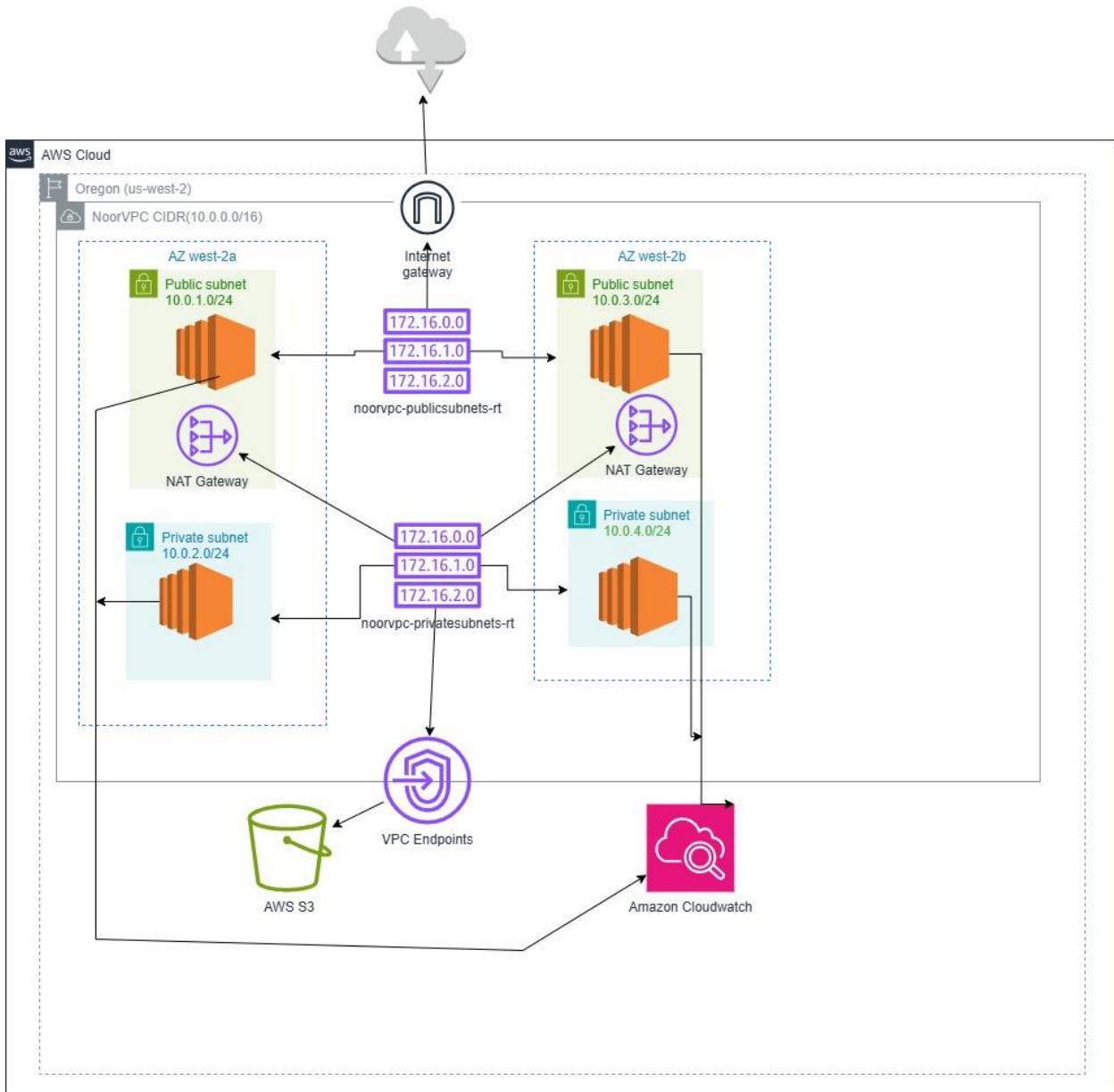


# AWS VPC Architecture Implementation Documentation

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

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

**IPv4 CIDR**  
  
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](#)

**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
<input type="text" value="Name"/>	<input type="text" value="noor-vpc"/> <a href="#">Remove tag</a>

[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](#)

