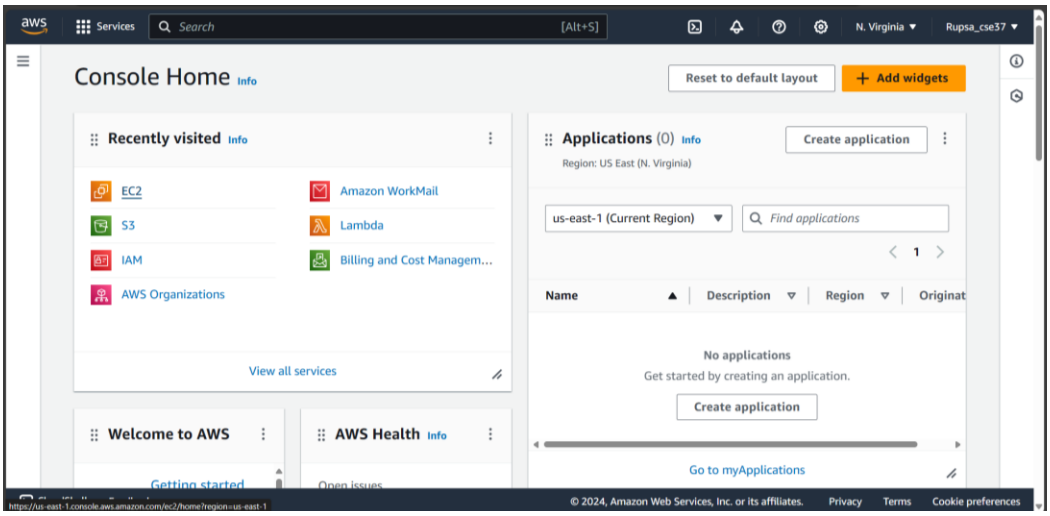
<u>PROBLEM STATEMENT :</u>

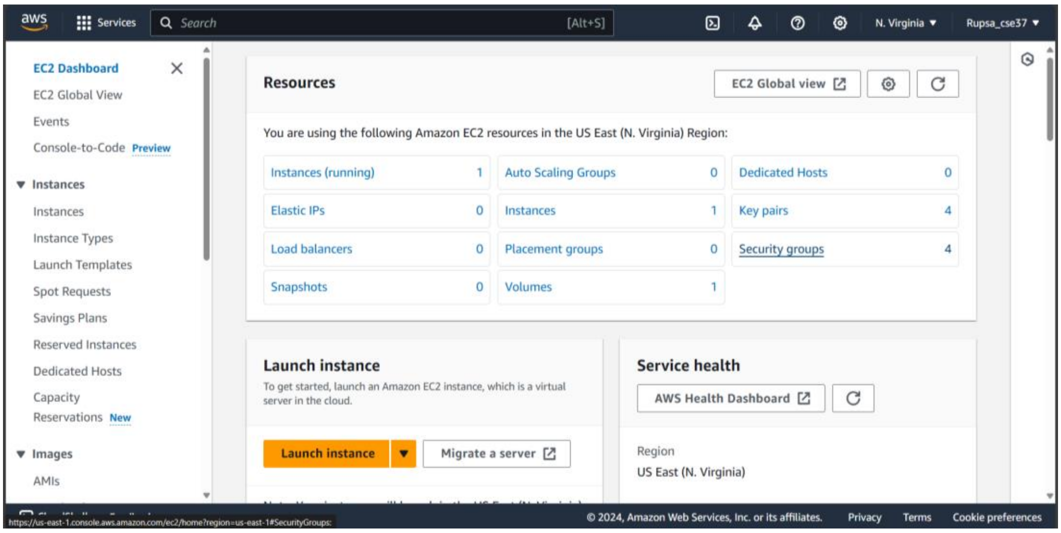
11) Build scaling plans in AWS that balance the load on different EC2 instances.

Steps to build scaling plans :

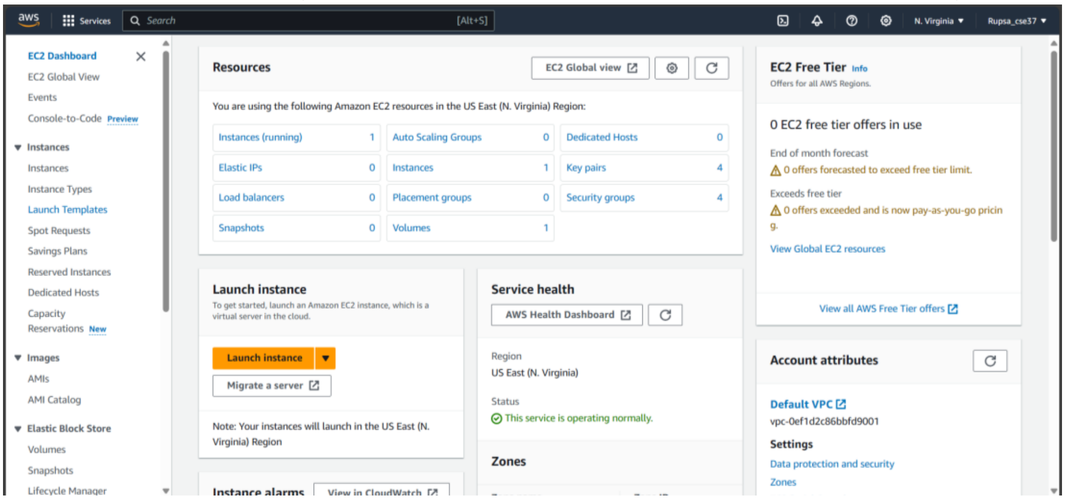
1. Sign up for an AWS account, search for ‘EC2’ then click on it.



