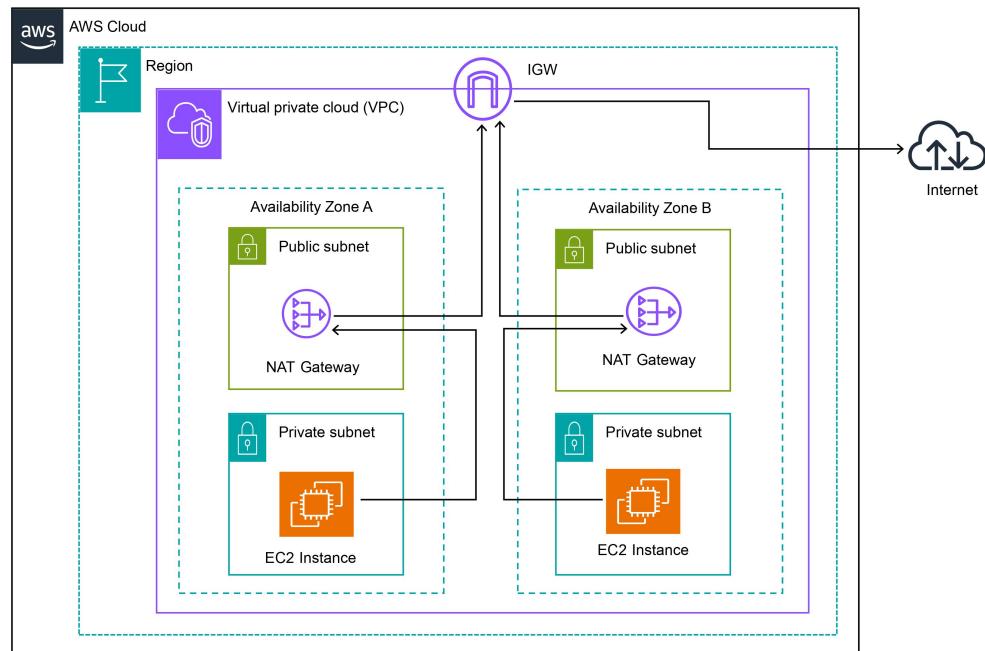


Step-by-Step Configuration of AWS NAT Gateways for Production Use



By
Mahendran Selvakumar
<https://devopstronaut.com/>



1.Create your Own VPC

Search for VPC in the AWS Management Console

The screenshot shows the AWS Management Console search interface. The search bar at the top contains the query 'vpc'. Below the search bar, there is a sidebar with various navigation links: Services (12), Features (59), Resources (New), Documentation (16,919), Knowledge Articles (244), Marketplace (657), and Blogs (897). The main content area displays search results for 'vpc', with 'VPC' being the top result. The VPC entry includes a small icon, the name 'VPC', a star rating, and the description 'Isolated Cloud Resources'. There is also a link 'See all 12 results ▶'. To the right of the search results, there are several widgets, including one for 'Create application'.

Click “Create VPC”

The screenshot shows the VPC dashboard. On the left, there is a sidebar with a 'Virtual private cloud' section containing links for Your VPCs, Subnets, Route tables, Internet gateways, Egress-only Internet gateways, DHCP option sets, and Elastic IPs. The main content area has a heading 'Resources by Region' and a note stating 'You are using the following Amazon VPC resources'. It lists four categories: 'VPCs' (Europe 1, See all regions), 'Subnets' (Europe 3, See all regions), 'Route Tables' (Europe 1, See all regions), 'NAT Gateways' (Europe 0, See all regions), 'VPC Peering Connections' (Europe 0, See all regions), and 'Network ACLs' (Europe 1, See all regions). At the top of the dashboard, there are two prominent buttons: 'Create VPC' (orange) and 'Launch EC2 Instances'.



Select VPC only, provide the VPC name and IPv4 CIDR, then click Create VPC

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

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 - <i>optional</i> | |
|--|---|---|
| <input type="text" value="Name"/> <input type="button" value="X"/> | <input type="text" value="devopstronaut-eks-vpc"/> <input type="button" value="X"/> | <input type="button" value="Remove tag"/> |
| <input type="button" value="Add tag"/> | | |

You can add 49 more tags



The VPC has been created

The screenshot shows the AWS VPC Details page for the VPC 'devopstronaut-eks-vpc'. The VPC ID is 'vpc-000802024dce1d377'. Key details include:

| VPC ID | State | DNS hostnames | DNS resolution |
|-------------------------------|--|-----------------------|-----------------------|
| vpc-000802024dce1d377 | Available | Disabled | Enabled |
| Tenancy | DHCP option set | Main route table | Main network ACL |
| Default | dopt-0c4ea0752b84cb15a | rtb-00693a8dc41cc3414 | acl-045c675f0256ada10 |
| Default VPC | IPv4 CIDR | IPv6 pool | IPv6 CIDR |
| No | 10.0.0.0/16 | - | - |
| Network Address Usage metrics | Route 53 Resolver DNS Firewall rule groups | Owner ID | |
| Disabled | - | 85172553489 | |

Below the details, there are tabs for Resource map, CIDRs, Flow logs, Tags, and Integrations. The Resource map section shows:

- VPC: devopstronaut-eks-vpc
- Subnets (0)
- Route tables (1): rtb-00693a8dc41cc3414
- Network connections (0)

2. Create Public and Private Subnets

Click “Create Subnet”

