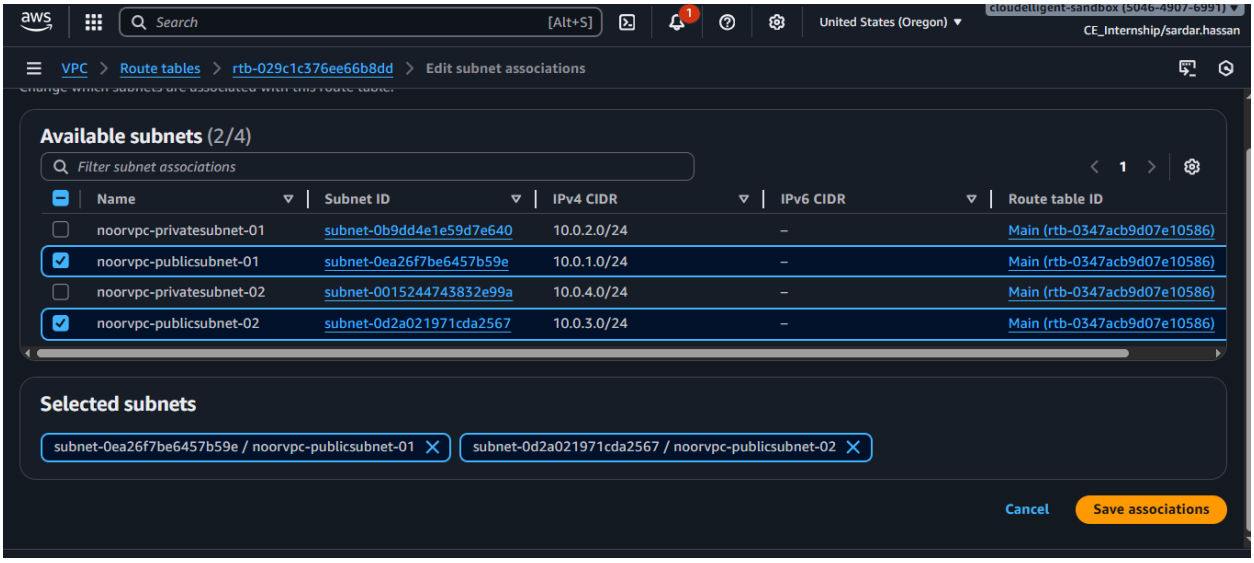

Search
[Alt+S]
United States (Oregon)
CE_Internship/sardar.hassan
VPC
Route tables
rtb-029c1c376ee66b8dd
Edit routes
Edit routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
CreateRouteTable
local
0.0.0.0/0
Internet Gateway
–
No
CreateRoute
Remove
igw-0bbadec5abef73db8
Add route
Cancel
Preview
Save changes


rtb-029c1c376ee66b8dd
rtb-029c1c376ee66b8dd / noorvpc-publicsubnets-rt
Actions
Details Info
Route table ID
rtb-029c1c376ee66b8dd
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0e761bd1615be0167 | noor-vpc
Owner ID
504649076991
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
Route Origin
0.0.0.0/0
igw-0bbadec5abef73db8
Active
No
Create Route
10.0.0.0/16
local
Active
No
Create Route Table


VPC
Route tables
Create route table
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
noorvpc-privatesubnets-rt
VPC
The VPC to use for this route table.
vpc-0e761bd1615be0167 (noor-vpc)
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
noorvpc-privatesubnets-rt
Remove
Add new tag
You can add 49 more tags.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Search
[Alt+S]
United States (Oregon)
cloudelligent-sandbox (5046-4907-6991)
CE_Internship/sardar.hassan
VPC > Route tables > rtb-093d4613167323eb5 > Edit routes
Edit routes
Destination
Target
Status
Propagated
Route Origin
10.0.0.0/16
local
Active
No
CreateRouteTable
local
0.0.0.0/0
NAT Gateway
–
No
CreateRoute
Remove
nat-0e1d4b702d2b9a90f
Add route
Cancel
Preview
Save changes


rtb-093d4613167323eb5 / noorvpc-privatesubnets-rt
Actions
Details Info
Route table ID
rtb-093d4613167323eb5
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0e761bd1615be0167 | noor-vpc
Owner ID
504649076991
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
Route Origin
0.0.0.0/0
nat-0e1d4b702d2b9a90f
Active
No
Create Route
10.0.0.0/16
local
Active
No
Create Route Table

