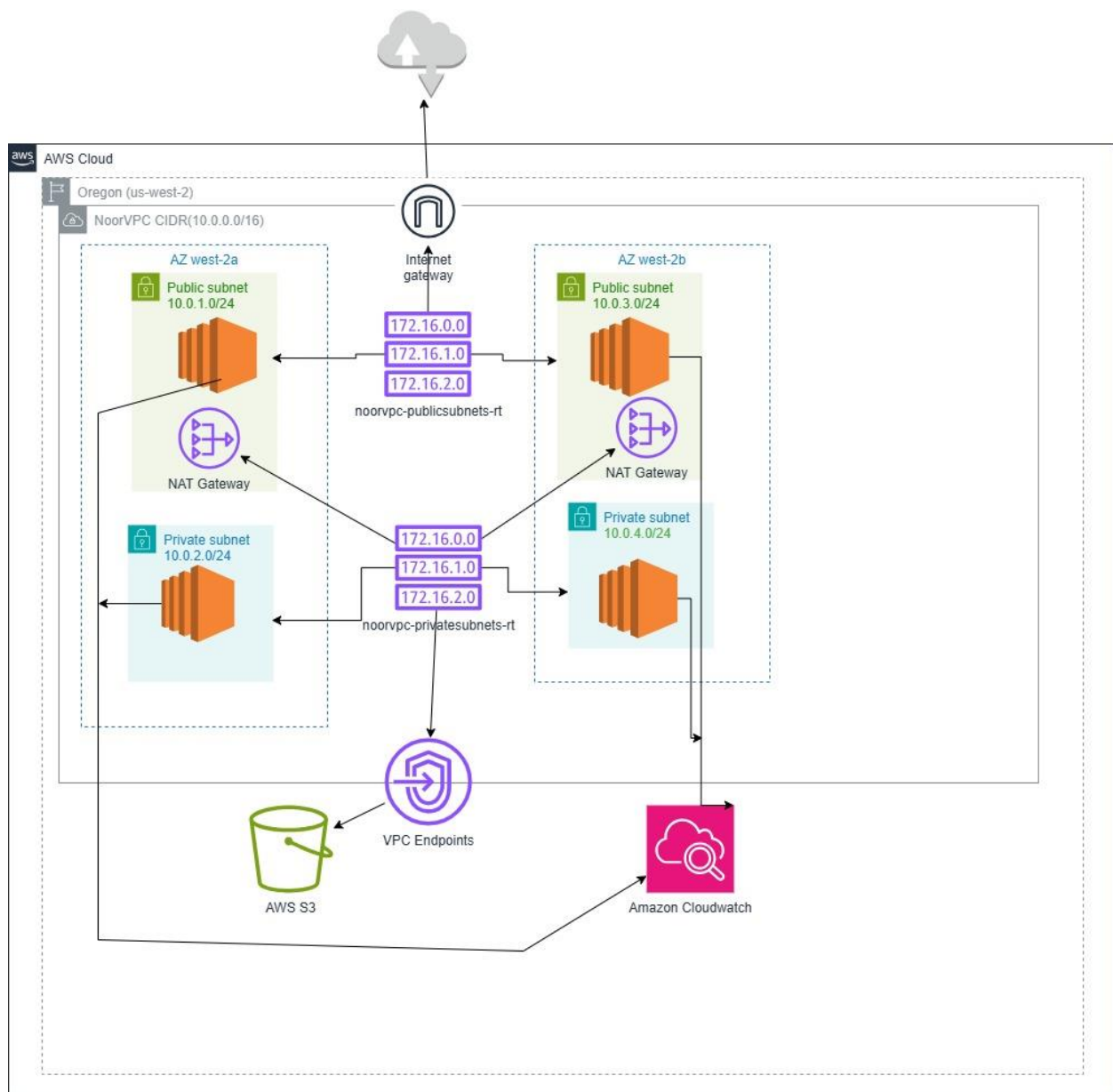


AWS VPC Architecture Implementation Documentation

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.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

Name tag - optional [Info](#)
Creates a tag with a key of 'Name' and a value that you specify.

noor-vpc

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy [Info](#)
Default

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**

Q Name X Q noor-vpc X Remove tag

Add tag

You can add 49 more tags

Cancel Preview code Create VPC

You successfully created vpc-0e761bd1615be0167 / noor-vpc

vpc-0e761bd1615be0167 / noor-vpc [Actions](#)

Details [Info](#)

VPC ID vpc-0e761bd1615be0167	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-04ce359903ec5a75b	Main route table rtb-0347acb9d07e10586
Main network ACL acl-08da2cc01d3ef647b	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 504649076991