The screenshot shows the AWS Subnets page under the VPC dashboard. There are three subnets listed:

| Name | Subnet ID | State | VPC | IPv4 CIDR | IPv6 CIDR |
|------|--------------------------|-----------|-----------------------|----------------|-----------|
| - | subnet-03d52168870814283 | Available | vpc-02243fa94bdf7d0e0 | 172.31.32.0/20 | - |
| - | subnet-0a43ad8c0a17da0a1 | Available | vpc-02243fa94bdf7d0e0 | 172.31.0.0/20 | - |
| - | subnet-0685b31f36a7d6ba5 | Available | vpc-02243fa94bdf7d0e0 | 172.31.16.0/20 | - |

Select the VPC under the VPC ID

The screenshot shows the AWS Create subnet page. Under the VPC section, it says "Select a VPC". A dropdown menu is open, showing two options:

- vpc-02243fa94bdf7d0e0 (172.31.0.0/16) (default)
- vpc-000802024dce1d377 (devopstronaut-eks-vpc) (10.0.0.0/16)

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



Provide the subnet name, choose the Availability Zone, and enter the IPv4 CIDR block

Subnet 1 of 4

Subnet name

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

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.



IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.



IPv4 subnet CIDR block

256 IPs



▼ Tags - optional

Key

Value - optional



[Remove](#)

[Add new tag](#)

You can add 49 more tags.

[Remove](#)

Click 'Add new subnet,' then provide the subnet name, choose the Availability Zone, and enter the IPv4 subnet CIDR

Subnet 2 of 4

Subnet name

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

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.



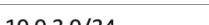
IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.



IPv4 subnet CIDR block

256 IPs



▼ Tags - optional

Key

Value - optional



[Remove](#)

[Add new tag](#)

You can add 49 more tags.

[Remove](#)



Click 'Add new subnet,' then provide the subnet name, choose the Availability Zone, and enter the IPv4 subnet CIDR

Subnet 3 of 4

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

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs
< > ^ ▼

Tags - optional

| Key | Value - optional | Remove |
|--|--|---------------------------------------|
| <input type="text" value="Name"/> <input type="button" value="X"/> | <input type="text" value="devopstronaut-eks-prisubnet-1a"/> <input type="button" value="X"/> | <input type="button" value="Remove"/> |
| <input type="button" value="Add new tag"/> | | |

You can add 49 more tags.

Click 'Add new subnet,' provide the subnet name, choose the Availability Zone, enter the IPv4 subnet CIDR, and then click 'Create Subnet'

Subnet 4 of 4

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

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs
< > ^ ▼

Tags - optional

| Key | Value - optional | Remove |
|--|--|---------------------------------------|
| <input type="text" value="Name"/> <input type="button" value="X"/> | <input type="text" value="devopstronaut-eks-prisubnet-1b"/> <input type="button" value="X"/> | <input type="button" value="Remove"/> |
| <input type="button" value="Add new tag"/> | | |

You can add 49 more tags.



The subnets have been created

You have successfully created 4 subnets: subnet-071193b1542ef9cbb, subnet-02e375ae831d5a677, subnet-0e52f191004e42a26, subnet-0d2f87e24274ce774

| Subnets (4) <small>Info</small> | | | | | | |
|--|--|------------------------|--------------------------------|--|--------------|--|
| Subnet ID : subnet-071193b1542ef9cbb | | | | Subnet ID : subnet-02e375ae831d5a677 | | |
| <input type="button"/> <input type="text"/> Find resources by attribute or tag | | | | <input type="button"/> Actions <small>▼</small> <input type="button"/> Create subnet | | |
| Name | Subnet ID | State | VPC | IPv4 CIDR | Availability | |
| devopstronaut-eks-pubsubnet-1a | subnet-071193b1542ef9cbb | Available | vpc-000802024dce1d377 dev... | 10.0.1.0/24 | eu-west-1a | |
| devopstronaut-eks-prisubnet-1b | subnet-0d2f87e24274ce774 | Available | vpc-000802024dce1d377 dev... | 10.0.4.0/24 | eu-west-1b | |
| devopstronaut-eks-pubsubnet-1b | subnet-02e375ae831d5a677 | Available | vpc-000802024dce1d377 dev... | 10.0.2.0/24 | eu-west-1a | |
| devopstronaut-eks-prisubnet-1a | subnet-0e52f191004e42a26 | Available | vpc-000802024dce1d377 dev... | 10.0.3.0/24 | eu-west-1a | |

3.Create an Internet Gateway and Attach to your VPC

Navigate to the Internet Gateways section and click 'Create Internet Gateway'

VPC dashboard Services Search [Option+S]

Internet gateways (1) Info

| Internet gateways (1) <small>Info</small> | | | | |
|---|---------------------------------------|-----------------------|-----------------------|--------------|
| Search | | | | |
| Name | Internet gateway ID | State | VPC ID | Owner |
| - | igw-0386df9328fa6b78d | Attached | vpc-02243fa94bdf7d0e0 | 851725583489 |

Provide the Internet Gateway name and click 'Create Internet Gateway'

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.

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 |
|-----------------------------------|--|
| <input type="text" value="Name"/> | <input type="text" value="devopstronaut-igw"/> <input type="button"/> Remove |

Add new tag
You can add 49 more tags.

Cancel

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



The Internet Gateway has been created, but it needs to be attached to the VPC

The screenshot shows the AWS VPC Internet Gateways page. A green banner at the top states: "The following internet gateway was created: igw-076935c447680e45f - devopstrounaut-igw. You can now attach to a VPC to enable the VPC to communicate with the internet." Below the banner, the Internet Gateway details are listed: ID: igw-076935c447680e45f, State: Detached, VPC ID: -, Owner: 851725583489. Under the "Tags" section, there is a single tag: Name: devopstrounaut-igw.