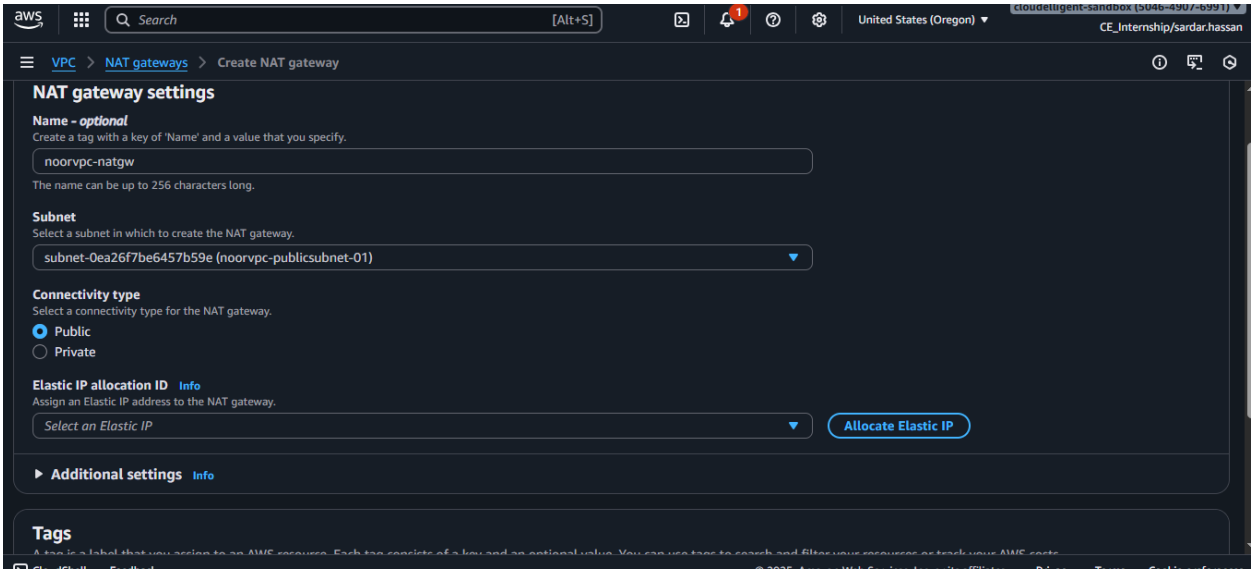


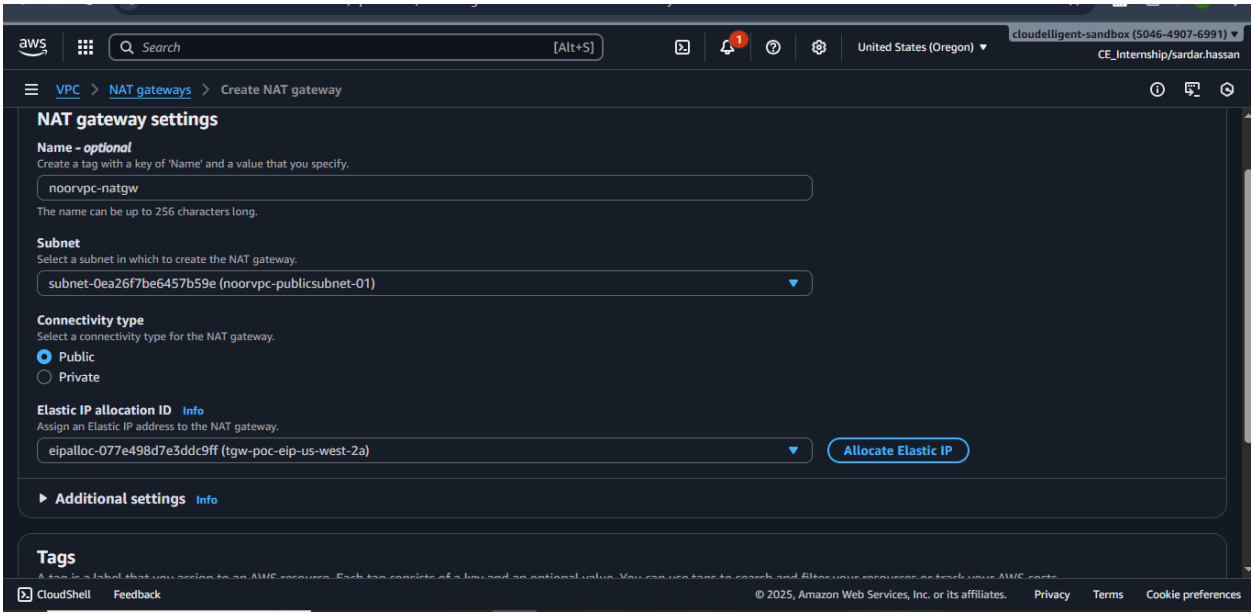
---

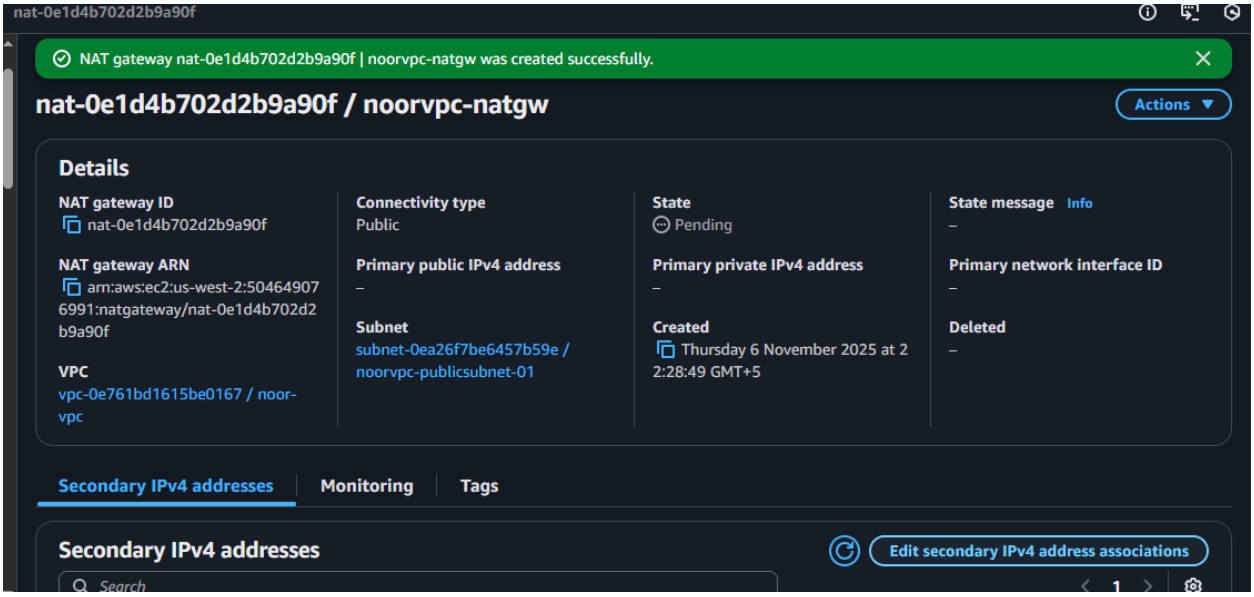
5. Configure NAT Gateway

Steps Performed:

1. Allocated an **Elastic IP**.
2. Created **NAT Gateway** in Public Subnet-A.
3. Assigned the Elastic IP to the NAT Gateway.
4. Updated **Private Route Table**:
    - Added route: 0.0.0.0/0 → NAT Gateway.
    - Associated it with both private subnets.