<b>VPC ID</b> <input type="text" value="vpc-0e761bd1615be0167"/>	<b>State</b> <input checked="" type="radio"/> <b>Available</b>	<b>Block Public Access</b> <input checked="" type="radio"/> <b>Off</b>	<b>DNS hostnames</b> <b>Disabled</b>
<b>DNS resolution</b> <b>Enabled</b>	<b>Tenancy</b> <b>default</b>	<b>DHCP option set</b> <b>dopt-04ce359903ec5a75b</b>	<b>Main route table</b> <b>rtb-0347acb9d07e10586</b>
<b>Main network ACL</b> <a href="#">acl-08da2cc01d3ef647b</a>	<b>Default VPC</b> <b>No</b>	<b>IPv4 CIDR</b> <b>10.0.0.0/16</b>	<b>IPv6 pool</b> <b>-</b>
<b>IPv6 CIDR (Network border group)</b> <b>-</b>	<b>Network Address Usage metrics</b> <b>Disabled</b>	<b>Route 53 Resolver DNS Firewall rule groups</b> <b>-</b>	<b>Owner ID</b> <input type="text" value="504649076991"/>

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

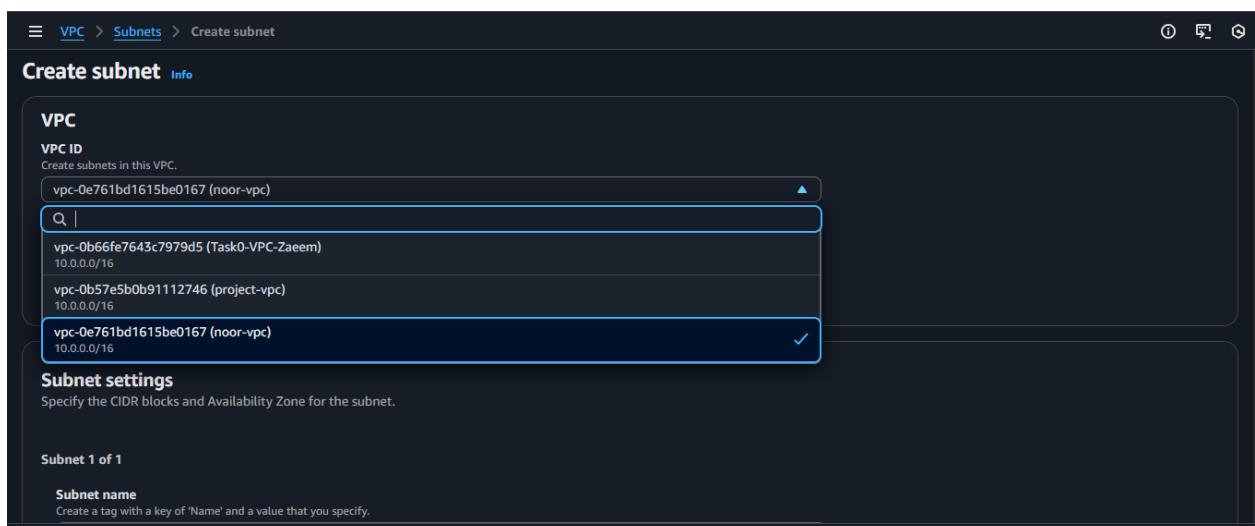
**Resource map** [Info](#) [Show all details](#)

---

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

### Steps Performed:

1. Created **4 subnets** under the VPC:
  - o **Noorvpc-publicsubnet-01:** 10.0.1.0/24 (AZ-1)
  - o **Noorvpc-privatesubnet-01:** 10.0.2.0/24 (AZ-1)
  - o **Noorvpc-publicsubnet-02:** 10.0.3.0/24 (AZ-2)
  - o **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.



The screenshot shows the 'Create subnet' wizard in the AWS VPC console. In the 'VPC' section, the 'VPC ID' dropdown is set to 'noor-vpc'. Below it, a list of existing subnets is shown, with 'noorvpc-publicsubnet-01' selected. In the 'Subnet settings' section, 'Subnet 1 of 1' is listed with a 'Subnet name' field containing 'noorvpc-publicsubnet-01'. The 'Block Public' checkbox is unchecked.