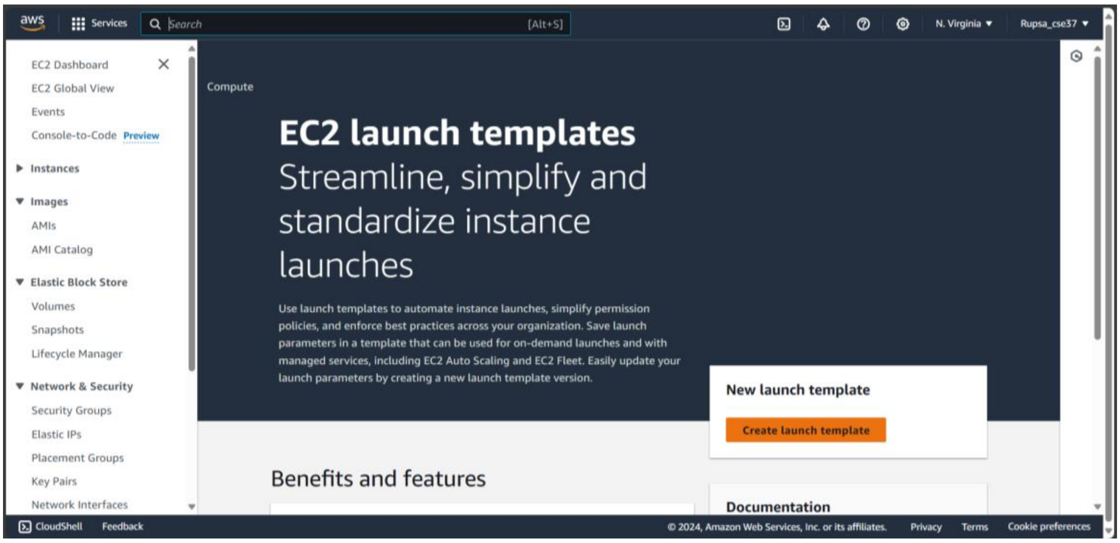
2. If you have an existing Security group then no need to create it if not then create it.



3. Create one template. Click Instances & there click on “Launch template”.



4. Now click on “Create launch template”.



Compute

EC2 launch templates

Streamline, simplify and standardize instance launches

Use launch templates to automate instance launches, simplify permission policies, and enforce best practices across your organization. Save launch parameters in a template that can be used for on-demand launches and with managed services, including EC2 Auto Scaling and EC2 Fleet. Easily update your launch parameters by creating a new launch template version.

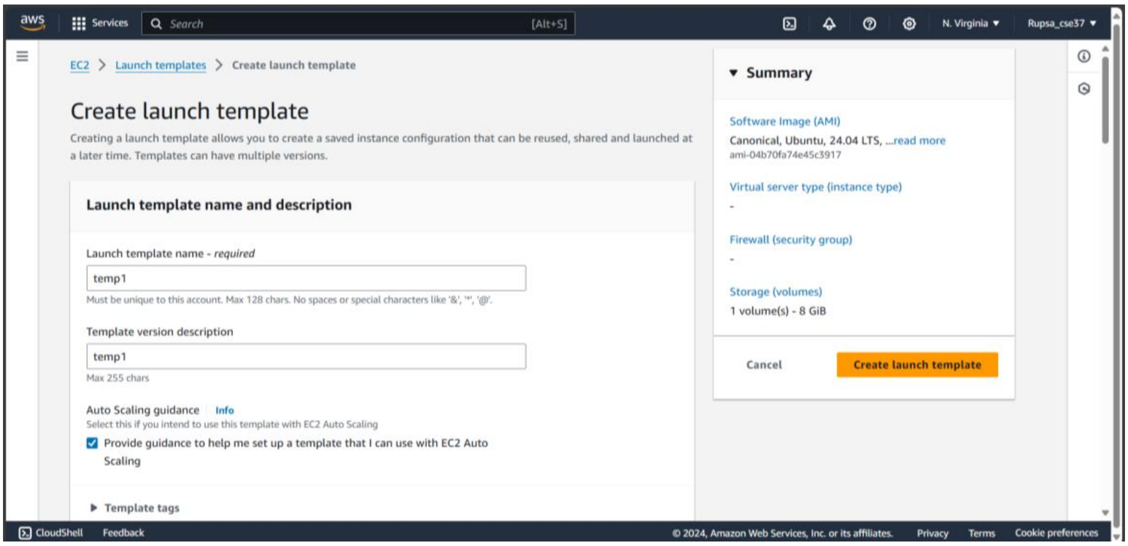
New launch template

Benefits and features

Documentation

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

5. Under “Create launch template”, give the following details.



EC2 > Launch templates > Create launch template

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Launch template name - *required*

temp1

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

temp1

Max 255 chars

Auto Scaling guidance Info

Select this if you intend to use this template with EC2 Auto Scaling

☑ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

Template tags

Summary

Software Image (AMI)

