

Bharath Kumar N(Ps ID:10843180)

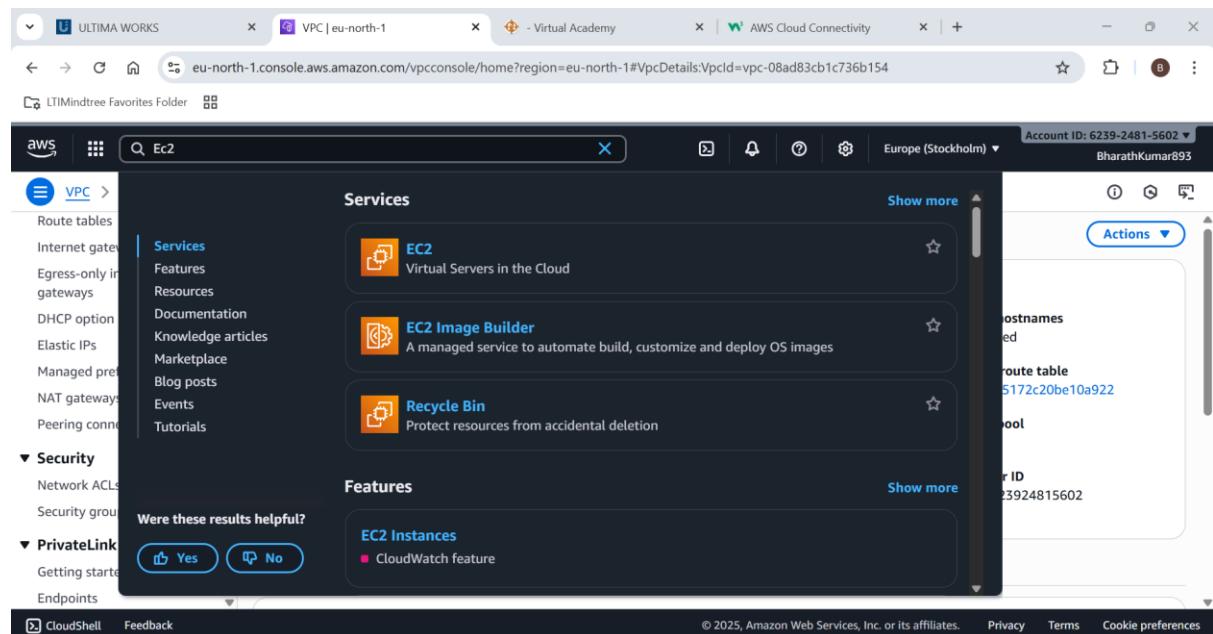
Weekly assessment 3 AWS (Linux 1.2)

You are a Cloud Administrator for a startup called LTIM, which is developing a webbased application for its clients. The goal is to host the web application on AWS using EC2 instances, store files in S3, and design a secure and scalable VPC architecture with both public and private subnets.

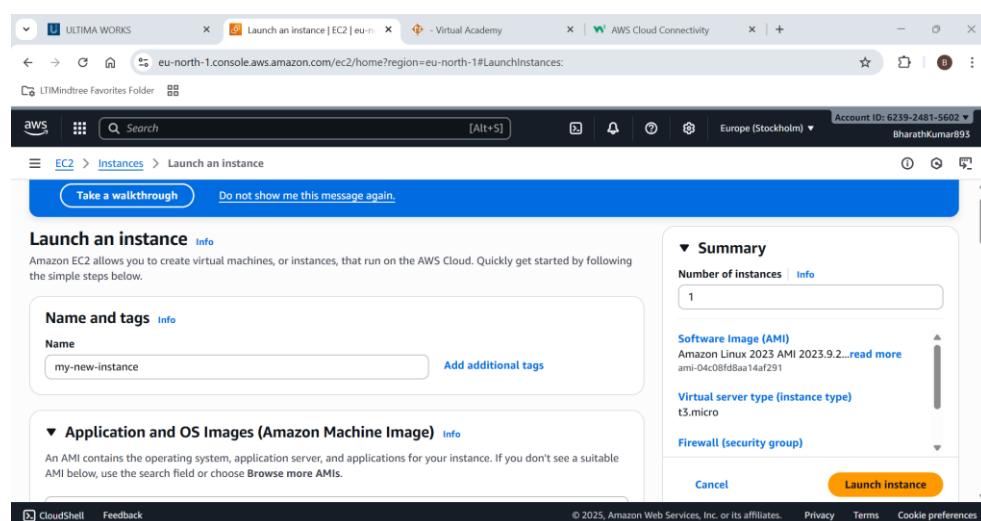
Questions:

1. Launch an EC2 instance with Amazon Linux 2 in a new VPC and connect via SSH.

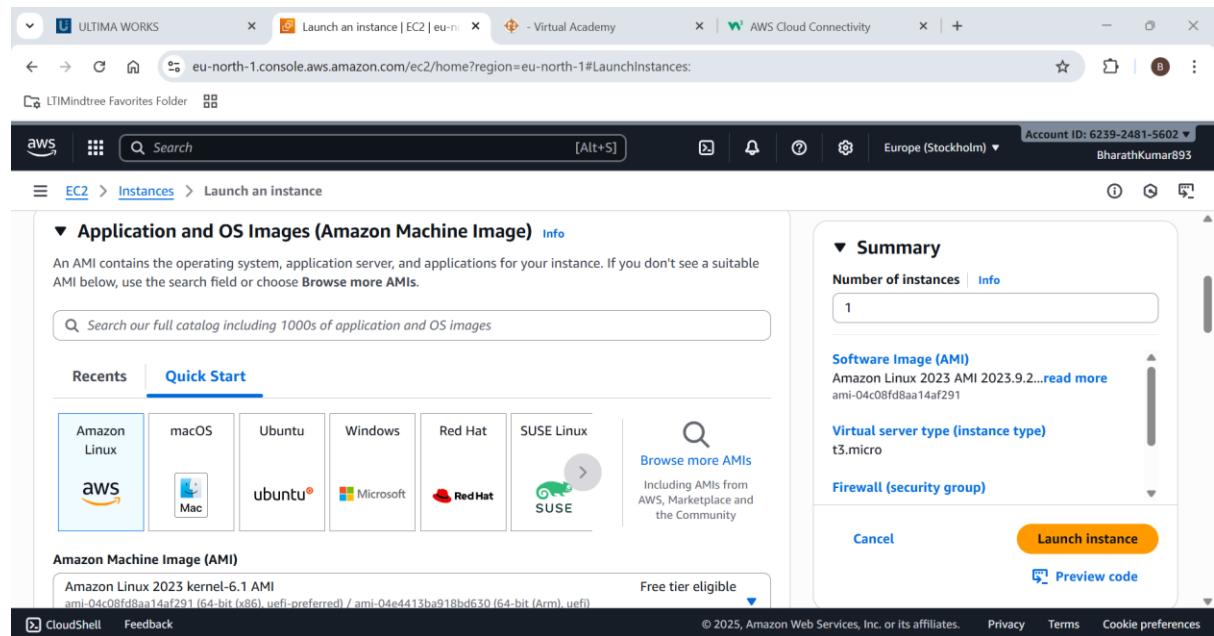
Step 1: Open EC2 Service



Step 2: Launch an instance .Give name for your EC2 Instance.



Step 3: Select your AMI as Amazon linux



ULTIMA WORKS

Launch an instance | EC2 | eu-n

- Virtual Academy

AWS Cloud Connectivity

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

LTIMindtree Favorites Folder

Search

EC2 > Instances > Launch an instance

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

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

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-04c08fd8aa14af291 (64-bit (x86), uefi-preferred) / ami-04e4413ba918bd630 (64-bit (Arm), uefi)

Free tier eligible

CloudShell Feedback

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

Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2... [read more](#)
ami-04c08fd8aa14af291

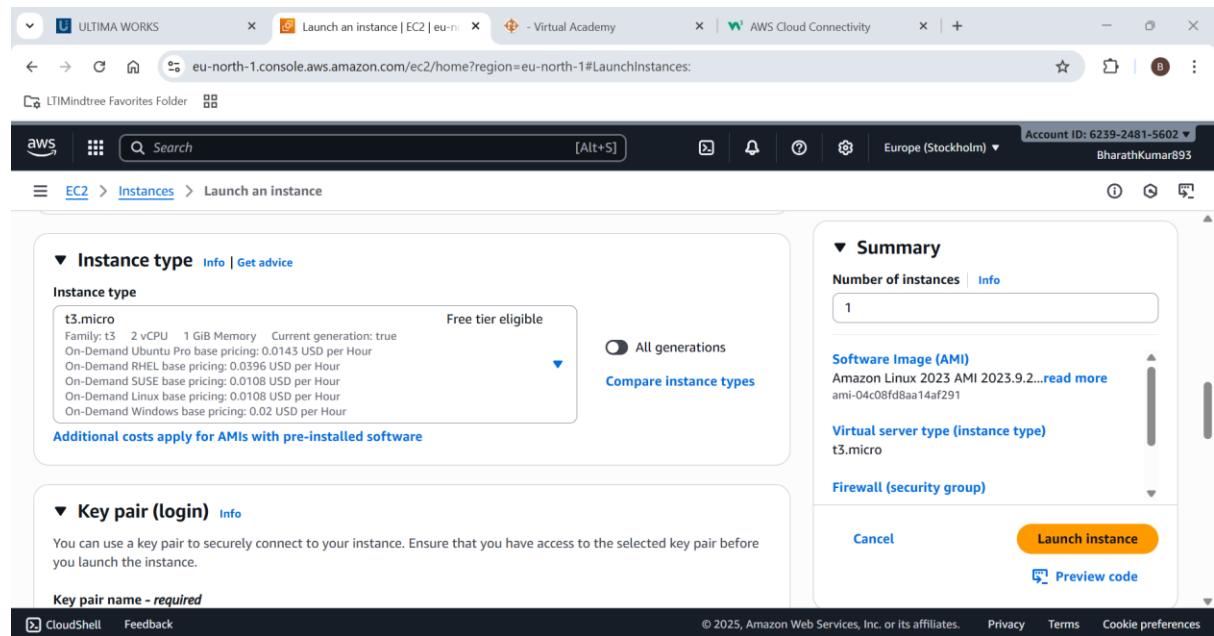
Virtual server type (instance type)

t3.micro

Firewall (security group)

Cancel [Launch instance](#) [Preview code](#)

Step 4: Choose your instance type (here t as it is free tier)



ULTIMA WORKS

Launch an instance | EC2 | eu-n

- Virtual Academy

AWS Cloud Connectivity

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

LTIMindtree Favorites Folder

Search

EC2 > Instances > Launch an instance

Instance type [Info](#) | [Get advice](#)

Instance type

t3.micro Free tier eligible

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand Ubuntu Pro base pricing: 0.0143 USD per Hour

On-Demand RHEL base pricing: 0.0396 USD per Hour

On-Demand SUSE base pricing: 0.0108 USD per Hour

On-Demand Linux base pricing: 0.0108 USD per Hour

On-Demand Windows base pricing: 0.02 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

CloudShell Feedback

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

Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2... [read more](#)
ami-04c08fd8aa14af291

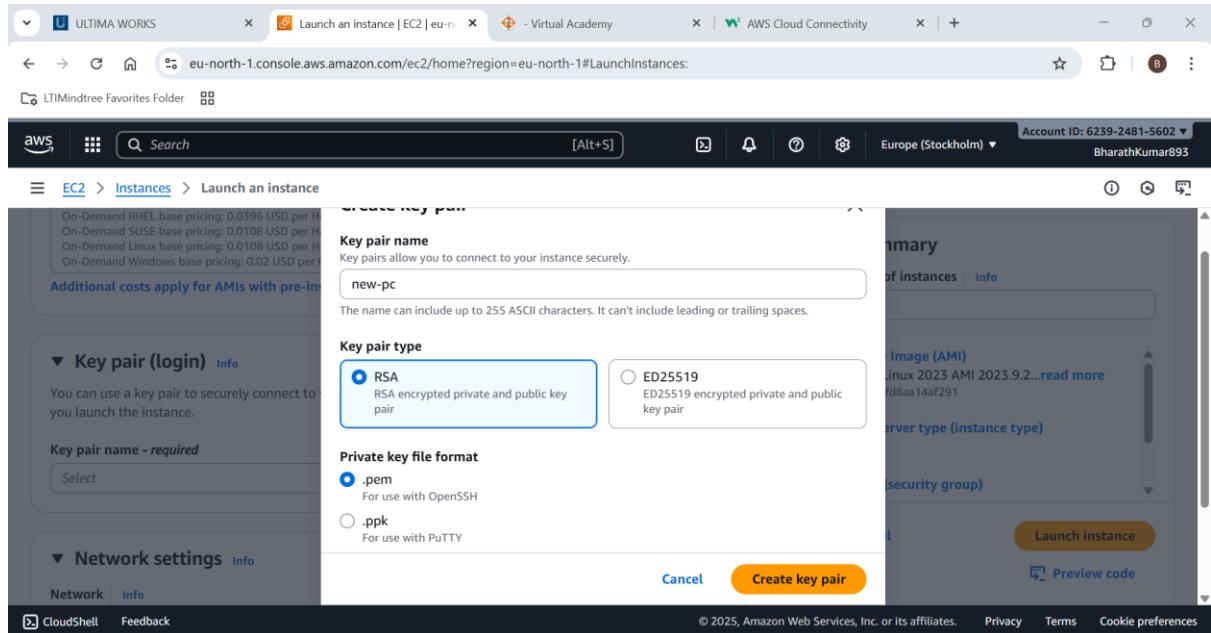
Virtual server type (instance type)

t3.micro

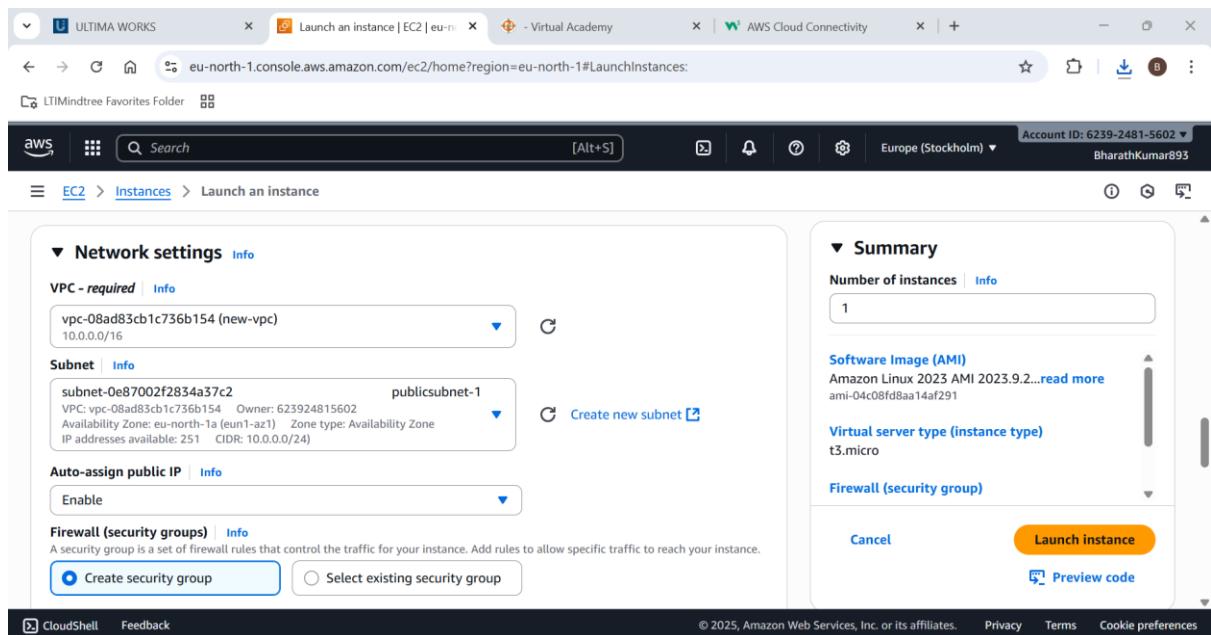
Firewall (security group)

Cancel [Launch instance](#) [Preview code](#)

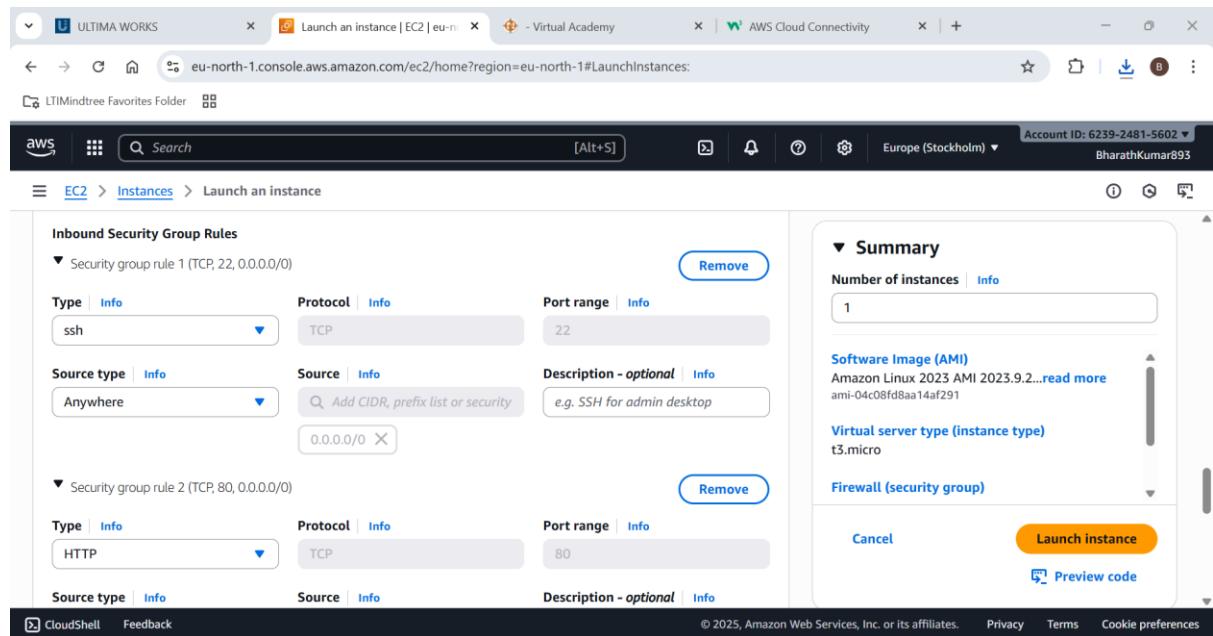
Step 5: Create a key value pair for later connections