Select the VPC to attach and click 'Attach Internet Gateway'

The screenshot shows the "Attach to VPC" dialog box. It displays a message: "The following internet gateway was created: igw-076935c447680e45f - devopstrounaut-igw. You can now attach to a VPC to enable the VPC to communicate with the internet." Below this, the URL is shown: VPC > Internet gateways > Attach to VPC (igw-076935c447680e45f). The main section is titled "VPC" and contains the instruction: "Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below." Under "Available VPCs", it says "Attach the internet gateway to this VPC." A dropdown menu shows "Select a VPC" and lists "vpc-000802024dce1d377 - devopstrounaut-eks-vpc". At the bottom are "Cancel" and "Attach internet gateway" buttons.

4.Create Public Route table and associate Subnet

Navigate to Route Tables and click 'Create Route Table'

The screenshot shows the AWS VPC dashboard. On the left, a sidebar navigation includes EC2 Global View, Virtual private cloud, Your VPCs, Subnets, and Route tables (which is currently selected). The main area is titled "Route tables (1) Info" and shows a table with one row: Name: rtb-0761214b61b16f9d5, Route table ID: rtb-0761214b61b16f9d5, Explicit subnet associations: -, Edge associations: -, Main: Yes, VPC: vpc-02243fa94bd7d0e0. A "Create route table" button is located at the top right of the table.



Provide the route table name, select the VPC, and click '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.

VPC
The VPC to use for this route table.
 (selected)

 (selected) can use tags to search and filter your resources or track your AWS costs.

Key Value - *optional*

You can add 49 more tags.

Go to Subnet Associations and click 'Edit Subnet Associations'

VPC > Route tables > rtb-0abb174fed44cd2c1

rtb-0abb174fed44cd2c1 / devopstronaut-publicrt Actions ▾

Details Info

| | | | |
|---|---|-----------------------------------|------------------------|
| Route table ID <input type="text" value="rtb-0abb174fed44cd2c1"/> | Main <input type="text" value="No"/> | Explicit subnet associations - | Edge associations - |
| VPC <input type="text" value="vpc-000802024dce1d377 devopstronaut-eks-vpc"/> | Owner ID <input type="text" value="851725583489"/> | | |

Explicit subnet associations (0)

< 1 > @

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|--|-----------|-----------|-----------|
| No subnet associations You do not have any subnet associations. | | | |



Select the public subnets and click 'Save Associations'

VPC > Route tables > rtb-0abb174fed44cd2c1 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR | Route table ID |
|--|--------------------------|-------------|-----------|------------------------------|
| <input checked="" type="checkbox"/> devopstronaut-eks-pubsubnet-1a | subnet-071193b1542ef9cbb | 10.0.1.0/24 | - | Main (rtb-00693a8dc41cc3414) |
| <input type="checkbox"/> devopstronaut-eks-prisubnet-1b | subnet-0d2f87e24274ce774 | 10.0.4.0/24 | - | Main (rtb-00693a8dc41cc3414) |
| <input checked="" type="checkbox"/> devopstronaut-eks-pubsubnet-1b | subnet-02e375ae831d5a677 | 10.0.2.0/24 | - | Main (rtb-00693a8dc41cc3414) |
| <input type="checkbox"/> devopstronaut-eks-prisubnet-1a | subnet-0e52f191004e42a26 | 10.0.3.0/24 | - | Main (rtb-00693a8dc41cc3414) |

Selected subnets

subnet-071193b1542ef9cbb / devopstronaut-eks-pubsubnet-1a X subnet-02e375ae831d5a677 / devopstronaut-eks-pubsubnet-1b X

Actions: Cancel Save associations

The public subnet has been associated with the route table

✓ You have successfully updated subnet associations for rtb-0abb174fed44cd2c1 / devopstronaut-publicrt.

rtb-0abb174fed44cd2c1 / devopstronaut-publicrt

Details **Info**

| | | | |
|--|--------------------------|---|------------------------|
| Route table ID rtb-0abb174fed44cd2c1 | Main No | Explicit subnet associations 2 subnets | Edge associations - |
| VPC vpc-000802024dce1d377 devopstronaut-eks-vpc | Owner ID 851725583489 | | |

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

Explicit subnet associations (2)

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|--------------------------------|--------------------------|-------------|-----------|
| devopstronaut-eks-pubsubnet-1a | subnet-071193b1542ef9cbb | 10.0.1.0/24 | - |
| devopstronaut-eks-pubsubnet-1b | subnet-02e375ae831d5a677 | 10.0.2.0/24 | - |

Subnets without explicit associations (2)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|--------------------------------|--------------------------|-------------|-----------|
| devopstronaut-eks-prisubnet-1b | subnet-0d2f87e24274ce774 | 10.0.4.0/24 | - |
| devopstronaut-eks-prisubnet-1a | subnet-0e52f191004e42a26 | 10.0.3.0/24 | - |

4a. Add Routes to the route tables

Go to Routes and click 'Edit Routes'

VPC > Route tables > rtb-0abb174fed44cd2c1

rtb-0abb174fed44cd2c1 / devopstronaut-publicrt

Details **Info**

| | | | |
|--|--------------------------|---|------------------------|
| Route table ID rtb-0abb174fed44cd2c1 | Main No | Explicit subnet associations 2 subnets | Edge associations - |
| VPC vpc-000802024dce1d377 devopstronaut-eks-vpc | Owner ID 851725583489 | | |