Name	Subnet ID	State	VPC	Block Public
noorvpc-privatesubnet-01	subnet-0b9dd4e1e59d7e640	Available	vpc-0e761bd1615be0167   noo...	Off
noorvpc-publicsubnet-01	subnet-0ea26f7be6457b59e	Available	vpc-0e761bd1615be0167   noo...	Off
noorvpc-privatesubnet-02	subnet-0015244743832e99a	Available	vpc-0e761bd1615be0167   noo...	Off
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**.

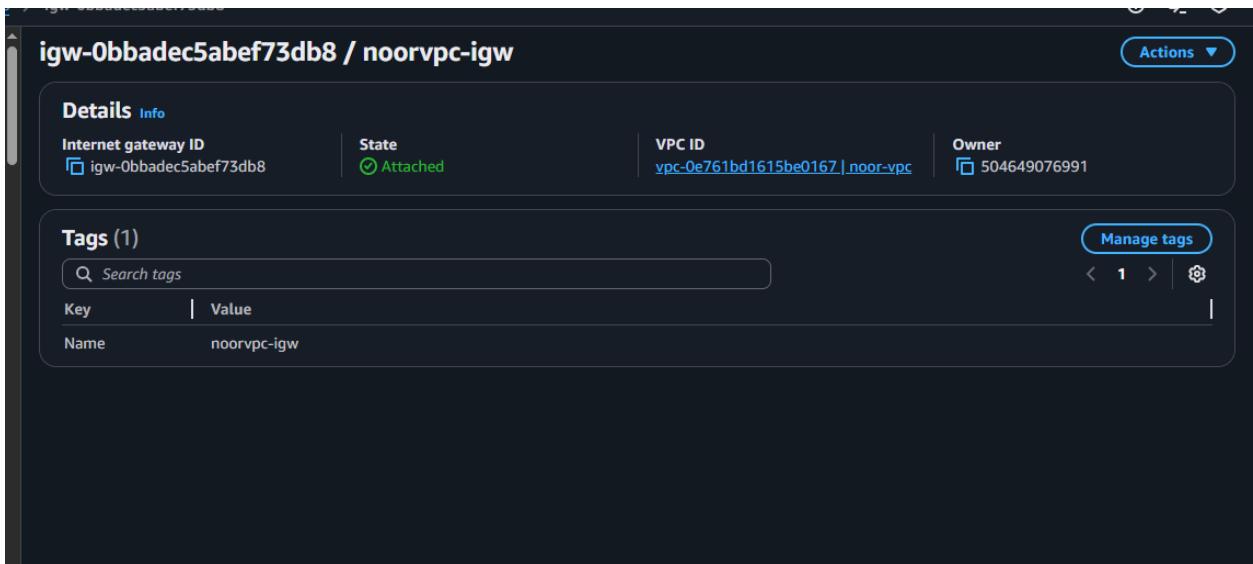
The screenshot shows two sequential steps in the AWS VPC console.

**Step 1: Create internet gateway**

The user is creating a new Internet Gateway. In the "Name tag" section, they have entered "noorvpc-igw". Under "Tags - optional", they have added a tag with the key "Name" and value "noorvpc-igw". The "Create internet gateway" button is visible at the bottom right.

**Step 2: Attach to VPC**

The user is attaching the previously created Internet Gateway (igw-0bbadec5abef73db8) to a VPC. They have selected the VPC with ID "vpc-0e761bd1615be0167". The "Attach to a VPC" button is visible at the bottom right.



## 4. Create Route Tables

### Steps Performed:

1. Created two route tables: (i.e **noorvpc-publicsubnets-rt** and **noorvpc-privatesubnets-rt**
  - o **Public Route Table**
    - Added route: 0.0.0.0/0 → Internet Gateway (NoorVPC-IGW).
    - Associated with both public subnets.
  - o **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	Value - optional
<input type="text" value="Name"/> <span>X</span>	<input type="text" value="noorvpc-publicsubnets-rt"/> <span>X</span> <span>Remove</span>

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) ▾ 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	
0.0.0.0/0	local	-	No	CreateRoute	<span>Remove</span>
0.0.0.0/0	Internet Gateway	-	No	CreateRoute	<span>Remove</span>
0.0.0.0/0	igw-0bbadec5abef73db8	-	No	CreateRoute	<span>Remove</span>