Canonical, Ubuntu, 24.04 LTS, ...read more

ami-04b70fa74e45c3917

Virtual server type (instance type)

-

Firewall (security group)

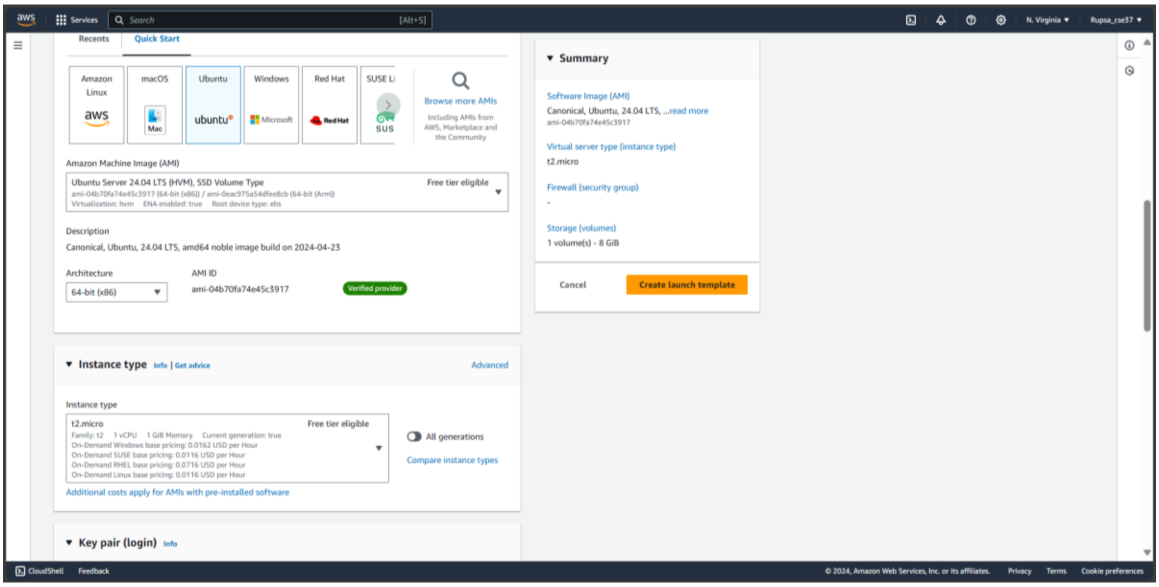
-

Storage (volumes)

1 volume(s) - 8 GiB

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

Click on “Quick start”->ubuntu & “Instance type”->t2.micro as it is free.



Amazon Machine Image (AMI)

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

ami-04b70fa74e45c3917 (64-bit (x86)) / ami-0eac975a54dfee8cb (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Canonical, Ubuntu, 24.04 LTS, amd64 noble image build on 2024-04-23

Architecture

64-bit (x86)

AMI ID

ami-04b70fa74e45c3917

Verified provider

Instance type

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 SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.0716 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)

Summary

Software Image (AMI)

Canonical, Ubuntu, 24.04 LTS, ...read more

ami-04b70fa74e45c3917

Virtual server type (instance type)

t2.micro

Firewall (security group)

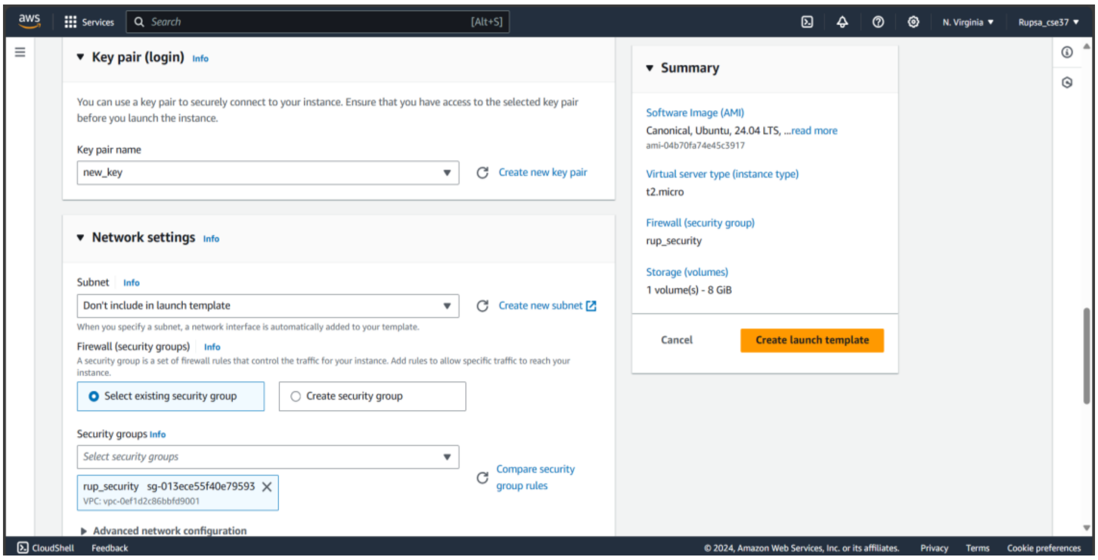
-

Storage (volumes)

1 volume(s) - 8 GiB

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

Now select the key pair & the existing security group.