Step 6: Configure your network settings (Choose your VPC, Subnet and enable auto ip assign)



Step 7: Configure security group rules (Add http)



Inbound Security Group Rules

- Security group rule 1 (TCP, 22, 0.0.0.0/0)
 - Type: ssh
 - Protocol: TCP
 - Port range: 22
 - Source type: Anywhere
 - Source: 0.0.0.0/0
 - Description - optional: e.g. SSH for admin desktop
- Security group rule 2 (TCP, 80, 0.0.0.0/0)
 - Type: HTTP
 - Protocol: TCP
 - Port range: 80
 - Source type: Anywhere
 - Source: 0.0.0.0/0
 - Description - optional:

Summary

Number of instances: 1

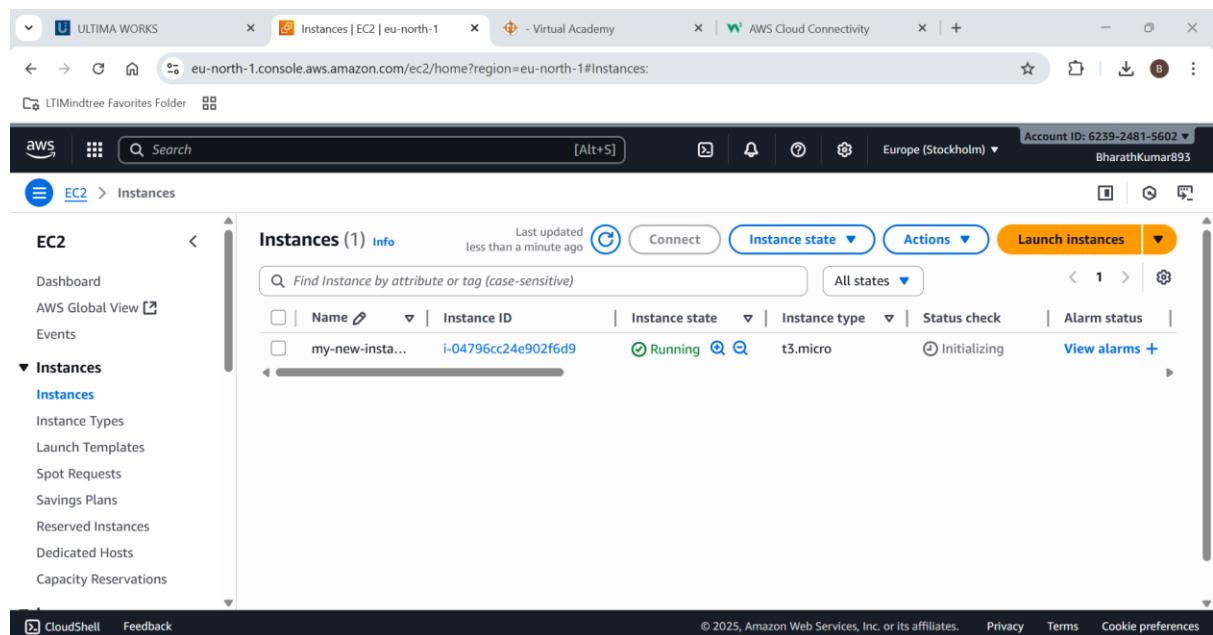
Software Image (AMI): Amazon Linux 2023 AMI 2023.9.2...read more

Virtual server type (instance type): t3.micro

Firewall (security group)

Launch instance

Our new EC2 instance is created



EC2

Instances (1) info

Last updated less than a minute ago

Connect Instance state Actions Launch instances

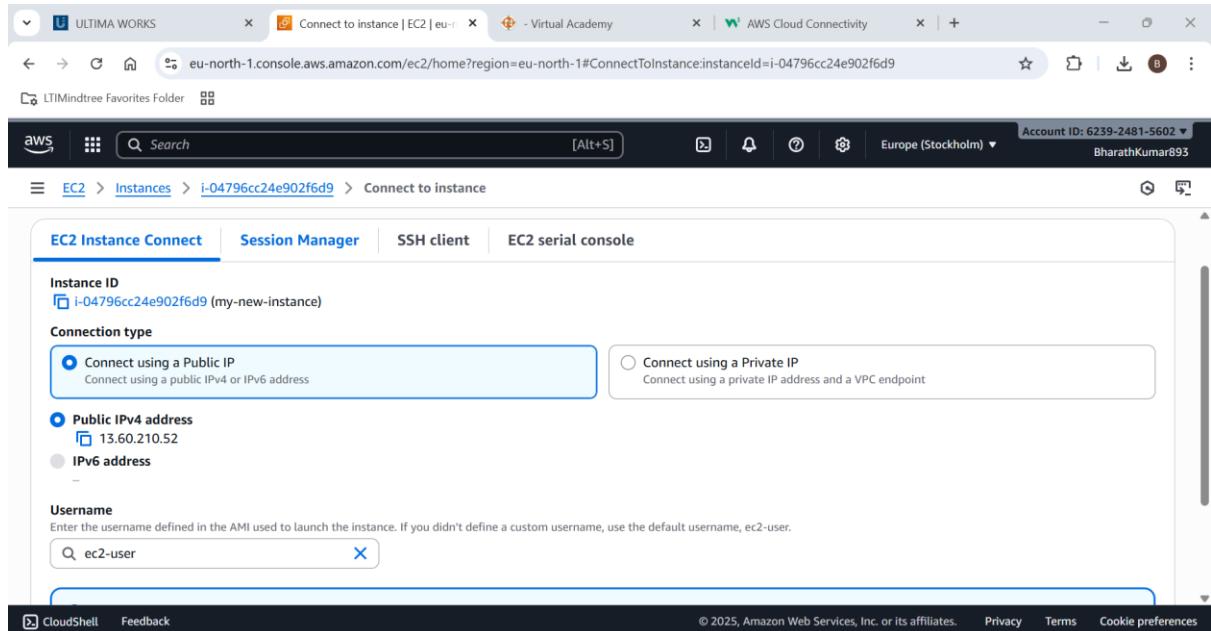
Name	Instance ID	Instance state	Instance type	Status check	Alarm status
my-new-inst...	i-04796cc24e902f6d9	Running	t3.micro	Initializing	View alarms +

Find Instance by attribute or tag (case-sensitive)

All states

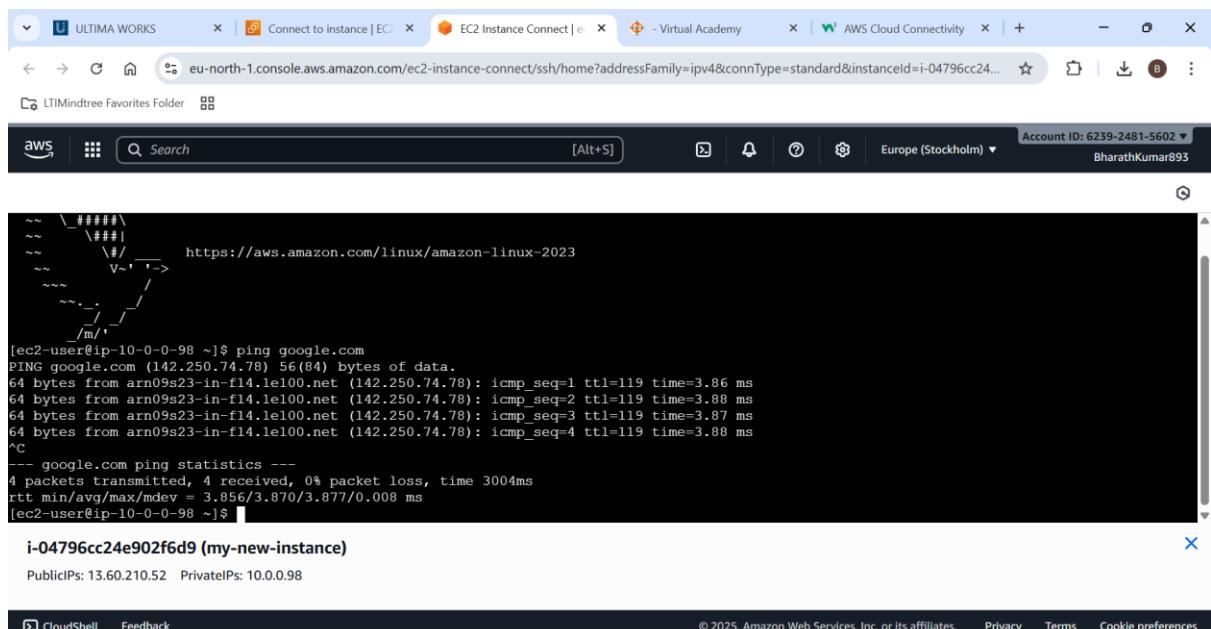
CloudShell Feedback

Step 8: Connect to your instance



The screenshot shows the AWS EC2 Instance Connect interface. At the top, the instance ID is listed as **i-04796cc24e902f6d9 (my-new-instance)**. Under the **Connection type** section, the **Public IPv4 address** is selected, showing **13.60.210.52**. The **Username** field contains **ec2-user**. The interface includes tabs for **EC2 Instance Connect**, **Session Manager**, **SSH client**, and **EC2 serial console**. The status bar at the bottom indicates the account ID is **6239-2481-5602** and the region is **Europe (Stockholm)**.