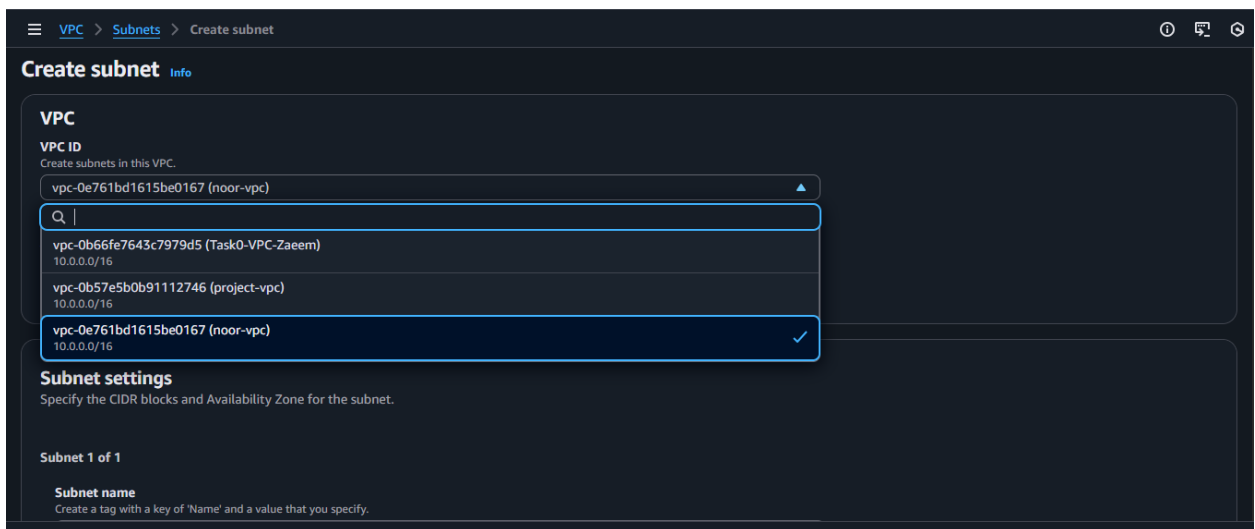
[Resource map](#) [CIDRs](#) [Flow logs](#) [Tags](#) [Integrations](#)

Resource map [Info](#) ☐ Show all details

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.



<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Publi
<input type="checkbox"/>	noorvpc-privatesubnet-01	subnet-0b9dd4e1e59d7e640	Available	vpc-0e761bd1615be0167 noo...	Off
<input type="checkbox"/>	noorvpc-publicsubnet-01	subnet-0ea26f7be6457b59e	Available	vpc-0e761bd1615be0167 noo...	Off
<input type="checkbox"/>	noorvpc-privatesubnet-02	subnet-0015244743832e99a	Available	vpc-0e761bd1615be0167 noo...	Off
<input type="checkbox"/>	noorvpc-publicsubnet-02	subnet-0d2a021971cda2567	Available	vpc-0e761bd1615be0167 noo...	Off

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**.

The screenshot shows the AWS Management Console interface for creating a new internet gateway. The breadcrumb navigation indicates the path: VPC > Internet gateways > Create internet gateway. The page title is 'Create internet gateway' with an 'Info' link. A descriptive text states: 'An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.' Under the 'Internet gateway settings' section, the 'Name tag' field is populated with 'noorvpc-igw'. The 'Tags - optional' section shows a table with one tag: Key 'Name' and Value 'noorvpc-igw'. At the bottom right, there are 'Cancel' and 'Create internet gateway' buttons.

aws [Search] [Alt+S] United States (Oregon) cloudelligent-sandbox [046-4907-8591] CE_Internship/sardar.hassan

VPC > Internet gateways > Create internet gateway

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

noorvpc-igw

Tags - optional

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-igw	Remove

[Add new tag](#)

You can add 49 more tags.

[Cancel](#) [Create internet gateway](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS Management Console interface for attaching an existing internet gateway to a VPC. The breadcrumb navigation indicates the path: VPC > Internet gateways > Attach to VPC (igw-0bbadec5abef73db8). A green notification banner at the top states: 'The following internet gateway was created: igw-0bbadec5abef73db8 - noorvpc-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.' with an 'Attach to a VPC' button. The page title is 'Attach to VPC (igw-0bbadec5abef73db8)' with an 'Info' link. Under the 'VPC' section, the instruction is: 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' The 'Available VPCs' section shows a search bar with 'vpc-0e761bd1615be0167' entered. At the bottom right, there are 'Cancel' and 'Attach internet gateway' buttons.