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

Routes (1)

| Destination | Target | Status | Propagated |
|-------------|--------|--------|------------|
| 10.0.0.0/16 | local | Active | No |

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



Provide the destination as 0.0.0.0/0, choose 'Internet Gateway' as the target, select the IGW that was created, and click 'Save Changes'

The screenshot shows the 'Edit routes' interface for a specific route table. A new route is being configured with the following details:

| Destination | Target | Status | Propagated |
|-------------|---|--------|------------|
| 10.0.0.0/16 | local | Active | No |
| 0.0.0.0/0 | Internet Gateway | - | No |
| | igw-076935c447680e45f (devopstronaut-igw) | - | - |

At the bottom right, there are buttons for 'Cancel', 'Preview', and 'Save changes'.

The route has been added to the route table

The screenshot shows the details for the route table 'rtb-0abb174fed44cd2c1 / devopstronaut-publicrt'. Key information includes:

| Route table ID | Main | Explicit subnet associations | Edge associations |
|---|--------------|------------------------------|-------------------|
| rtb-0abb174fed44cd2c1 | No | 2 subnets | - |
| VPC | Owner ID | | |
| vpc-000802024dce1d377 devopstronaut-eks-vpc | 851725583489 | | |

The 'Routes' tab is selected, displaying two routes:

| Destination | Target | Status | Propagated |
|-------------|-----------------------|--------|------------|
| 0.0.0.0/0 | igw-076935c447680e45f | Active | No |
| 10.0.0.0/16 | local | Active | No |

5.Create Private Route table and associate Subnet

Click 'Create Route Table'

The screenshot shows the 'Route tables' list page with three entries:

| Name | Route table ID | Explicit subnet assoc... | Main | VPC |
|------------------------|-----------------------|--------------------------|------|---------------------------------------|
| - | rtb-0761214b61b16f9d5 | - | Yes | vpc-02243fa94bd7d0e0 |
| - | rtb-00693a8dc41cc3414 | - | Yes | vpc-000802024dce1d377 devopstron... |
| devopstronaut-publicrt | rtb-0abb174fed44cd2c1 | 2 subnets | No | vpc-000802024dce1d377 devopstron... |



Provide the name, select the VPC, and click '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.

devopstronaut-privatert

VPC
The VPC to use for this route table.

vpc-000802024dce1d377 (devopstronaut-eks-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 - <i>optional</i> |
|-------------------------------------|--|
| <input type="text" value="Name"/> X | <input type="text" value="devopstronaut-privatert"/> X |

Add new tag

You can add 49 more tags.

Cancel **Create route table**

Go to Subnet Associations and click 'Edit Subnet Associations'

VPC > Route tables > rtb-0d1aa44cb1ee55ef0

rtb-0d1aa44cb1ee55ef0 / devopstronaut-privatert Actions ▾

Details Info

| | | | |
|---|---|-----------------------------------|------------------------|
| Route table ID <input type="text" value="rtb-0d1aa44cb1ee55ef0"/> | Main <input type="checkbox"/> | Explicit subnet associations - | Edge associations - |
| VPC <input type="text" value="vpc-000802024dce1d377 devopstronaut-eks-vpc"/> | Owner ID <input type="text" value="851725583489"/> | | |

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

Explicit subnet associations (0)

No subnet associations

You do not have any subnet associations.

Subnets without explicit associations (2)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|--------------------------------|--|-------------|-----------|
| devopstronaut-eks-prisubnet-1b | subnet-0d2f87e24274ce774 | 10.4.0.0/24 | - |
| devopstronaut-eks-prisubnet-1a | subnet-0e52f191004e42a26 | 10.0.3.0/24 | - |

Edit subnet associations

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



Select the private subnets and click 'Save Associations'

VPC > Route tables > rtb-0d1aa44cb1ee55ef0 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR | Route table ID |
|--|--|-------------|-----------|--|
| devopstronaut-eks-pubsubnet-1a | subnet-071193b1542ef9ccb | 10.0.1.0/24 | - | rtb-0abb174fed44cd2c1 / devopstrona... |
| <input checked="" type="checkbox"/> devopstronaut-eks-prisubnet-1b | subnet-0d2f87e24274ce774 | 10.0.4.0/24 | - | Main (rtb-00693a8dc41cc3414) |
| devopstronaut-eks-pubsubnet-1b | subnet-02e375a8e31d5a677 | 10.0.2.0/24 | - | rtb-0abb174fed44cd2c1 / devopstrona... |
| <input checked="" type="checkbox"/> devopstronaut-eks-prisubnet-1a | subnet-0e52f191004e42a26 | 10.0.3.0/24 | - | Main (rtb-00693a8dc41cc3414) |

Selected subnets

subnet-0d2f87e24274ce774 / devopstronaut-eks-prisubnet-1b X subnet-0e52f191004e42a26 / devopstronaut-eks-prisubnet-1a X

Cancel Save associations

The private subnet has been associated with the route table. Here I have created one private route table and associated it with all private subnets. You need to create a route table for each private subnet so that route can be created for each NAT gateway

You have successfully updated subnet associations for rtb-0d1aa44cb1ee55ef0 / devopstronaut-privatert.

