AWS EC2 Server Creation Documentation

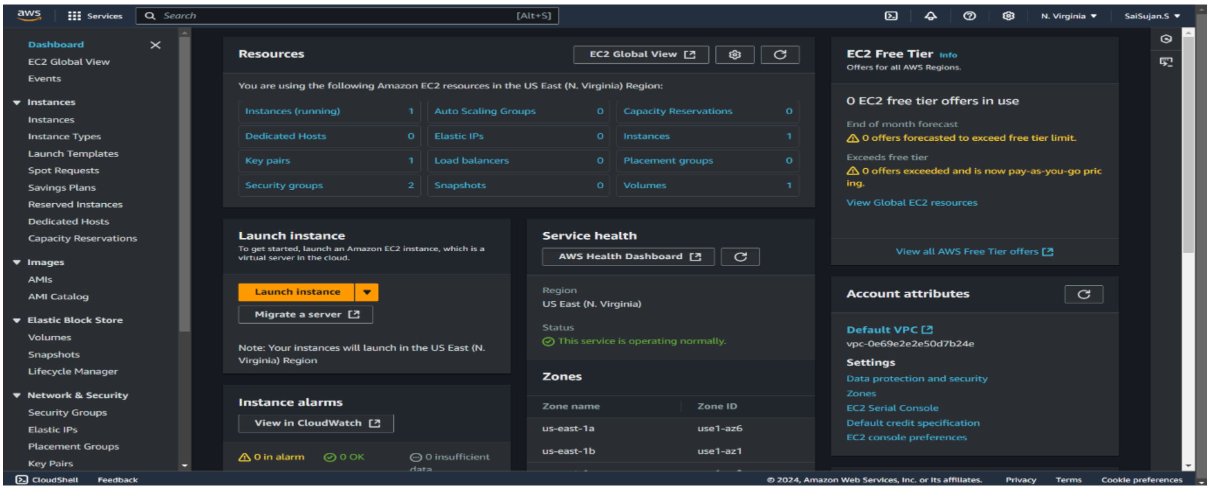
This document guides you through the process of creating and launching an Amazon Elastic Compute Cloud (EC2) instance on AWS.

Step 1: Log in to AWS Management Console

1. *Navigate to the AWS Management Console.*
2. *Log in with your credentials (username and password).*

Step 2: Open the EC2 Dashboard

1. *In the AWS Console, search for **EC2** in the search bar.*
2. *Select **EC2** to open the EC2 Dashboard.*



Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	1	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	1
Key pairs	1	Load balancers	0	Placement groups	0
Security groups	2	Snapshots	0	Volumes	1

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

Region: US East (N. Virginia)

Status: This service is operating normally.

Zones

Zone name	Zone ID
us-east-1a	use1-az6
us-east-1b	use1-az1

Instance alarms

0 in alarm · 0 OK · 0 insufficient data

EC2 Free Tier Info

Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast

0 offers forecasted to exceed free tier limit.

Exceeds free tier

0 offers exceeded and is now pay-as-you-go pricing.