Step 9: Try to Connect it to the internet



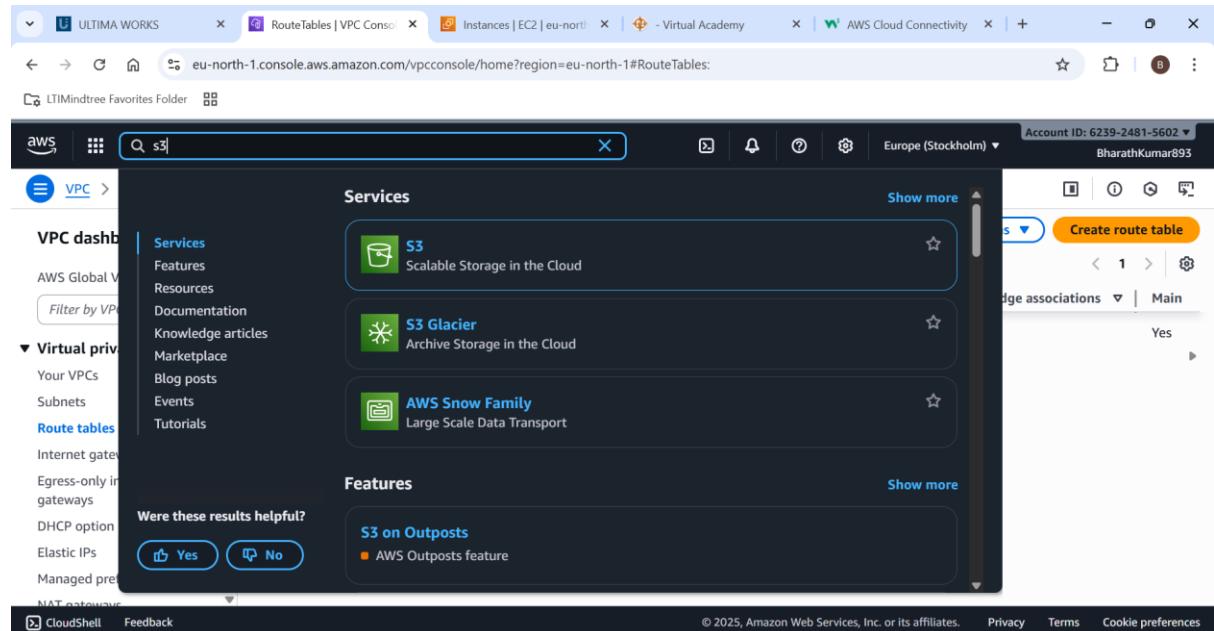
The screenshot shows the EC2 Instance Connect terminal window. The terminal output shows a successful ping to **google.com** with a round-trip time of **3.86 ms**. The terminal prompt is **[ec2-user@ip-10-0-0-98 ~]\$**. The status bar at the bottom indicates the instance ID is **i-04796cc24e902f6d9 (my-new-instance)** and the public IP is **13.60.210.52**.

```
~~ \_\#\#\#\`\\#\#\#
~~ \#\#` V-` ,--> https://aws.amazon.com/linux/amazon-linux-2023
~~ /` /
~~ .` /` /
~~ /` /` /
/m/`[ec2-user@ip-10-0-0-98 ~]$ ping google.com
PING google.com (142.250.74.78) 56(84) bytes of data.
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=1 ttl=119 time=3.86 ms
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=2 ttl=119 time=3.88 ms
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=3 ttl=119 time=3.87 ms
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=4 ttl=119 time=3.88 ms
```
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 3.856/3.870/3.877/0.008 ms
[ec2-user@ip-10-0-0-98 ~]$
```

An EC2 instance is created and is done successfully.

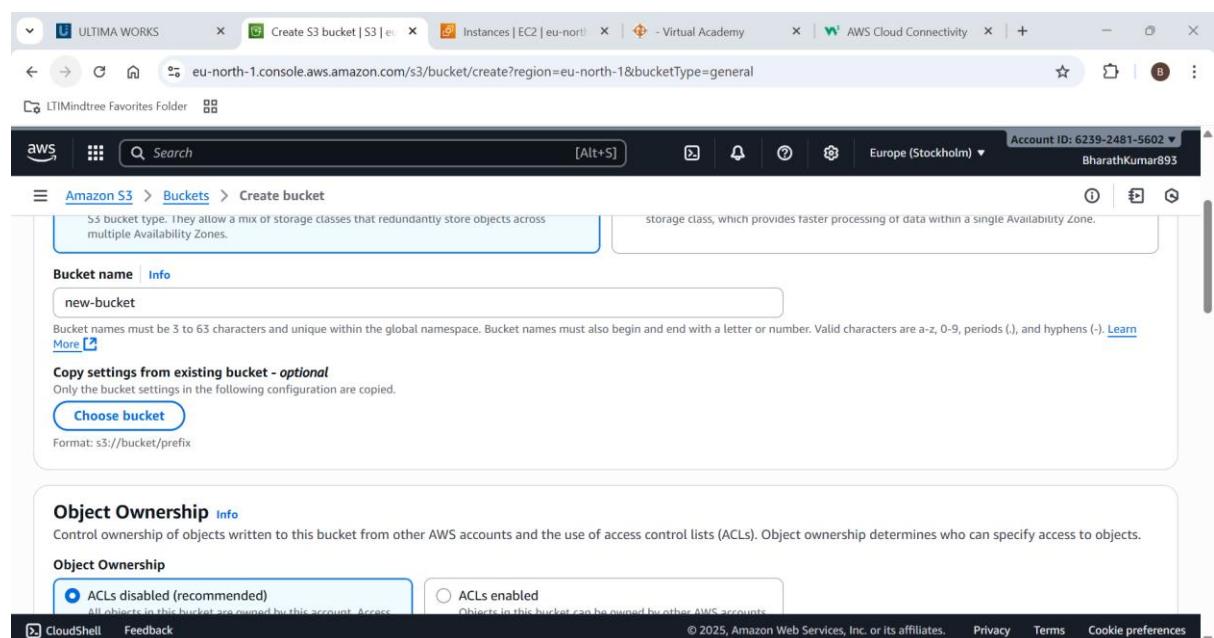
## 2. Create an S3 bucket, upload a file, and make it publicly accessible.

### Step 1: Open S3 bucket service



The screenshot shows the AWS VPC console with a search bar at the top containing 's3'. The 'Services' section is expanded, showing 'S3 Scalable Storage in the Cloud' as the top result. Other services listed include 'S3 Glacier Archive Storage in the Cloud' and 'AWS Snow Family Large Scale Data Transport'. The 'Features' section below shows 'S3 on Outposts' and 'AWS Outposts feature'. On the right side of the screen, there is a 'Create route table' button and a 'Route tables' section with a table showing route table associations.

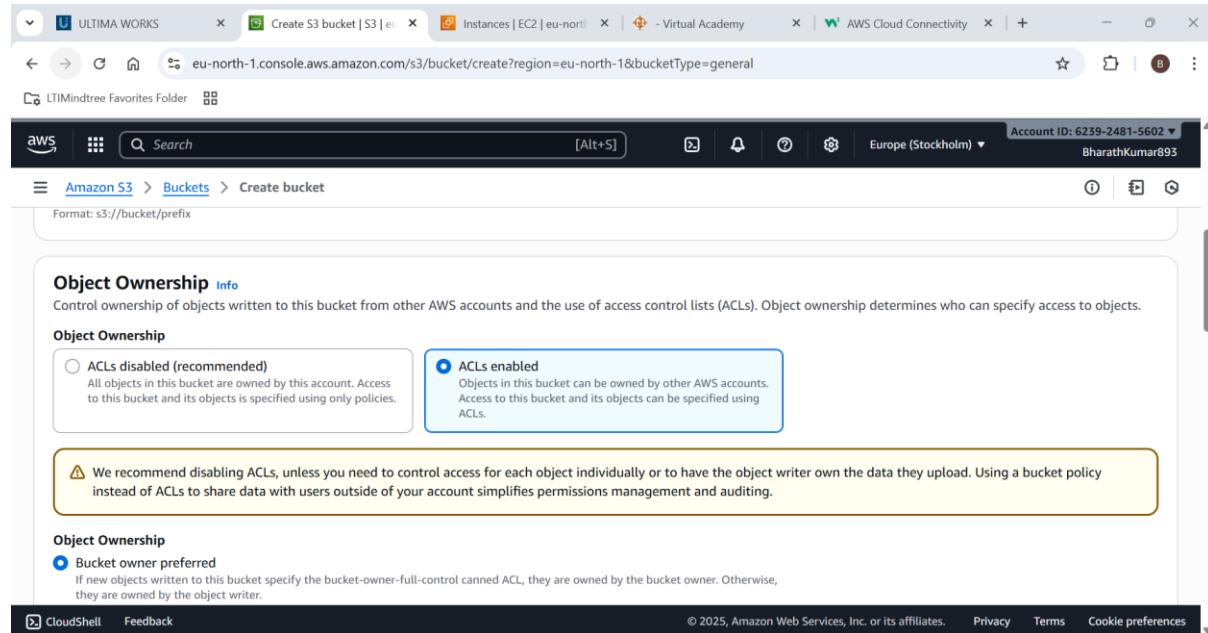
### Step 2: Create a bucket service and give it a name.



The screenshot shows the 'Create bucket' wizard in the AWS S3 console. The 'Bucket name' field is populated with 'new-bucket'. Below the field, a note states: 'Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)'.

Under the 'Object Ownership' section, there are two options: 'ACLs disabled (recommended)' (selected) and 'ACLs enabled'. The 'ACLs disabled' option is described as 'All objects in this bucket are owned by this account. Access'.

## Step 3: Enable ACL



Object Ownership Info  
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

**ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

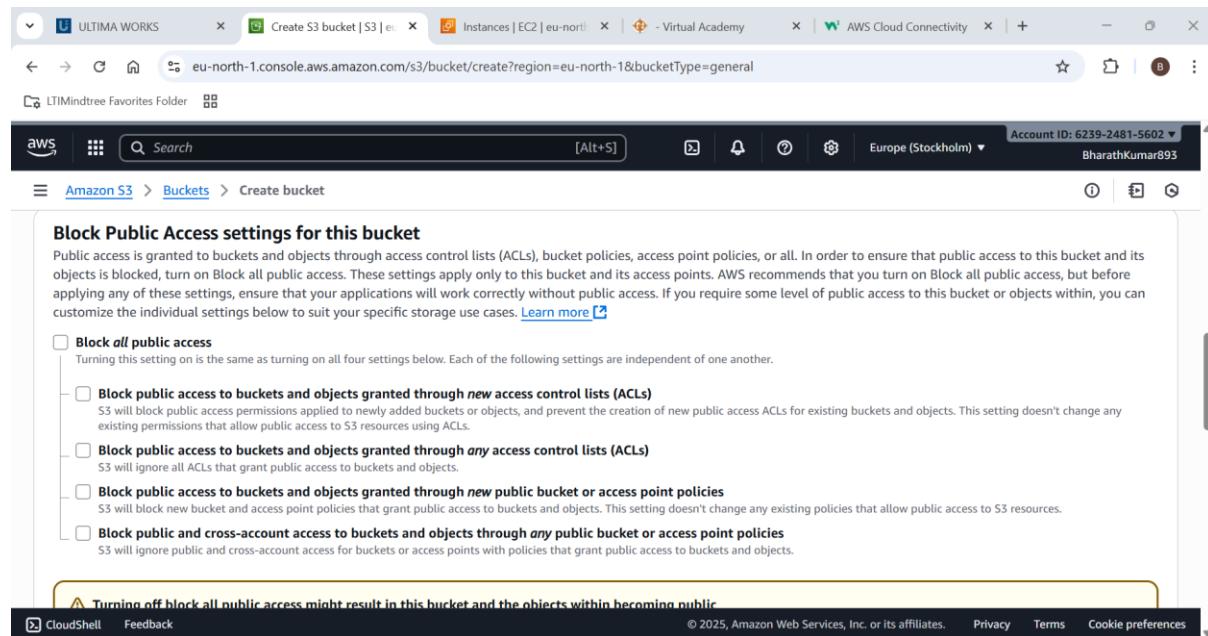
**ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**⚠️** We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

**Object Ownership**  
 **Bucket owner preferred**  
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

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

## Step 4: Disable the blocked public access settings



**Block Public Access settings for this bucket**  
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

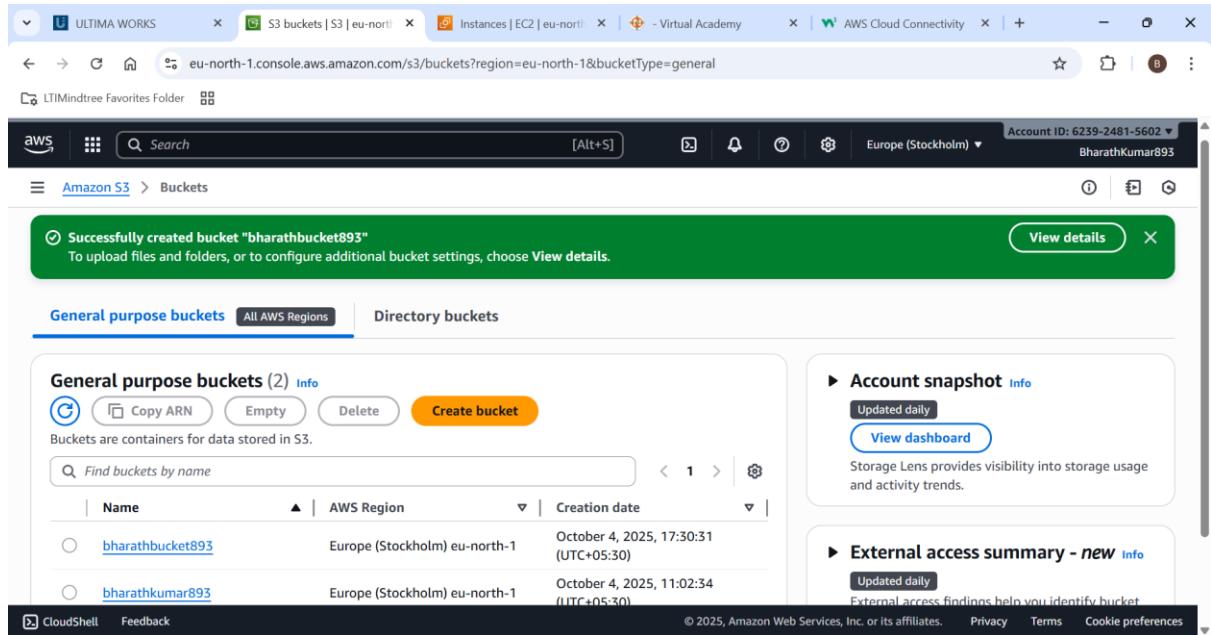
**Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**⚠️** Turning off block all public access might result in this bucket and the objects within becoming public

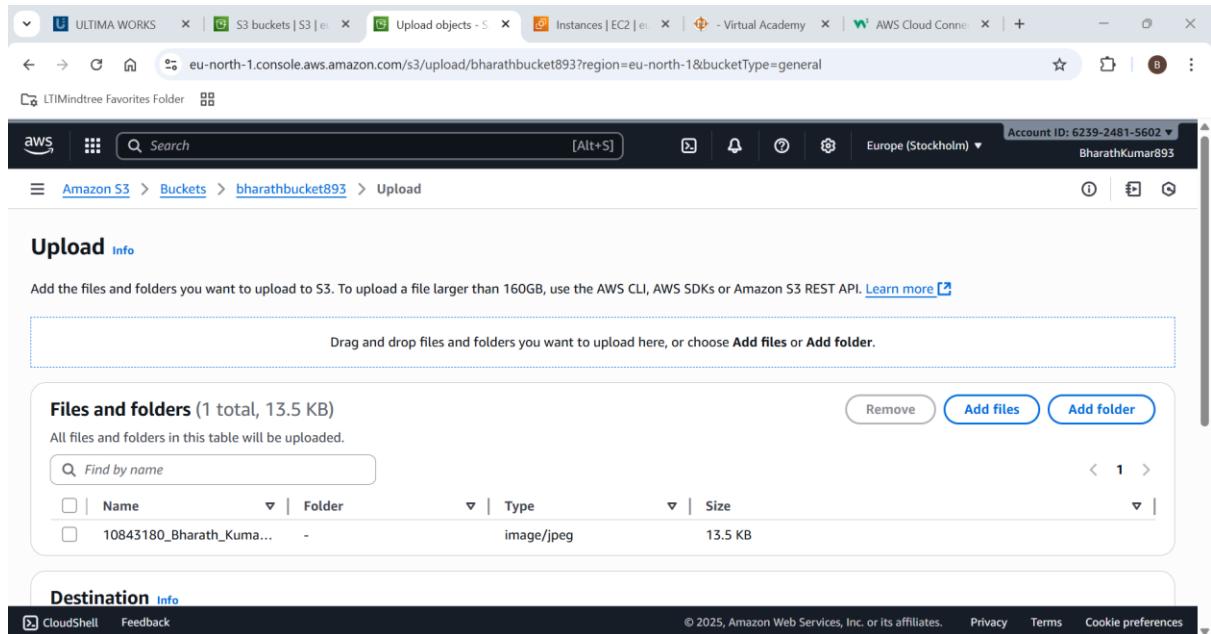
CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## A bucket is created



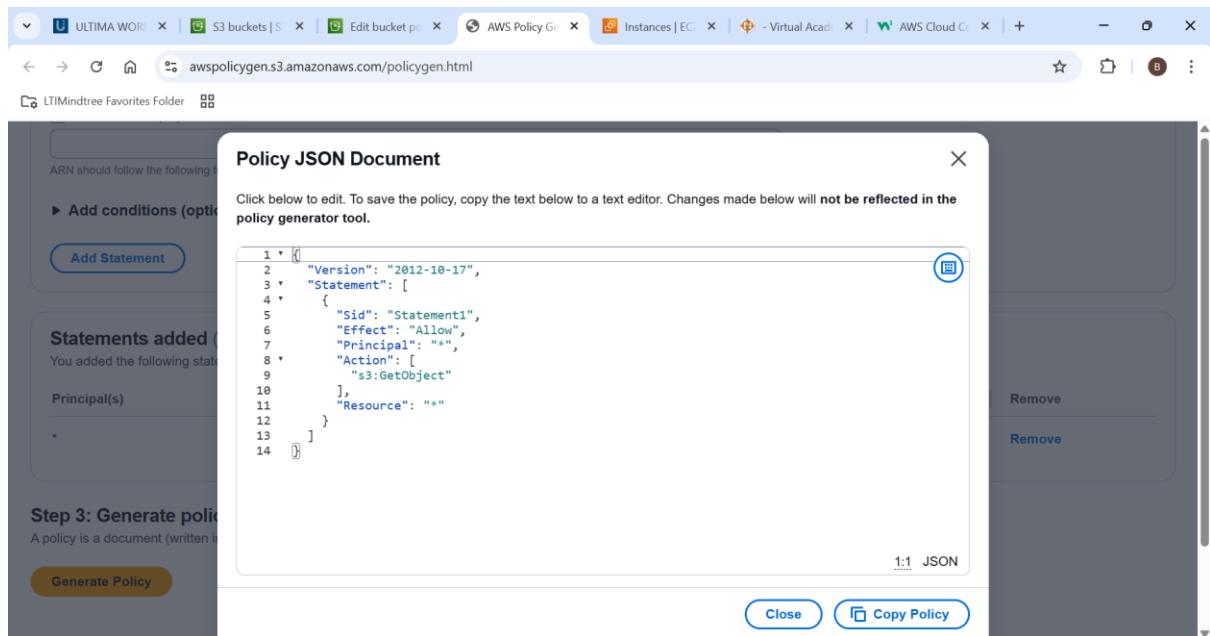
The screenshot shows the AWS S3 buckets page. At the top, a green success message box states: "Successfully created bucket 'bharathbucket893'. To upload files and folders, or to configure additional bucket settings, choose View details." Below this, the "General purpose buckets" section is visible, showing two buckets: "bharathbucket893" and "bharathkumar893". The "bharathbucket893" bucket is selected. On the right side of the page, there are "Account snapshot" and "External access summary" sections. The bottom of the page includes standard AWS navigation links like CloudShell and Feedback.

## Step 5: Upload a file in S3 bucket.



The screenshot shows the AWS S3 upload objects page. The URL in the address bar is "eu-north-1.console.aws.amazon.com/s3/upload/bharathbucket893?region=eu-north-1&bucketType=general". The main area is titled "Upload" and contains a large blue "Drag and drop files and folders you want to upload here, or choose Add files or Add folder." button. Below this, a "Files and folders" table shows one item: "10843180\_Bharath\_Kuma..." (13.5 KB). The "Destination" section is empty. The bottom of the page includes standard AWS navigation links like CloudShell and Feedback.

## Step 6: Generate a S3 bucket policy

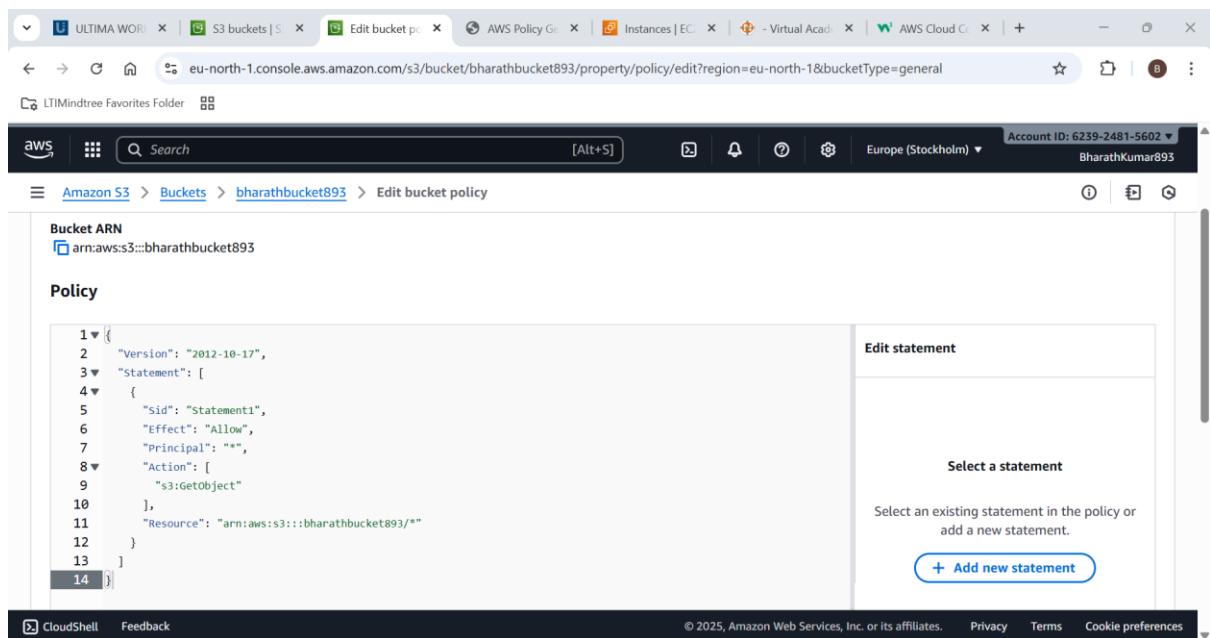


The screenshot shows the AWS Policy Generator tool interface. The main area displays a Policy JSON Document with the following content:

```
1 {
2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Sid": "Statement1",
6 "Effect": "Allow",
7 "Principal": "*",
8 "Action": [
9 "s3:GetObject"
10],
11 "Resource": "*"
12 }
13]
14 }
```

Below the JSON editor, there are buttons for "Close" and "Copy Policy". To the right, there are "Remove" buttons for statements. The interface also includes sections for "ARN should follow the following format" and "Add conditions (optional)".

## Step 7: Add your arn number in the resource for allowing access.

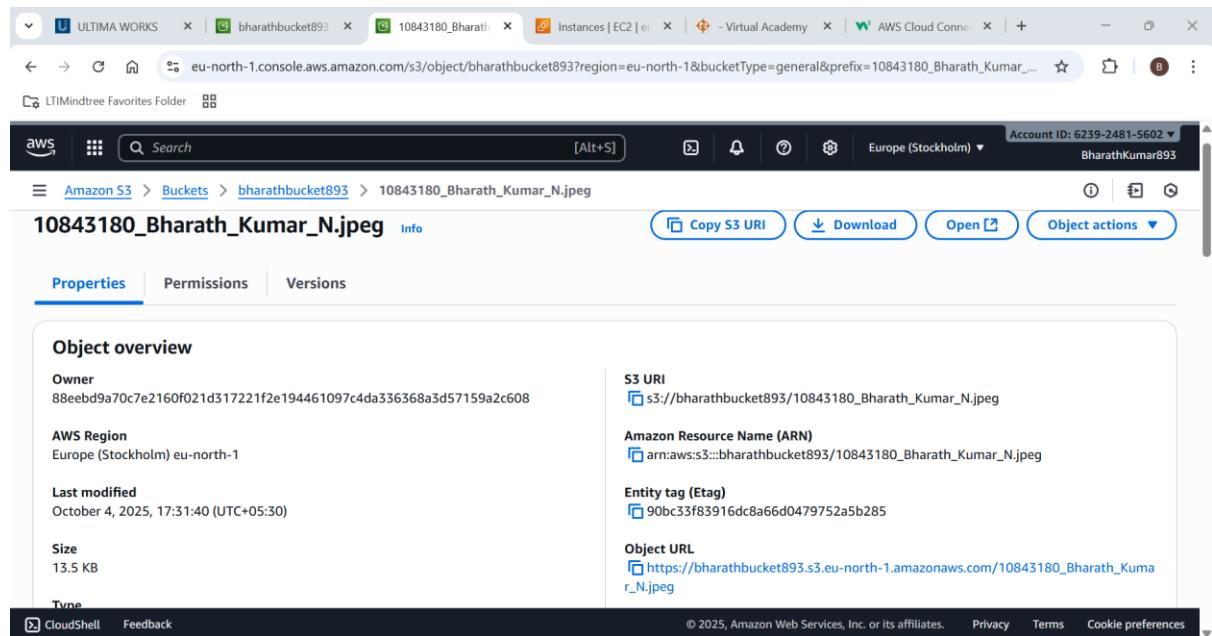


The screenshot shows the AWS S3 Bucket Policy editor for the bucket "bharathbucket893". The "Policy" section displays the following JSON policy:

```
1 {
2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Sid": "Statement1",
6 "Effect": "Allow",
7 "Principal": "*",
8 "Action": [
9 "s3:GetObject"
10],
11 "Resource": "arn:aws:s3:::bharathbucket893/*"
12 }
13]
14 }
```

To the right of the policy editor, there is a "Select a statement" dropdown and a "+ Add new statement" button. The top of the screen shows the AWS navigation bar and the user account information.

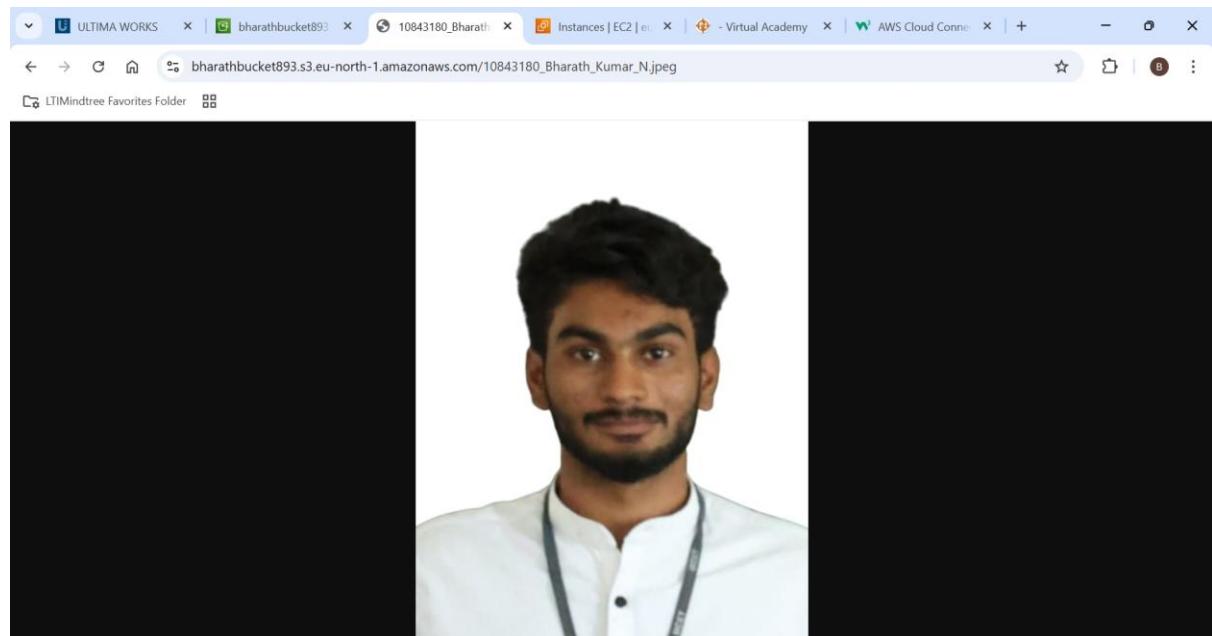
Now this displays the details about the resource



The screenshot shows the AWS S3 Object Details page for the file '10843180\_Bharath\_Kumar\_N.jpeg'. The object is located in the 'bharathbucket893' bucket. The 'Properties' tab is selected, displaying the following details:

| Object overview            | Properties                                                                                                                                                                          |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Owner                      | 88eebd9a70c7e2160f021d317221f2e194461097c4da336368a3d57159a2c608                                                                                                                    |
| AWS Region                 | Europe (Stockholm) eu-north-1                                                                                                                                                       |
| Last modified              | October 4, 2025, 17:31:40 (UTC+05:30)                                                                                                                                               |
| Size                       | 13.5 KB                                                                                                                                                                             |
| Type                       |                                                                                                                                                                                     |
| S3 URI                     | <a href="s3://bharathbucket893/10843180_Bharath_Kumar_N.jpeg">s3://bharathbucket893/10843180_Bharath_Kumar_N.jpeg</a>                                                               |
| Amazon Resource Name (ARN) | <a href="arn:aws:s3:::bharathbucket893/10843180_Bharath_Kumar_N.jpeg">arn:aws:s3:::bharathbucket893/10843180_Bharath_Kumar_N.jpeg</a>                                               |
| Entity tag (Etag)          | <a href="#">90bc3f83916dc8a66d0479752a5b285</a>                                                                                                                                     |
| Object URL                 | <a href="https://bharathbucket893.s3.eu-north-1.amazonaws.com/10843180_Bharath_Kumar_N.jpeg">https://bharathbucket893.s3.eu-north-1.amazonaws.com/10843180_Bharath_Kumar_N.jpeg</a> |

Now open the object URL

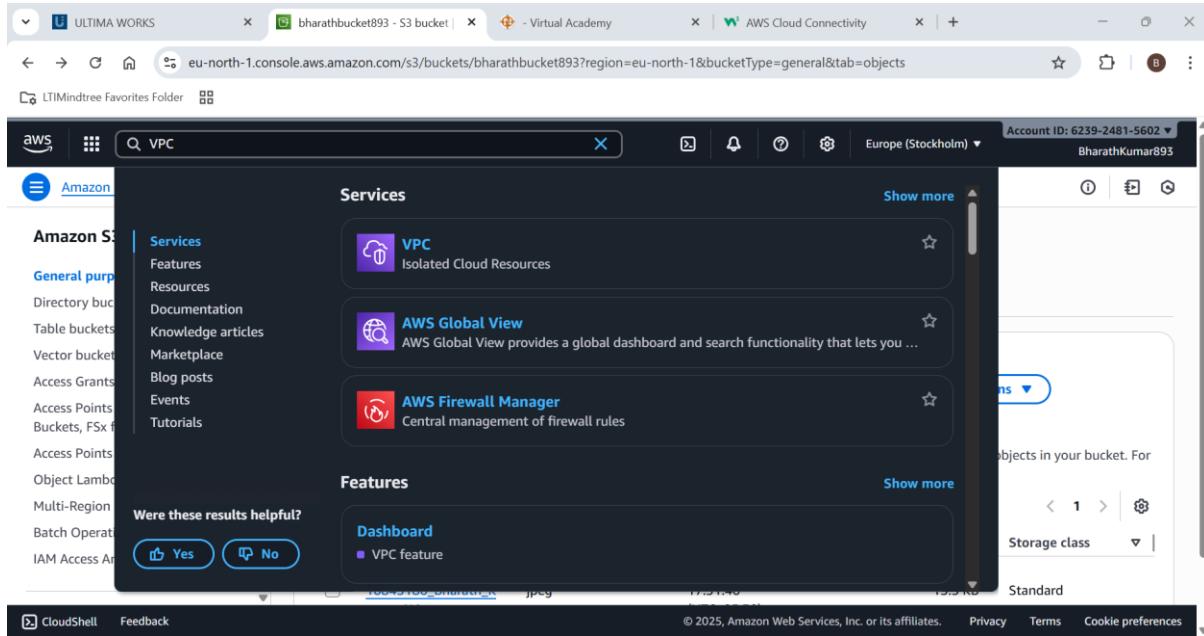


The screenshot shows a web browser displaying the image at the object URL. The image is a portrait of a young man with dark hair and a beard, wearing a white shirt. The image is centered on a white background, surrounded by black borders on the left and right sides.

If the Object is displayed in the URL , the experiment was a success.

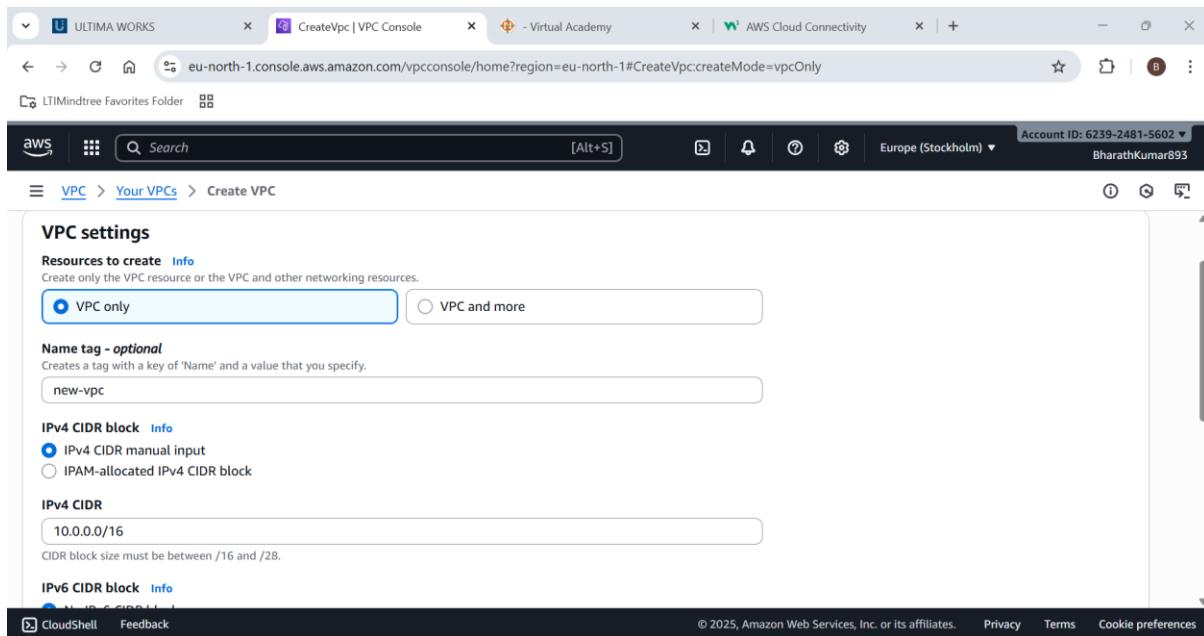
### 3. Configure a VPC with 2 public and 2 private subnets.

#### Step 1: Open VPC service



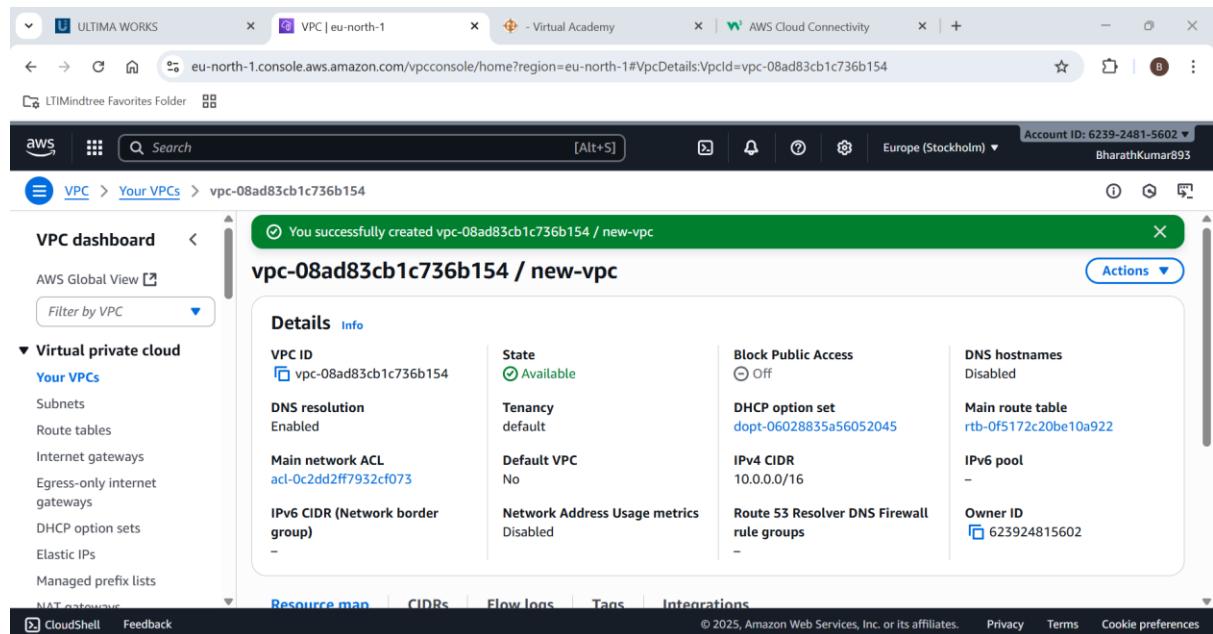
The screenshot shows the AWS Services page. The VPC service is selected and highlighted with a blue border. Other services like AWS Global View and AWS Firewall Manager are also listed. The page includes a sidebar with general purpose services and a features section with a dashboard.

Give VPC name,CIDR range



The screenshot shows the 'Create VPC' console. Under 'VPC settings', the 'Resources to create' dropdown is set to 'VPC only'. A 'Name tag - optional' field contains 'new-vc'. Under 'IPv4 CIDR block', the input is '10.0.0.0/16'. The page also includes sections for 'IPv6 CIDR block' and 'Subnet settings'.

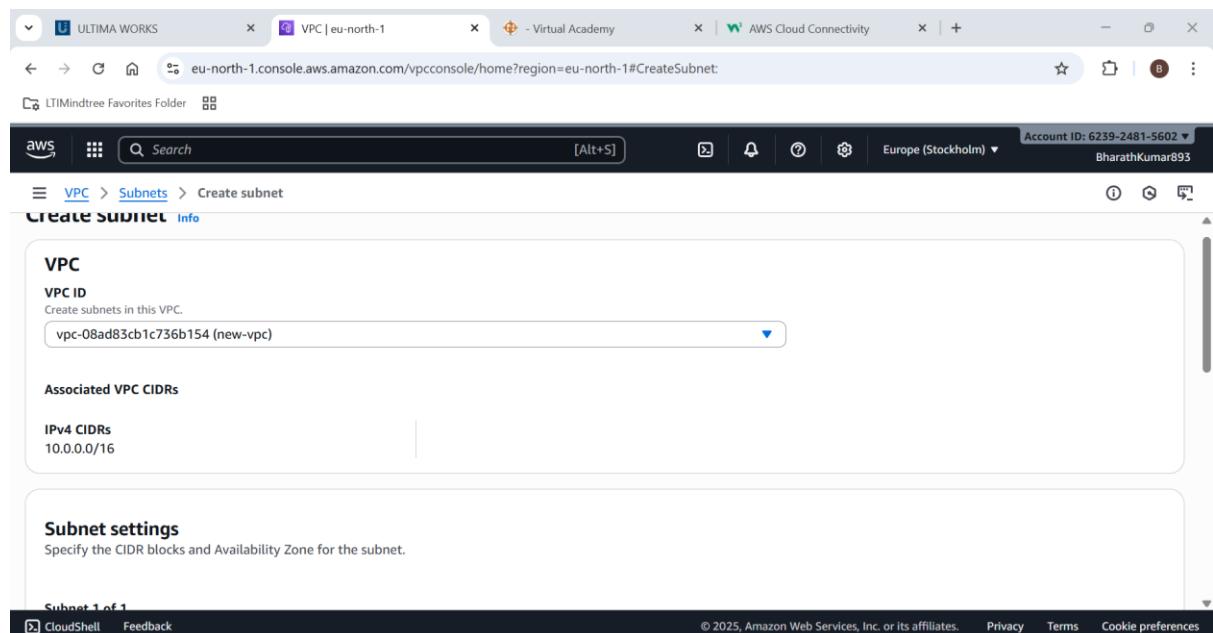
## VPC Created Successfully



The screenshot shows the AWS VPC console with a success message: "You successfully created **new-vpc**". The VPC details are listed as follows:

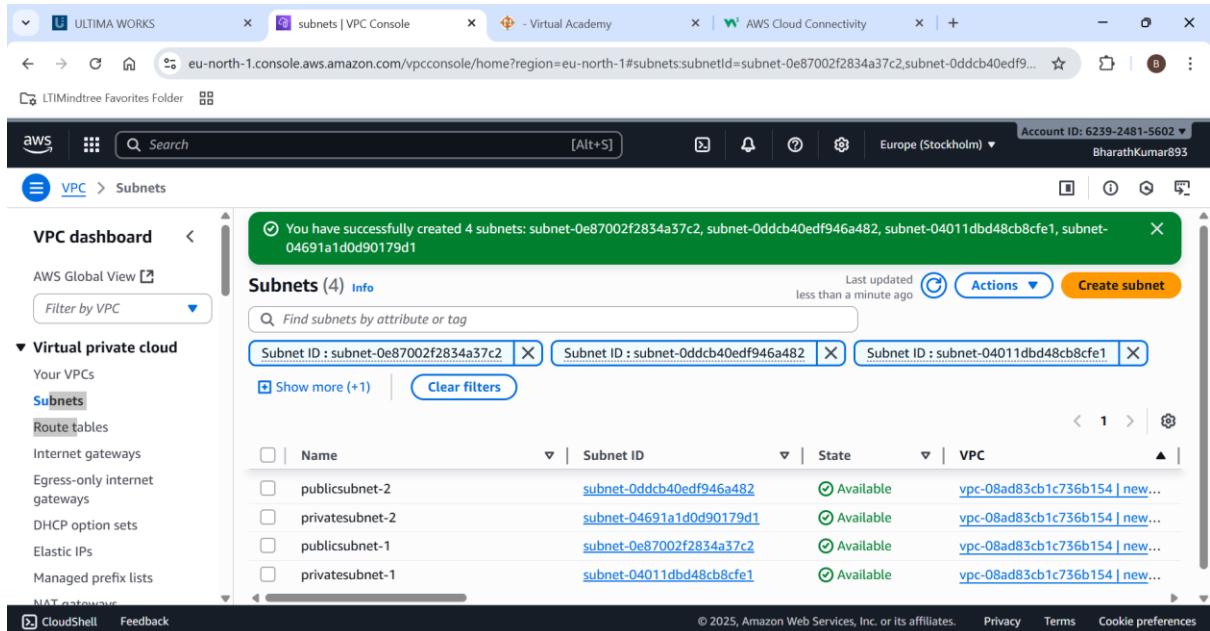
| Details                          |                       | Info                                       |                       |
|----------------------------------|-----------------------|--------------------------------------------|-----------------------|
| VPC ID                           | vpc-08ad83cb1c736b154 | State                                      | Available             |
| DNS resolution                   | Enabled               | Tenancy                                    | default               |
| Main network ACL                 | acl-0c2dd2ff7932cf073 | Default VPC                                | No                    |
| IPv6 CIDR (Network border group) | -                     | Network Address Usage metrics              | Disabled              |
|                                  |                       | Route 53 Resolver DNS Firewall rule groups | -                     |
|                                  |                       | DNS hostnames                              | Disabled              |
|                                  |                       | Main route table                           | rtb-0f5172c20be10a922 |
|                                  |                       | IPv6 pool                                  | -                     |
|                                  |                       | Owner ID                                   | 623924815602          |

Go to subnets and add your VPC to it



The screenshot shows the "Create subnet" wizard. The "VPC" section shows the VPC ID: **vpc-08ad83cb1c736b154 (new-vpc)**. The "Associated VPC CIDRs" section shows the IPv4 CIDR: **10.0.0.0/16**. The "Subnet settings" section is currently empty, with the subtext: "Specify the CIDR blocks and Availability Zone for the subnet." The wizard is on "Subnet 1 of 1".

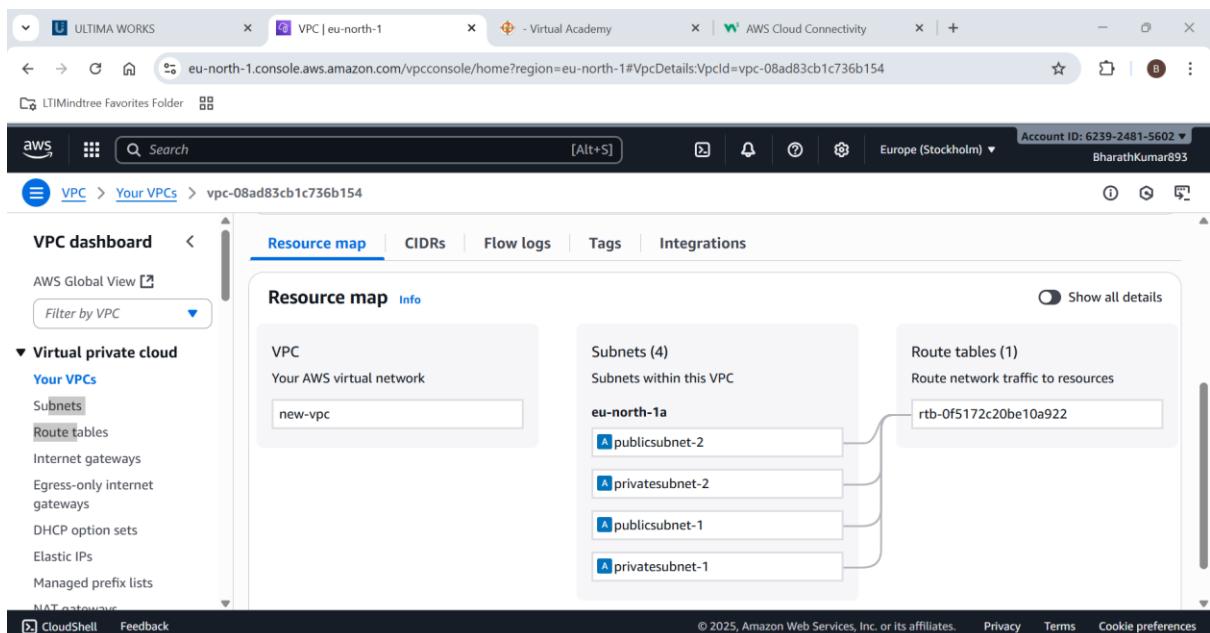
Create 2 public and 2 private subnet to it



The screenshot shows the AWS VPC Subnets page. A success message at the top states: "You have successfully created 4 subnets: subnet-0e87002f2834a37c2, subnet-0ddcb40edf946a482, subnet-04011dbd48cb8cfe1, subnet-04691a1d0d90179d1". The Subnets table lists four entries:

| Name            | Subnet ID                | State     | VPC                            |
|-----------------|--------------------------|-----------|--------------------------------|
| publicsubnet-2  | subnet-0ddcb40edf946a482 | Available | vpc-08ad83cb1c736b154   new... |
| privatesubnet-2 | subnet-04691a1d0d90179d1 | Available | vpc-08ad83cb1c736b154   new... |
| publicsubnet-1  | subnet-0e87002f2834a37c2 | Available | vpc-08ad83cb1c736b154   new... |