Search
[Alt+S]
United States (Oregon)
CE_Internship/sardar.hassan
VPC
NAT gateways
Create NAT gateway
NAT gateway settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
noorvpc-natgw
The name can be up to 256 characters long.
Subnet
Select a subnet in which to create the NAT gateway.
subnet-0ea26f7be6457b59e (noorvpc-publicsubnet-01)
Connectivity type
Select a connectivity type for the NAT gateway.
Public
Private
Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
Select an Elastic IP
Allocate Elastic IP
Additional settings Info
Tags


Search
[Alt+S]
United States (Oregon)
cloudelligent-sandbox (5046-4907-6991)
CE_Internship/sardar.hassan
VPC
NAT gateways
Create NAT gateway
NAT gateway settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
noorvpc-natgw
The name can be up to 256 characters long.
Subnet
Select a subnet in which to create the NAT gateway.
subnet-0ea26f7be6457b59e (noorvpc-publicsubnet-01)
Connectivity type
Select a connectivity type for the NAT gateway.
Public
Private
Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-077e498d7e3ddc9ff (tgw-poc-eip-us-west-2a)
Allocate Elastic IP
Additional settings Info
Tags
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

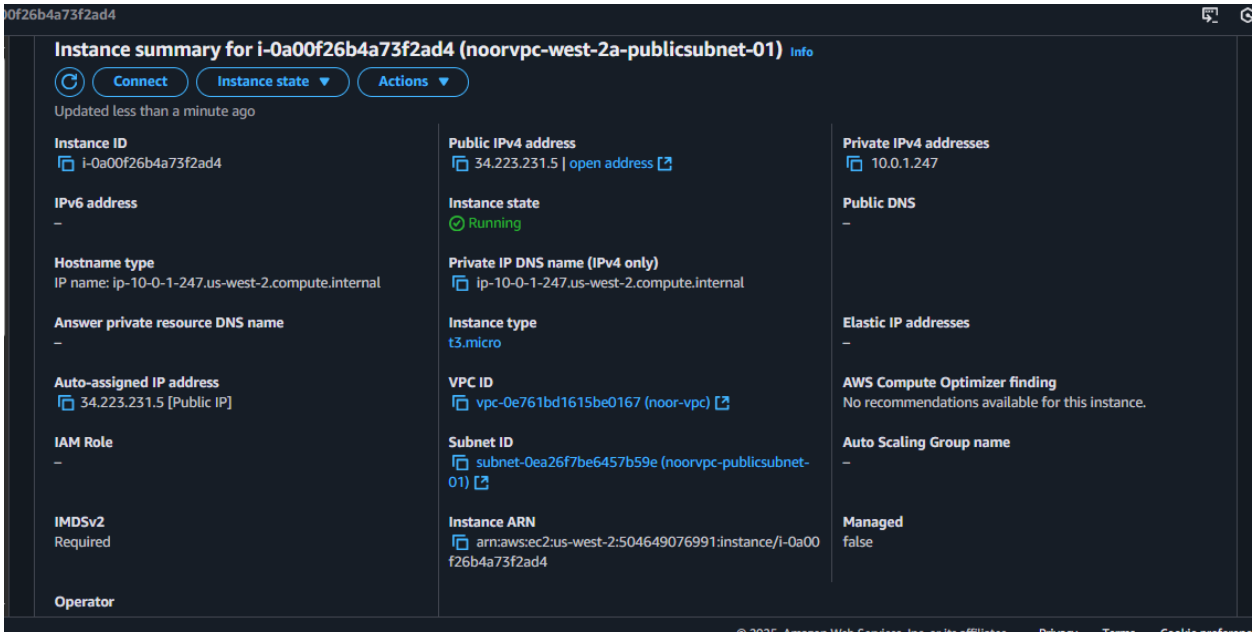


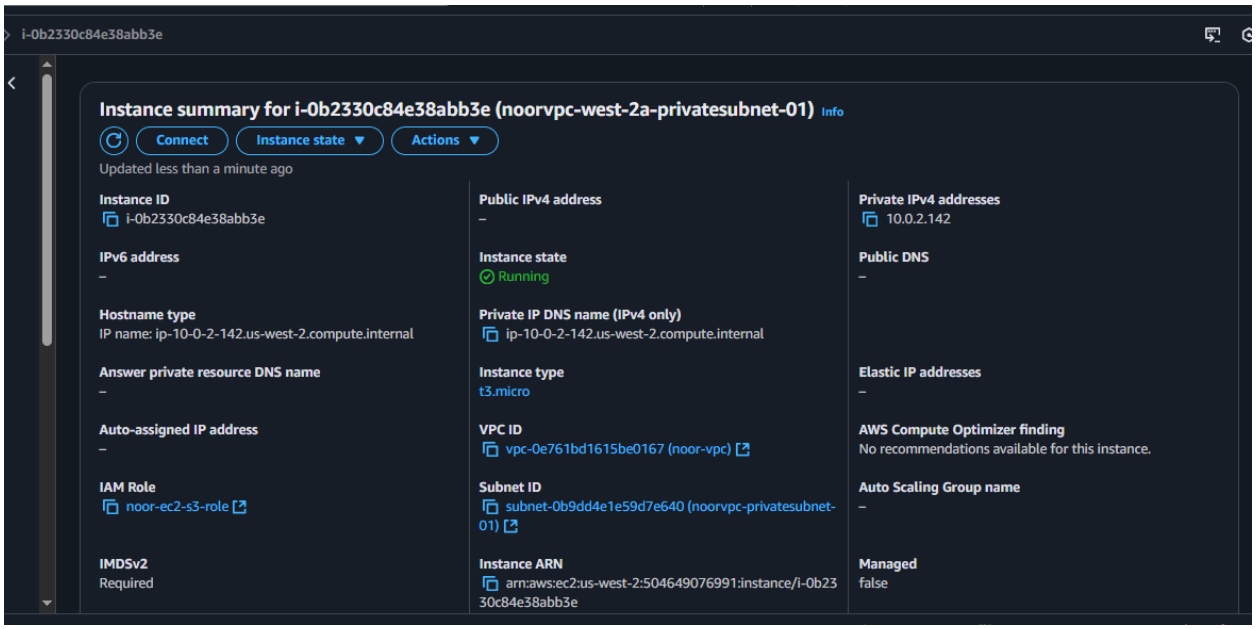
---

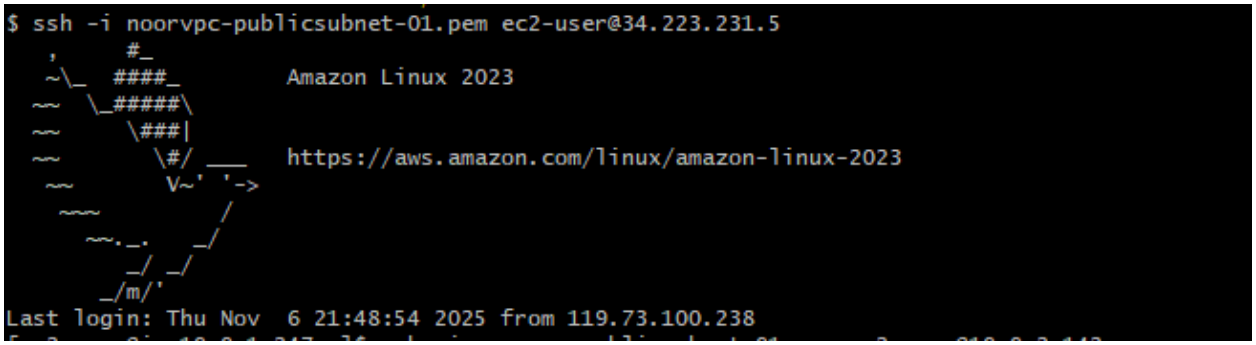
6. Launch EC2 Instances

Steps Performed:

1. Launched:
    - **Public EC2 Instance:**
        - Subnet: Public Subnet-A
        - Security Group: Allow SSH (port 22) and ICMP (ping) from anywhere.
    - **Private EC2 Instance:**
        - Subnet: Private Subnet-A
        - Security Group: Allow SSH from public instance only.
2. Used **SSH key pair** for secure authentication.
3. Verified SSH access from local to public EC2 and from public EC2 → private EC2.


0f26b4a73f2ad4
Instance summary for i-0a00f26b4a73f2ad4 (noorvpc-west-2a-publicsubnet-01) Info
Connect
Instance state
Actions
Updated less than a minute ago
Instance ID
i-0a00f26b4a73f2ad4
Public IPv4 address
34.223.231.5 | open address
Private IPv4 addresses
10.0.1.247
IPv6 address
–
Instance state
Running
Public DNS
–
Hostname type
IP name: ip-10-0-1-247.us-west-2.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-1-247.us-west-2.compute.internal
Answer private resource DNS name
–
Instance type
t3.micro
Elastic IP addresses
–
Auto-assigned IP address
34.223.231.5 [Public IP]
VPC ID
vpc-0e761bd1615be0167 (noor-vpc)
AWS Compute Optimizer finding
No recommendations available for this instance.
IAM Role
–
Subnet ID
subnet-0ea26f7be6457b59e (noorvpc-publicsubnet-01)
Auto Scaling Group name
–
IMDSv2
Required
Instance ARN
arn:aws:ec2:us-west-2:504649076991:instance/i-0a00f26b4a73f2ad4
Managed
false
Operator