Account attributes

Default VPC

vpc-0e69e2e2e50d7b24e

Settings

Data protection and security

Zones

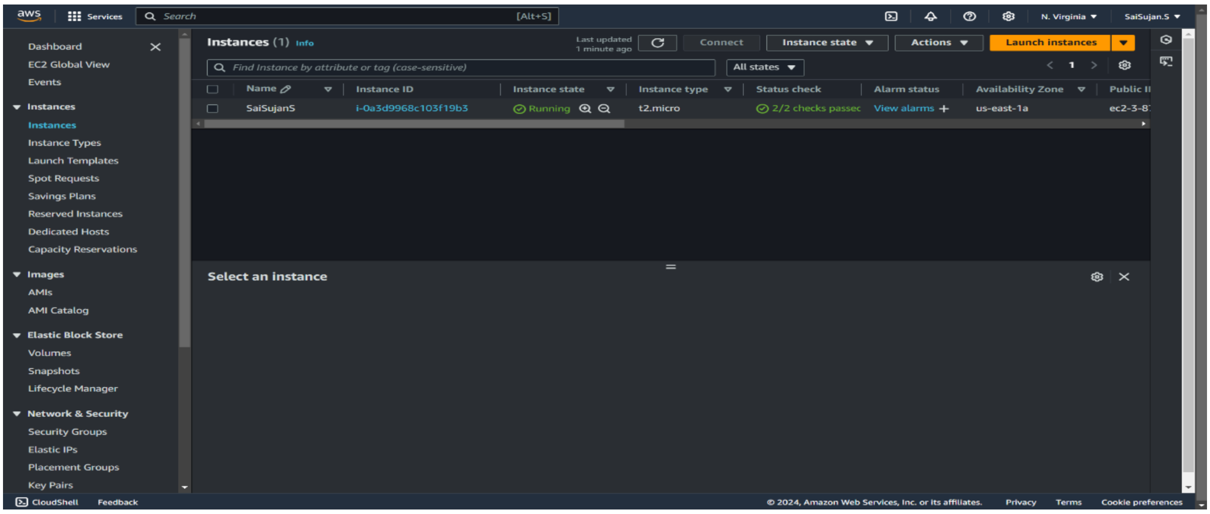
EC2 Serial Console

Default credit specification

EC2 console preferences

Step 3: Launch an EC2 Instance

1. *Click **Launch Instances** on the EC2 Dashboard.*



Instances (1) Info

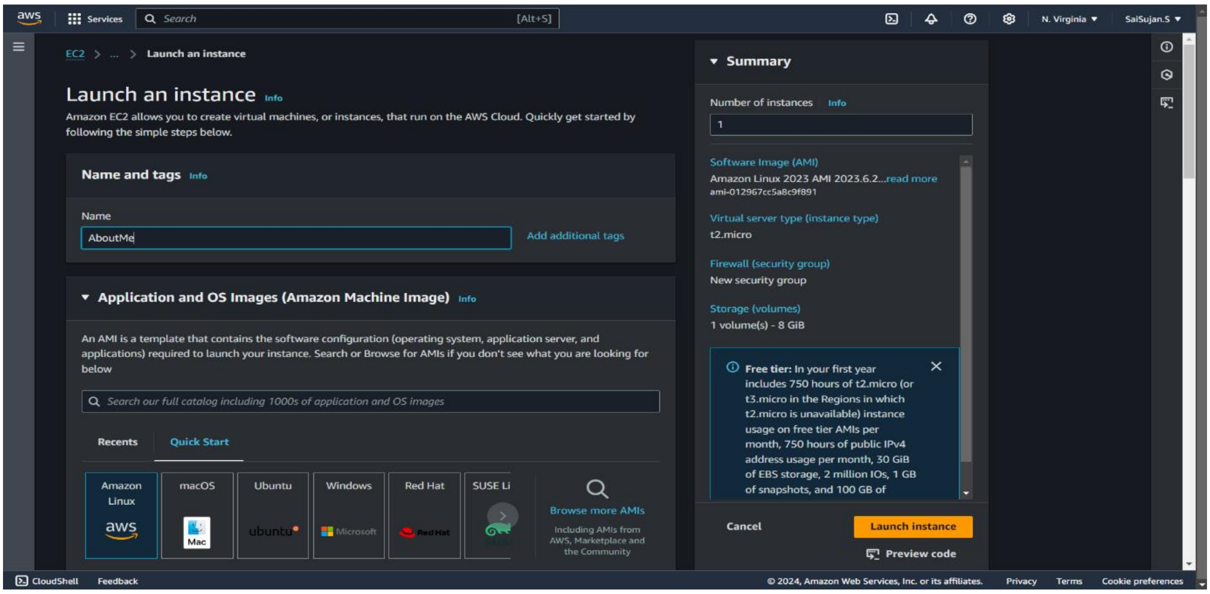
Last updated 1 minute ago

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public I
SaiSujanS	i-0a3d9968c103f19b3	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-3-8

2. *Enter an **Instance Name** (e.g., "MyServer").*

3. *Select an **Amazon Machine Image (AMI)**:*

   - *Choose the operating system you want for the instance (e.g., Amazon Linux, Ubuntu, Windows Server).*



EC2 > ... > 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: AboutMe

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

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...read more ami-012967cc5a8c9f891

Virtual server type (instance type): t2.micro

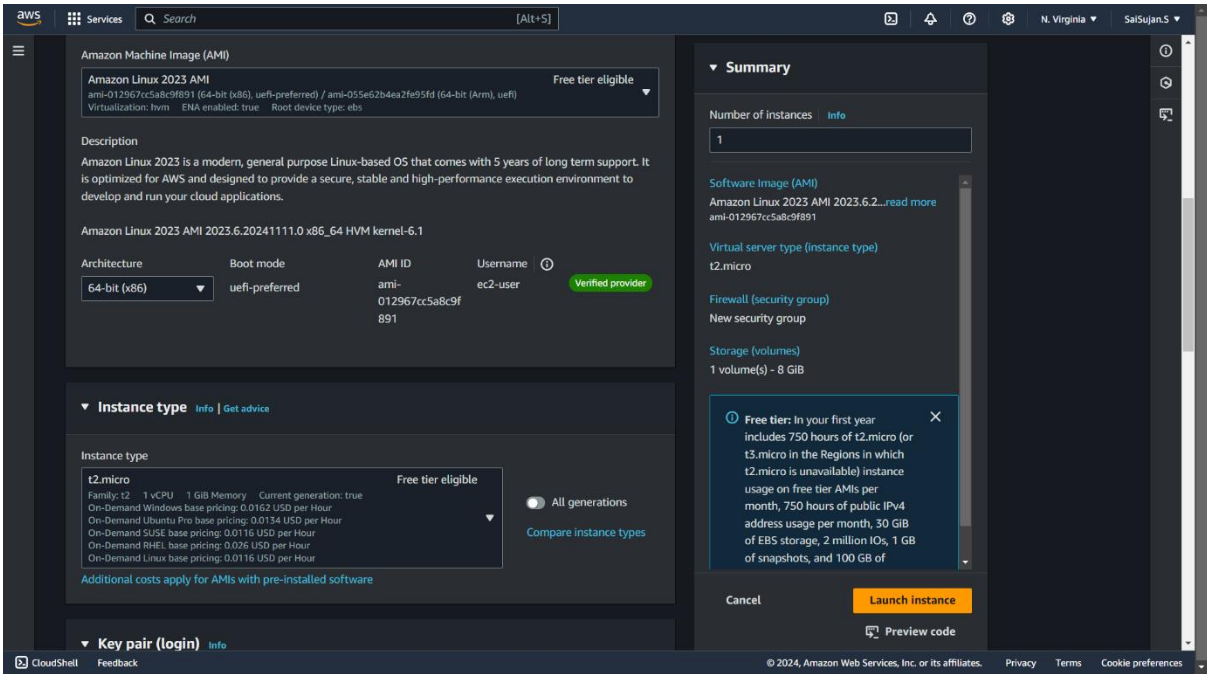
Firewall (security group): New security group

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

4. *Select an **Instance Type**:*

   - *For basic usage, choose **t2.micro** (eligible for Free Tier).*



Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-012967cc5a8c9f891 (64-bit (x86), uefi-preferred) / ami-055e62b4ea2fe95fd (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20241111.0 x86_64 HVM kernel-6.1

Architecture: 64-bit (x86)
Boot mode: uefi-preferred
AMI ID: ami-012967cc5a8c9f891
Username: ec2-user
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 Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...read more ami-012967cc5a8c9f891