| privatesubnet-1 | subnet-04011dbd48cb8cfe1 | Available | vpc-08ad83cb1c736b154   new... |

Here the resource map displays the subnets and its associations



The screenshot shows the AWS VPC Resource map page for the VPC `vpc-08ad83cb1c736b154`. The Resource map displays the following associations:

- VPC:** `new-vpc`
- Subnets (4):** `eu-north-1a` (publicsubnet-2, privatesubnet-2, publicsubnet-1, privatesubnet-1)
- Route tables (1):** `rtb-0f5172c20be10a922`

Arrows indicate the flow of traffic from the subnets to the route table.

Hence a VPC with 2 public and 2 private subnet is created successfully.

4. Attach an Internet Gateway to a VPC and update the route table to enable internet access.

Step 1: We are using an already opened the VPC

VPC dashboard

**Details**

|                                  |                       |                               |           |                                            |                        |                  |                       |
|----------------------------------|-----------------------|-------------------------------|-----------|--------------------------------------------|------------------------|------------------|-----------------------|
| VPC ID                           | vpc-08ad83cb1c736b154 | State                         | Available | Block Public Access                        | Off                    | DNS hostnames    | Disabled              |
| DNS resolution                   | Enabled               | Tenancy                       | default   | DHCP option set                            | dopt-06028835a56052045 | Main route table | rtb-0f5172c20be10a922 |
| Main network ACL                 | acl-0c2dd2ff7932cf073 | Default VPC                   | No        | IPv4 CIDR                                  | 10.0.0.0/16            | IPv6 pool        | -                     |
| IPv6 CIDR (Network border group) | -                     | Network Address Usage metrics | Disabled  | Route 53 Resolver DNS Firewall rule groups | -                      | Owner ID         | 623924815602          |

Resource map | CIDRs | Flow logs | Tags | Integrations

Create a new gateway

Create internet gateway

**Internet gateway settings**

**Name tag**  
Creates a tag with a key of 'Name' and a value that you specify.  
my-new-IGW

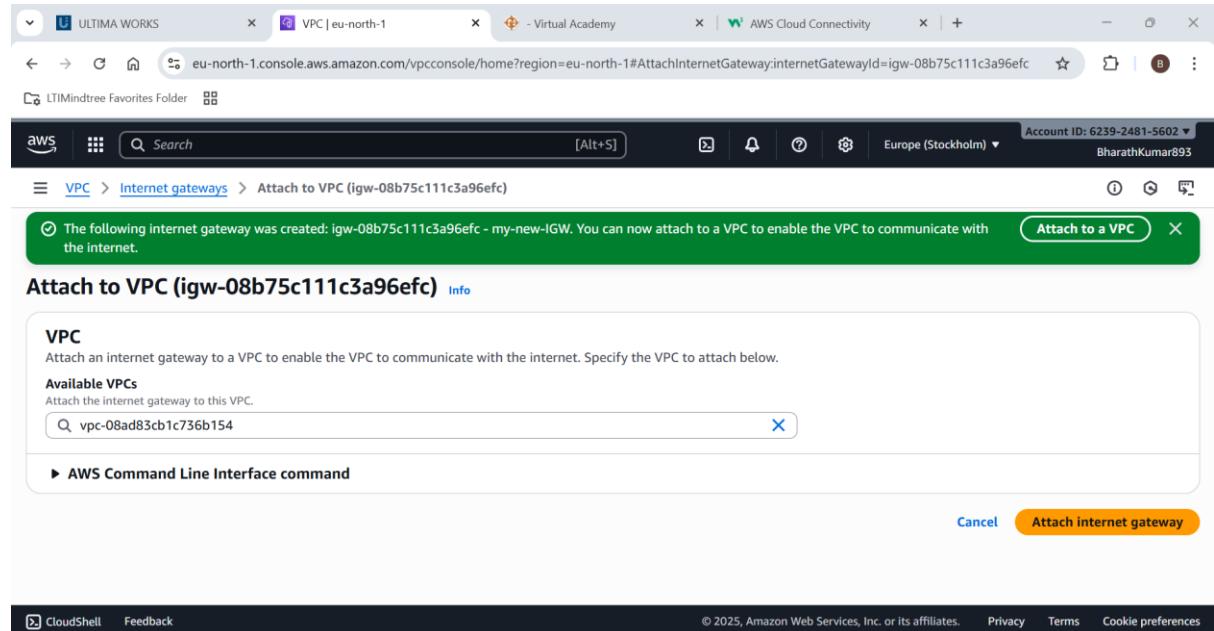
**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

| Key        | Value - optional |
|------------|------------------|
| my-new-IGW | my-new-IGW       |

Add new tag

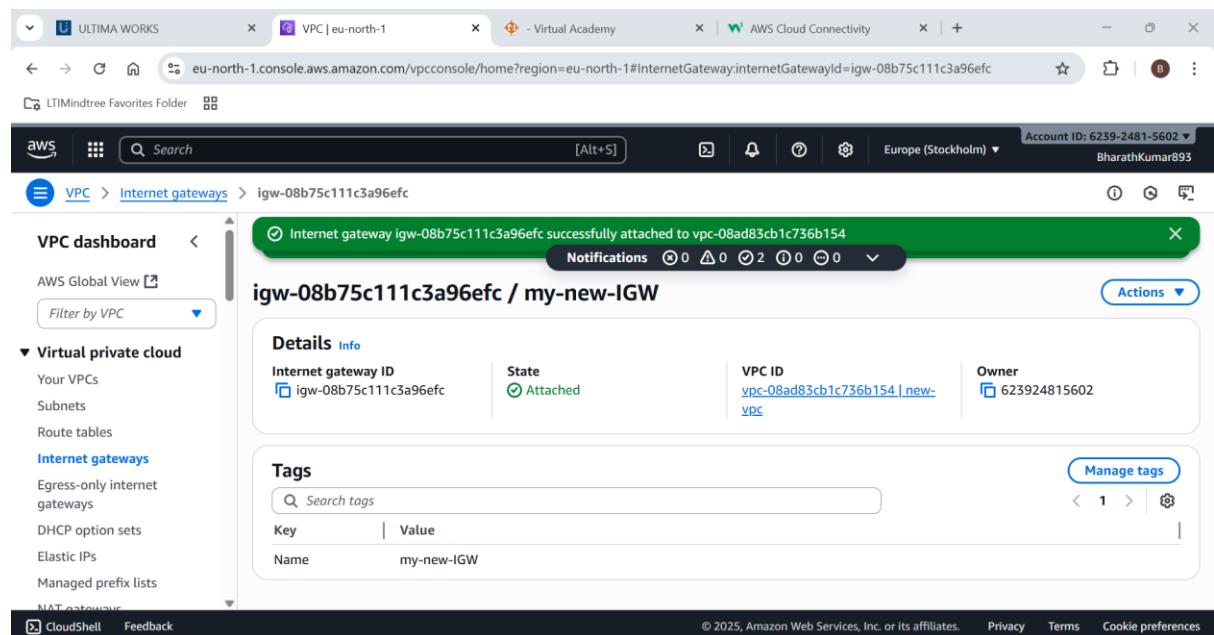
You can add 49 more tags.

## Attach it to the VPC



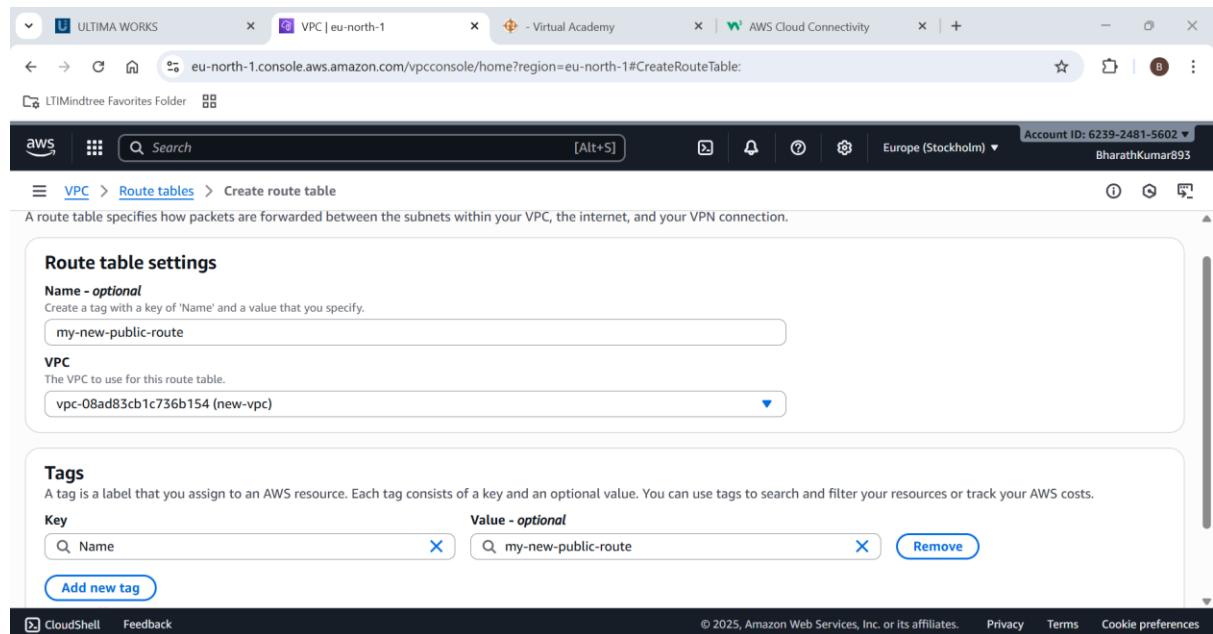
The screenshot shows the AWS VPC console with the URL [eu-north-1.console.aws.amazon.com/vpcconsole/home?region=eu-north-1#AttachInternetGateway:internetGatewayId=igw-08b75c111c3a96efc](https://eu-north-1.console.aws.amazon.com/vpcconsole/home?region=eu-north-1#AttachInternetGateway:internetGatewayId=igw-08b75c111c3a96efc). The page title is "Attach to VPC (igw-08b75c111c3a96efc)". A green success message at the top states: "The following internet gateway was created: igw-08b75c111c3a96efc - my-new-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet." A "Attach to a VPC" button is visible. The main form is titled "VPC" and contains a sub-section "Available VPCs" with a search bar containing "vpc-08ad83cb1c736b154". A "Cancel" button and an "Attach internet gateway" button are at the bottom right. The bottom navigation bar includes "CloudShell" and "Feedback".

## VPC is attached with the Internet gateway



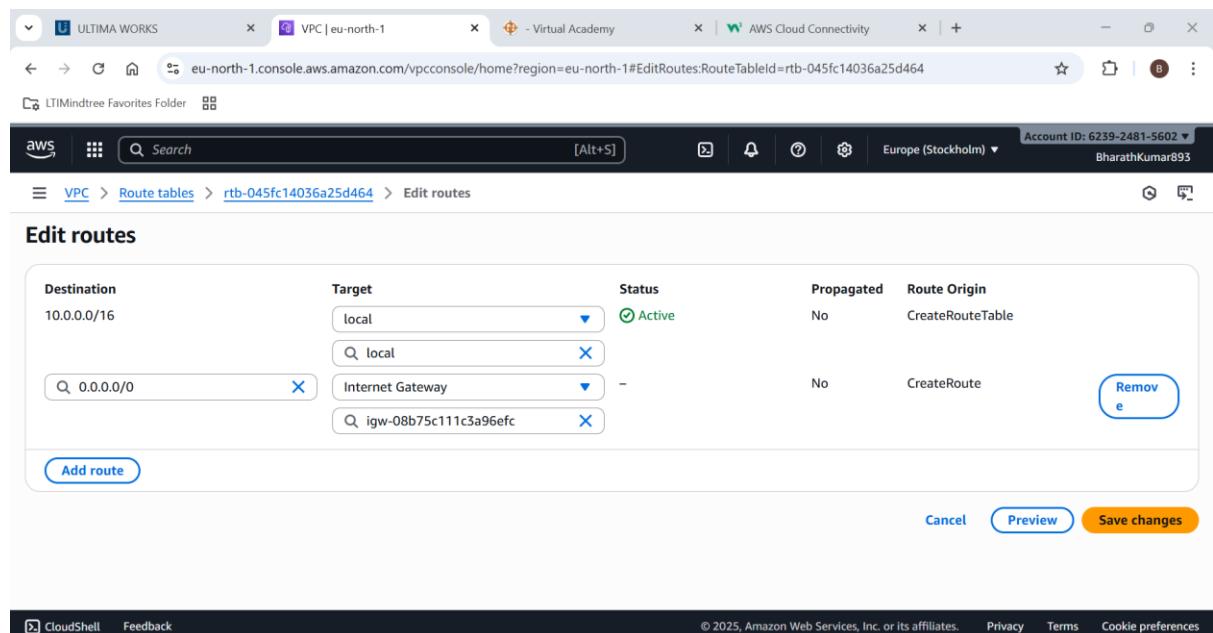
The screenshot shows the AWS VPC dashboard with the URL [eu-north-1.console.aws.amazon.com/vpcconsole/home?region=eu-north-1#InternetGateway:internetGatewayId=igw-08b75c111c3a96efc](https://eu-north-1.console.aws.amazon.com/vpcconsole/home?region=eu-north-1#InternetGateway:internetGatewayId=igw-08b75c111c3a96efc). The page title is "igw-08b75c111c3a96efc / my-new-IGW". A green success message at the top states: "Internet gateway igw-08b75c111c3a96efc successfully attached to vpc-08ad83cb1c736b154". The main content area shows "Details" for the Internet gateway, including its ID (igw-08b75c111c3a96efc), state (Attached), VPC ID (vpc-08ad83cb1c736b154), and owner (623924815602). It also shows a "Tags" section with a single tag: Name: my-new-IGW. A "Manage tags" button is available. The left sidebar shows navigation links for "Virtual private cloud" (Your VPCs, Subnets, Route tables), "Internet gateways" (Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists), and "NAT gateways". The bottom navigation bar includes "CloudShell" and "Feedback".

Now create a routing table and configure it.



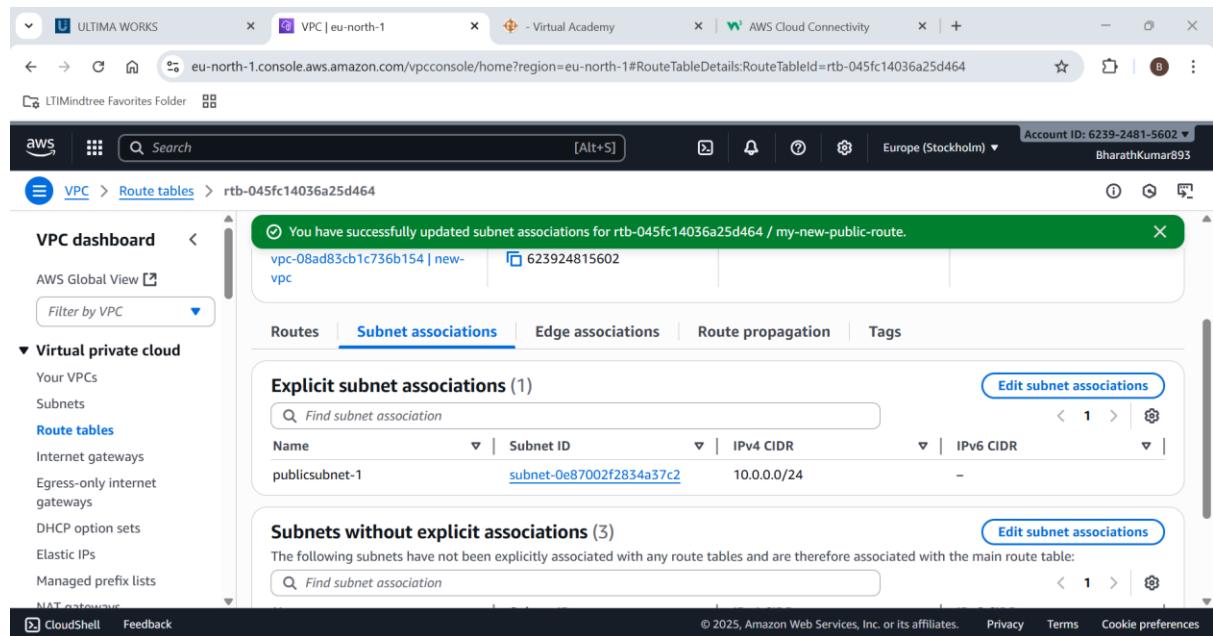
The screenshot shows the 'Create route table' wizard in the AWS VPC console. The 'Route table settings' step is active. A route table is being created with the name 'my-new-public-route'. The VPC selected is 'vpc-08ad83cb1c736b154 (new-vpc)'. A tag 'Name' is added with the value 'my-new-public-route'. The 'Tags' section is also visible.

Add Internet gateway to the public subnet



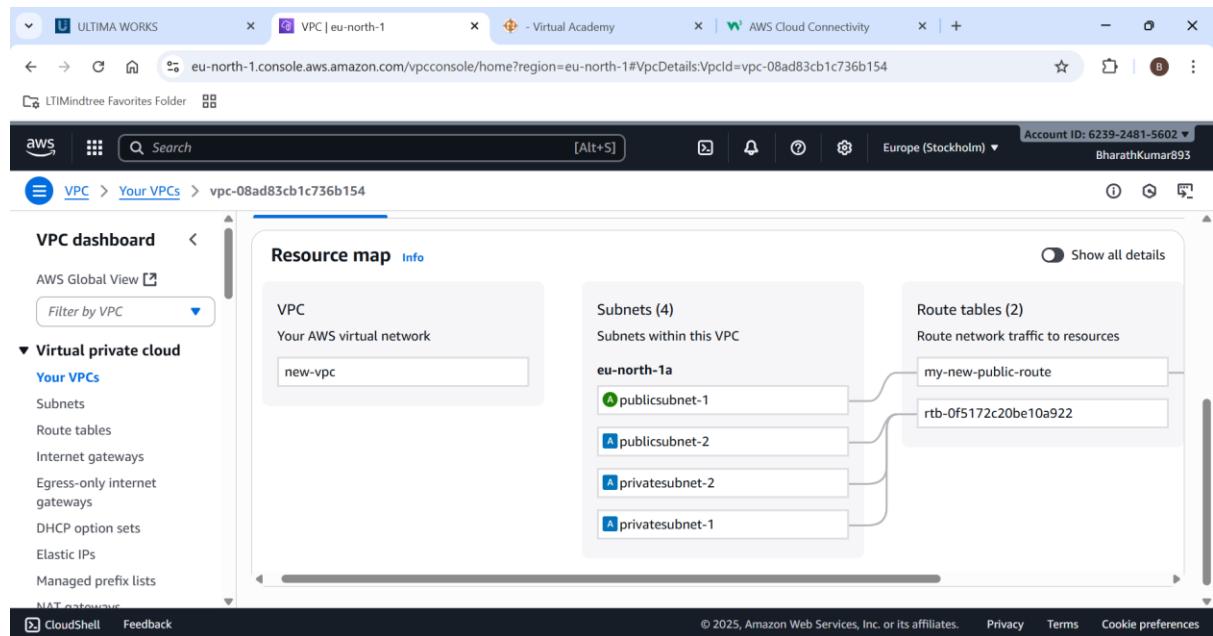
The screenshot shows the 'Edit routes' configuration for a route table. A route is being added to target an Internet Gateway. The destination is '10.0.0.0/16' and the target is 'Internet Gateway'. The route is in an 'Active' status and was created via the 'CreateRouteTable' origin. The 'Save changes' button is highlighted.

## Create subnet associations for public subnet



The screenshot shows the AWS VPC Route Tables page for a specific route table (rtb-045fc14036a25d464). A green success message at the top states: "You have successfully updated subnet associations for rtb-045fc14036a25d464 / my-new-public-route." Below this, the "Subnet associations" tab is selected. It displays one explicit subnet association for a public subnet (publicsubnet-1) with a CIDR of 10.0.0.0/24. There are also three subnets listed under "Subnets without explicit associations". The page includes standard AWS navigation and search bars.

## The Resource map shows the data

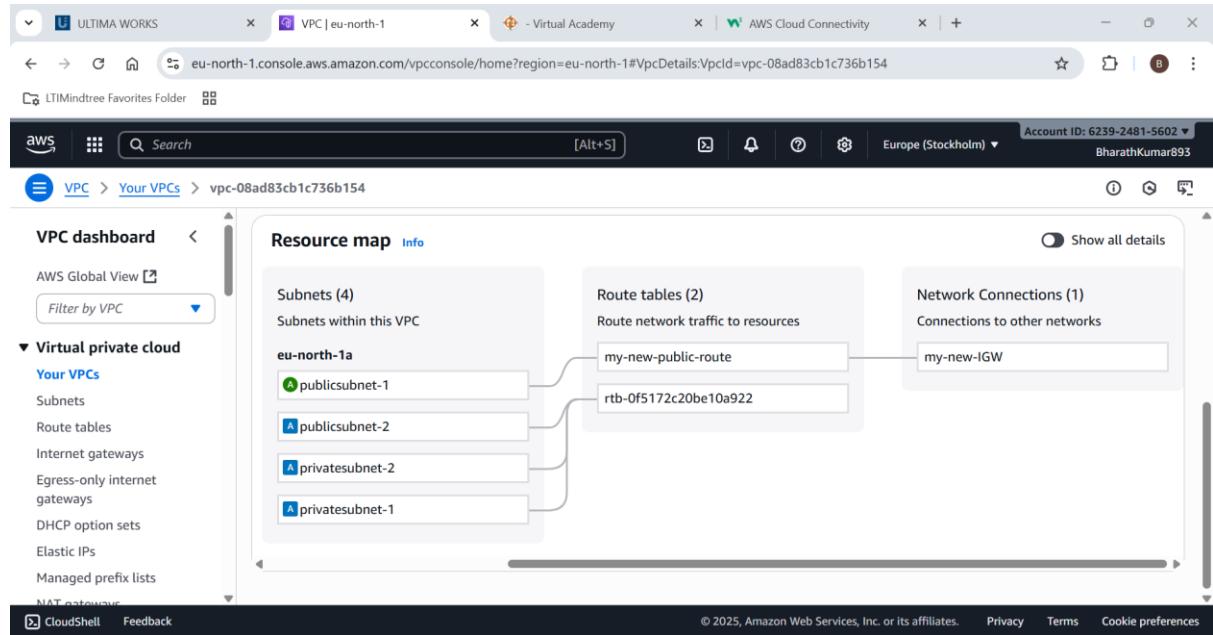


The screenshot shows the AWS VPC Resource Map for a VPC named "new-vpc". The map displays the following associations:

- VPC:** new-vpc
- Subnets (4):** eu-north-1 (publicsubnet-1, publicsubnet-2, privatesubnet-2, privatesubnet-1)
- Route tables (2):** my-new-public-route, rtb-0f5172c20be10a922
- Associations:** publicsubnet-1 is associated with both route tables; publicsubnet-2, privatesubnet-2, and privatesubnet-1 are associated with the route table "my-new-public-route".

The Resource map interface includes a "Show all details" button and standard AWS navigation and search bars.

You can see the Internet gateway connected to it.



Try to use the internet in EC2 where the VPC is connected

The screenshot shows an EC2 Instance Connect terminal window. The user has run a 'ping google.com' command. The terminal output is as follows:

```
~~~ \####\  
~~~ \#\#\|  
~~~ \#\#\| V- ' ' -> https://aws.amazon.com/linux/amazon-linux-2023  
~~~ \#\#\| /  
~~~ \#\#\| /  
~~~ \#\#\| /  
~~~ \#\#\| /  
[ec2-user@ip-10-0-0-98 ~]$ ping google.com  
PING google.com (142.250.74.78) 56(84) bytes of data.  
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=1 ttl=119 time=3.86 ms  
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=2 ttl=119 time=3.88 ms  
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=3 ttl=119 time=3.87 ms  
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=4 ttl=119 time=3.88 ms  
^C  
--- google.com ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 3.856/3.870/3.877/0.008 ms  
[ec2-user@ip-10-0-0-98 ~]$
```

Below the terminal, the instance identifier 'i-04796cc24e902f6d9 (my-new-instance)' and public/private IP addresses are displayed.

5. Create a NAT Gateway in a public subnet and configure private subnet instances to access the internet.

### Step 1: Create a private EC2 instance

**Route table settings**

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

my-new-private-route

**VPC**  
The VPC to use for this route table.

vpc-08ad83cb1c736b154 (new-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** Name **Value - optional** my-new-private-route **Remove**

**Add new tag**

You can add 49 more tags.

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

### Configure the subnet associations

You have successfully updated subnet associations for rtb-08308405014dae764 / my-new-private-route.

**rtb-08308405014dae764 / my-new-private-route**

**Details** **Info**

Route table ID: rtb-08308405014dae764

Main: No

VPC: vpc-08ad83cb1c736b154 | new-vpc

Owner ID: 623924815602

**Explicit subnet associations**  
subnet-04011dbd48cb8cfe1 / privatesubnet-1

**Edge associations**  
-

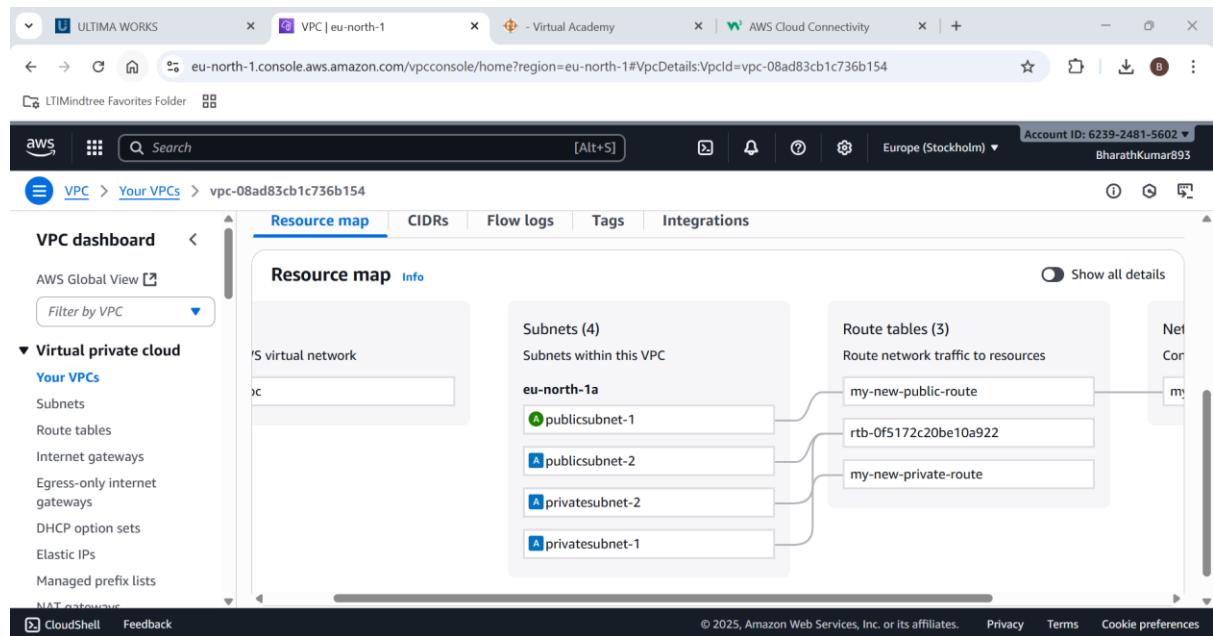
**Routes** **Subnet associations** **Edge associations** **Route propagation** **Tags**

**Routes (1)**

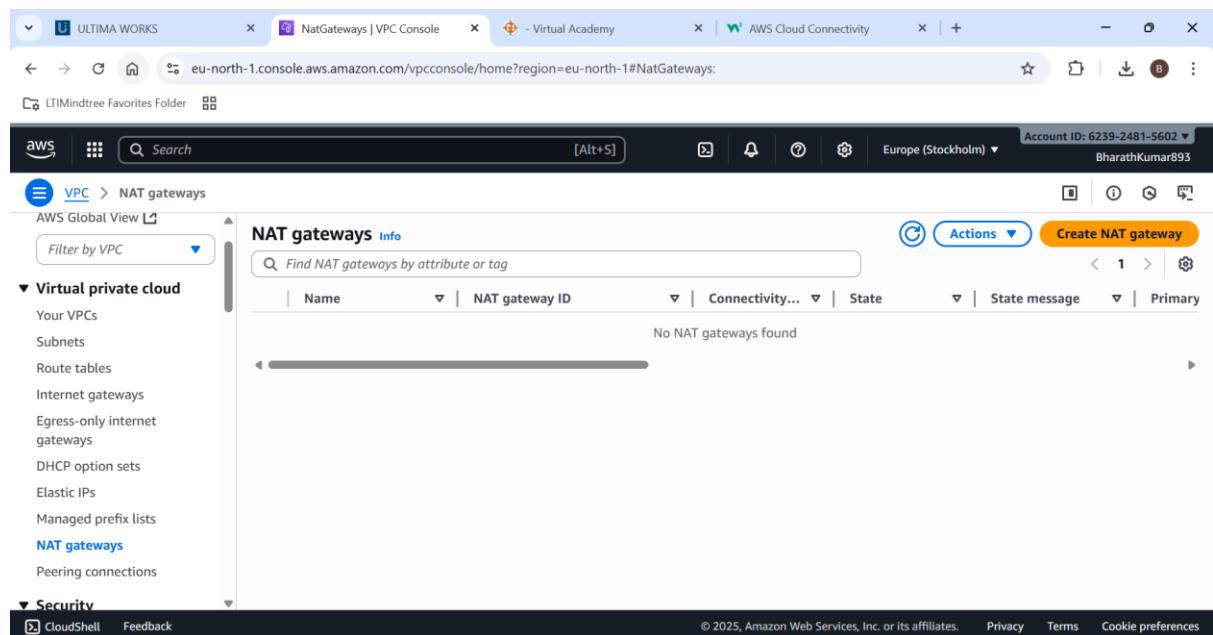
Both **Edit routes**

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

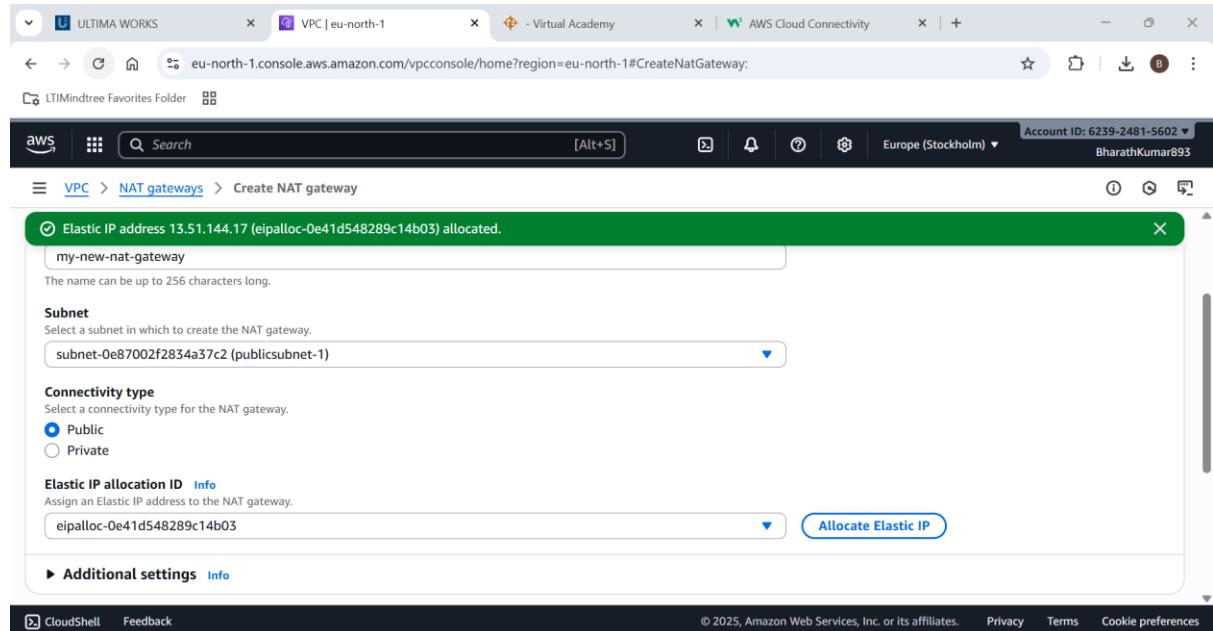
## Use resource map for checking



## Go to NAT gateways



## Create the NAT gateway in public subnet



Elastic IP address 13.51.144.17 (eipalloc-0e41d548289c14b03) allocated.

my-new-nat-gateway

The name can be up to 256 characters long.