VPC > Internet gateways > Attach to VPC (igw-0bbadec5abef73db8)

☑ The following internet gateway was created: igw-0bbadec5abef73db8 - noorvpc-igw. You can now attach to a VPC to enable the VPC to communicate with the internet. [Attach to a VPC](#) ✕

Attach to VPC (igw-0bbadec5abef73db8) [Info](#)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

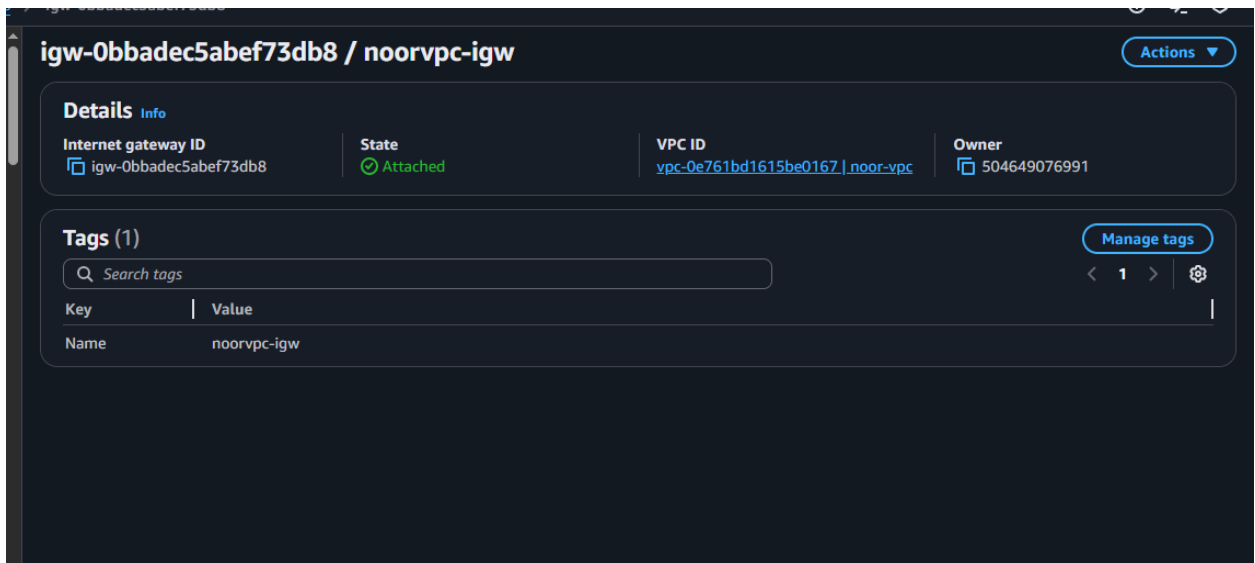
Available VPCs
Attach the internet gateway to this VPC.

vpc-0e761bd1615be0167

▶ AWS Command Line Interface command

[Cancel](#) [Attach internet gateway](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



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).

aws

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

Q Name

Value - optional

Q 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

aws

Search

[Alt+S]

United States (Oregon)

cloudtugent-sandbox (b-046-4907-5591)

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
Q 0.0.0.0/0	Internet Gateway	-	No	CreateRoute
	igw-0bbadec5abef73db8			Remove