VPC > Route tables > rtb-0d1aa44cb1ee55ef0

rtb-0d1aa44cb1ee55ef0 / devopstronaut-privatert

Details Info

| | | | |
|--|--------------------------|---|------------------------|
| Route table ID rtb-0d1aa44cb1ee55ef0 | Main No | Explicit subnet associations 2 subnets | Edge associations - |
| VPC vpc-000802024dce1d377 devopstronaut-eks-vpc | Owner ID 851725583489 | | |

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (2)

| Name | Subnet ID | IPv4 CIDR | IPv6 CIDR |
|--------------------------------|--|-------------|-----------|
| devopstronaut-eks-prisubnet-1b | subnet-0d2f87e24274ce774 | 10.0.4.0/24 | - |
| devopstronaut-eks-prisubnet-1a | subnet-0e52f191004e42a26 | 10.0.3.0/24 | - |

6.Launch instance in Public Subnet

Click “Launch Instances”

AWS Services Search [Option+S]

EC2 Dashboard EC2 Global View Events Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts

Instances Info Last updated less than a minute ago Connect Actions Launch instances

Find Instance by attribute or tag (case-sensitive) All states

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS |
|--|-------------|----------------|---------------|--------------|--------------|-------------------|-----------------|
| No instances You do not have any instances in this region | | | | | | | |

Launch instances

Provide the name and choose the operating system

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

devopstronaut-pub-instance

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start



Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0c38b837cd80f13bb (64-bit (x86)) / ami-008101e20d5a4ceaf (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Select the instance type and click 'Create new key pair' if you don't have one

▼ Instance type Info | Get advice

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.027 USD per Hour
On-Demand Linux base pricing: 0.0126 USD per Hour
On-Demand SUSE base pricing: 0.0126 USD per Hour
On-Demand Windows base pricing: 0.0172 USD per Hour

All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select

[Create new key pair](#)



Provide the name, select the key pair type, choose the private key file format, click 'Create Key Pair,' and save the key

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

devopstronaut-pubkey

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA
RSA encrypted private and public key pair

ED25519
ED25519 encrypted private and public key pair

Private key file format

.pem
For use with OpenSSH

.ppk
For use with PuTTY

⚠️ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel **Create key pair**

Select the VPC and public subnet, enable 'Auto-assign Public IP,' then click 'Create New Security Group' and provide the name



▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-000802024dce1d377 (devopstronaut-eks-vpc)
10.0.0.0/16



Subnet [Info](#)

subnet-071193b1542ef9cbb devopstronaut-eks-pubsubnet-1a
VPC: vpc-000802024dce1d377 Owner: 851725583489
Availability Zone: eu-west-1a Zone type: Availability Zone
IP addresses available: 251 CIDR: 10.0.1.0/24

[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of [free tier allowance](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - required

devopstronaut-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#@[]+=&;!\$*

Description - required [Info](#)

EC2 instance security group

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

[Remove](#)

Type [Info](#)

ssh

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

Anywhere

Source [Info](#)

Add CIDR, prefix list or security

Description - optional [Info](#)

e.g. SSH for admin desktop

0.0.0.0/0

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Add security group rule](#)

Leave the storage size as is and click 'Launch Instance'



EC2 instance security group

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type Info Protocol Info Port range Info
ssh TCP 22

Source type Info Source Info Description - optional Info
Anywhere Add CIDR, prefix list or security e.g. SSH for admin desktop
0.0.0.0/0 X

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Add security group rule Advanced network configuration

▼ Configure storage Info Advanced

1x 8 GiB gp3 Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage X

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

ⓘ Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

▼ Summary

Number of instances Info 1

Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0c38bb837cd80f13bb

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

ⓘ Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Review commands

The EC2 instance has been created in the public subnet

Instances (1/1) Info

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 | Elastic IP |
|----------------------------|---------------------|----------------|---------------|-------------------|---------------|-------------------|-----------------|---------------|------------|
| devopstronaut-pub-instance | i-053b23317d91d56f0 | Running | t2.micro | 2/2 checks passed | View alarms + | eu-west-1a | - | 52.50.207.240 | - |

i-053b23317d91d56f0 (devopstronaut-pub-instance)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary Info

Instance ID i-053b23317d91d56f0 (devopstronaut-pub-instance)
IPv6 address -
Hostname type IP name: ip-10-0-1-59.eu-west-1.compute.internal
Answer private resource DNS name -
Auto-assigned IP address 52.50.207.240 [Public IP]
IAM Role -
IMDSv2 Required
Instance details Info

Platform Ubuntu (Inferred)
Platform details Linux/UNIX
Stop protection Disabled
Instance auto-recovery Default

Private IPv4 addresses 10.0.1.39
Public IPv4 DNS -
Elastic IP addresses -
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. | Learn more
Auto Scaling Group name -
Monitoring disabled
Termination protection Disabled
AMI location amazon/ubuntu/images/hvm-ssd-gp3/ubuntu-noble-24.04-amd64-server-20240701.1
Stop-Hibernate behavior Disabled



7.Launch instance in Private Subnet

Follow the same steps to launch an EC2 instance in the private subnet

EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Li [Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type Free tier eligible

ami-0c38b837cd80f13bb (64-bit (x86)) / ami-008101e20d5a4ceaf (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture 64-bit (x86) **AMI ID** ami-0c38b837cd80f13bb **Verified provider**

▼ Instance type Info | Get advice

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.027 USD per Hour
On-Demand Linux base pricing: 0.0126 USD per Hour
On-Demand SUSE base pricing: 0.0126 USD per Hour
On-Demand Windows base pricing: 0.0172 USD per Hour

All generations [Compare instance types](#)

Additional costs apply for AMIs with pre-installed software



▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

devopstronaut-pubkey [Create new key pair](#)