Add route Cancel Preview Save changes

tb-029c1c376ee66b8dd

rtb-029c1c376ee66b8dd / noorvpc-publicsubnets-rt Actions ▾

**Details** Info

Route table ID	Main	Explicit subnet associations	Edge associations
<a href="#">rtb-029c1c376ee66b8dd</a>	<input type="checkbox"/> No	-	-
VPC	Owner ID		
vpc-0e761bd1615be0167   noor-vpc	<a href="#">504649076991</a>		

**Routes** Subnet associations Edge associations Route propagation Tags

**Routes (2)** Both Edit routes

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	<a href="#">igw-0bbadec5abef73db8</a>	<span>Active</span>	No	Create Route
10.0.0.0/16	local	<span>Active</span>	No	Create Route Table

The screenshot shows the 'Create route table' wizard in the AWS VPC service. The top navigation bar includes 'VPC', 'Route tables', and 'Create route table'. A sub-header 'Route table settings' is followed by a 'Name - optional' field containing 'noorvpc-privatesubnets-rt'. The 'VPC' section shows 'vpc-0e761bd1615be0167 (noor-vpc)' selected. Below this is a 'Tags' section with a single tag 'Name: noorvpc-privatesubnets-rt'. A note at the bottom says 'You can add 49 more tags.'

AWS VPC Edit routes

Destination Target Status Propagated Route Origin

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
Q 0.0.0.0/0	X			
	NAT Gateway	-	No	CreateRoute
	nat-0e1d4b702d2b9a90f	X		

Add route Remove 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

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

The screenshot shows the AWS VPC Route Tables interface. The top navigation bar includes the AWS logo, search bar, and tabs for 'Route tables' and 'rtb-029c1c376ee66b8dd'. The main content area is titled 'Edit subnet associations' under 'Available subnets (2/4)'. A table lists four subnets: 'noorvpc-privatesubnet-01', 'noorvpc-publicsubnet-01', 'noorvpc-privatesubnet-02', and 'noorvpc-publicsubnet-02'. The first two subnets have checkboxes checked, indicating they are selected. The 'Selected subnets' section contains two entries: 'subnet-0ea26f7be6457b59e / noorvpc-publicsubnet-01' and 'subnet-0d2a021971cda2567 / noorvpc-publicsubnet-02'. At the bottom right are 'Cancel' and 'Save associations' buttons.

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
noorvpc-privatesubnet-01	subnet-0b9dd4e1e59d7e640	10.0.2.0/24	-	Main (rtb-0347acb9d07e10586)
noorvpc-publicsubnet-01	subnet-0ea26f7be6457b59e	10.0.1.0/24	-	Main (rtb-0347acb9d07e10586)
noorvpc-privatesubnet-02	subnet-0015244743832e99a	10.0.4.0/24	-	Main (rtb-0347acb9d07e10586)
noorvpc-publicsubnet-02	subnet-0d2a021971cda2567	10.0.3.0/24	-	Main (rtb-0347acb9d07e10586)

## 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**:
  - o Added route: 0.0.0.0/0 → NAT Gateway.
  - o Associated it with both private subnets.

Screenshot of the AWS VPC NAT gateways creation page.

**NAT gateway settings**

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.  
  
The name can be up to 256 characters long.

**Subnet**  
Select a subnet in which to create the NAT gateway.

**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.  
 [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

Screenshot of the AWS VPC NAT gateways creation page.

**NAT gateway settings**

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.  
  
The name can be up to 256 characters long.

**Subnet**  
Select a subnet in which to create the NAT gateway.

**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.  
 [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

NAT gateway nat-0e1d4b702d2b9a90f | noorvpc-natgw was created successfully.