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

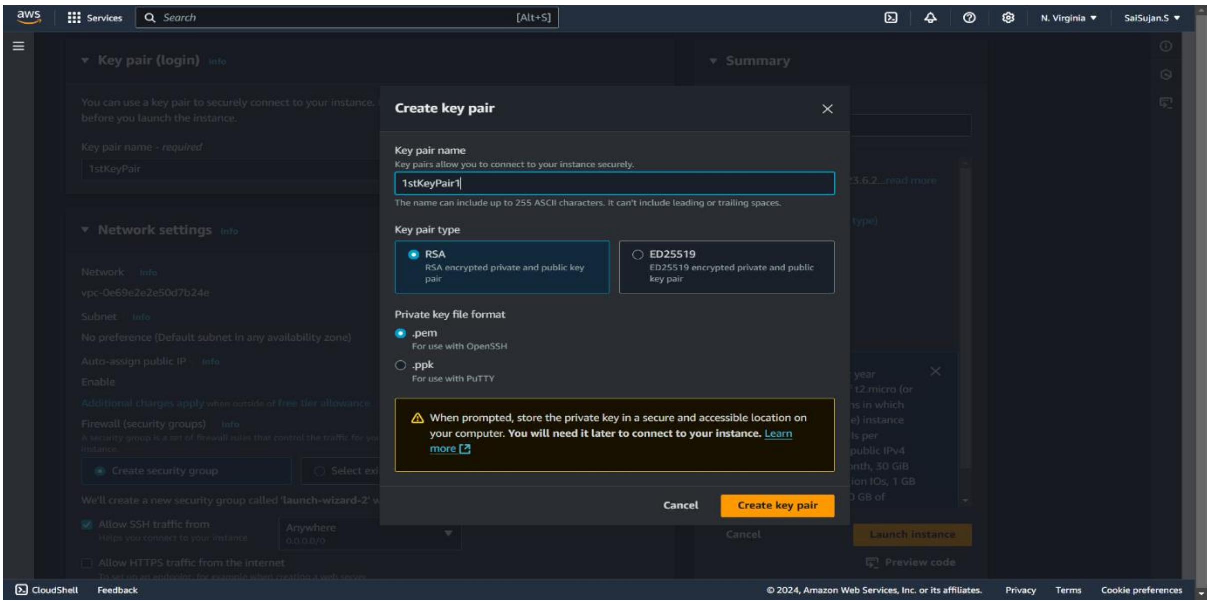
Storage (volumes): 1 volume(s) - 8 GiB

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

5. *Configure **Key Pair**:*

   - *Create a new key pair or use an existing one.*

- *Download the private key file (.pem) and keep it safe; it will be required to access the instance.*



Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

1stKeyPair1

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

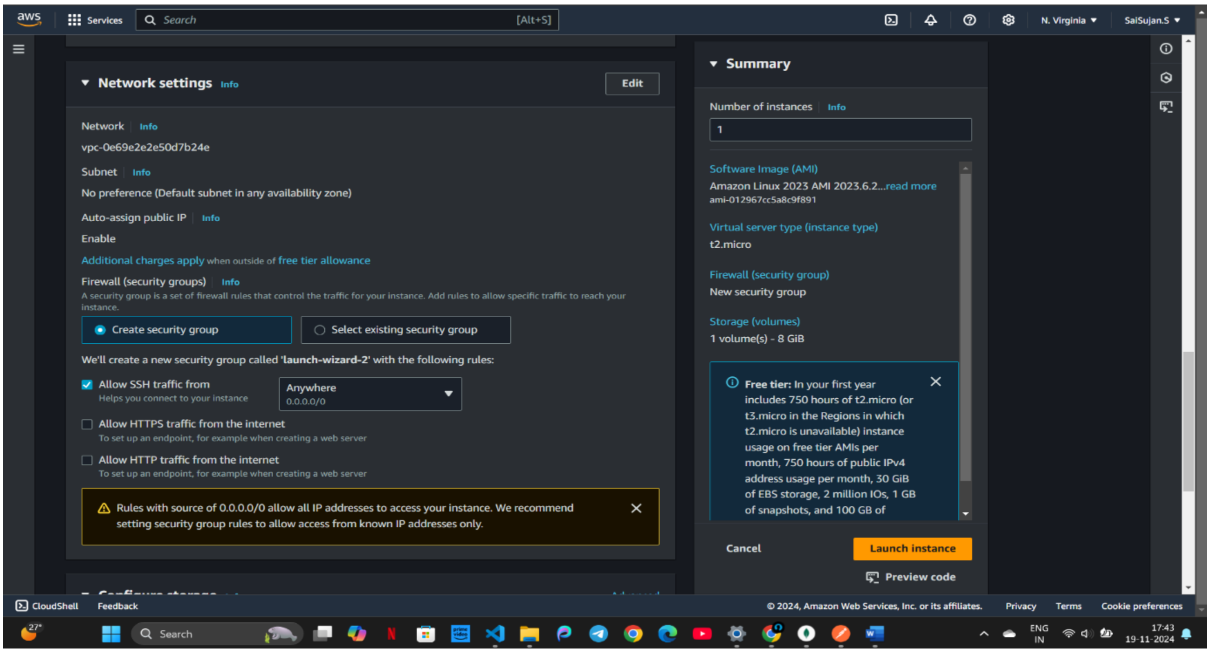
Private key file format

● .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

6. *Configure **Network Settings**:*
    - *Default VPC and Subnet will be selected automatically.*
    - *Enable **Auto-assign Public IP**.*
    - *Set up **Security Groups**:*
        - *Allow **SSH (port 22)** for Linux or **RDP (port 3389)** for Windows.*
        - *Optionally, allow other protocols (HTTP/HTTPS for web servers).*



Network settings

Network: vpc-0e69e2e2e50d7b24e

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

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

We'll create a new security group called **'launch-wizard-2'** with the following rules:

☑ Allow SSH traffic from — Helps you connect to your instance — Anywhere 0.0.0.0/0

□ Allow HTTPS traffic from the internet — To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet — To set up an endpoint, for example when creating a web server

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.

