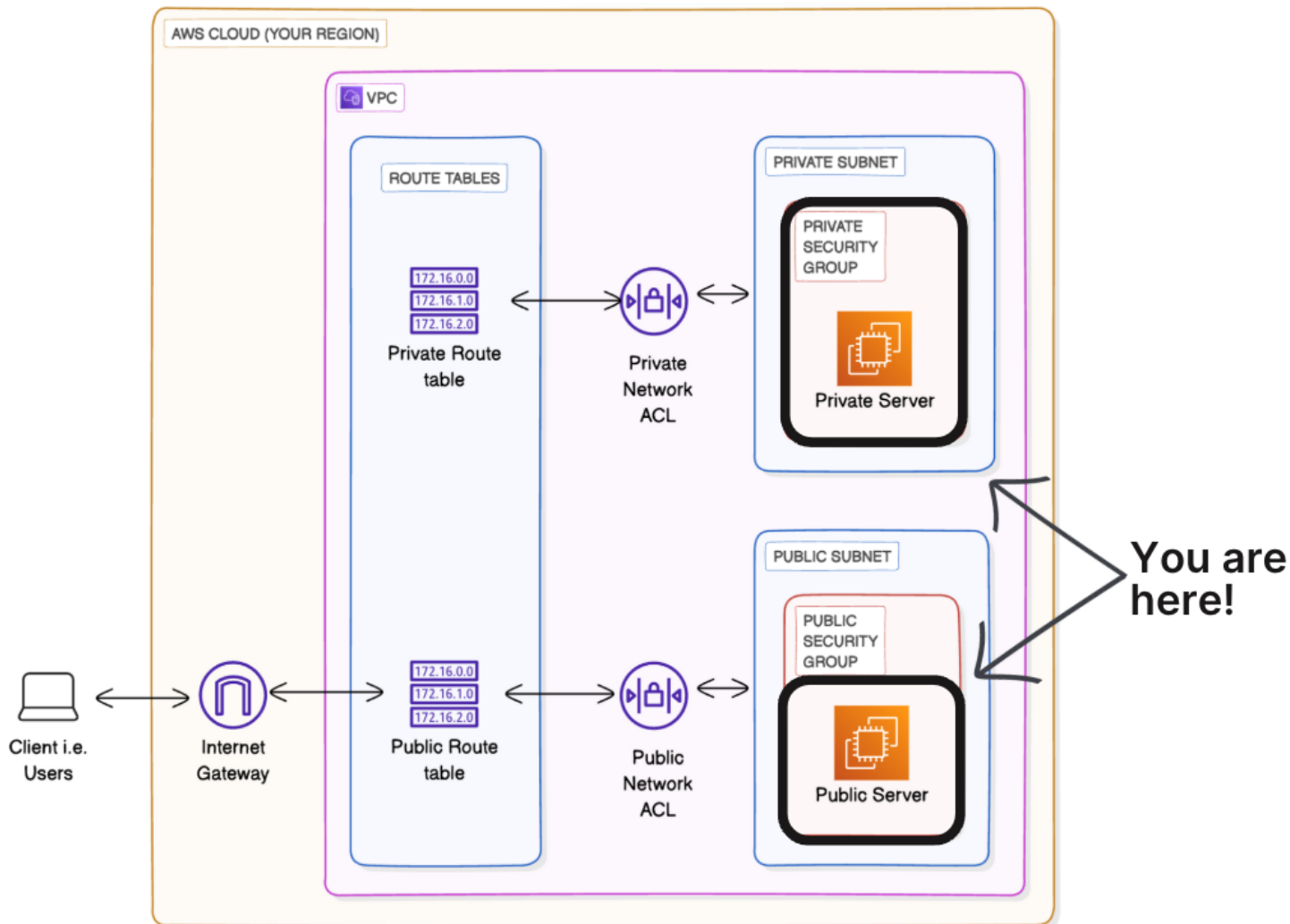


## LAUNCHING VPC RESOURCES - STEP-BY-STEP DOCUMENTATION



This documentation provides a comprehensive, step-by-step process for launching resources into your Amazon VPC. It builds on the earlier projects 'Build a Virtual Private Cloud', 'VPC Traffic Flow and Security', and 'Creating a Private Subnet'. This guide includes both the foundational steps and the new tasks required to launch EC2 instances in public and private subnets, and to use the VPC wizard.