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-000802024dce1d377 (devopstronaut-eks-vpc) 10.0.0.0/16 [Create new subnet](#)

Subnet [Info](#)

subnet-0e52f191004e42a26 devopstronaut-eks-prisubnet-1a
VPC: vpc-000802024dce1d377 Owner: 851725583489
Availability Zone: eu-west-1a Zone type: Availability Zone
IP addresses available: 251 CIDR: 10.0.3.0/24

Auto-assign public IP [Info](#)

Disable [Create new subnet](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Common security groups [Info](#)

Select security groups devopstronaut-sg sg-0c951ee735f22ee53 X
VPC: vpc-000802024dce1d377

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

▼ Configure storage [Info](#) Advanced

1x 8 GiB gp3 Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage X

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

ⓘ Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 24.04 LTS, ...[read more](#)
ami-0c38b837cd80f13bb

Virtual server type (instance type)

t2.micro

Firewall (security group)

devopstronaut-sg

Storage (volumes)

1 volume(s) - 8 GiB

ⓘ Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet. X

[Cancel](#) [Launch instance](#) [Review commands](#)

The instance has been created in the private subnet



Instances (1/2) [Info](#)

| Name | Instance ID | Instance state | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 ... | Elastic IP | IPv6 IPs | Monitoring | Security group name | Key name |
|--------------------------|---------------------|------------------------------------|-------------------|-------------------------------|-------------------|-----------------|-----------------|------------|----------|------------|---------------------|------------------|
| devopsonaut-pri-instance | i-0c41c3a0502ecf0e9 | Running Q t2.micro | 2/2 checks passed | View alarms + | eu-west-1a | - | - | - | - | disabled | devopsonaut-sg | devopsonaut... 2 |
| devopsonaut-pub-instance | i-053623317891d506 | Running Q t2.micro | 2/2 checks passed | View alarms + | eu-west-1a | - | 52.50.207.240 | - | - | disabled | devopsonaut-sg | devopsonaut... 2 |

i-0c41c3a0502ecf0e9 (devopsonaut-pri-instance)

IPv4 address -

Hostname type IP name: ip-10-0-3-45.eu-west-1.compute.internal

Answer private resource DNS name -

Auto-assigned IP address -

IAM Role -

IMDSv2 Required

Instance details

Platform [Ubuntu \(Inferred\)](#)

Platform details [Linux/UNIX](#)

Stop protection [Disabled](#)

Instance auto-recovery [Default](#)

AMI Launch index 0

Credit specification standard

Usage operation [Run instances](#)

Encaves Support -

Allow tags in instance metadata [Disabled](#)

Host and placement group [Info](#)

Host ID -

Affinity -

Public IPv4 DNS -

Elastic IP addresses -

AWS Compute Optimizer finding [Opt-in to AWS Compute Optimizer for recommendations | Learn more](#)

Auto Scaling Group name -

Monitoring disabled

Termination protection [Disabled](#)

AMI location [amazon/ubuntu/images/hvm-ssd-gp3/ubuntu-noble-24.04-amd64-server-20240701.1](#)

Stop-hibernate behavior [Disabled](#)

State transition reason -

State transition message -

Owner [851725583489](#)

Current instance boot mode [legacy-bios](#)

Answer RIN DNS hostname IPv4 [Disabled](#)

Placement group -

8.Create IAM Role for SSM

Create an IAM Role to enable EC2 instance connections via SSM

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

IAM > Roles

Roles (17) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

| Role name | Trusted entities | Last activity |
|---|--------------------------------------|---------------|
| AWSServiceRoleForAmazonEKS | AWS Service: eks (Service-Linked Rol | 2 days ago |
| AWSServiceRoleForAmazonEKSNodegroup | AWS Service: eks-nodegroup (Service- | 2 days ago |
| AWSServiceRoleForAutoScaling | AWS Service: autoscaling (Service-Li | 2 days ago |
| AWSServiceRoleForECS | AWS Service: ecs (Service-Linked Rol | 17 days ago |
| AWSServiceRoleForElasticLoadBalancing | AWS Service: elasticloadbalancing (S | 22 hours ago |
| AWSServiceRoleForGitSync | AWS Service: repository.sync.codeco | 11 days ago |

Select “AWS Service”

Select trusted entity [Info](#)

Trusted entity type

AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



Select “EC2 Role for AWS Systems Manager”

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

EC2

Allows EC2 instances to call AWS services on your behalf.

EC2 Role for AWS Systems Manager

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

EC2 Spot Fleet Role

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

EC2 - Spot Fleet Auto Scaling

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

EC2 - Spot Fleet Tagging

Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

EC2 - Spot Instances

Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

EC2 - Spot Fleet

Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

EC2 - Scheduled Instances

Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancel

Next

Click “Next”

Add permissions Info

Permissions policies (1) Info

The type of role that you selected requires the following policy.

Policy name ?

AmazonSSMManagedInstanceCore

► Set permissions boundary - *optional*

Cancel

Previous

Next

Enter the role name and click 'Create Role'



Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
ec2_ssm

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

Step 1: Select trusted entities

Trust policy

```
1: { "Version": "2012-10-17",  
2:   "Statement": [  
3:     {  
4:       "Sid": "",  
5:       "Effect": "Allow",  
6:       "Principal": {  
7:         "Service": "ec2.amazonaws.com"  
8:       },  
9:       "Action": "sts:AssumeRole"  
10:    }  
11:  ]  
12: }  
13: }
```

Step 2: Add permissions

Permissions policy summary

| Policy name | Type | Attached as | Permissions policy |
|------------------------------|-------------|-------------|--------------------|
| AmazonSSMManagedInstanceCore | AWS managed | | |

Step 3: Add tags

Add tags - optional info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag You can add up to 50 more tags.