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...read more
ami-012967cc5a8c9f891

Virtual server type (instance type): t2.micro

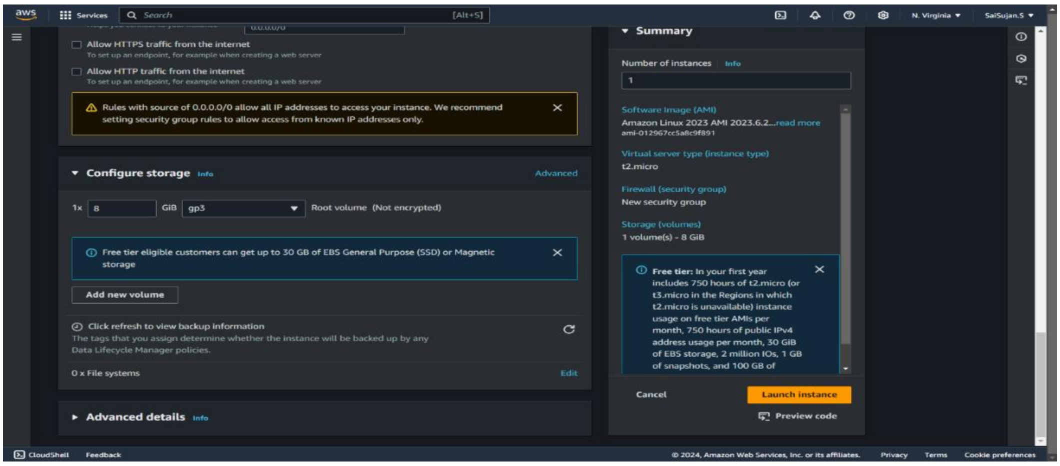
Firewall (security group): New security group

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

7. *Add **Storage**:*

   - *Use the default storage (8GB for most AMIs) or customize as needed.*



☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ 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.

▾ 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

Add new volume

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

▸ Advanced details Info

▾ Summary

Number of instances Info: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...read more ami-012967cc5a8c9f891

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

Cancel | Launch instance | Preview code

© 2024, Amazon Web Services, Inc. or its affiliates.

8. *Add **Advanced details** (optional):*

   - *In It Navigate to the last section where you will able to type the code or choose the file.*

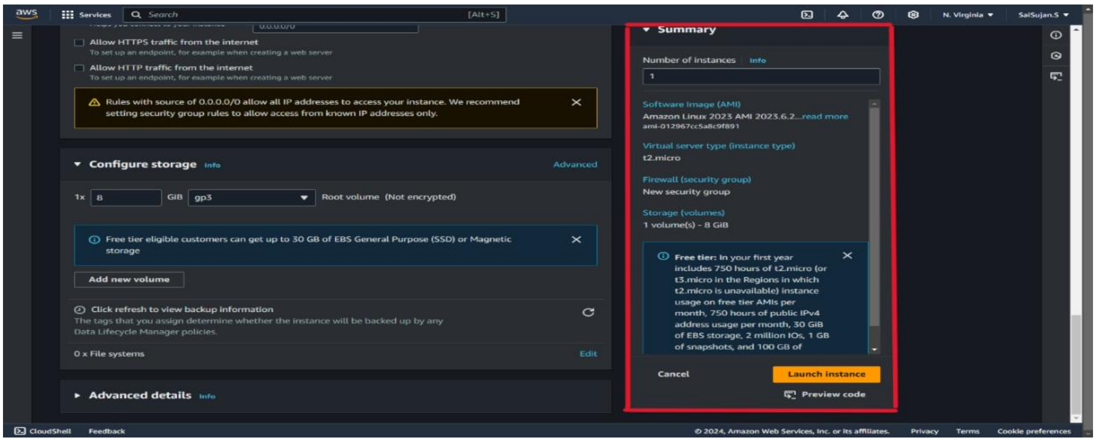
   - *Type the modules you need to install or give any index.html content.*

```
1)  #!/bin/bash                 //bash says its linux
2)  yum install httpd -y        // Install httpd module using yum
3)  systemctl status httpd      // Verify that httpd is installed
4)  systemctl enable httpd      // Enable the httpd server
5)  systemctl start httpd       // Start the httpd server
6)  yum install git -y          // Install git module
7)  git --version               // Verify that git is installed
```

Step 4: Review and Launch

1. *Review your instance configuration.*

2. *Click **Launch Instance**.*



☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ 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.

▾ 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

Add new volume

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

▸ Advanced details Info

▾ Summary

Number of instances Info: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...read more ami-012967cc5a8c9f891

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

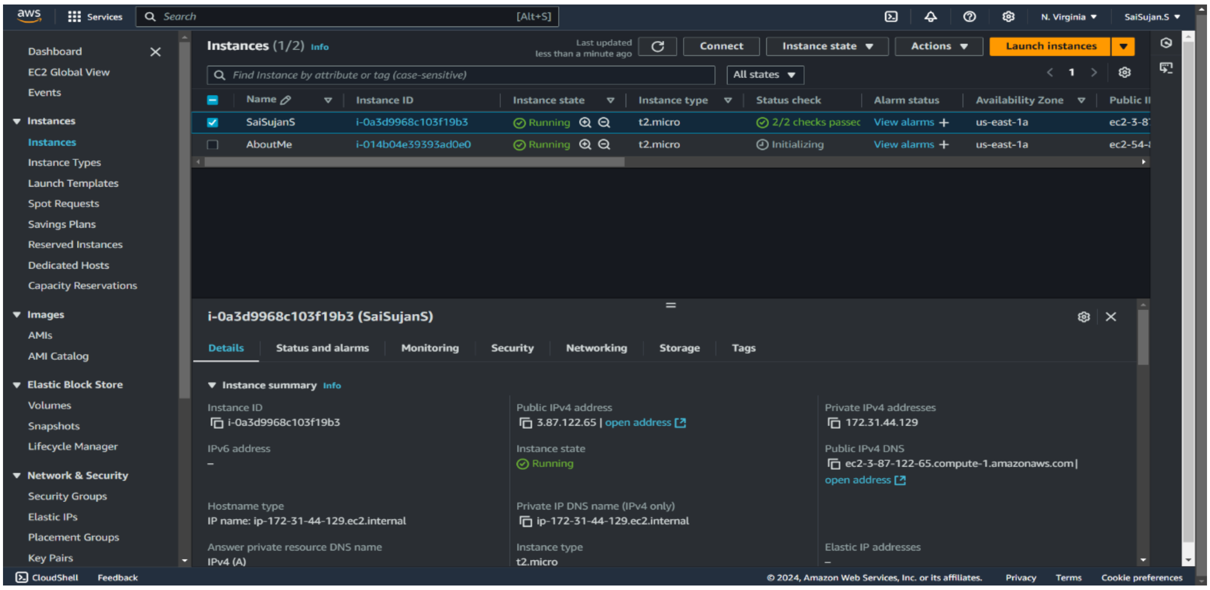
Storage (volumes): 1 volume(s) - 8 GiB

ⓘ 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

Cancel | Launch instance | Preview code

© 2024, Amazon Web Services, Inc. or its affiliates.