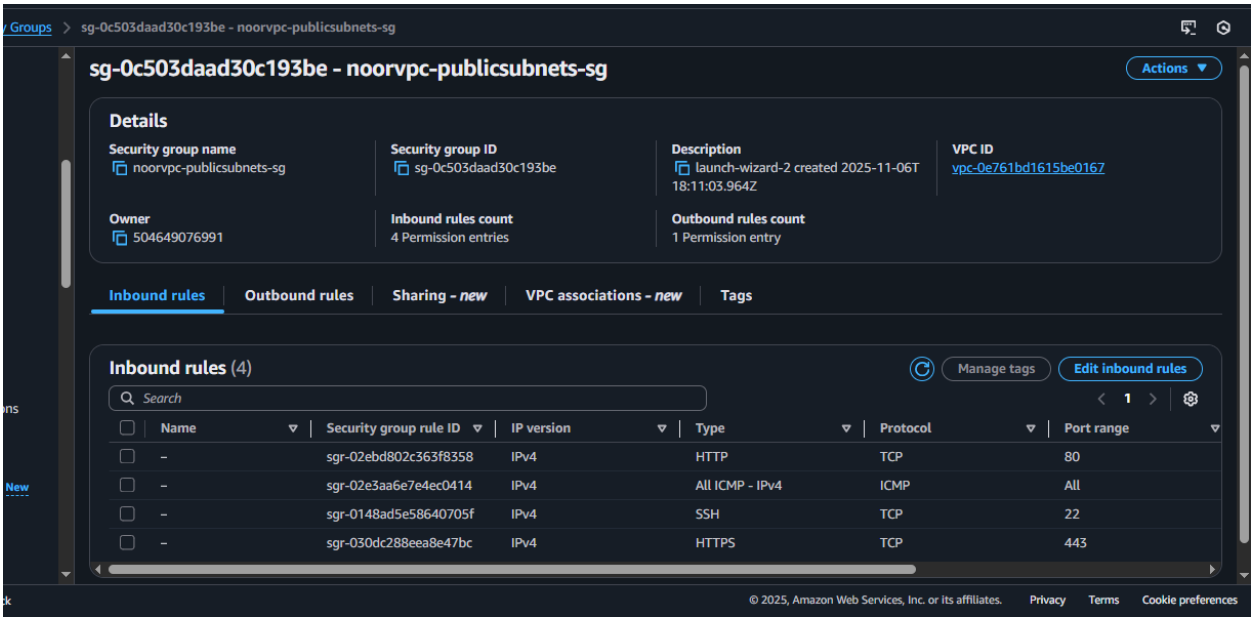

i-0b2330c84e38abb3e
Instance summary for i-0b2330c84e38abb3e (noorvpc-west-2a-privatesubnet-01) Info
Connect
Instance state
Actions
Updated less than a minute ago
Instance ID
i-0b2330c84e38abb3e
Public IPv4 address
–
Private IPv4 addresses
10.0.2.142
IPv6 address
–
Instance state
Running
Public DNS
–
Hostname type
IP name: ip-10-0-2-142.us-west-2.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-2-142.us-west-2.compute.internal
Answer private resource DNS name
–
Instance type
t3.micro
Elastic IP addresses
–
Auto-assigned IP address
–
VPC ID
vpc-0e761bd1615be0167 (noor-vpc)
AWS Compute Optimizer finding
No recommendations available for this instance.
IAM Role
noor-ec2-s3-role
Subnet ID
subnet-0b9dd4e1e59d7e640 (noorvpc-privatesubnet-01)
Auto Scaling Group name
–
IMDSv2
Required
Instance ARN
arn:aws:ec2:us-west-2:504649076991:instance/i-0b2330c84e38abb3e
Managed
false

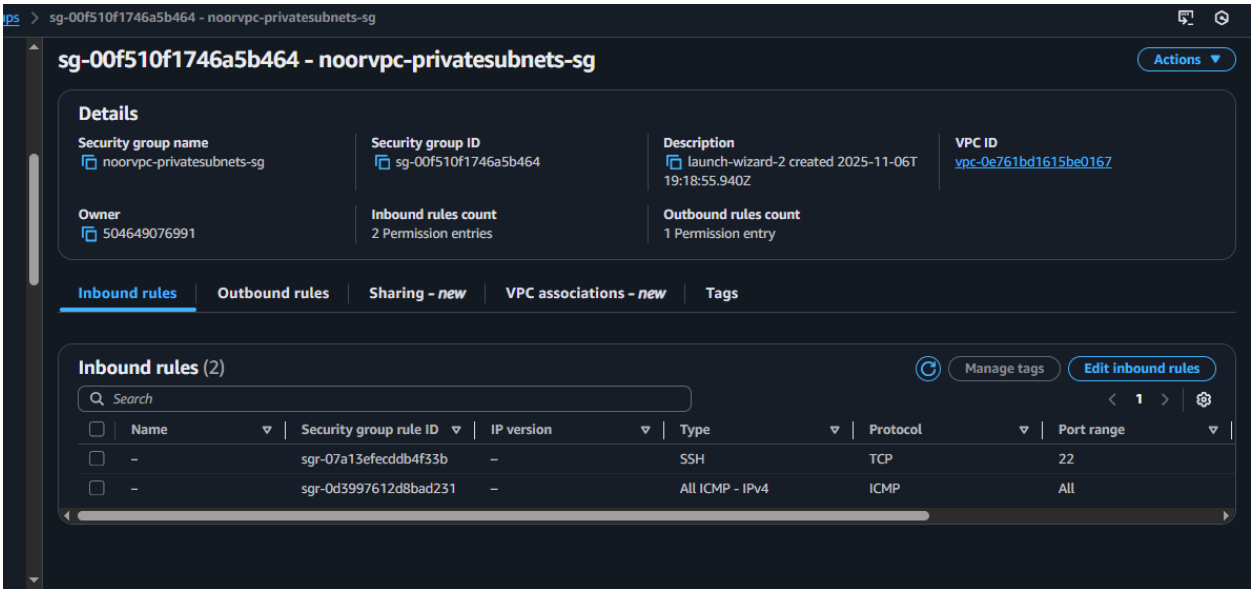

$ ssh -i noorvpc-publicsubnet-01.pem ec2-user@34.223.231.5
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
Last login: Thu Nov 6 21:48:54 2025 from 119.73.100.238