Add route

Cancel

Preview

Save changes

tb-029c1c376ee66b8dd

rtb-029c1c376ee66b8dd / noorvpc-publicsubnets-rt

Actions

Details

Info

Route table ID

rtb-029c1c376ee66b8dd

VPC

vpc-0e761bd1615be0167 | noor-vpc

Main

No

Owner ID

504649076991

Explicit subnet associations

-

Edge associations

-

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

Q Name

noorvpc-privatesubnets-rt

Remove

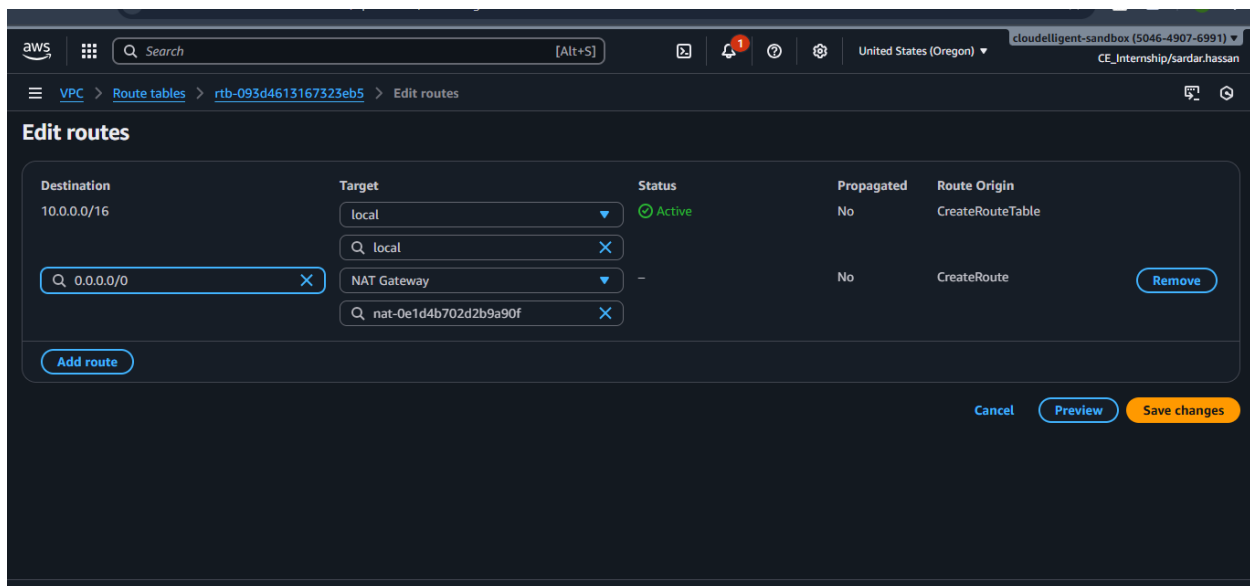
Add new tag

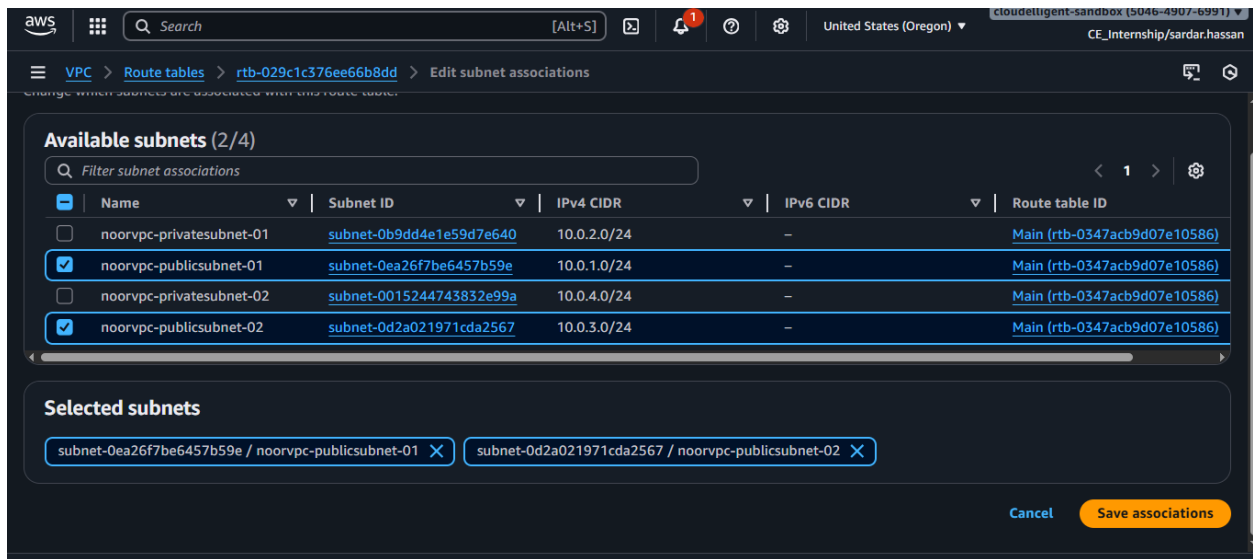
You can add 49 more tags.

CloudShell

Feedback

© 2025 Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences





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.

aws

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.
Select an Elastic IP
Allocate Elastic IP

Additional settings [Info](#)

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.

aws

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](#)