Cancel Previous Create role

The role has been created

Role ec2_ssm created. View role X

IAM > Roles

Roles (18) Info An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

| <input type="checkbox"/> Role name | ▲ Trusted entities | Last activity |
|--|--------------------------------------|---------------|
| AWSServiceRoleForAmazonEKS | AWS Service: eks (Service-Linked Rol | 2 days ago |

Go to the EC2 instances, navigate to 'Security,' and click 'Modify IAM Role'

ch [Option+S] Ireland Mahi

Instances (1/2) Info Last updated less than a minute ago

| <input checked="" type="checkbox"/> Name | Instance ID | Instance state | Instance t |
|--|---------------------|----------------|------------|
| devopstronaut-pub-instance | i-053b23317d91d56f0 | Running | t2.micro |
| devopstronaut-pri-instance | i-0c41c3a0502ecf0e9 | Running | t2.micro |

i-053b23317d91d56f0 (devopstronaut-pub-instance)

Actions ▲ Launch instances

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

Details Status and alarms Monitoring Security Networking Storage Tags

Choose the IAM role and click 'Update IAM Role'

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



[EC2](#) > [Instances](#) > [i-053b23317d91d56f0](#) > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

[i-053b23317d91d56f0 \(devopstronaut-pub-instance\)](#)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

ec2_ssm



Create new IAM role [\[\]](#)

[Cancel](#)

[Update IAM role](#)

Connect to the public EC2 instance

[EC2](#) > [Instances](#) > [i-053b23317d91d56f0](#) > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-053b23317d91d56f0 (devopstronaut-pub-instance) using any of these options

[EC2 Instance Connect](#)

[Session Manager](#)

[SSH client](#)

[EC2 serial console](#)

Session Manager usage:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) [\[\]](#) page.

[Cancel](#)

[Connect](#)

Run the `apt update` command to update the OS and verify internet access

Session ID: root@bcgvwzuly4evsc7n7xowiytvqu Instance ID: i-053b23317d91d56f0

[Terminate](#)

```
root@ip-10-0-1-39:/home/ubuntu# apt update
Warning: The unit file, source configuration file or drop-ins of apt-news.service changed on disk. Run 'systemctl daemon-reload' to reload units.
Warning: The unit file, source configuration file or drop-ins of esm-cache.service changed on disk. Run 'systemctl daemon-reload' to reload units.
Hit:1 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
36 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ip-10-0-1-39:/home/ubuntu#
```



When attempting to update from the private EC2 instance, the operation failed. To resolve this issue, you need to create a NAT Gateway

```
root@ip-10-0-3-45:~# apt update
Ign1: http://security.ubuntu.com/ubuntu noble-security InRelease
Ign2: http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Ign3: http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Ign4: http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Ign1: http://security.ubuntu.com/ubuntu noble-security InRelease
Ign2: http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Ign3: http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Ign4: http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Ign2: http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Ign1: http://security.ubuntu.com/ubuntu noble-security InRelease
Ign3: http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Ign4: http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Err:2 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
      Cannot initiate the connection to eu-west-1.ec2.archive.ubuntu.com:80 (2a05:d018:fd:f300:58d3:2098:a755:addr). - connect (101: Network is unreachable) Cannot initiate the connection to eu-west-1.ec2.archive.ubuntu.com:80 (2a05:d018:fd:f300:6ee0:9bd8:239d:aalc). - connect (101: Network is unreachable) Cannot initiate the connection to eu-west-1.ec2.archive.ubuntu.com:80 (2a05:d018:fd:f301:175a:3a40:9acff:2880). - connect (101: Network is unreachable) Cannot initiate the connection to eu-west-1.ec2.archive.ubuntu.com:80 (2a05:d018:fd:f301:a3e6:28b5:ca:eif317). - connect (101: Network is unreachable) Cannot initiate the connection to eu-west-1.ec2.archive.ubuntu.com:80 (2a05:d018:fd:f302:55ec:6d1c:c751:1067). - connect (101: Network is unreachable) Cannot initiate the connection to eu-west-1.ec2.archive.ubuntu.com:80 (34.253.189.82), connection timed out Could not connect to eu-west-1.ec2.archive.ubuntu.com:80 (34.253.229.19), connection timed out Could not connect to eu-west-1.ec2.archive.ubuntu.com:80 (54.229.116.227), connection timed out Could not connect to eu-west-1.ec2.archive.ubuntu.com:80 (54.246.214.20), connection timed out Could not connect to eu-west-1.ec2.archive.ubuntu.com:80 (54.246.214.20), connection timed out Could not connect to eu-west-1.ec2.archive.ubuntu.com:80 (34.241.117.189), connection timed out
```

9.Create NAT Gateway

Go to NAT Gateways and click 'Create NAT Gateway'

The screenshot shows the AWS VPC dashboard with the 'NAT gateways' section selected. The table header includes columns for Name, NAT gateway ID, Connectivity..., State, State message, Primary public IP..., and Public IP. Below the table, a message says 'No NAT gateways found'. At the bottom left, there's a 'Select a NAT gateway' button. On the far right of the table, there are icons for creating a new gateway, deleting existing ones, and other actions.

Provide the NAT Gateway name, choose the public subnet, select 'Public' as the connectivity type, and click 'Allocate Elastic IP'



[VPC](#) > [NAT gateways](#) > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

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.