7. Implement Security Groups and Network ACLs

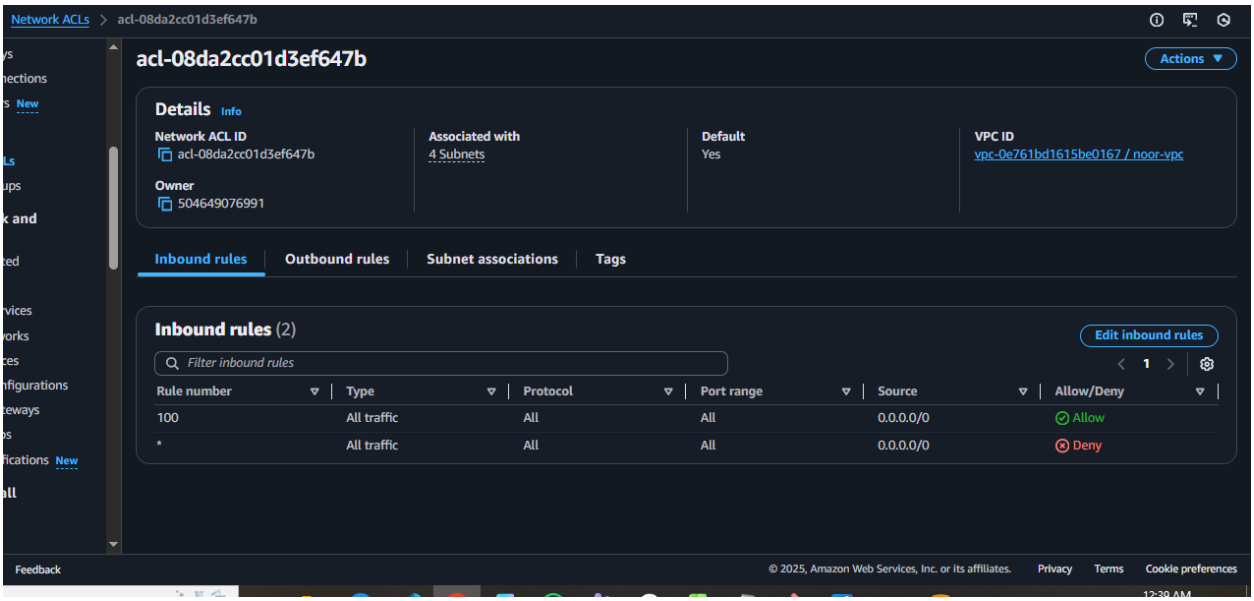
Steps Performed:

- **Security Groups:**
    - **Public-SG:**
        - Inbound: SSH (22), ICMP from anywhere,HTTP/HTTPS
        - Outbound: All traffic allowed.
    - **Private-SG:**
        - Inbound: SSH from Public-SG only,ICMP
        - Outbound: All traffic allowed.





- **Network ACLs:**
  - Public Subnets: Allowed inbound/outbound for HTTP, HTTPS, SSH, ICMP.
  - Private Subnets: Allowed outbound for HTTP/HTTPS only.