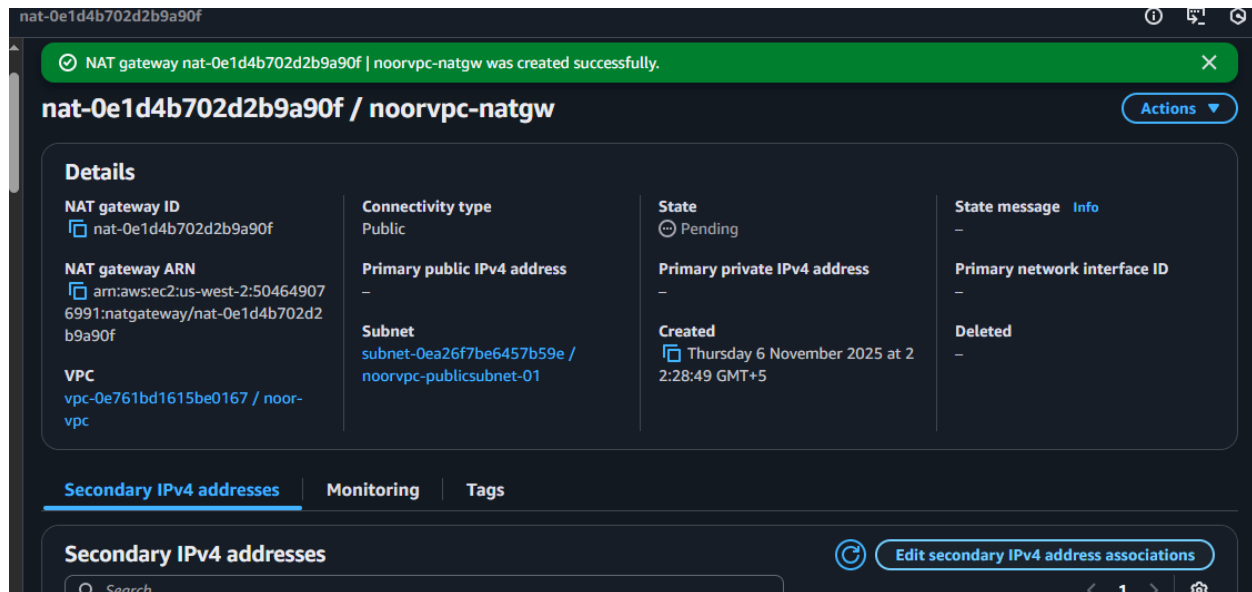
Tags

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.

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.

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.

The screenshot displays the AWS Management Console interface for a security group. The breadcrumb navigation shows 'Groups > sg-0c503daad30c193be - noorvpc-publicsubnets-sg'. The main header for the security group is 'sg-0c503daad30c193be - noorvpc-publicsubnets-sg' with an 'Actions' dropdown menu.

Details

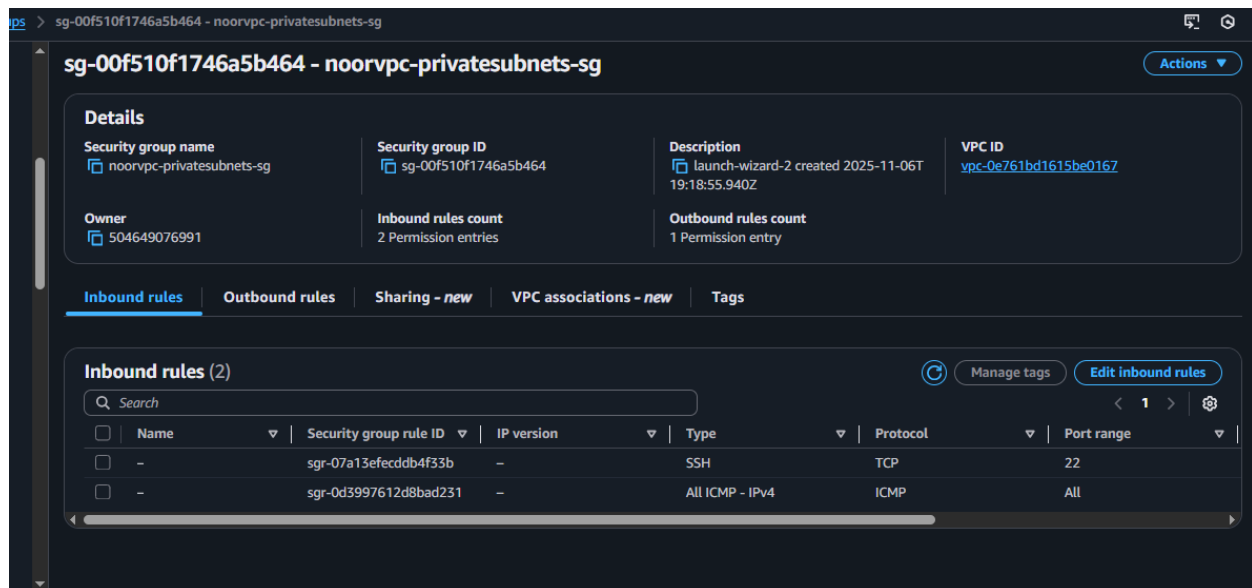
Security group name noorvpc-publicsubnets-sg	Security group ID sg-0c503daad30c193be	Description launch-wizard-2 created 2025-11-06T 18:11:03.964Z	VPC ID vpc-0e761bd1615be0167
Owner 504649076991	Inbound rules count 4 Permission entries	Outbound rules count 1 Permission entry	