▾ **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: new_key ▾ — Create new key pair

▾ **Network settings** Info

Subnet Info: Don't include in launch template ▾ — Create new subnet

When you specify a subnet, a network interface is automatically added to your template.

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.

● Select existing security group ○ Create security group

Security groups Info: Select security groups ▾ — Compare security group rules

rup_security sg-013ece55f40e79593 ✕
VPC: vpc-0ef1d2c86bbfd9001

▸ Advanced network configuration

▾ **Summary**

Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-04b70fa74e45c3917

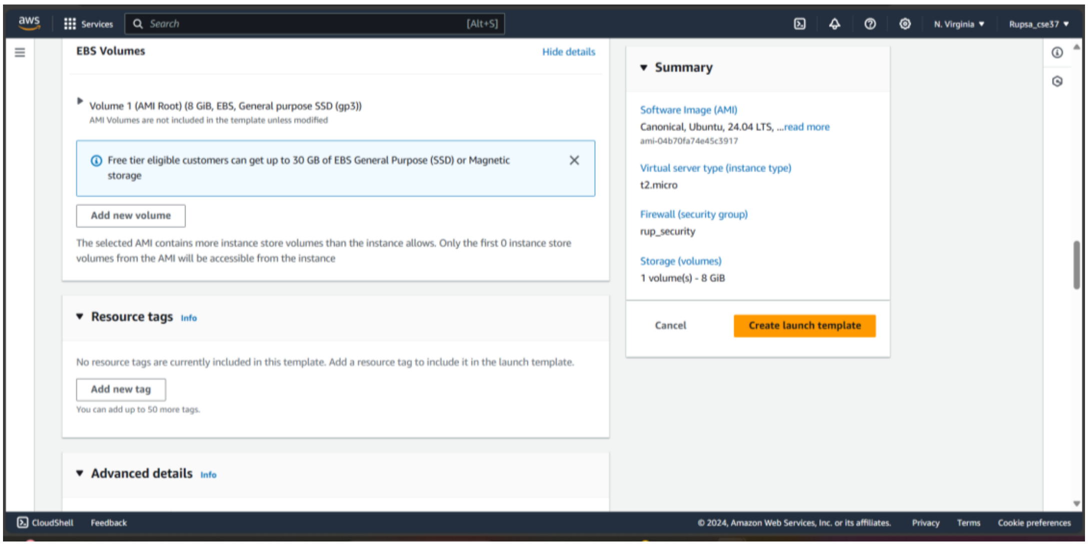
Virtual server type (instance type)
t2.micro

Firewall (security group)
rup_security

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

Cancel | Create launch template

Expand the "Advanced Details" & scroll down to the bottom, in the bash console type the following commands, give the address & repository name from GitHub. Then click on "Create Launch template".



EBS Volumes — Hide details

▸ Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp3))
AMI Volumes are not included in the template unless modified

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

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

▾ **Resource tags** Info

No resource tags are currently included in this template. Add a resource tag to include it in the launch template.

Add new tag

You can add up to 50 more tags.

▾ **Advanced details** Info

▾ **Summary**

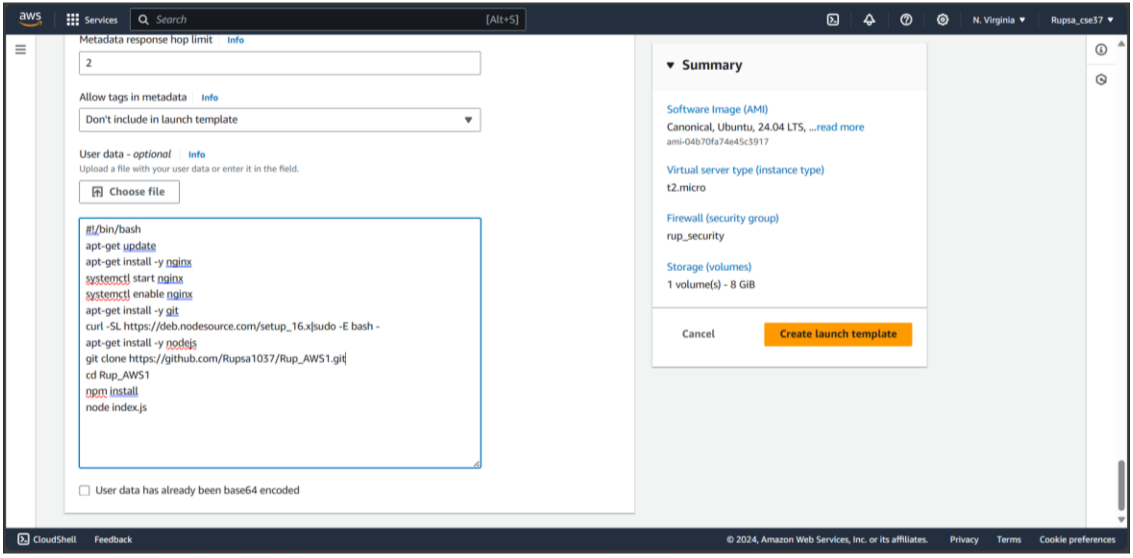
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-04b70fa74e45c3917