## Step 1: Create a VPC

## Set up a new Virtual Private Cloud in AWS.

### Actions:

- - Log in to AWS Management Console.
- - Search for 'VPC' in the search bar and select it.
- - In the left-hand navigation pane, choose 'Your VPCs'.
- - Click 'Create VPC'.
- - Select 'VPC only' option.
- - Enter a Name tag (e.g., NextWork VPC).
- - Enter an IPv4 CIDR block (e.g., 10.0.0.0/16).
- - Click 'Create VPC' to finalize.

aws [Search] [Alt+S] Asia Pacific (Mumbai) Account ID: 9443-6243-3406 Alex

VPC > Your VPCs > vpc-09e17cc4217fd6833

### VPC dashboard < vpc-09e17cc4217fd6833 / NextWork VPC

Actions

**Details** info

<b>VPC ID</b> vpc-09e17cc4217fd6833	<b>State</b> Available	<b>Block Public Access</b> Off	<b>DNS hostnames</b> Disabled
<b>DNS resolution</b> Enabled	<b>Tenancy</b> default	<b>DHCP option set</b> dopt-019ae45123624041f	<b>Main route table</b> rtb-090a8216aa87494dc
<b>Main network ACL</b> acl-02cda9780bb917383	<b>Default VPC</b> No	<b>IPv4 CIDR</b> 10.0.0.0/16	<b>IPv6 pool</b> -
<b>IPv6 CIDR (Network border group)</b> -	<b>Network Address Usage metrics</b> Disabled	<b>Route 53 Resolver DNS Firewall rule groups</b> -	<b>Owner ID</b> 944362433406

**Resource map** info

Subnets (0)  
Subnets within this VPC

Route tables (1)  
Route network traffic to resources  
rtb-090a8216aa87494dc

Network Connections (0)  
Connections to other networks

Show all details

CloudShell Feedback

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

## Step 2: Create Subnets

Divide your VPC into subnets for better resource organization.

### Actions:

- From the VPC Dashboard, select 'Subnets' in the navigation pane.
- Click 'Create subnet'.
- Choose the VPC you just created (NextWork VPC).
- Enter a Subnet name (e.g., Public 1).
- Select an Availability Zone.
- Enter an IPv4 CIDR block for the subnet (e.g., 10.0.0.0/24).
- Click 'Create subnet'.
- Select your new subnet and go to 'Edit subnet settings'.
- Enable 'Auto-assign public IPv4 address'.
- Click 'Save' to apply changes.
- Repeat the process to create a private subnet (e.g., 10.0.1.0/24) without enabling public IPs.

aws [Search] [Alt+S] Asia Pacific (Mumbai) Account ID: 9443-6243-3406 Alex

VPC > Subnets

Filter by VPC

### Subnets (5) info

Find subnets by attribute or tag

	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	NextWork Private Subnet	subnet-0379a4c212fe472b4	Available	vpc-09e17cc4217fd6833   Next...	Off	10.0.1.0/24	-
<input type="checkbox"/>	-	subnet-0543cdd4ce031a9a3	Available	vpc-0dccc2a2993f222607	Off	172.31.0.0/20	-
<input type="checkbox"/>	-	subnet-03131cfee49ee58a7	Available	vpc-0dccc2a2993f222607	Off	172.31.16.0/20	-
<input type="checkbox"/>	-	subnet-0ebe845dd631e1915	Available	vpc-0dccc2a2993f222607	Off	172.31.32.0/20	-
<input type="checkbox"/>	NextWork Public Subnet	subnet-06a323ed31fac6ef8	Available	vpc-09e17cc4217fd6833   Next...	Off	10.0.0.0/24	-