**nat-0e1d4b702d2b9a90f / noorvpc-natgw**

**Details**

NAT gateway ID nat-0e1d4b702d2b9a90f	Connectivity type Public	State Pending	State message Info
NAT gateway ARN arn:aws:ec2:us-west-2:504649076991:natgateway/nat-0e1d4b702d2b9a90f	Primary public IPv4 address -	Primary private IPv4 address -	Primary network interface ID -
VPC vpc-0e761bd1615be0167 / noorvpc	Subnet subnet-0ea26f7be6457b59e / noorvpc-publicsubnet-01	Created Thursday 6 November 2025 at 2:28:49 GMT+5	Deleted -

**Secondary IPv4 addresses** | Monitoring | Tags

**Secondary IPv4 addresses**

Search

Edit secondary IPv4 address associations

## 6. Launch EC2 Instances

### Steps Performed:

1. Launched:
  - o **Public EC2 Instance:**
    - Subnet: Public Subnet-A
    - Security Group: Allow SSH (port 22) and ICMP (ping) from anywhere.
  - o **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 <a href="#">i-0a00f26b4a73f2ad4</a>	Public IPv4 address <a href="#">34.223.231.5</a>   open address	Private IPv4 addresses <a href="#">10.0.1.247</a>
IPv6 address -	Instance state <span style="color: green;">Running</span>	Public DNS -
Hostname type IP name: ip-10-0-1-247.us-west-2.compute.internal	Private IP DNS name (IPv4 only) <a href="#">ip-10-0-1-247.us-west-2.compute.internal</a>	
Answer private resource DNS name -	Instance type <a href="#">t3.micro</a>	Elastic IP addresses -
Auto-assigned IP address <a href="#">34.223.231.5 [Public IP]</a>	VPC ID <a href="#">vpc-0e761bd1615be0167 (noor-vpc)</a>	AWS Compute Optimizer finding No recommendations available for this instance.
IAM Role -	Subnet ID <a href="#">subnet-0ea26f7be6457b59e (noorvpc-publicsubnet-01)</a>	Auto Scaling Group name -
IMDSv2 Required	Instance ARN <a href="#">arn:aws:ec2:us-west-2:504649076991:instance/i-0a00f26b4a73f2ad4</a>	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 <a href="#">i-0b2330c84e38abb3e</a>	Public IPv4 address -	Private IPv4 addresses <a href="#">10.0.2.142</a>
IPv6 address -	Instance state <span style="color: green;">Running</span>	Public DNS -
Hostname type IP name: ip-10-0-2-142.us-west-2.compute.internal	Private IP DNS name (IPv4 only) <a href="#">ip-10-0-2-142.us-west-2.compute.internal</a>	
Answer private resource DNS name -	Instance type <a href="#">t3.micro</a>	Elastic IP addresses -
Auto-assigned IP address -	VPC ID <a href="#">vpc-0e761bd1615be0167 (noor-vpc)</a>	AWS Compute Optimizer finding No recommendations available for this instance.
IAM Role <a href="#">noor-ec2-s3-role</a>	Subnet ID <a href="#">subnet-0b9dd4e1e59d7e640 (noorvpc-privatesubnet-01)</a>	Auto Scaling Group name -
IMDSv2 Required	Instance ARN <a href="#">arn:aws:ec2:us-west-2:504649076991:instance/i-0b2330c84e38abb3e</a>	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
~~   V~' '-->
~~
~~ .___. / \
~~  _/ / /
~~ /m/ '
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.

The screenshot shows the AWS Security Groups console. The top navigation bar includes 'Groups' and the specific security group name 'sg-0c503daad30c193be - noorvpc-publicsubnets-sg'. The main area displays the 'Details' section with fields: Security group name (noorvpc-publicsubnets-sg), Security group ID (sg-0c503daad30c193be), Description (launch-wizard-2 created 2025-11-06T18:11:03.964Z), VPC ID (vpc-0e761bd1615be0167), Owner (504649076991), Inbound rules count (4 Permission entries), and Outbound rules count (1 Permission entry). Below the details, there are tabs for 'Inbound rules', 'Outbound rules', 'Sharing - new', 'VPC associations - new', and 'Tags'. The 'Inbound rules' tab is selected, showing a table with four rows of rules. The columns include Name, Security group rule ID, IP version, Type, Protocol, and Port range. The rules are: 1. sgr-02ebd802c363f8358 (IPv4, HTTP, TCP, 80); 2. sgr-02e3aa6e7e4ec0414 (IPv4, All ICMP - IPv4, ICMP, All); 3. sgr-0148ad5e58640705f (IPv4, SSH, TCP, 22); 4. sgr-030dc288eea8e47bc (IPv4, HTTPS, TCP, 443). There are also buttons for 'Manage tags' and 'Edit inbound rules'.