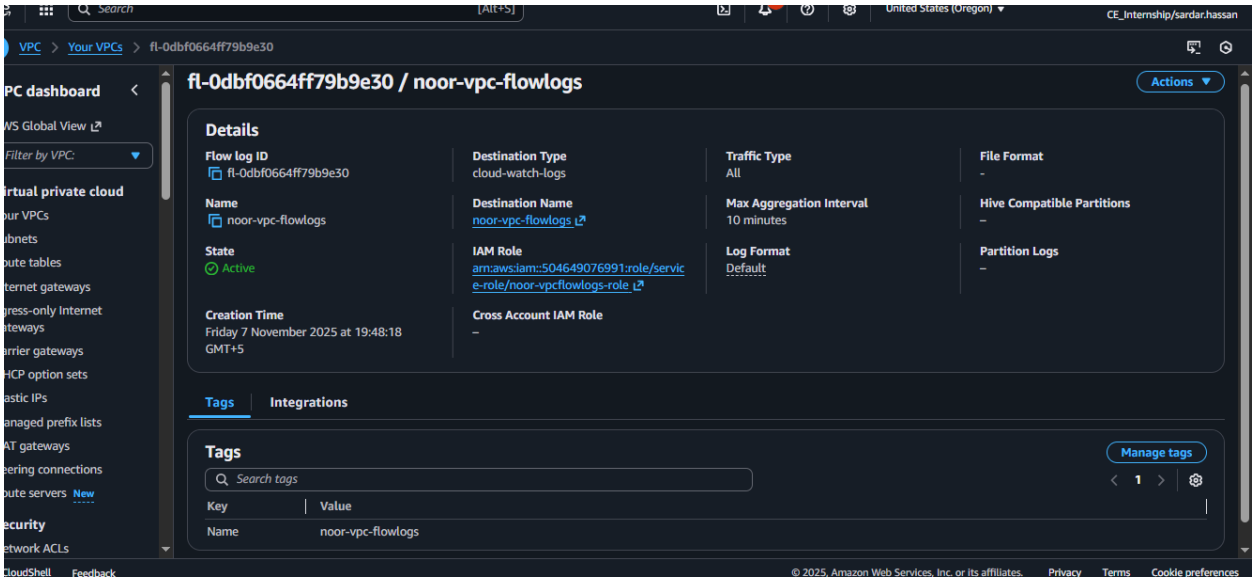


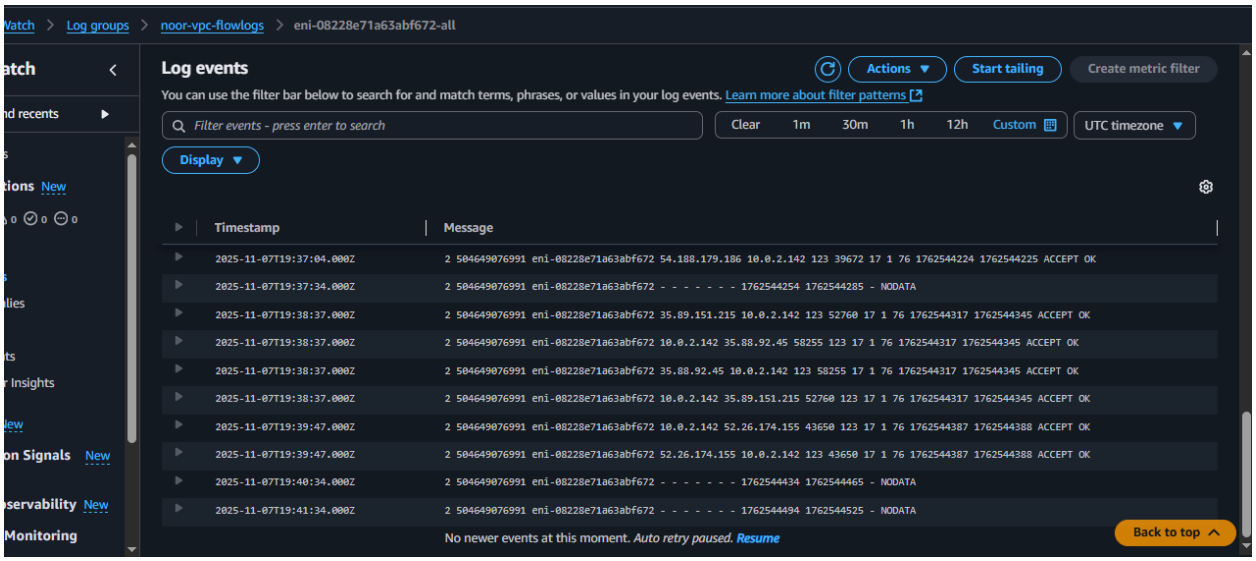
---

8. Enable VPC Flow Logs

Steps Performed:

1. Opened **VPC → Flow Logs → Create Flow Log**.
2. Selected **VPC NoorVPC**.
3. Destination: **CloudWatch Logs Group**.