3. *Wait for the instance state to change to* ***Running*** *on the EC2 Dashboard.*



Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public II
☑ SaiSujanS	i-0a3d9968c103f19b3	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1a	ec2-3-87
□ AboutMe	i-014b04e39393ad0e0	Running	t2.micro	Initializing	View alarms +	us-east-1a	ec2-54-

i-0a3d9968c103f19b3 (SaiSujanS)

Instance summary Info

Instance ID: i-0a3d9968c103f19b3

Public IPv4 address: 3.87.122.65 | open address

Private IPv4 addresses: 172.31.44.129

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-3-87-122-65.compute-1.amazonaws.com | open address

Hostname type: IP name: ip-172-31-44-129.ec2.internal

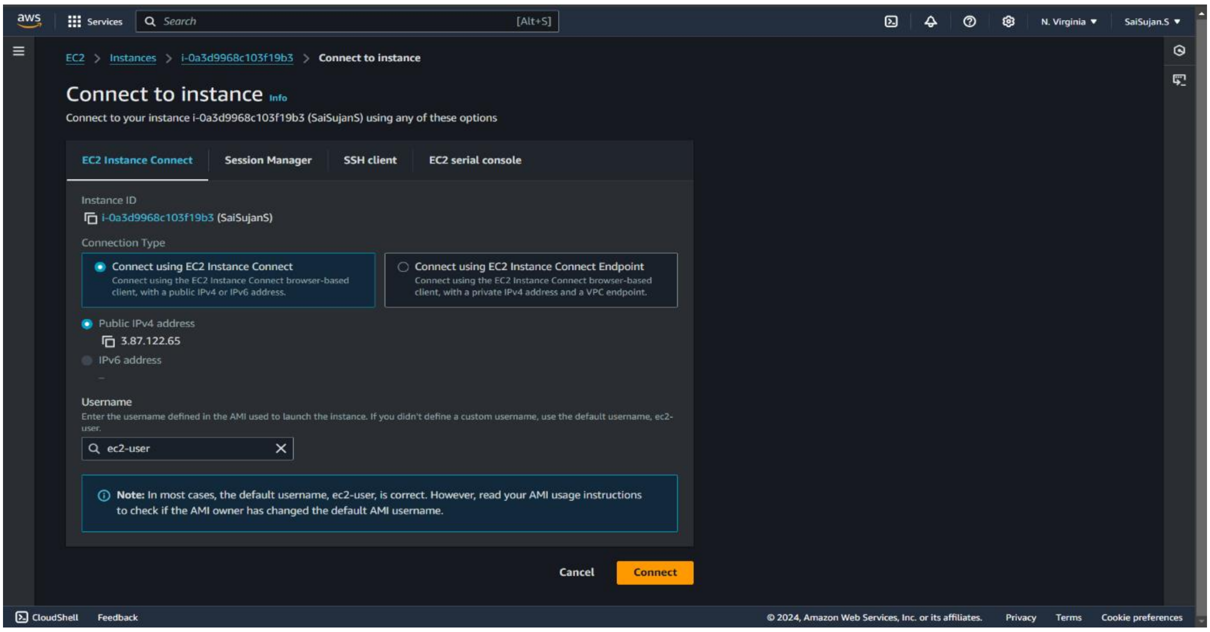
Private IP DNS name (IPv4 only): ip-172-31-44-129.ec2.internal

Answer private resource DNS name: IPv4 (A)

Instance type: t2.micro

Elastic IP addresses: –

Step 5: Access the EC2 Instance



Connect to instance Info

Connect to your instance i-0a3d9968c103f19b3 (SaiSujanS) using any of these options

Instance ID: i-0a3d9968c103f19b3 (SaiSujanS)

Connection Type

● Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 or IPv6 address.

○ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

● Public IPv4 address: 3.87.122.65

○ IPv6 address: –

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

ec2-user

Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

For Linux Instances:

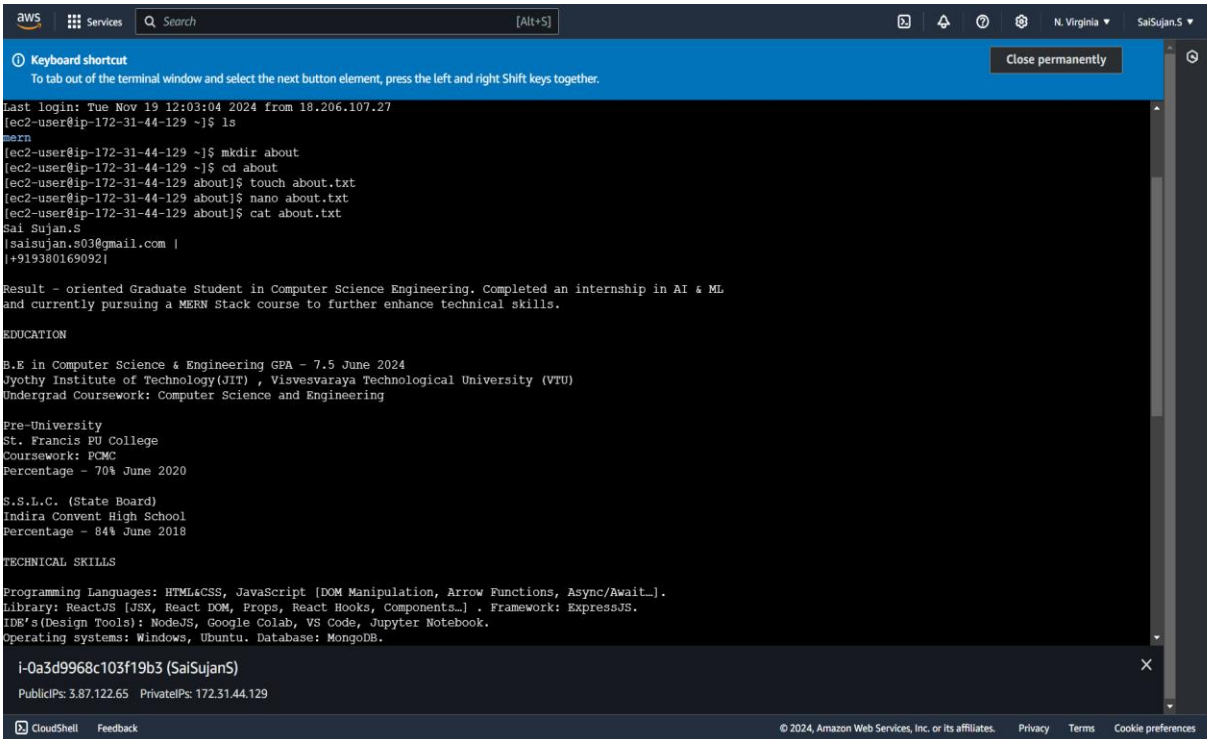
1. *Open a terminal (Linux/macOS) or a tool like PuTTY (Windows).*
2. *Use the following command to connect via SSH:*