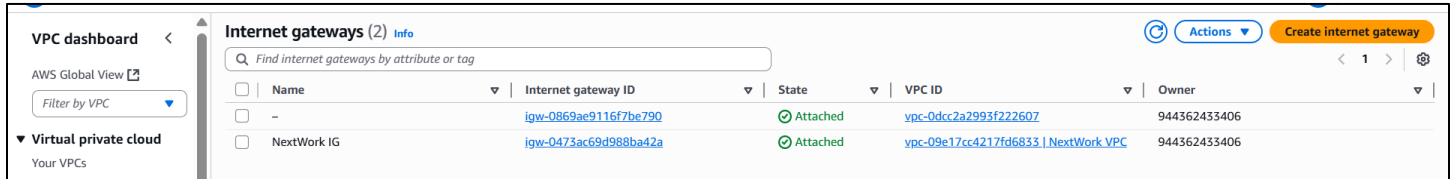
1

### Step 3: Create an Internet Gateway

Attach an internet gateway to your VPC to enable internet access for public subnets.

#### Actions:

- In the VPC Dashboard, select 'Internet gateways' from the left-hand panel.
- Click 'Create internet gateway'.
- Enter a Name tag (e.g., NextWork IG).
- Click 'Create internet gateway'.
- Select your newly created gateway and choose 'Attach to VPC'.
- Select your VPC (NextWork VPC) and confirm.



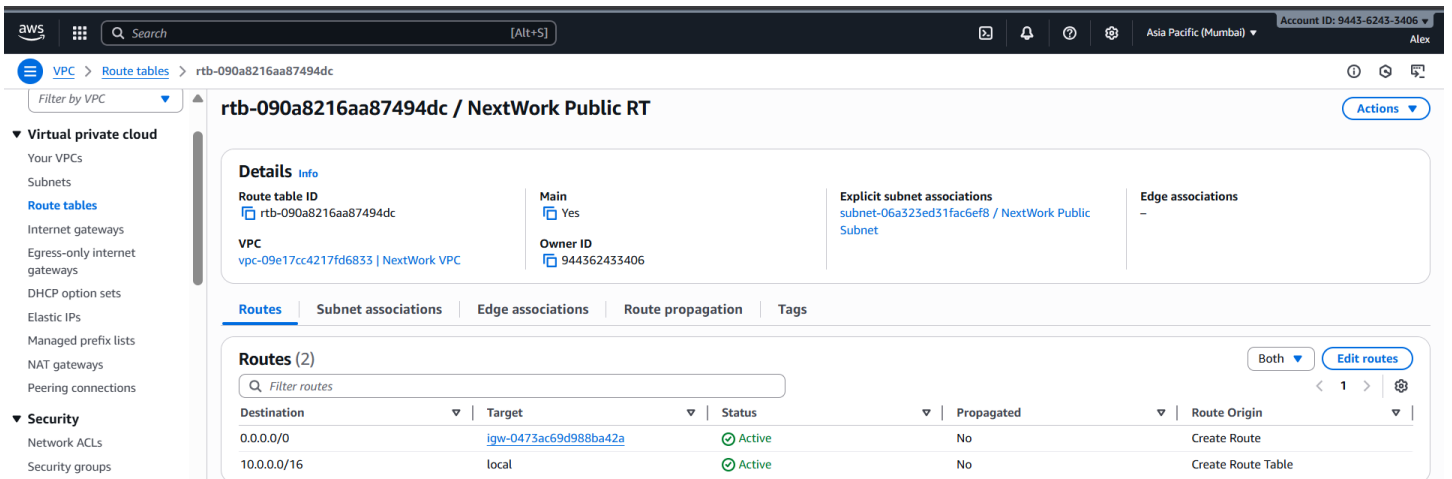
Name	Internet gateway ID	State	VPC ID	Owner
-	igw-0869ae9116f7be790	Attached	vpc-0dccc2a2993f222607	944362433406
NextWork IG	igw-0473ac69d988ba42a	Attached	vpc-09e17cc4217fd6833   NextWork VPC	944362433406

### Step 4: Configure Route Tables

Set up route tables for both public and private subnets.