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

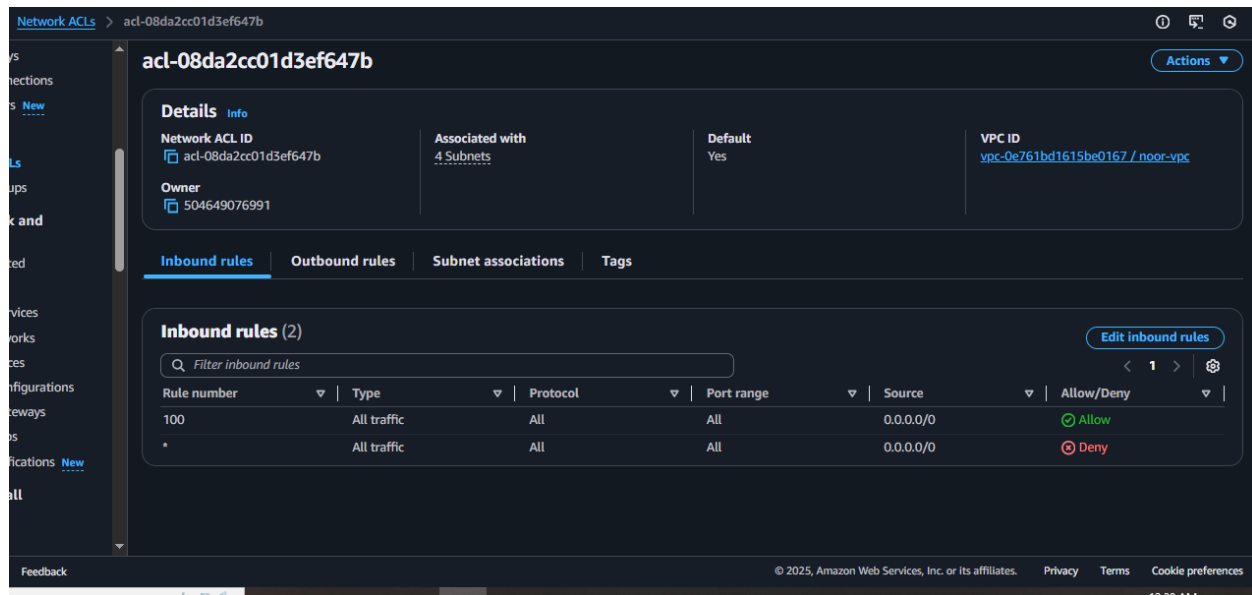
Inbound rules (4) [Manage tags] [Edit inbound rules]

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-02ebd802c363f8358	IPv4	HTTP	TCP	80
<input type="checkbox"/>	-	sgr-02e3aa6e7e4ec0414	IPv4	All ICMP - IPv4	ICMP	All
<input type="checkbox"/>	-	sgr-0148ad5e58640705f	IPv4	SSH	TCP	22
<input type="checkbox"/>	-	sgr-030dc288eea8e47bc	IPv4	HTTPS	TCP	443