bash

Copy code

```
ssh -i /path/to/your-key.pem ec2-user@<Public_IP>
```

Replace /path/to/your-key.pem with the path to your private key file and <Public_IP> with your instance's public IP.



aws
Services
Search
[Alt+S]
N. Virginia
SaiSujan.S
Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.
Close permanently

```
Last login: Tue Nov 19 12:03:04 2024 from 18.206.107.27
[ec2-user@ip-172-31-44-129 ~]$ ls
mern
[ec2-user@ip-172-31-44-129 ~]$ mkdir about
[ec2-user@ip-172-31-44-129 ~]$ cd about
[ec2-user@ip-172-31-44-129 about]$ touch about.txt
[ec2-user@ip-172-31-44-129 about]$ nano about.txt
[ec2-user@ip-172-31-44-129 about]$ cat about.txt
Sai Sujan.S
|saisujan.s03@gmail.com |
|+919380169092|

Result - oriented Graduate Student in Computer Science Engineering. Completed an internship in AI & ML
and currently pursuing a MERN Stack course to further enhance technical skills.

EDUCATION

B.E in Computer Science & Engineering GPA - 7.5 June 2024
Jyothy Institute of Technology(JIT) , Visvesvaraya Technological University (VTU)
Undergrad Coursework: Computer Science and Engineering

Pre-University
St. Francis PU College
Coursework: PCMC
Percentage - 70% June 2020

S.S.L.C. (State Board)
Indira Convent High School
Percentage - 84% June 2018

TECHNICAL SKILLS

Programming Languages: HTML&CSS, JavaScript [DOM Manipulation, Arrow Functions, Async/Await…].
Library: ReactJS [JSX, React DOM, Props, React Hooks, Components…] . Framework: ExpressJS.
IDE's(Design Tools): NodeJS, Google Colab, VS Code, Jupyter Notebook.
Operating systems: Windows, Ubuntu. Database: MongoDB.
```

i-0a3d9968c103f19b3 (SaiSujanS)

PublicIPs: 3.87.122.65 PrivateIPs: 172.31.44.129

For Windows Instances:

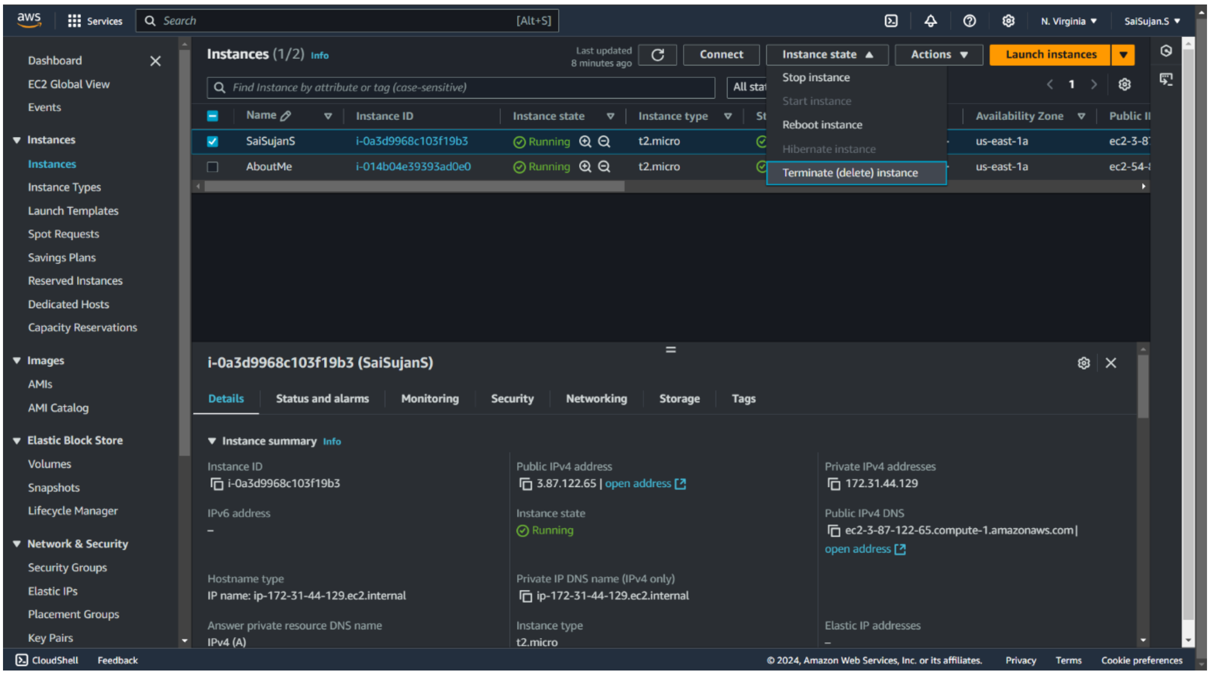
1. *Use Remote Desktop Protocol (RDP) to connect.*
2. *Retrieve the password:*
   - *In the EC2 Dashboard, select the instance, click **Actions > Security > Get Windows Password**.*
   - *Decrypt the password using your private key.*
3. *Open RDP client, enter the public IP, and use the retrieved password.*