#### Actions:

- Go to 'Route tables' in the VPC Dashboard.
- Create a public route table and associate it with your public subnet.
- Edit the routes to add Destination = 0.0.0.0/0 and Target = Internet Gateway.
- Create a private route table and associate it with your private subnet.
- Do not add a route to the internet gateway to keep the subnet private.



Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0473ac69d988ba42a	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

aws [Search] [Alt+S] Asia Pacific (Mumbai) Account ID: 9443-6243-3406 Alex

VPC > Route tables > rtb-0dddfbb889d37a644

Filter by VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections

Security

- Network ACLs

rtb-0dddfbb889d37a644 / NextWork Private RT

Details Info

Route table ID  
rtb-0dddfbb889d37a644

VPC  
vpc-09e17cc4217fd6833 | NextWork VPC

Main  
No

Owner ID  
944362433406

Explicit subnet associations  
subnet-0379a4c212fe472b4 / NextWork Private Subnet

Edge associations  
-

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

## Step 5: Create Security Groups and NACLs

Set up security groups and network ACLs for your subnets.

### Actions:

- In the VPC Dashboard, go to 'Security groups' and create a new one (e.g., NextWork-SG).
- Allow inbound HTTP (80), HTTPS (443), and SSH (22) traffic for your public subnet.
- Create a separate security group for the private subnet with limited inbound rules.
- In 'Network ACLs', create and configure one for the public subnet (allow web and SSH traffic).
- Create and configure one for the private subnet with restricted inbound/outbound rules.

aws [Search] [Alt+S] Asia Pacific (Mumbai) Account ID: 9443-6243-3406 Alex

VPC > Security Groups > sg-065c1930e477d4ec3 - NextWork SG

Filter by VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections

Security

- Network ACLs
- Security groups

PrivateLink and

sg-065c1930e477d4ec3 - NextWork SG

Details

Security group name  
NextWork SG

Security group ID  
sg-065c1930e477d4ec3

Description  
A security group for Nextwork

VPC ID  
vpc-09e17cc4217fd6833

Owner  
944362433406

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)

Search

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sgr-067216e4693050d6a	IPv4	SSH	TCP	22	0.0.0.0/0
<input type="checkbox"/>	-	sgr-05fcaa42ddd82875	IPv4	HTTP	TCP	80	0.0.0.0/0

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Account ID: 9443-6243-3406

Alex

VPC > Security Groups > sg-039c98087d3559604 - NextWork Private Security Group

sg-039c98087d3559604 - NextWork Private Security Group

Actions

VPC dashboard

AWS Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Details

Security group name

NextWork Private Security Group

Security group ID

sg-039c98087d3559604

Description

A Security Group for NextWork private subnet

VPC ID

vpc-09e17cc4217fd6833

Owner

944362433406

Inbound rules count

1 Permission entry

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

Inbound rules (1)

Manage tags

Edit inbound rules

1

Search

	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sgr-0082aac70bd1ae1fe	-	SSH	TCP	22	sg-065c1930e477d4ec...