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



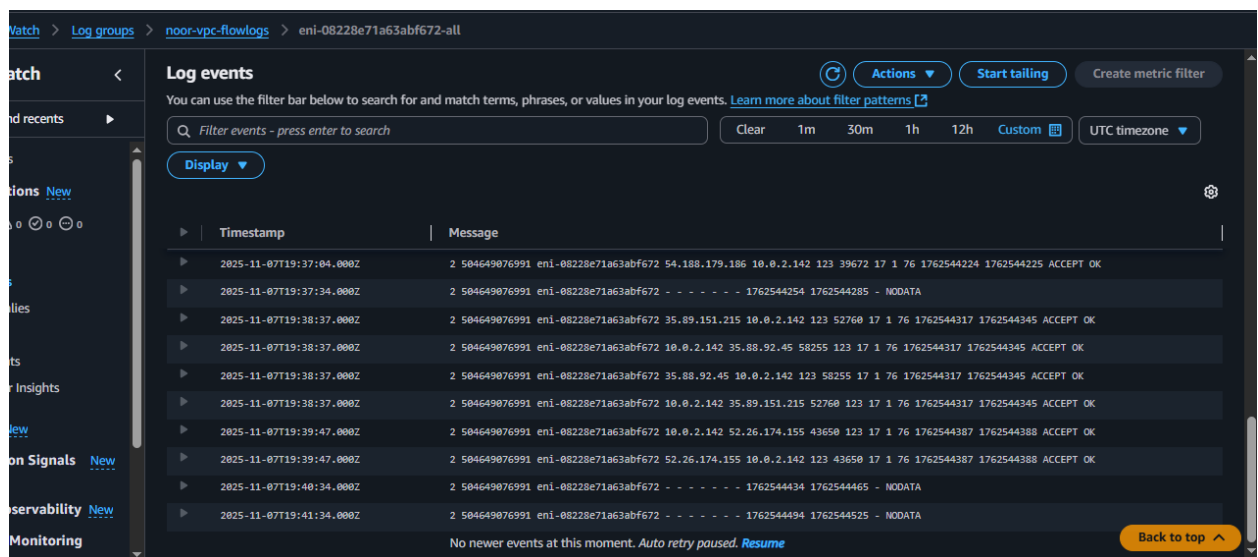
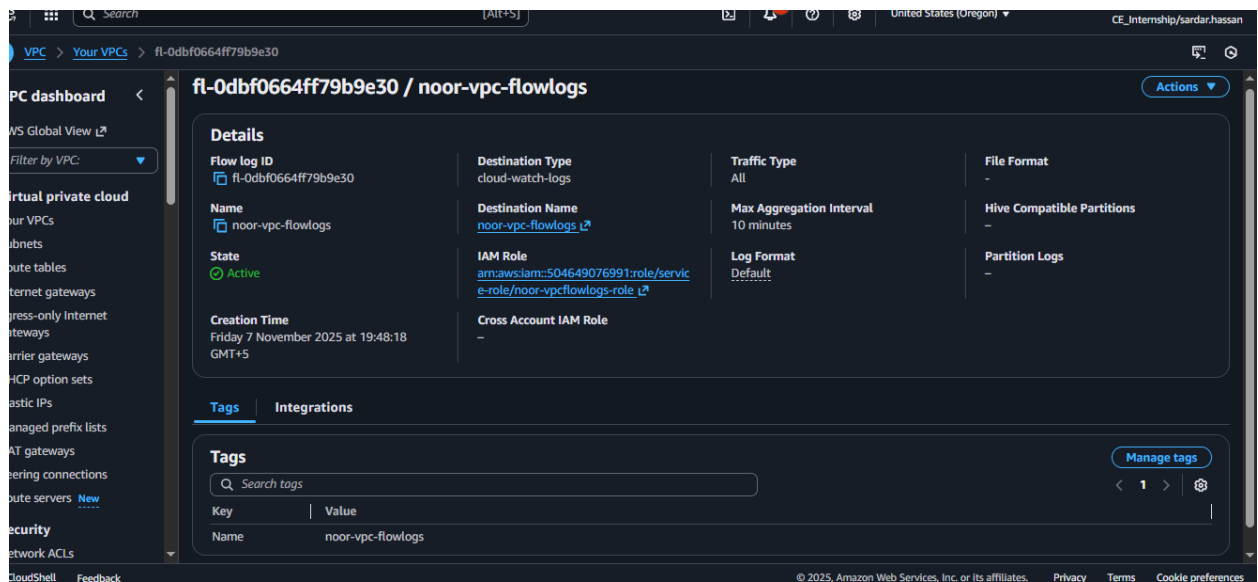
- **Network ACLs:**
 - Public Subnets: Allowed inbound/outbound for HTTP, HTTPS, SSH, ICMP.
 - Private Subnets: Allowed outbound for HTTP/HTTPS only.



8. Enable VPC Flow Logs

Steps Performed:

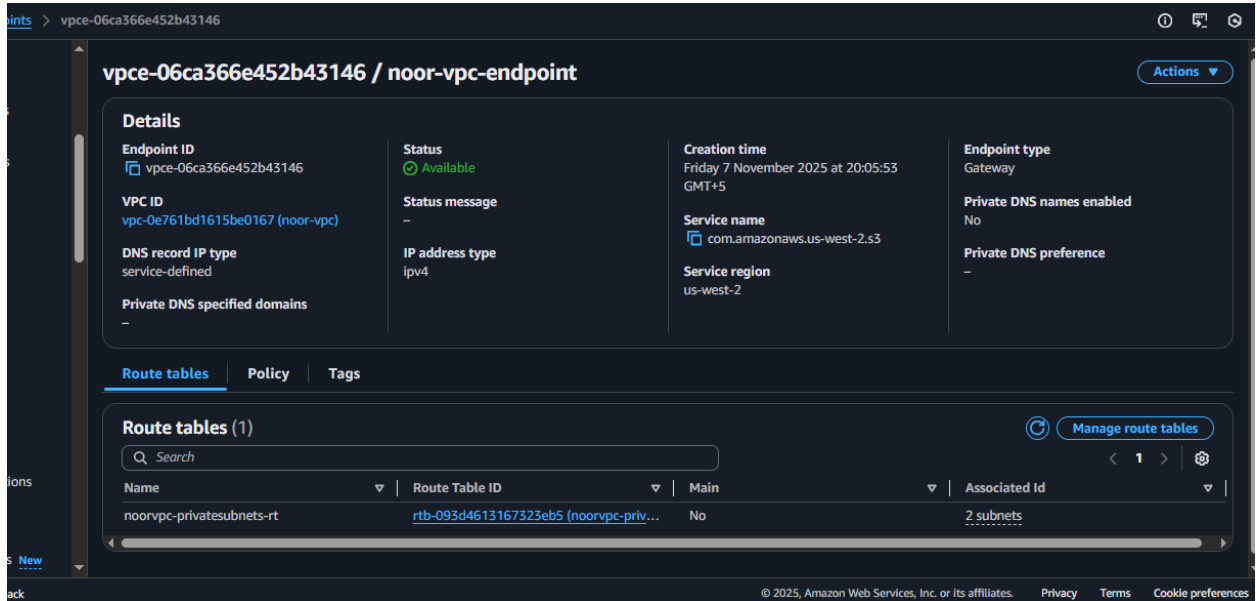
1. Opened **VPC** → **Flow Logs** → **Create Flow Log**.
2. Selected **VPC NoorVPC**.
3. Destination: **CloudWatch Logs Group**.
4. IAM Role: Configured permissions for log delivery.
5. Verified log entries in CloudWatch.