► Additional settings Info

The Elastic IP has been allocated

✔ Elastic IP address 52.51.51.102 (eipalloc-0dfaef478214c5cf5e) allocated.

[VPC](#) > [NAT gateways](#) > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

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.

► Additional settings Info



Click 'Create NAT Gateway'

▶ 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.

| Key | Value - optional |
|---|---|
| <input type="text" value="Name"/> X | <input type="text" value="devopstronaut-natgw-1a"/> X |
| Add new tag | |

You can add 49 more tags.

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

The NAT Gateway has been created

NAT gateways (1) [Info](#)

| Name | NAT gateway ID | Connectivity... | State | State message | Primary public I... |
|------------------------|---------------------------------------|-----------------|------------------------|---------------|------------------------------|
| devopstronaut-natgw-1a | nat-0f8a82d49e5c6fd5b | Public | Available | - | 52.51.51.102 |

Similarly, create another NAT Gateway in a different Availability Zone

NAT gateways (3) [Info](#)

| Name | NAT gateway ID | Connectivity... | State | State message | Primary public I... |
|------------------------|---------------------------------------|-----------------|------------------------|---------------|-------------------------------|
| devopstronaut-natgw-1b | nat-0f26b163ea4e03b2d | Public | Deleted | - | - |
| devopstronaut-natgw-1b | nat-03643b080720e55ce | Public | Available | - | 34.254.40.248 |
| devopstronaut-natgw-1a | nat-0f8a82d49e5c6fd5b | Public | Available | - | 52.51.51.102 |

9a. Add Routes to the route tables

Go to the Private Route Table and click 'Edit Routes'

Route tables (1/4) [Info](#)

| Name | Route table ID | Explicit subnet associ... | Edge associations | Main | VPC |
|--|---------------------------------------|---------------------------|-------------------|------|------------------------------|
| - | rtb-0761214b61b16f9d5 | - | - | Yes | vpc-02243fa9 |
| - | rtb-00693a8dc41cc3414 | - | - | Yes | vpc-00080202 |
| devopstronaut-publicrt | rtb-0abb174fed44cd2c1 | 2 subnets | - | No | vpc-00080202 |
| <input checked="" type="checkbox"/> devopstronaut-privatertr | rtb-0d1aa44cb1ee55ef0 | 2 subnets | - | No | vpc-00080202 |

rtb-0d1aa44cb1ee55ef0 / devopstronaut-privatertr

| Details | Routes | Subnet associations | Edge associations | Route propagation | Tags |
|-----------------------------|-------------------------------|---------------------|-------------------|-------------------|------|
| Edit routes | | | | | |
| Routes (1) | Filter routes | | | | |
| Destination | Target | Status | Propagated | | |
| 10.0.0.0/16 | local | Active | No | | |

<https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>



Add a destination of 0.0.0.0/0, set the target to 'NAT Gateway,' select the NAT Gateway ID, and click 'Save Changes'

The screenshot shows the 'Edit routes' interface for a specific route table. A new route is being configured with the following details:

| Destination | Target | Status | Propagated |
|-------------|-------------|--------|------------|
| 10.0.0.0/16 | local | Active | No |
| 0.0.0.0/0 | NAT Gateway | - | No |

The 'Target' field has a dropdown menu open, showing 'NAT Gateway' as the selected option. Below the dropdown, a search bar contains 'nat-' and a list of three NAT Gateway IDs: 'nat-0f26b163ea4e03b2d (devopstronaut-natgw-1b)', 'nat-03643b080720e55ce (devopstronaut-natgw-1b)', and 'nat-0f8a82d49e5c6fd5b (devopstronaut-natgw-1a)'. At the bottom right of the interface are 'Cancel', 'Preview', and 'Save changes' buttons, with 'Save changes' being the active button.

The route has been added to the route table

The screenshot shows the 'Routes' tab for the route table 'rtb-0d1aa44cb1ee55ef0'. The table lists the following routes:

| Destination | Target | Status | Propagated |
|-------------|-----------------------|--------|------------|
| 0.0.0.0/0 | nat-0f8a82d49e5c6fd5b | Active | No |
| 10.0.0.0/16 | local | Active | No |

Connect to the private EC2 instance from the public subnet

```
root@ip-10-0-1-39:~$ ssh -i "devopstronaut-pubkey.pem" ubuntu@10.0.3.45
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1009-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Aug 21 22:49:53 UTC 2024

System load:  0.0          Processes:      104
Usage of /:   22.9% of 6.71GB   Users logged in:   0
Memory usage: 19%           IPv4 address for enX0: 10.0.3.45
Swap usage:   0%
```

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See <https://ubuntu.com/esm> or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

```
Last login: Wed Aug 21 22:15:48 2024 from 10.0.1.39
ubuntu@ip-10-0-3-45:~$
```



Run the update command to verify internet access

```
ubuntu@ip-10-0-3-45:~$ sudo apt update
Get:1 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [319 kB]
Get:8 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:9 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:10 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:11 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:12 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:13 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:14 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [380 kB]
Get:15 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [93.2 kB]
Get:16 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [6004 B]
Get:17 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [325 kB]
Get:18 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [136 kB]
Get:19 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]
Get:20 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [12.9 kB]
Get:21 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [280 kB]
Get:22 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [54.8 kB]
```

You should now be able to update the operating system using the NAT Gateway

Keep Learning, Keep Deploying!!!

Feel free to reach out to me, if you have any other queries or suggestions

Stay connected on Linkedin: <https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>