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

subnet-0e87002f2834a37c2 (publicsubnet-1)

**Connectivity type**  
Select a connectivity type for the NAT gateway.

Public

Private

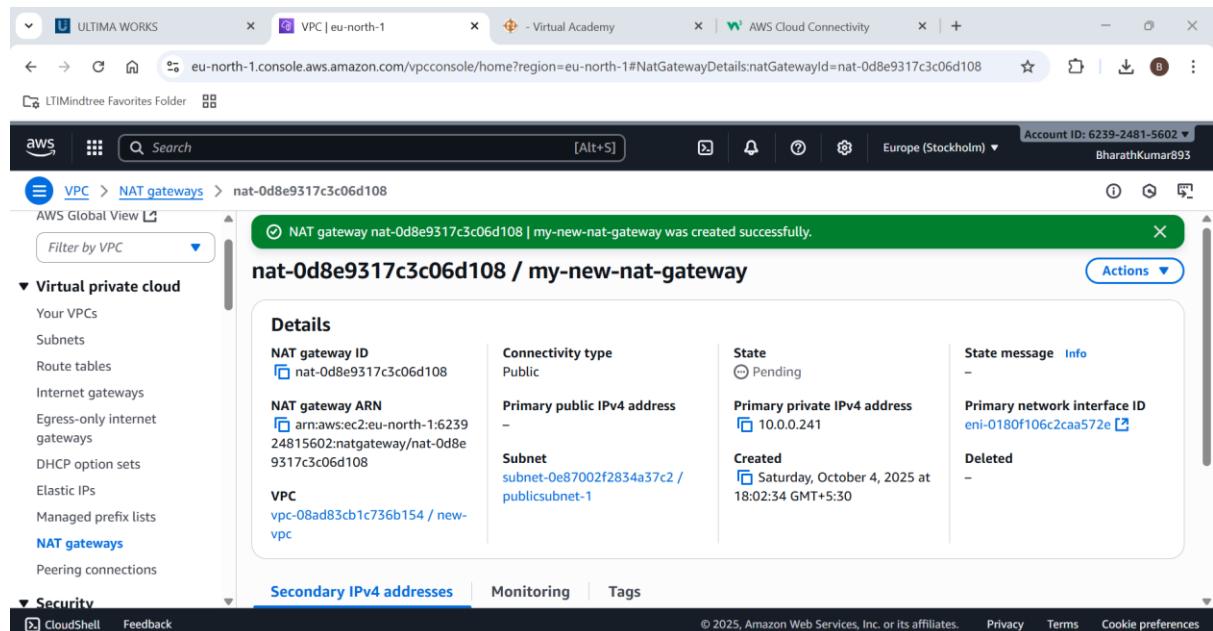
**Elastic IP allocation ID** [Info](#)  
Assign an Elastic IP address to the NAT gateway.

eipalloc-0e41d548289c14b03

[Allocate Elastic IP](#)

**Additional settings** [Info](#)

## Nat Gateway is created successfully



NAT gateway nat-0d8e9317c3c06d108 | my-new-nat-gateway was created successfully.

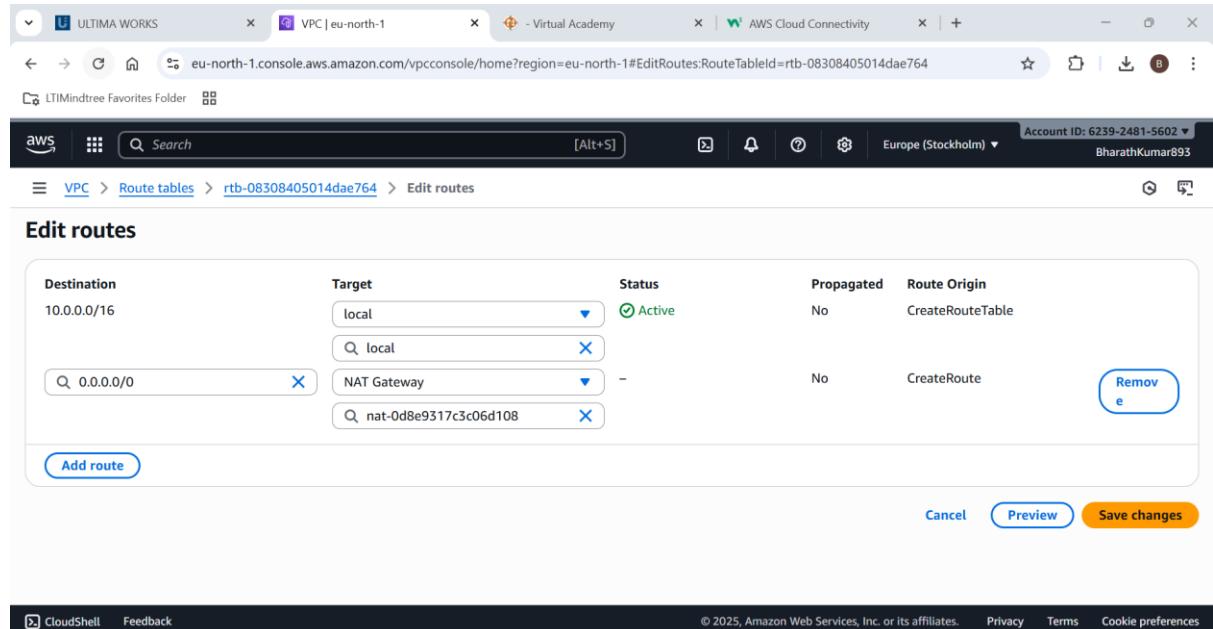
**nat-0d8e9317c3c06d108 / my-new-nat-gateway**

**Details**

|                                                                                                                |                                                                            |                                                                                  |                                                                              |
|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>NAT gateway ID</b><br><a href="#">nat-0d8e9317c3c06d108</a>                                                 | <b>Connectivity type</b><br>Public                                         | <b>State</b><br><a href="#">Pending</a>                                          | <b>State message</b> <a href="#">Info</a><br>-                               |
| <b>NAT gateway ARN</b><br><a href="#">arn:aws:ec2:eu-north-1:623924815602:natgateway/nat-0d8e9317c3c06d108</a> | <b>Primary public IPv4 address</b><br>-                                    | <b>Primary private IPv4 address</b><br><a href="#">10.0.0.241</a>                | <b>Primary network interface ID</b><br><a href="#">eni-0180f106c2caa572e</a> |
| <b>VPC</b><br><a href="#">vpc-08ad83cb1c736b154 / new-vpc</a>                                                  | <b>Subnet</b><br><a href="#">subnet-0e87002f2834a37c2 / publicsubnet-1</a> | <b>Created</b><br><a href="#">Saturday, October 4, 2025 at 18:02:34 GMT+5:30</a> | <b>Deleted</b><br>-                                                          |

**Secondary IPv4 addresses** | **Monitoring** | **Tags**

## Edit routes in Private subnet connect it to Nat gateway



The screenshot shows the 'Edit routes' page for a specific route table. The table has one entry:

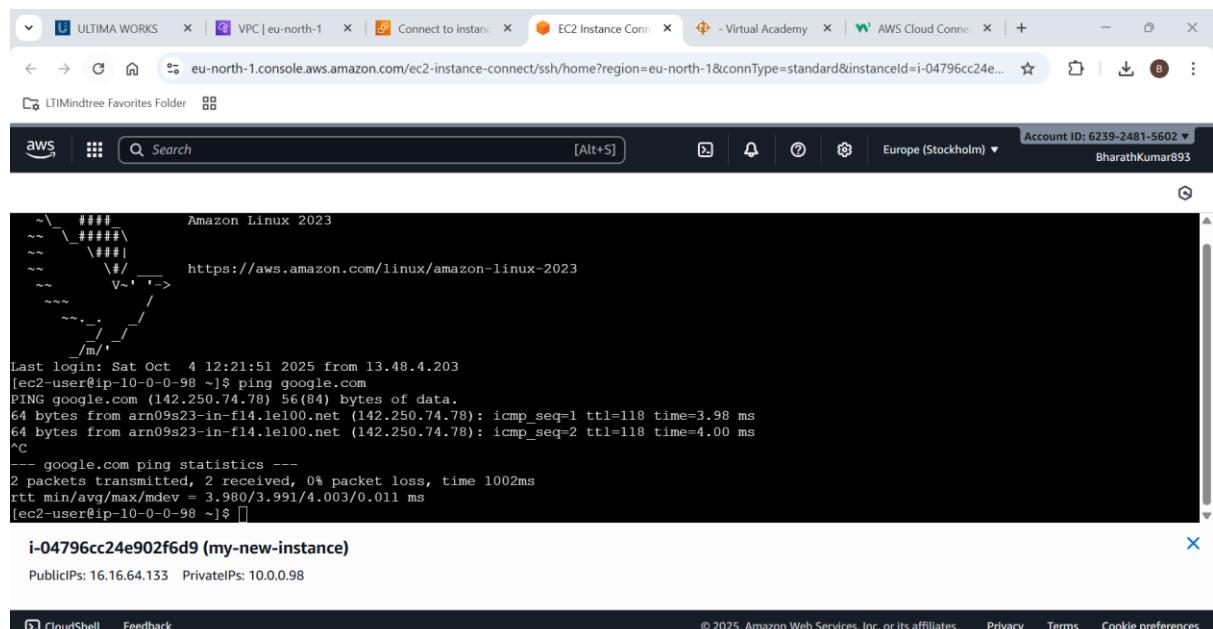
| Destination | Target | Status | Propagated | Route Origin     |
|-------------|--------|--------|------------|------------------|
| 10.0.0.0/16 | local  | Active | No         | CreateRouteTable |

Below this, there is a section for adding a new route:

| Destination | Target      | Status | Propagated | Route Origin |
|-------------|-------------|--------|------------|--------------|
| 0.0.0.0/0   | NAT Gateway | -      | No         | CreateRoute  |

Buttons at the bottom include 'Add route', 'Cancel', 'Preview', and 'Save changes'.

## Use the public EC2 instance and check for internet connectivity



The screenshot shows a terminal window on an EC2 instance. The user has run a 'ping' command to google.com:

```
>Last login: Sat Oct 4 12:21:51 2025 from 13.48.4.203
[ec2-user@ip-10-0-0-98 ~]$ ping google.com
PING google.com (142.250.74.78) 56(84) bytes of data.
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=1 ttl=118 time=3.98 ms
64 bytes from arn09s23-in-f14.le100.net (142.250.74.78): icmp_seq=2 ttl=118 time=4.00 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.980/3.991/4.003/0.011 ms
[ec2-user@ip-10-0-0-98 ~]$
```

Below the terminal, the instance ID 'i-04796cc24e902f6d9 (my-new-instance)' and its public IP '16.16.64.133' are displayed.

Now create and configure the private key

-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEAvwEZXOna54A8ETWfZ1trXBSE4Gbc5zV7f0Hj1hWwo82WBW0g  
/iABhJRxCljBee1fRTDdkNeKoIWSS1TCEt4EOpbdM1VDrqCauVPFyusLfiB  
96UoW78gCrjcszCdyRrmRhiKx+1ACnVfHq2qbUepeD1HevFfT448+1FyKrfjy1Ay  
b1KmgcBB5zpwAtuNgs1U80zhmsnt16S3z0V41nhbp8kTRnxr3U101Rv2HOiuP  
oBFWf5z5yRQ2VYzg65fbFB/01JXy3oRR7FosWg4QLfUNT00TxwQtQgrG5CD  
eUpvJPY5PDUUC2hjgZC7oY9k2HORzgTH27tWn1DQAQABAOIBAQCsA1hfhHRNrsvo  
z2oSzF1w1gWgrsBcUwXCArzw3Ex1kFz3M7JYVY3T5awoQNrh9K12/P1k3WvRkd  
V508311/dWEU2mduqVpm3e4JkRg9F7KdxbGpxxj6ewmZRxg6z3wgKrv33K1ZyJ  
LQgw0hJurlmfwCetoSpxlshLBKoRdhhwCby+dnUgRv4AkYgQkpx2yk5r3t9d6h  
mhah+P019JhwQK3pSsAemU5HZK/SQwCtfVmuk2Kz63SLIMrhGbkkrz  
Y2t7uTs/qgQPA7e9MukxRfVrdvhgc3vg5o1PUS/fGmOrWlmb/xazL1l0rc65pKe  
R6YBHQgX1Sc6ZhbascYVw/FbO2Nrvgsb5npF+w1Sfahin5KtcXCMXgPthhX09+q  
rt2BQ+2NFQq4pqfZj+ampckG+1WqbSuqSqnkyZacFxFeUyVidAogBAMob  
hENIWFmNxB2At75PqN+dDC68XPLs7/+Nmuv3W5kd4udmCSkq7p/LU476NaUpeu  
4rP4FU2spNrrQqlUs4KXUfQ67uIy4CtpSe5UN/Gkt56PuIzt9o4CJR6Ie8ID  
sAjLWq/ule+DbhFOQvOOExn25nk/08LISrqJ3UVbAoGAQIWkoBOZNI1DchWkdoi+  
"private.pem" (readonly) 27L, 1675B

i-04796cc24e902f6d9 (my-new-instance)

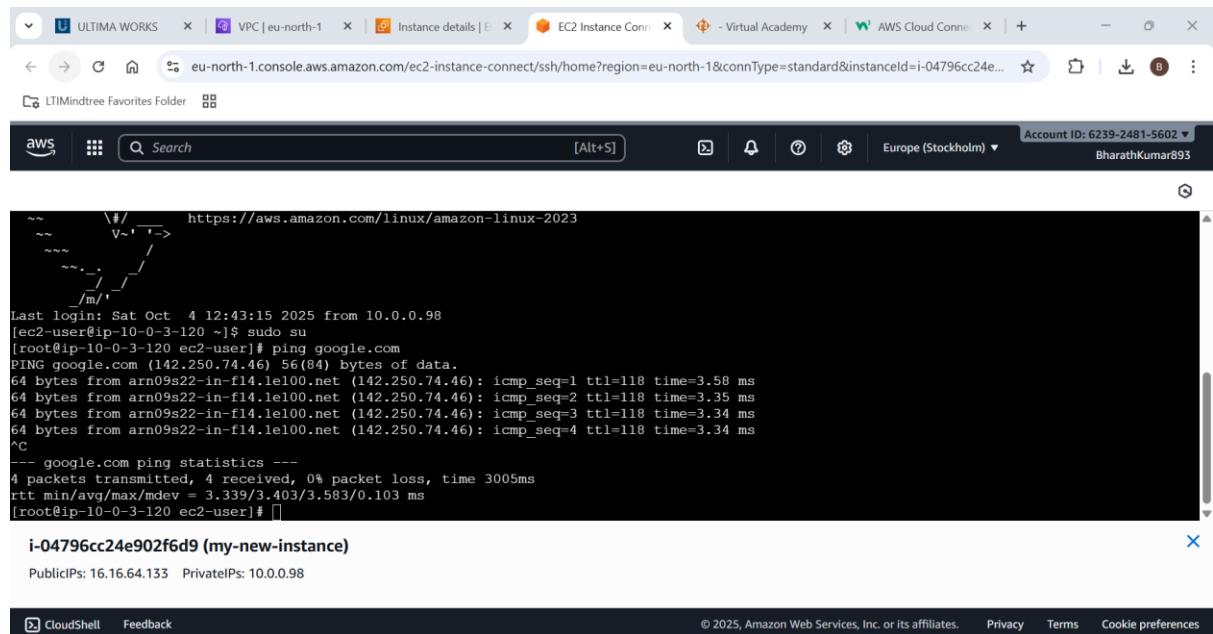
Public IPs: 16.16.64.133 Private IPs: 10.0.0.98

Now do SSH for private EC2 instance

```
[ec2-user@ip-10-0-0-98 ~]$ ^C
[ec2-user@ip-10-0-0-98 ~]$ vi private.pem
[ec2-user@ip-10-0-0-98 ~]$ sudo su
[root@ip-10-0-0-98 ec2-user]# ssh -i "private.pem" ec2-user@13.60.226.4
^C
[root@ip-10-0-0-98 ec2-user]# chmod 400 "private.pem"
[root@ip-10-0-0-98 ec2-user]# ssh -i "private.pem" ec2-user@13.60.226.4
^C
[root@ip-10-0-0-98 ec2-user]# ssh -i "private.pem" ec2-user@10.0.3.120
The authenticity of host '10.0.3.120 (10.0.3.120)' can't be established.
ED25519 key fingerprint is SHA256:nZ0BKJDldnHx7W3ZF4077YcwgKDxd9NWGzYYEcLrlPM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.120' (ED25519) to the list of known hosts.

,   #
~\_ ####      Amazon Linux 2023
~~ \_\#\#\#\\
~~ \#\#\#\#
~~ \#\#/
https://aws.amazon.com/linux/amazon-linux-2023
```