Public and Private NACL's

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Account ID: 9443-6243-3406

Alex

VPC > Network ACLs > acl-02cda9780bb917383 / NextWork NACL

acl-02cda9780bb917383 / NextWork NACL

Actions

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Security

Network ACLs

Security groups

PrivateLink and Lattice

Getting started

Updated

Details

Network ACL ID

acl-02cda9780bb917383

Associated with

subnet-06a323ed31fac6ef8 / Public 1

Default

Yes

VPC ID

vpc-09e17cc4217fd6833 / NextWork VPC

Owner

944362433406

Inbound rules

Outbound rules

Subnet associations

Tags

Inbound rules (4)

Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
110	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
120	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

Account ID: 9443-6243-3406

Alex

VPC > Network ACLs > acl-0e40cd9519ae96251 / NextWork Private NACL

acl-0e40cd9519ae96251 / NextWork Private NACL

Actions

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Security

Network ACLs

Security groups

Details

Network ACL ID

acl-0e40cd9519ae96251

Associated with

subnet-0379a4c212fe472b4 / Private 1

Default

No

VPC ID

vpc-09e17cc4217fd6833 / NextWork VPC

Owner

944362433406

Inbound rules

Outbound rules

Subnet associations

Tags

Inbound rules (1)

Edit inbound rules

Filter inbound rules

1

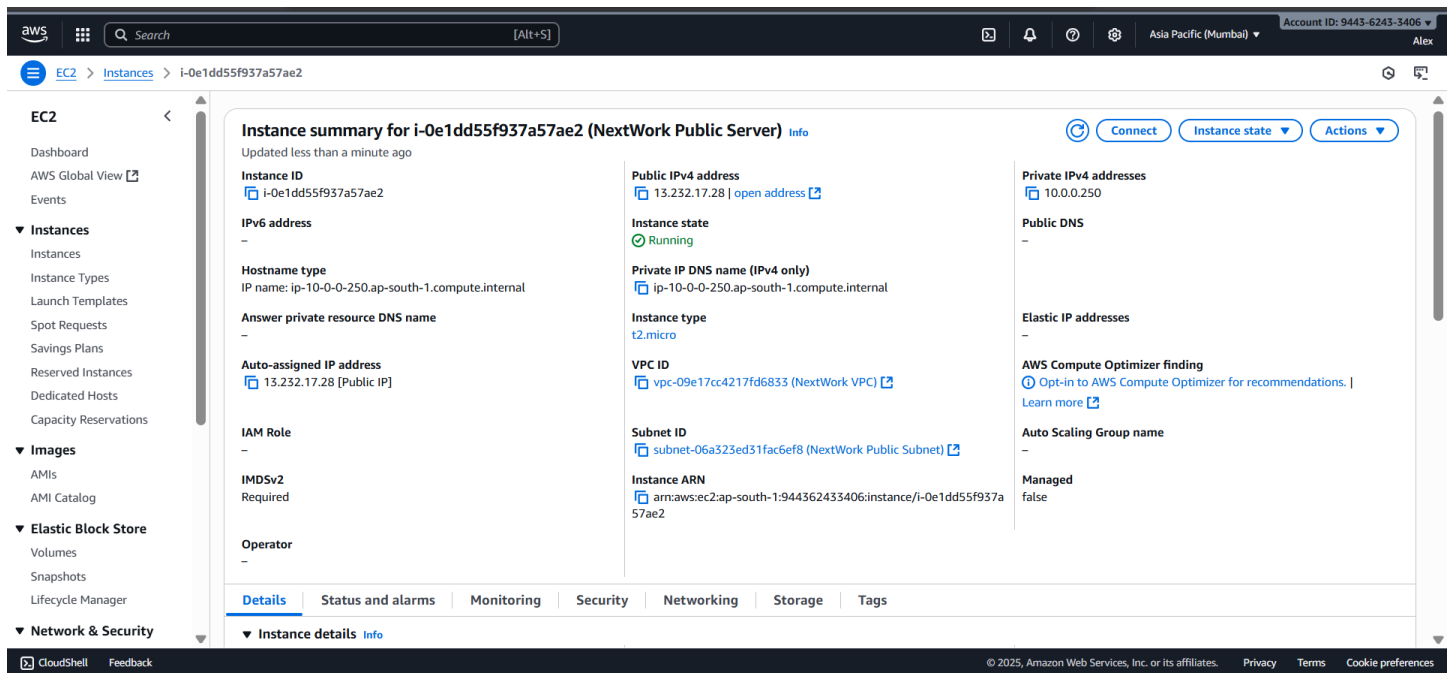
Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

## Step 6: Launch an EC2 Instance in the Public Subnet

Deploy a virtual machine that can be accessed over the internet.