Step 6: Manage the EC2 Instance

1. *Monitor your instance in the EC2 Dashboard (CPU, memory usage, etc.).*
2. *Modify instance settings as needed (e.g., stop/restart, resize).*

Step 7: Terminate the Instance (Optional)

1. *To stop incurring costs, terminate the instance when not in use:*
   - *In the EC2 Dashboard, select the instance.*
   - *Click **Actions > Instance State > Terminate**.*



Name	Instance ID	Instance state	Instance type	Availability Zone	Public I
☑ SaiSujanS	i-0a3d9968c103f19b3	Running	t2.micro	us-east-1a	ec2-3-8
□ AboutMe	i-014b04e39393ad0e0	Running	t2.micro	us-east-1a	ec2-54-

i-0a3d9968c103f19b3 (SaiSujanS)

Instance summary Info

Instance ID: i-0a3d9968c103f19b3

Public IPv4 address: 3.87.122.65 | open address

Private IPv4 addresses: 172.31.44.129

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-3-87-122-65.compute-1.amazonaws.com | open address

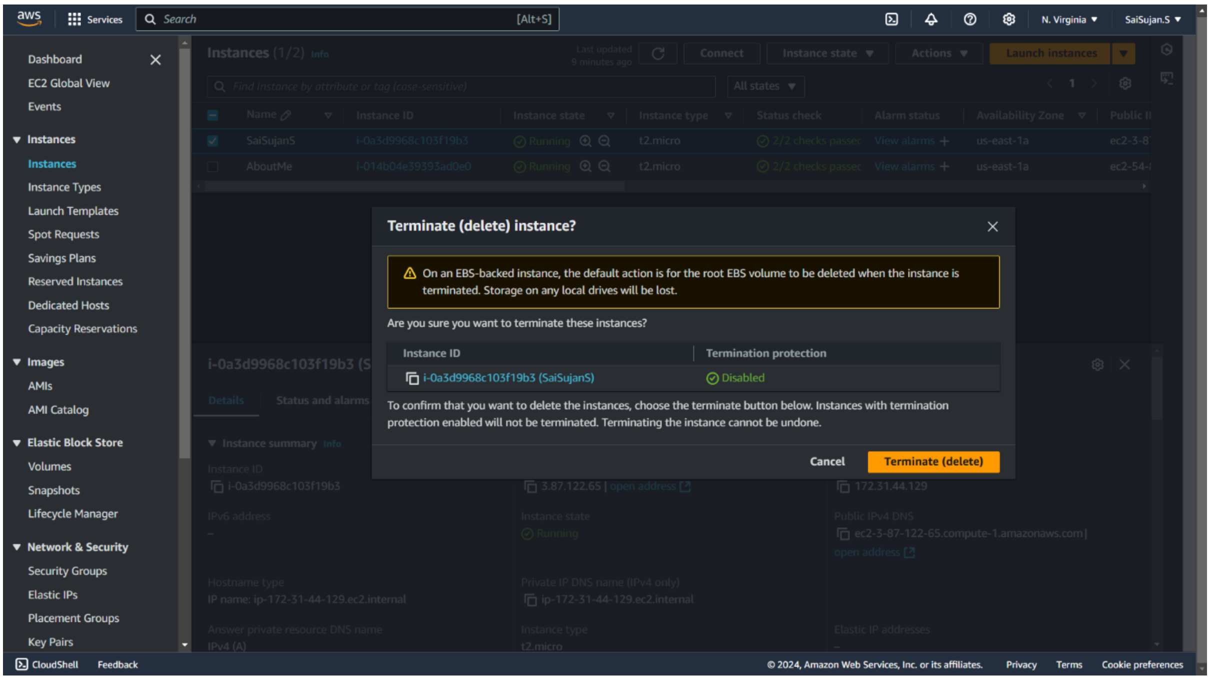
Hostname type: IP name: ip-172-31-44-129.ec2.internal

Private IP DNS name (IPv4 only): ip-172-31-44-129.ec2.internal

Answer private resource DNS name: IPv4 (A)

Instance type: t2.micro

Elastic IP addresses: –



Terminate (delete) instance?

On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

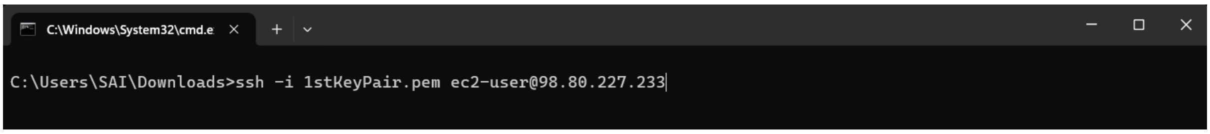
Are you sure you want to terminate these instances?

Instance ID	Termination protection
i-0a3d9968c103f19b3 (SaiSujanS)	Disabled

To confirm that you want to delete the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.