4. IAM Role: Configured permissions for log delivery.
5. Verified log entries in CloudWatch.



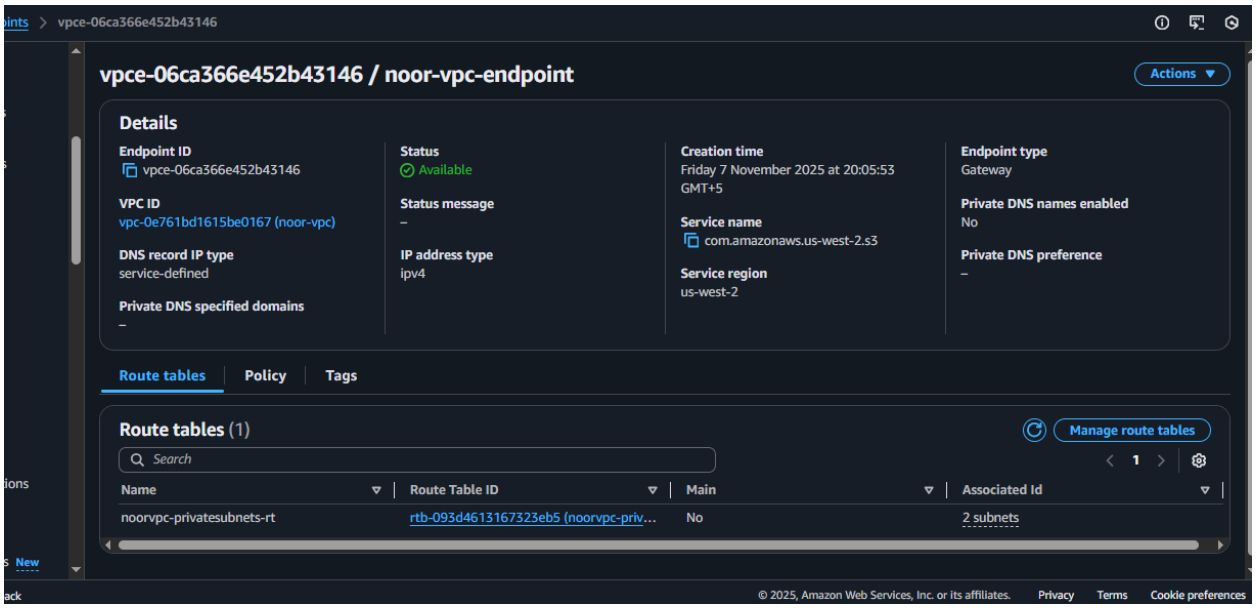


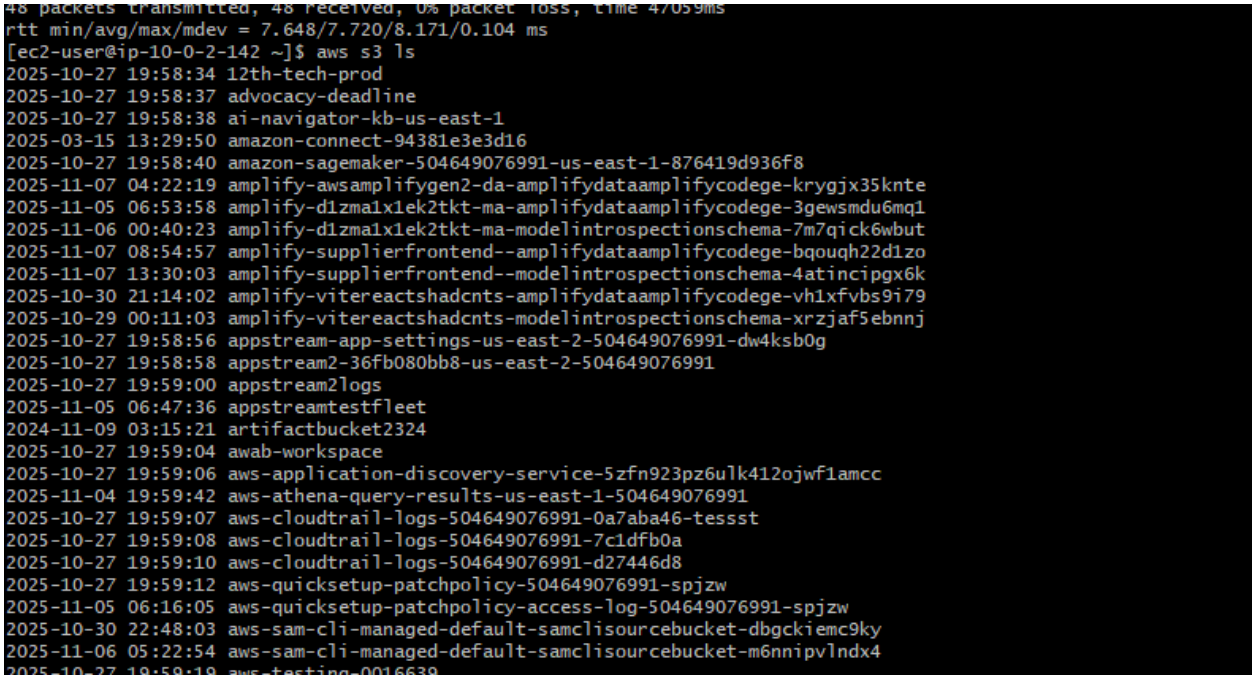
---

9. Create VPC Endpoints

Steps Performed:

1. Created **Gateway Endpoint** for **S3**.
2. Selected NoorVPC and associated **Private Route Table** (i.e noorvpc-privatesubnets-rt)
3. Verified S3 access from private EC2 without using the Internet Gateway.





---

10. Use Elastic IPs

Steps Performed:

1. Allocated **Elastic IP** via EC2 console.
2. Attached it to **NAT Gateway** and **Public EC2 Instance** for persistent access.

---

11. Tag All Resources

Applied tags to **VPC, Subnets, Route Tables, Gateways, EC2 Instances, and Security Groups.**

---

12. Test Connectivity

Objective:
To verify routing and access configuration.

Tests Performed:

1. Ping from **local machine → Public EC2** (successful).
2. SSH from **Public EC2 → Private EC2** (successful).
3. Internet access from **Private EC2** (via NAT Gateway) verified using ping google.com.
4. Confirmed **S3 access from Private EC2** through VPC Endpoint.
5. Verified traffic logs in **CloudWatch Flow Logs**.

```
$ ssh -i noorvpc-publicsubnet-01.pem ec2-user@34.223.231.5
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Thu Nov  6 21:48:54 2025 from 119.73.100.238
```

```
[ec2-user@ip-10-0-1-247 ~]$ ssh -i noorvpc-publicsubnet-01.pem ec2-user@10.0.2.142
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Thu Nov  6 21:49:54 2025 from 10.0.1.247
```

```
[ec2-user@ip-10-0-2-142 ~]$ ping google.com
PING google.com (142.251.33.78) 56(84) bytes of data.
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=1 ttl=114 time=8.17 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=2 ttl=114 time=7.68 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=3 ttl=114 time=7.66 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=4 ttl=114 time=7.69 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=5 ttl=114 time=7.67 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=6 ttl=114 time=8.01 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=7 ttl=114 time=7.67 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=8 ttl=114 time=7.68 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=9 ttl=114 time=7.69 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=10 ttl=114 time=7.67 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=11 ttl=114 time=7.68 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=12 ttl=114 time=7.73 ms
64 bytes from sea09s28-in-f14.1e100.net (142.251.33.78): icmp_seq=13 ttl=114 time=7.69 ms
```

```
48 packets transmitted, 48 received, 0% packet loss, time 47059ms
rtt min/avg/max/mdev = 7.648/7.720/8.171/0.104 ms
[ec2-user@ip-10-0-2-142 ~]$ aws s3 ls
2025-10-27 19:58:34 12th-tech-prod
2025-10-27 19:58:37 advocacy-deadline
2025-10-27 19:58:38 ai-navigator-kb-us-east-1
2025-03-15 13:29:50 amazon-connect-94381e3e3d16
2025-10-27 19:58:40 amazon-sagemaker-504649076991-us-east-1-876419d936f8
2025-11-07 04:22:19 amplify-awsamplifygen2-da-amplifydataamplifycodege-krygjx35knte
2025-11-05 06:53:58 amplify-d1zma1x1ek2tkt-ma-amplifydataamplifycodege-3gewsmdu6mq1
2025-11-06 00:40:23 amplify-d1zma1x1ek2tkt-ma-modelintrospectionschema-7m7qick6wbut
2025-11-07 08:54:57 amplify-supplierfrontend--amplifydataamplifycodege-bqouqh22d1zo
2025-11-07 13:30:03 amplify-supplierfrontend--modelintrospectionschema-4atincipgx6k
2025-10-30 21:14:02 amplify-vitereactshadcnts-amplifydataamplifycodege-vh1xfvbs9i79
2025-10-29 00:11:03 amplify-vitereactshadcnts-modelintrospectionschema-xrzjaf5ebnnj
2025-10-27 19:58:56 appstream-app-settings-us-east-2-504649076991-dw4ksb0g
2025-10-27 19:58:58 appstream2-36fb080bb8-us-east-2-504649076991
2025-10-27 19:59:00 appstream2logs
2025-11-05 06:47:36 appstreamtestfleet
2024-11-09 03:15:21 artifactbucket2324
2025-10-27 19:59:04 awab-workspace
2025-10-27 19:59:06 aws-application-discovery-service-5zfn923pz6ulk412ojwf1amcc
2025-11-04 19:59:42 aws-athena-query-results-us-east-1-504649076991
2025-10-27 19:59:07 aws-cloudtrail-logs-504649076991-0a7aba46-tessst
2025-10-27 19:59:08 aws-cloudtrail-logs-504649076991-7c1dfb0a
2025-10-27 19:59:10 aws-cloudtrail-logs-504649076991-d27446d8
2025-10-27 19:59:12 aws-quicksetup-patchpolicy-504649076991-spjzw
2025-11-05 06:16:05 aws-quicksetup-patchpolicy-access-log-504649076991-spjzw
2025-10-30 22:48:03 aws-sam-cli-managed-default-samclisourcebucket-dbgckiemc9ky
2025-11-06 05:22:54 aws-sam-cli-managed-default-samclisourcebucket-m6nnipvlndx4
2025-10-27 19:59:19 aws-testing-0016639
```