### Actions:

- - In the AWS Management Console, go to the EC2 Dashboard.
- - Click 'Launch instance'.
- - Enter a Name tag (e.g., Public-EC2).
- - Select an Amazon Machine Image (e.g., Amazon Linux 2).
- - Choose an instance type (e.g., t2.micro).
- - In the Network settings, choose your VPC and the Public subnet.
- - Enable Auto-assign Public IP.
- - Select your public security group (NextWork-SG).
- - Click 'Launch' and download a new key pair if needed.
- - Wait for the instance to launch and test connectivity via EC2 Instance Connect.



## Step 7: Launch an EC2 Instance in the Private Subnet

Deploy a virtual machine in your private subnet without internet access.

### Actions:

- - From the EC2 Dashboard, click 'Launch instance'.
- - Enter a Name tag (e.g., Private-EC2).
- - Select the same Amazon Machine Image (Amazon Linux 2).
- - Choose an instance type (e.g., t2.micro).
- - In Network settings, choose your VPC and the Private subnet.
- - Disable Auto-assign Public IP.
- - Select your private subnet security group.

- - Click 'Launch'.
- - Note: This instance will not have internet access; you can connect via a Bastion host in the public subnet if required.

**Instance summary for i-00649070774e88de6 (NextWork Private Server)** Info

Updated less than a minute ago

<b>Instance ID</b> i-00649070774e88de6	<b>Public IPv4 address</b> -	<b>Private IPv4 addresses</b> 10.0.1.165
<b>IPv6 address</b> -	<b>Instance state</b> Running	<b>Public DNS</b> -
<b>Hostname type</b> IP name: ip-10-0-1-165.ap-south-1.compute.internal	<b>Private IP DNS name (IPv4 only)</b> ip-10-0-1-165.ap-south-1.compute.internal	<b>Elastic IP addresses</b> -
<b>Answer private resource DNS name</b> -	<b>Instance type</b> t2.micro	<b>AWS Compute Optimizer finding</b> Opt-in to AWS Compute Optimizer for recommendations.   Learn more
<b>Auto-assigned IP address</b> -	<b>VPC ID</b> vpc-09e17cc4217fd6833 (NextWork VPC)	<b>Auto Scaling Group name</b> -
<b>IAM Role</b> -	<b>Subnet ID</b> subnet-0379a4c212fe472b4 (NextWork Private Subnet)	<b>Managed</b> false
<b>IMDSv2</b> Required	<b>Instance ARN</b> arn:aws:ec2:ap-south-1:944362433406:instance/i-00649070774e88de6	
<b>Operator</b> -		

**Details** | Status and alarms | Monitoring | Security | Networking | Storage | Tags

**Instance details** Info

## Step 8: Use Amazon VPC Wizard

Quickly set up a VPC with pre-configured subnets, route tables, and internet gateways.

### Actions:

- - In the VPC Dashboard, click on 'Launch VPC Wizard'.
- - Select a configuration template (e.g., VPC with Public and Private Subnets).
- - Follow the wizard prompts to create the VPC.
- - Review the automatically created components: subnets, route tables, internet gateway, and NACLs.
- - Compare this with your manually created VPC to understand the differences.

**Resource map** Info

Showing all details

**VPC**  
Your AWS virtual network  
Demo-vpc

**Subnets (2)**  
Subnets within this VPC  
ap-south-1a  
Demo-subnet-public1-ap-south-1a  
Demo-subnet-private1-ap-south-1a

**Route tables (3)**  
Route network traffic to resources  
Demo-rtb-private1-ap-south-1a  
Demo-rtb-public  
rtb-0e1e3785e4d270e68

**Network Connections (1)**  
Connections to other networks  
Demo-igw