Virtual server type (instance type)
t2.micro

Firewall (security group)
rup_security

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

Cancel | Create launch template



Metadata response hop limit Info: 2

Allow tags in metadata Info: Don't include in launch template ▾

User data - *optional* Info

Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
apt-get update
apt-get install -y nginx
systemctl start nginx
systemctl enable nginx
apt-get install -y git
curl -SL https://deb.nodesource.com/setup_16.x|sudo -E bash -
apt-get install -y nodejs
git clone https://github.com/Rupsa1037/Rup_AWS1.git
cd Rup_AWS1
npm install
node index.js
```

□ User data has already been base64 encoded

▾ **Summary**

Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-04b70fa74e45c3917

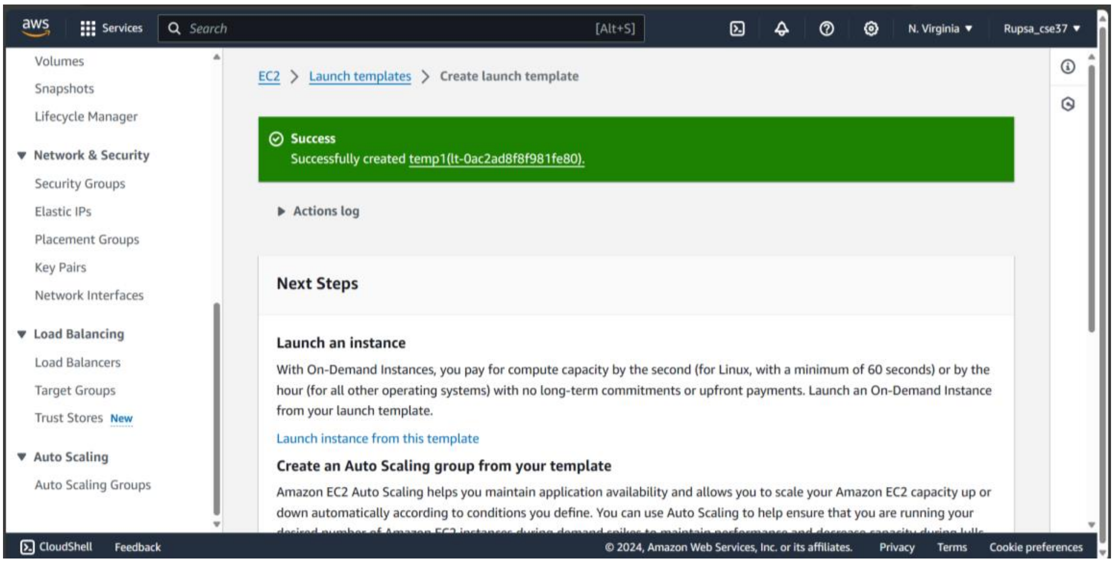
Virtual server type (instance type)
t2.micro

Firewall (security group)
rup_security

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

Cancel | Create launch template

6. Template has been successfully created & now click on “Auto Scaling Groups”.



EC2 > Launch templates > Create launch template

Success
Successfully created temp1(lt-0ac2ad8f8f981fe80).

▶ Actions log

Next Steps

Launch an instance

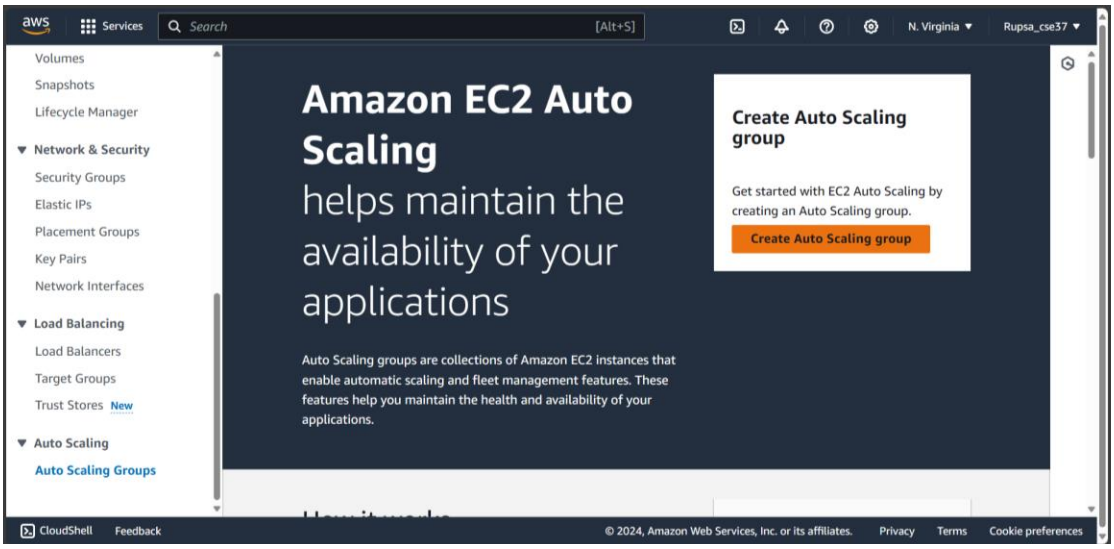
With On-Demand Instances, you pay for compute capacity by the second (for Linux, with a minimum of 60 seconds) or by the hour (for all other operating systems) with no long-term commitments or upfront payments. Launch an On-Demand Instance from your launch template.

Launch instance from this template

Create an Auto Scaling group from your template