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.



```

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-krygjjx35knte
2025-11-05 06:53:58 amplify-d1zma1x1ek2tkk-ma-amplifydataamplifycodege-3gewsmdu6mq1
2025-11-06 00:40:23 amplify-d1zma1x1ek2tkk-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-tesst
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 19:58:19 aws-testing-0016638

```

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**.

[illegible]

~~East logn. mid Nov 0 21.48.54 2025 110m 119.75.100.256 1 04 3 048 0 3 443~~

[illegible]

5 3 6 40 6 3 4 13 74 3 3

```
[ec2-user@ip-10-0-2-142 ~]$ ping google.com
```

```
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-krygjjx35knte
2025-11-05 06:53:58 amplify-d1zma1x1ek2tkk-ma-amplifydataamplifycodege-3gewsmdu6mq1
2025-11-06 00:40:23 amplify-d1zma1x1ek2tkk-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-tesst
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-m6nnipv1ndx4
2025-10-27 19:59:19 aws-testing-0016639
```

CloudWatch

Log groups

noor-vpc-flowlogs

eni-02542675bbb4cd7cf-all

Favorites and recents

Dashboards

AI Operations

Alarms

Logs

Log groups

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

Metrics

Application Signals (APM)

GenAI Observability

Network Monitoring

Log events

Actions

Start tailing

Create metric filter

You can use the filter bar below to search for and match terms, phrases, or values in your log events.

Filter events - press enter to search

Clear

1m

30m

1h

12h

Custom

UTC timezone

Display

Timestamp	Message
2025-11-07T17:16:35.000Z	2 504649076991 eni-02542675bbb4cd7cf 35.203.210.217 10.0.1.241 53781 9468 6 1 44 1762535795 1762535808 ACCEPT OK
2025-11-07T17:16:35.000Z	2 504649076991 eni-02542675bbb4cd7cf 147.185.132.53 10.0.1.241 56256 26789 6 1 44 1762535795 1762535808 ACCEPT OK
2025-11-07T17:16:38.000Z	2 504649076991 eni-02542675bbb4cd7cf 179.43.169.98 10.0.1.241 47450 80 6 1 40 1762535798 1762535800 ACCEPT OK
2025-11-07T17:16:38.000Z	2 504649076991 eni-02542675bbb4cd7cf 10.0.1.241 142.251.33.78 0 0 1 34 2056 1762535798 1762535800 ACCEPT OK
2025-11-07T17:16:52.000Z	2 504649076991 eni-02542675bbb4cd7cf 27.223.85.234 10.0.1.241 52857 8538 6 1 40 1762535812 1762535826 ACCEPT OK
2025-11-07T17:16:52.000Z	2 504649076991 eni-02542675bbb4cd7cf 10.0.2.142 10.0.1.241 0 0 1 7 588 1762535812 1762535826 ACCEPT OK
2025-11-07T17:16:56.000Z	2 504649076991 eni-02542675bbb4cd7cf 45.79.82.114 10.0.1.241 48290 8388 6 1 44 1762535816 1762535817 ACCEPT OK
2025-11-07T17:17:01.000Z	2 504649076991 eni-02542675bbb4cd7cf 10.0.1.241 10.0.2.142 0 0 1 10 840 1762535821 1762535831 ACCEPT OK
2025-11-07T17:17:01.000Z	2 504649076991 eni-02542675bbb4cd7cf 87.251.67.50 10.0.1.241 58598 11950 6 1 40 1762535821 1762535831 ACCEPT OK
2025-11-07T17:17:15.000Z	2 504649076991 eni-02542675bbb4cd7cf 148.113.214.212 10.0.1.241 55402 3128 6 1 52 1762535835 1762535836 ACCEPT OK

No newer events at this moment. Auto retry paused. Resume