sg-00f510f1746a5b464 - noorvpc-privatesubnets-sg

**Details**

Security group name sg-00f510f1746a5b464	Security group ID sg-00f510f1746a5b464	Description launch-wizard-2 created 2025-11-06T19:18:55.940Z	VPC ID vpc-0e761bd1615be0167
Owner 504649076991	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)**

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-07a13efecddbf33b	-	SSH	TCP	22
-	sgr-0d3997612d8bad231	-	All ICMP - IPv4	ICMP	All

- **Network ACLs:**

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

Network ACLs > acl-08da2cc01d3ef647b

**Details**

Network ACL ID acl-08da2cc01d3ef647b	Associated with 4 Subnets	Default Yes	VPC ID vpc-0e761bd1615be0167 / noor-vpc
Owner 504649076991			

**Inbound rules** | **Outbound rules** | **Subnet associations** | **Tags**

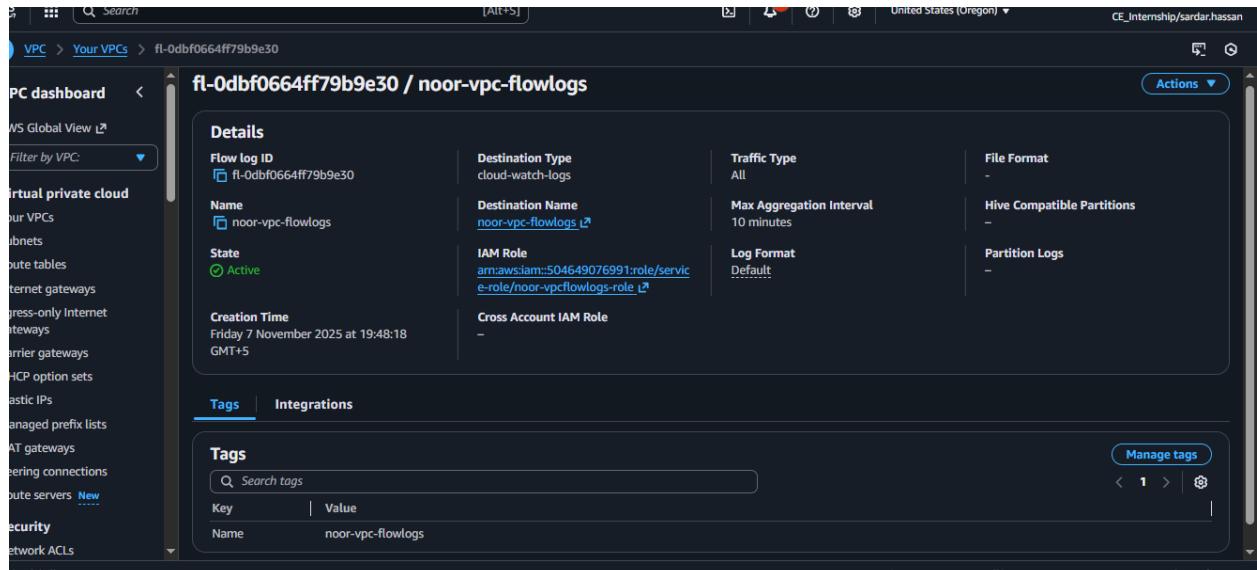
**Inbound rules (2)**

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

## 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.



The screenshot shows the AWS VPC Flow Logs configuration page. The flow log details are as follows:

- Flow log ID:** fl-0dbf0664ff79b9e30
- Name:** noor-vpc-flowlogs
- State:** Active
- Destination Type:** cloud-watch-logs
- Destination Name:** noor-vpc-flowlogs
- IAM Role:** arn:aws:iam::504649076991:role/service-role/noor-vpcflowlogs-role
- Traffic Type:** All
- Max Aggregation Interval:** 10 minutes
- Log Format:** Default
- File Format:** -
- Hive Compatible Partitions:** -
- Partition Logs:** -
- Cross Account IAM Role:** -

The CloudWatch Logs group configuration page shows log events for the eni-08228e71a63abf672 interface. The log events table has columns for Timestamp and Message. Some sample log entries are:

Timestamp	Message
2025-11-07T19:37:04.000Z	2 504649076991 eni-08228e71a63abf672 54.188.179.186 10.0.2.142 123 39672 17 1 76 1762544224 1762544225 ACCEPT OK
2025-11-07T19:37:34.000Z	2 504649076991 eni-08228e71a63abf672 - - - - - 1762544254 1762544285 - NODATA
2025-11-07T19:38:37.000Z	2 504649076991 eni-08228e71a63abf672 35.89.151.215 10.0.2.142 123 52760 17 1 76 1762544317 1762544345 ACCEPT OK
2025-11-07T19:38:37.000Z	2 504649076991 eni-08228e71a63abf672 18.0.2.142 35.88.92.45 58255 123 17 1 76 1762544317 1762544345 ACCEPT OK
2025-11-07T19:38:37.000Z	2 504649076991 eni-08228e71a63abf672 10.0.2.142 123 58255 17 1 76 1762544317 1762544345 ACCEPT OK
2025-11-07T19:38:37.000Z	2 504649076991 eni-08228e71a63abf672 35.89.151.215 52.26.174.155 10.0.2.142 123 52760 17 1 76 1762544317 1762544345 ACCEPT OK
2025-11-07T19:39:47.000Z	2 504649076991 eni-08228e71a63abf672 18.0.2.142 52.26.174.155 10.0.2.142 123 43650 17 1 76 1762544387 1762544388 ACCEPT OK
2025-11-07T19:40:34.000Z	2 504649076991 eni-08228e71a63abf672 - - - - - 1762544434 1762544465 - NODATA
2025-11-07T19:41:34.000Z	2 504649076991 eni-08228e71a63abf672 - - - - - 1762544494 1762544525 - NODATA

## 9. Create VPC Endpoints

### Steps Performed:

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

**vpce-06ca366e452b43146 / noor-vpc-endpoint**

Details		Actions	
Endpoint ID <a href="#">vpce-06ca366e452b43146</a>	Status <span style="color: green;">Available</span>	Creation time Friday 7 November 2025 at 20:05:53 GMT+5	Endpoint type Gateway
VPC ID <a href="#">vpc-0e761bd1615be0167 (noor-vpc)</a>	Status message -	Service name <a href="#">com.amazonaws.us-west-2.s3</a>	Private DNS names enabled No
DNS record IP type service-defined	IP address type ipv4	Service region us-west-2	Private DNS preference -
Private DNS specified domains -			

**Route tables (1)**

Name	Route Table ID	Main	Associated Id
noorvpc-privatesubnet-rt	<a href="#">rtb-093d4613167323eb5 (noorvpc-priv...)</a>	No	2 subnets

```

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-bquouqh22d1zo
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-test-ing-0016639

```

## 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-xrzjaf5ebnj
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-m6nnipvlnidx
2025-10-27 19:59:19 aws-taitting_0016639

```

The screenshot shows the AWS CloudWatch Logs interface. The left sidebar navigation includes 'CloudWatch' (selected), 'Favorites and recents', 'Dashboards', 'AI Operations', 'Alarms', 'Logs' (selected), 'Log groups' (selected), 'Log Anomalies', 'Live Tail', 'Logs Insights', 'Contributor Insights', 'Metrics', 'Application Signals (APM)', 'GenAI Observability', and 'Network Monitoring'. The main content area displays 'Log events' for the 'noor-vpc-flowlogs' log group. It features a search bar, filter buttons for time intervals (1m, 30m, 1h, 12h, Custom, UTC timezone), and a 'Display' dropdown. A table lists log entries with columns for 'Timestamp' and 'Message'. Each entry contains a timestamp and a detailed log message. At the bottom, a note says 'No newer events at this moment. Auto retry paused. Resume'.

Timestamp	Message
2025-11-07T17:16:35.000Z	2 504649076991 eni-02542675bbb4cd7cf 35.283.210.217 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 88 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 2856 1762535798 1762535800 ACCEPT OK
2025-11-07T17:16:52.000Z	2 504649076991 eni-02542675bbb4cd7cf 27.223.85.234 10.0.1.241 52057 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 45.79.62.114 10.0.1.241 48290 6388 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 16 846 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