Amazon EC2 Auto Scaling helps you maintain application availability and allows you to scale your Amazon EC2 capacity up or down automatically according to conditions you define. You can use Auto Scaling to help ensure that you are running your

7. Click on “Create Auto Scaling group”.



Amazon EC2 Auto Scaling helps maintain the availability of your applications

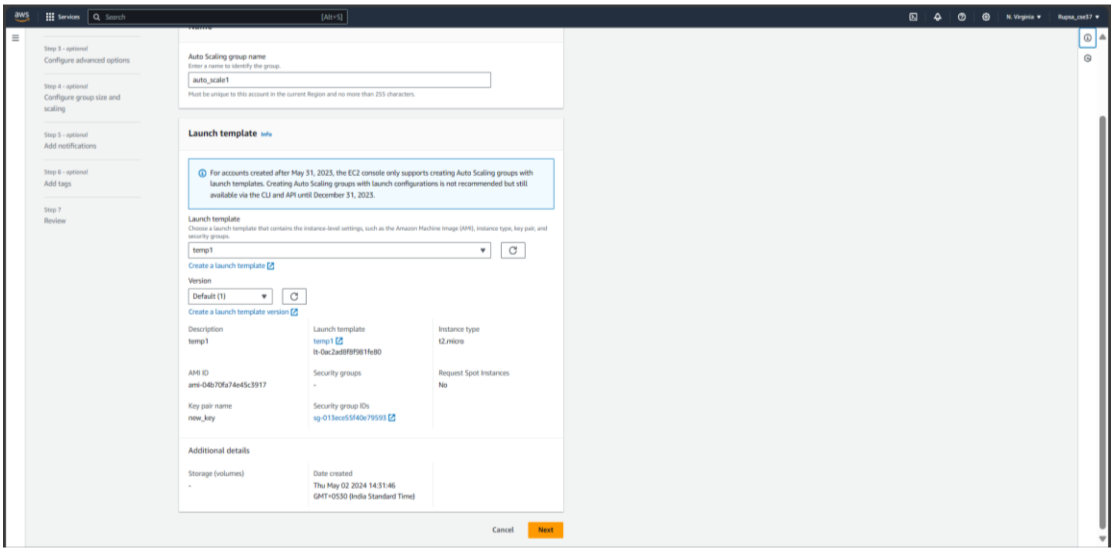
Auto Scaling groups are collections of Amazon EC2 instances that enable automatic scaling and fleet management features. These features help you maintain the health and availability of your applications.

Create Auto Scaling group

Get started with EC2 Auto Scaling by creating an Auto Scaling group.

Create Auto Scaling group

8. Under “Create Auto Scaling group”, give the name & choose the template that you have created then click on “Next”.



Auto Scaling group name
Enter a name to identify the group.
auto_scale1
Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.
temp1 ▾
Create a launch template

Version
Default (1) ▾
Create a launch template version

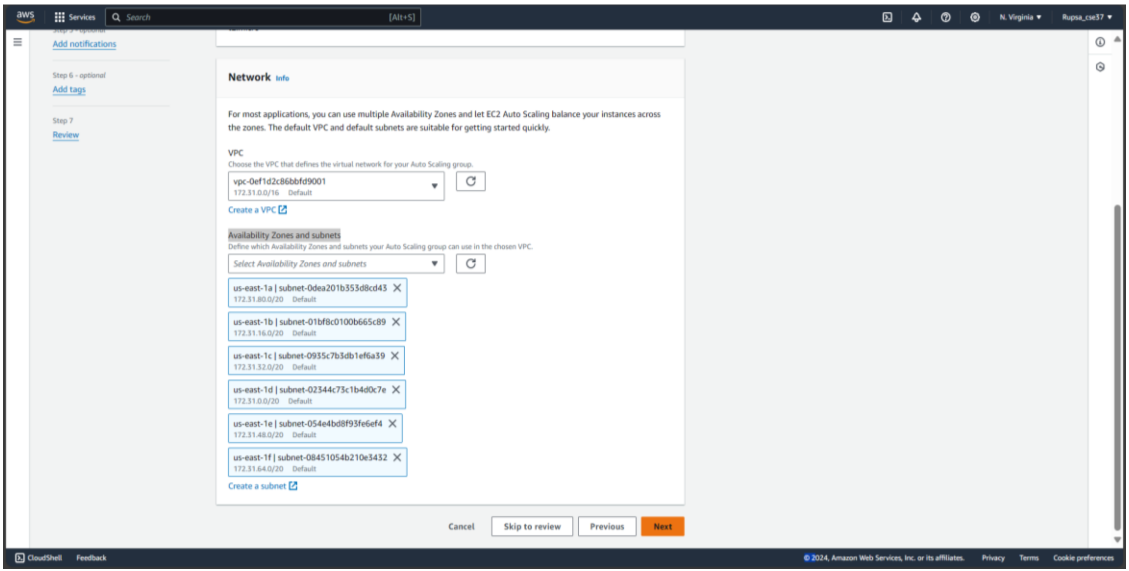
Description	Launch template	Instance type
temp1	temp1 lt-0ac2ad8f8f981fe80	t2.micro
AMI ID	Security groups	Request Spot Instances
ami-04b70fa74e45c3917	-	No
Key pair name	Security group IDs	
new_key	sg-013ece55f40e79593	

Additional details

Storage (volumes)	Date created
-	Thu May 02 2024 14:31:46 GMT+0530 (India Standard Time)

Cancel Next

Then select all the “Availability Zones and subnets” & click on “Next”.



Add notifications

Step 6 - *optional*

Add tags

Step 7

Review

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0ef1d2c86bbfd9001 ▾
172.31.0.0/16 Default