Step 8: To use the AWS instance in the Windows Command Prompt

1. *Navigate to the path where your key pair file is stored and type cmd and enter in the path bar*
2. *Then type **ssh -i <keypairname>.pem <UserName>@<Public IPv4 Address>** and enter.*



```
C:\Users\SAI\Downloads>ssh -i 1stKeyPair.pem ec2-user@98.80.227.233
```

Step 9: To Create Security Group

1. *Navigate to Security Groups section in sidebar of EC2 and then*
2. *Click the **Create security group** button.*

   Fill in the details:
   ***Security group name**: Provide a meaningful name (e.g., MyWebServerSG).*
   ***Description**: Add a description for the security group (e.g., Security group for my web server).*
   ***VPC**: Select the appropriate VPC for your instance.*

3. ***Add Inbound Rules**:*

   Specify the inbound traffic you want to allow:

   For a web server (HTTP), add:

   ***Type**: HTTP*

   ***Protocol**: TCP*

   ***Port Range**: 80*

   ***Source**: Custom (e.g., 0.0.0.0/0 to allow traffic from all IPs).*

   For SSH access:

   ***Type**: SSH*

   ***Protocol**: TCP*

   ***Port Range**: 22*

   ***Source**: Custom (e.g., your IP 203.0.113.25/32 for secure access).*

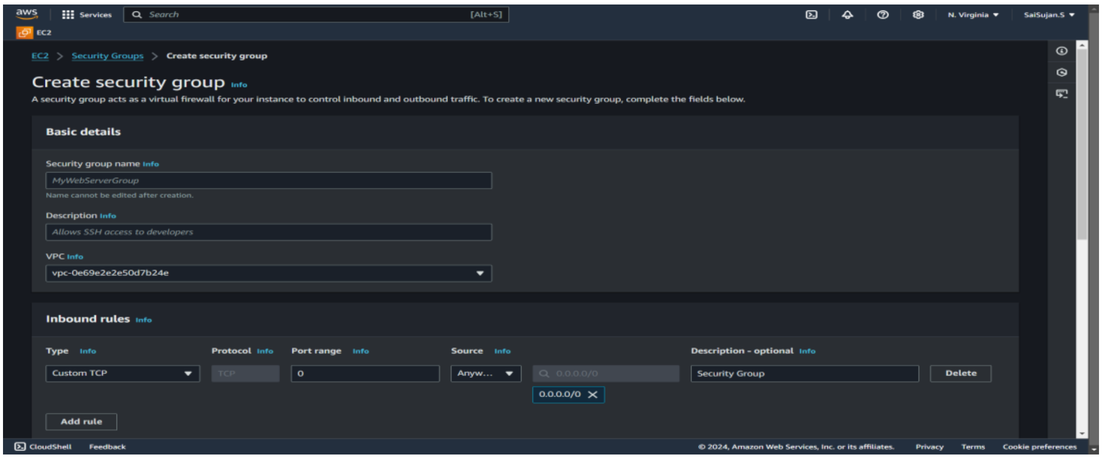
   *Click **Add Rule** to add multiple rules as needed.*

4. ***Add Outbound Rules (Optional)**:*

   AWS allows all outbound traffic by default. Modify if necessary.

5. ***Review and Create**:*

   *Review the configuration and click **Create security group**.*



EC2 > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
MyWebServerGroup
Name cannot be edited after creation.

Description Info
Allows SSH access to developers

VPC Info
vpc-0e69e2e2e50d7b24e

Inbound rules Info

Type	Protocol	Port range	Source		Description - optional	
Custom TCP	TCP	0	Anyw...	0.0.0.0/0 0.0.0.0/0	Security Group	Delete

Add rule

Step 10: To Deploy the files into the server using shellscript / command prompt

1. Ensure you are the root user of the EC2 instance by

   - **whoami** in shellscript.cmd you should be seeing root
   - If you are not the root user
     then type **sudo su** , then you will be the root user.

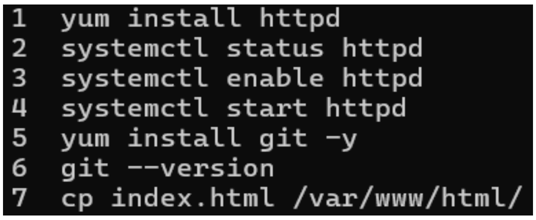
2. Then run the following command

   - **yum install httpd -y** // Install httpd module using yum
   - **systemctl status httpd** // Verify that httpd is installed
   - **systemctl enable httpd** // Enable the httpd server
   - **systemctl start httpd** // Start the httpd server
   - **yum install git -y** // Install git module
   - **git --version** // Verify that git is installed

3. Copy the files if you have them already or create a file and type it there itself

   - To copy the files
   - **cp [path_to_your_file or filename] /var/www/html/**
   - Now the file is deployed.

4. Now to access the webpage/website type your public id/address in the browser.



```
yum install httpd
systemctl status httpd
systemctl enable httpd
systemctl start httpd
yum install git -y
git --version
cp index.html /var/www/html/
```

Step 11: Using Redirection Commands (> and >>)

1. After accessing your EC2 instance, you can use redirection commands to manage files and output data.

2. **Using > (Overwrite Output)**

   The > command is used to redirect command output to a file, overwriting the file if it already exists.

   Example - 1:

   bash

   Copy code

   echo "Hello, World!" > example.txt

   Creates (or overwrites) example.txt with the text Hello, World!.

Example – 2:

echo “<h1>Hello World<h1>” > /var/www/html/index.html

Access the Result using your Public IP address.

3. ***Using >> (Append Output)***

   The >> command is used to append command output to a file without overwriting it.

   Example - 1

   bash

   Copy code

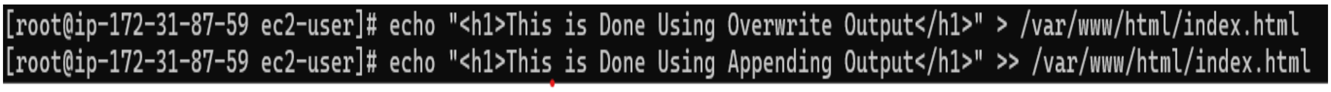
   echo "This is an appended line." >> example.txt

   Adds the line This is an appended line. to the end of example.txt.

   Example – 2

   echo “This is appended line.” >> /var/www/html/index.html

   Access the Result using your Public IP address.



```
[root@ip-172-31-87-59 ec2-user]# echo "<h1>This is Done Using Overwrite Output</h1>" > /var/www/html/index.html
[root@ip-172-31-87-59 ec2-user]# echo "<h1>This is Done Using Appending Output</h1>" >> /var/www/html/index.html
```

Notes:

- *Always ensure your private key file (.pem) is secure.*
- *Monitor your AWS billing to avoid unexpected charges.*
- *Use the AWS Free Tier to avoid costs for eligible resources (e.g., t2.micro).*

  For more details, refer to the AWS EC2 Documentation.