Now try using internet from private EC2 instance .



```
~~      \$/ https://aws.amazon.com/linux/amazon-linux-2023
~~      v-,->
~~      /
~~.-
~~.-
~~.-
/m/
Last login: Sat Oct  4 12:43:15 2025 from 10.0.0.98
[ec2-user@ip-10-0-3-120 ~]$ sudo su
[root@ip-10-0-3-120 ec2-user]# ping google.com
PING google.com (142.250.74.46) 56(84) bytes of data.
64 bytes from arn09s22-in-f14.le100.net (142.250.74.46): icmp_seq=1 ttl=118 time=3.58 ms
64 bytes from arn09s22-in-f14.le100.net (142.250.74.46): icmp_seq=2 ttl=118 time=3.35 ms
64 bytes from arn09s22-in-f14.le100.net (142.250.74.46): icmp_seq=3 ttl=118 time=3.34 ms
64 bytes from arn09s22-in-f14.le100.net (142.250.74.46): icmp_seq=4 ttl=118 time=3.34 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 3.339/3.403/3.583/0.103 ms
[root@ip-10-0-3-120 ec2-user]#
```

i-04796cc24e902f6d9 (my-new-instance)

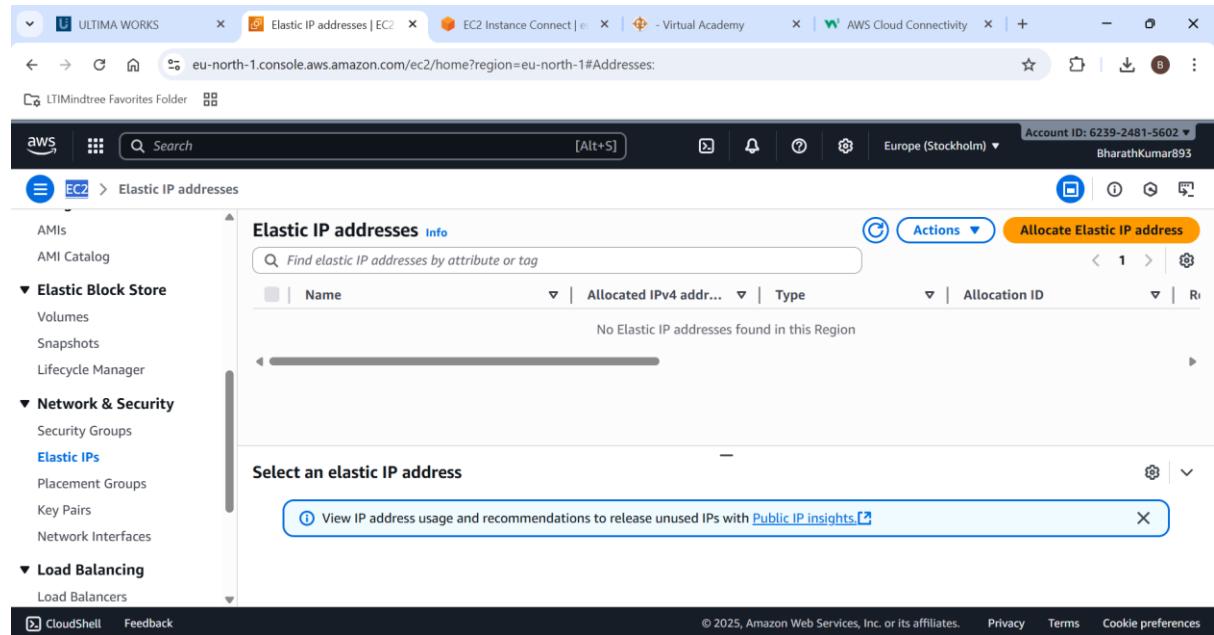
Public IPs: 16.16.64.133 Private IPs: 10.0.0.98

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

Internet is accessible from private EC2 instance.

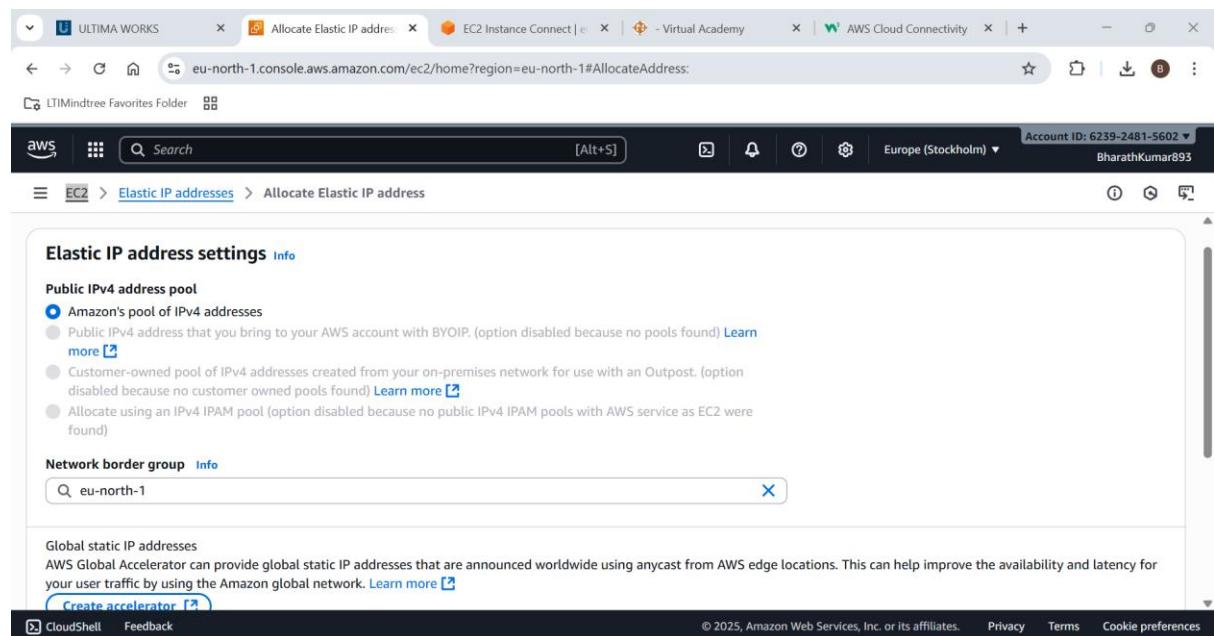
## 6. Allocate and associate an Elastic IP with an EC2 instance.

Go the network and security > Elastic Ip



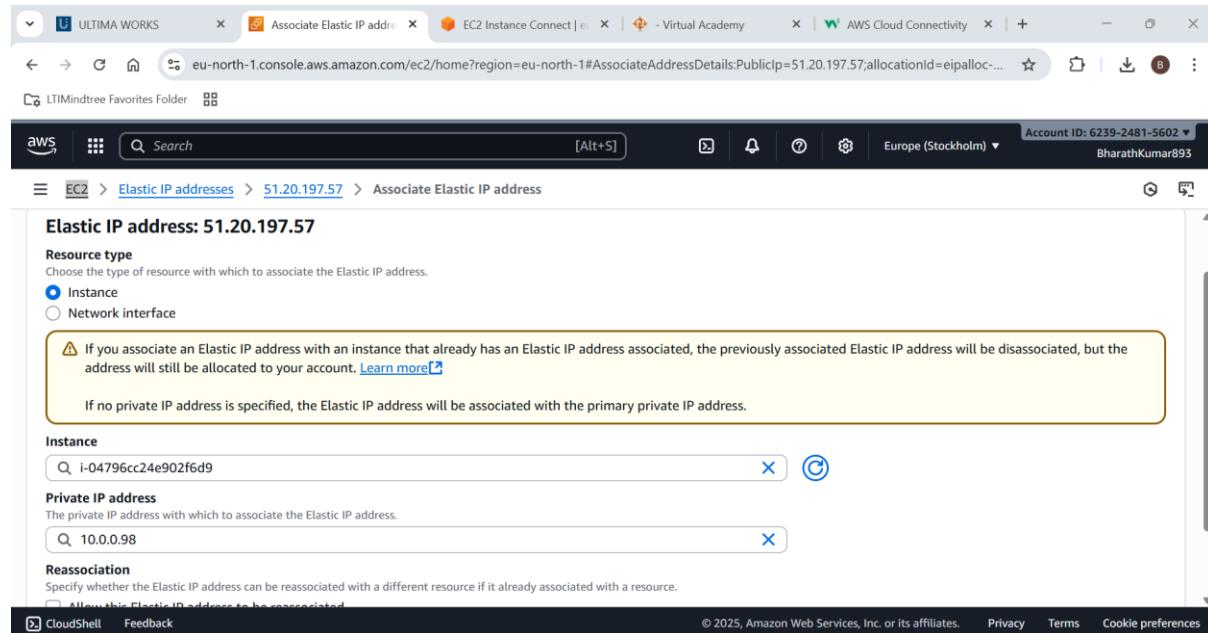
The screenshot shows the AWS EC2 console with the 'Elastic IP addresses' page open. The left sidebar is collapsed, and the main content area displays the 'Elastic IP addresses' section. The search bar at the top is empty. Below the search bar, there are filters for 'Name', 'Allocated IPv4 addr...', 'Type', and 'Allocation ID'. A message at the top right says 'No Elastic IP addresses found in this Region'. Below this, a section titled 'Select an elastic IP address' is shown, with a note: 'View IP address usage and recommendations to release unused IPs with Public IP insights.' The bottom of the page includes standard AWS footer links: CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

Allocate one EIP for EC2



The screenshot shows the 'Allocate Elastic IP address' page in the AWS EC2 console. The left sidebar is collapsed, and the main content area displays the 'Elastic IP address settings' section. Under 'Public IPv4 address pool', the 'Amazon's pool of IPv4 addresses' option is selected. Other options like 'Public IPv4 address that you bring to your AWS account with BYOIP' and 'Customer-owned pool of IPv4 addresses' are shown as disabled. Under 'Network border group', a search bar contains the value 'eu-north-1'. A note about AWS Global Accelerator is present at the bottom. The bottom of the page includes standard AWS footer links: CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

Now Associate it with the EC2 instance.



Elastic IP address: 51.20.197.57

Resource type

Choose the type of resource with which to associate the Elastic IP address.

Instance

Network interface

**⚠** If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Instance

Q i-04796cc24e902f6d9

Private IP address

The private IP address with which to associate the Elastic IP address.

Q 10.0.0.98

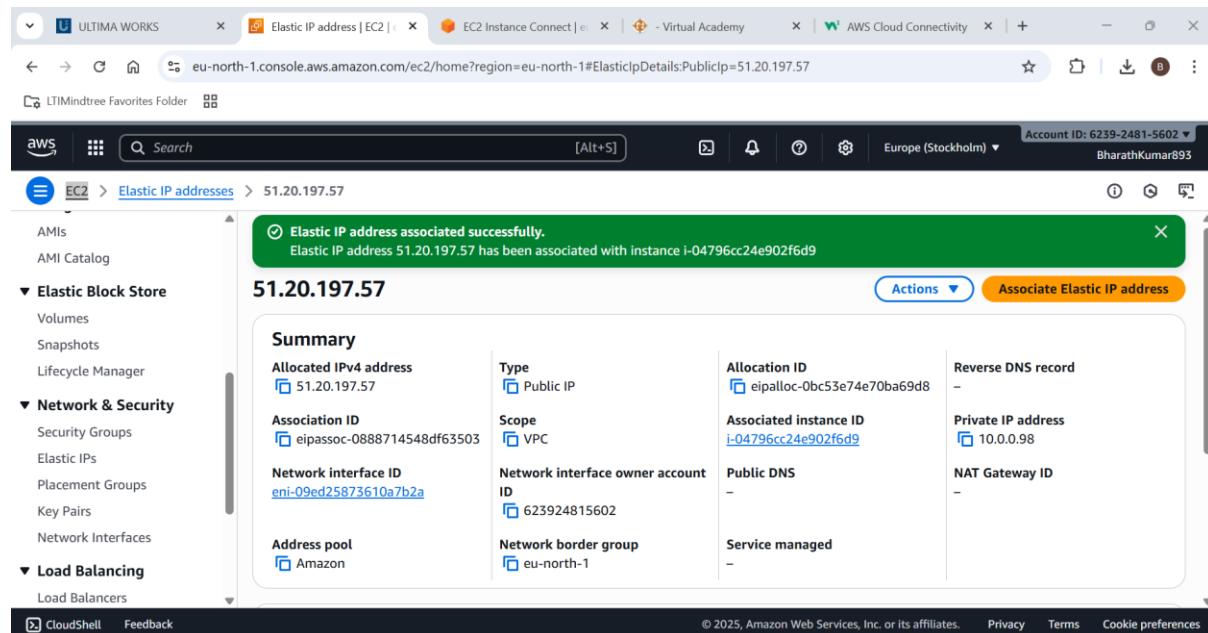
Reassociation

Specify whether the Elastic IP address can be reassigned with a different resource if it already associated with a resource.

Allow this Elastic IP address to be reassigned

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

EIP created successfully



AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

▼ Load Balancing

Load Balancers

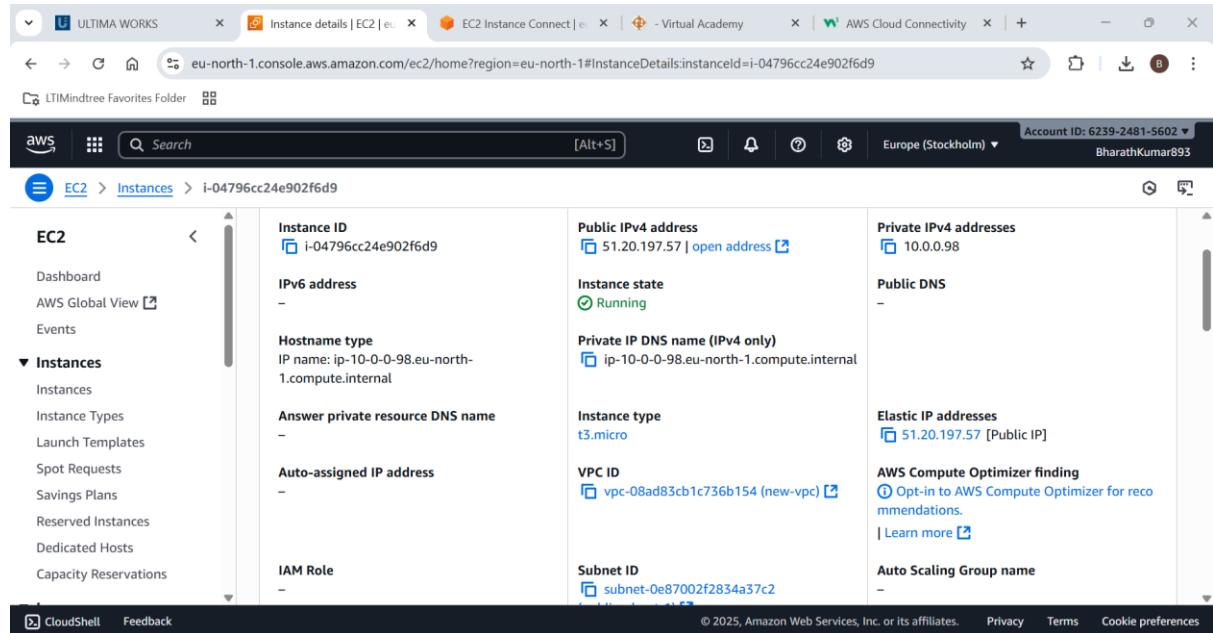
Elastic IP address associated successfully.

Elastic IP address 51.20.197.57 has been associated with instance i-04796cc24e902f6d9

| 51.20.197.57                                      |                                    |                                            |                           |
|---------------------------------------------------|------------------------------------|--------------------------------------------|---------------------------|
| Actions <span>Associate Elastic IP address</span> |                                    |                                            |                           |
| <b>Summary</b>                                    |                                    |                                            |                           |
| Allocated IPv4 address                            | Type                               | Allocation ID                              | Reverse DNS record        |
| <a href="#">51.20.197.57</a>                      | <a href="#">Public IP</a>          | <a href="#">eipalloc-0bc53e74e70ba69d8</a> | -                         |
| Association ID                                    | Scope                              | Associated instance ID                     | Private IP address        |
| <a href="#">eipassoc-0888714548df63503</a>        | <a href="#">VPC</a>                | <a href="#">i-04796cc24e902f6d9</a>        | <a href="#">10.0.0.98</a> |
| Network interface ID                              | Network interface owner account ID | Public DNS                                 | NAT Gateway ID            |
| <a href="#">eni-09ed25873610a7b2a</a>             | <a href="#">623924815602</a>       | -                                          | -                         |
| Address pool                                      | Network border group               | Service managed                            |                           |
| <a href="#">Amazon</a>                            | <a href="#">eu-north-1</a>         | -                                          |                           |

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

## Verify in the EC2 instance for EIP.



The screenshot shows the AWS EC2 Instance Details page for instance `i-04796cc24e902f6d9`. The instance is running in the `eu-north-1` region and is assigned a public IP address of `51.20.197.57`. The instance type is `t3.micro`, and it is associated with a VPC ID of `vpc-08ad83cb1c736b154` and a subnet ID of `subnet-0e87002f2834a37c2`. The instance has a private IP address of `10.0.0.98` and a private DNS name of `ip-10-0-0-98.eu-north-1.compute.internal`. The instance is currently running.

| Category                         | Value                                                                |
|----------------------------------|----------------------------------------------------------------------|
| Instance ID                      | <a href="#">i-04796cc24e902f6d9</a>                                  |
| IPv6 address                     | -                                                                    |
| Hostname type                    | IP name: ip-10-0-0-98.eu-north-1.compute.internal                    |
| Answer private resource DNS name | -                                                                    |
| Auto-assigned IP address         | -                                                                    |
| IAM Role                         | -                                                                    |
| Public IPv4 address              | <a href="#">51.20.197.57</a>   <a href="#">open address</a>          |
| Instance state                   | <span>Running</span>                                                 |
| Private IP DNS name (IPv4 only)  | <a href="#">ip-10-0-0-98.eu-north-1.compute.internal</a>             |
| Instance type                    | <a href="#">t3.micro</a>                                             |
| VPC ID                           | <a href="#">vpc-08ad83cb1c736b154 (new-vpc)</a>                      |
| Subnet ID                        | <a href="#">subnet-0e87002f2834a37c2</a>                             |
| Private IPv4 addresses           | <a href="#">10.0.0.98</a>                                            |
| Public DNS                       | -                                                                    |
| Elastic IP addresses             | <a href="#">51.20.197.57</a> [Public IP]                             |
| AWS Compute Optimizer finding    | <a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a> |
| Auto Scaling Group name          | -                                                                    |