Create a VPC

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets ▾

us-east-1a | subnet-0dea201b353d8cd43 ✕
172.31.80.0/20 Default

us-east-1b | subnet-01bf8c0100b665c89 ✕
172.31.16.0/20 Default

us-east-1c | subnet-0935c7b3db1ef6a39 ✕
172.31.32.0/20 Default

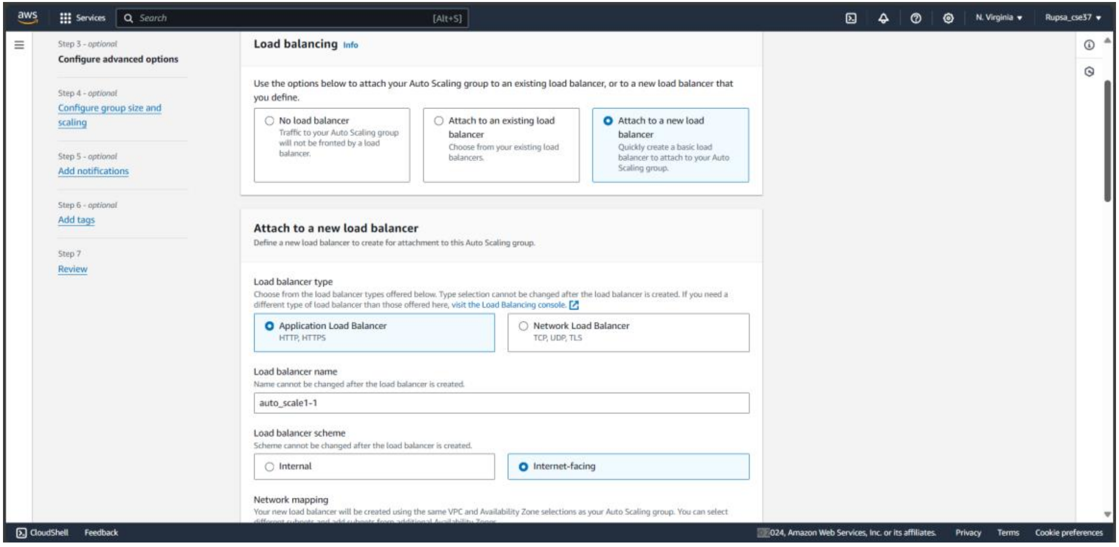
us-east-1d | subnet-02344c73c1b4d0c7e ✕
172.31.0.0/20 Default

us-east-1e | subnet-054e4bd8f93fe6ef4 ✕
172.31.48.0/20 Default

us-east-1f | subnet-08451054b210e3432 ✕
172.31.64.0/20 Default

Create a subnet

Cancel | Skip to review | Previous | Next



Step 3 - *optional*

Configure advanced options

Step 4 - *optional*

Configure group size and scaling

Step 5 - *optional*

Add notifications

Step 6 - *optional*

Add tags

Step 7

Review

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

○ No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.

○ Attach to an existing load balancer
Choose from your existing load balancers.

● Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to a new load balancer

Define a new load balancer to create for attachment to this Auto Scaling group.

Load balancer type

Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the Load Balancing console.

● Application Load Balancer
HTTP, HTTPS

○ Network Load Balancer
TCP, UDP, TLS

Load balancer name

Name cannot be changed after the load balancer is created.

auto_scale1-1

Load balancer scheme

Scheme cannot be changed after the load balancer is created.

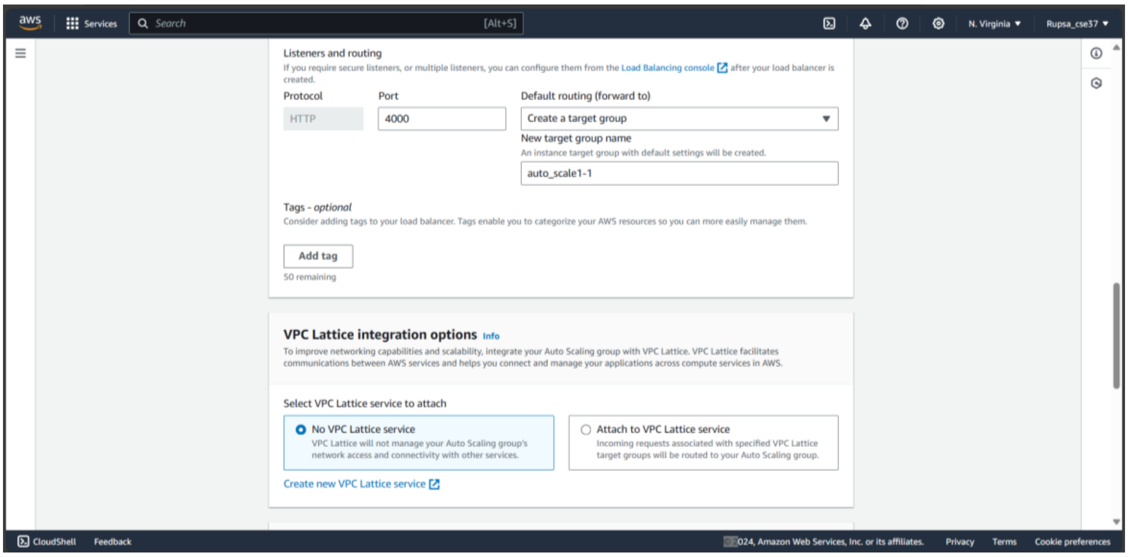
○ Internal

● Internet-facing

Network mapping

Your new load balancer will be created using the same VPC and Availability Zone selections as your Auto Scaling group. You can select

Click on “No VPC Lattice service”.



Listeners and routing

If you require secure listeners, or multiple listeners, you can configure them from the Load Balancing console after your load balancer is created.

Protocol	Port	Default routing (forward to)
HTTP	4000	Create a target group ▾

New target group name

An instance target group with default settings will be created.

auto_scale1-1

Tags - *optional*

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add tag

50 remaining

VPC Lattice integration options Info

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

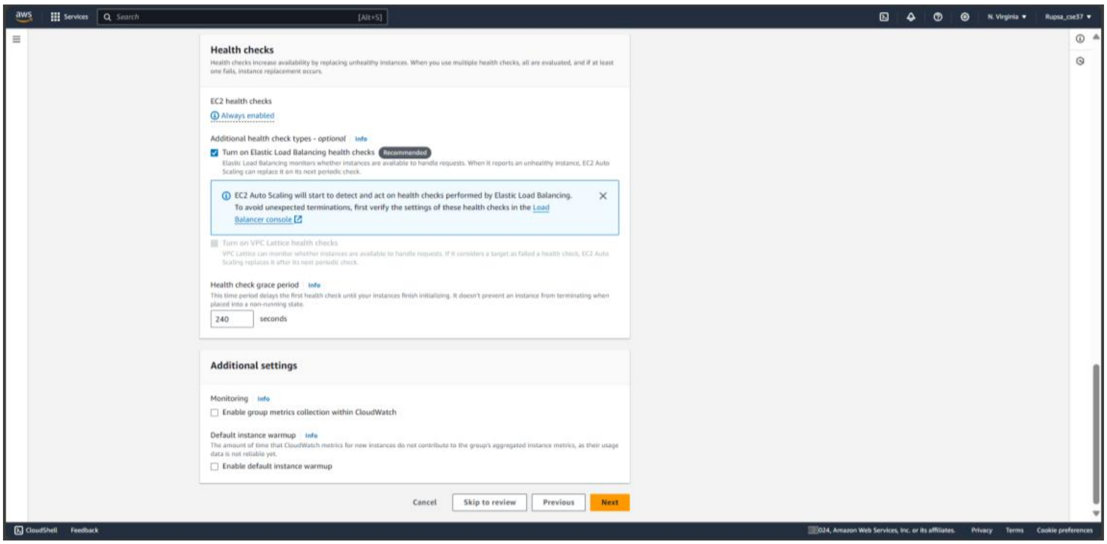
Select VPC Lattice service to attach

● No VPC Lattice service
VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.

○ Attach to VPC Lattice service
Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.

Create new VPC Lattice service

In “Health checks”, click on the checkbox “Turn on Elastic load …” Then click on “Next”.



Health checks

Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.

EC2 health checks

ⓘ Always enabled

Additional health check types - *optional* Info

☑ Turn on Elastic Load Balancing health checks Recommended

Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.

ⓘ EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing. To avoid unexpected terminations, first verify the settings of these health checks in the Load Balancer console

□ Turn on VPC Lattice health checks

VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.

Health check grace period Info

This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.

240 seconds

Additional settings

Monitoring Info

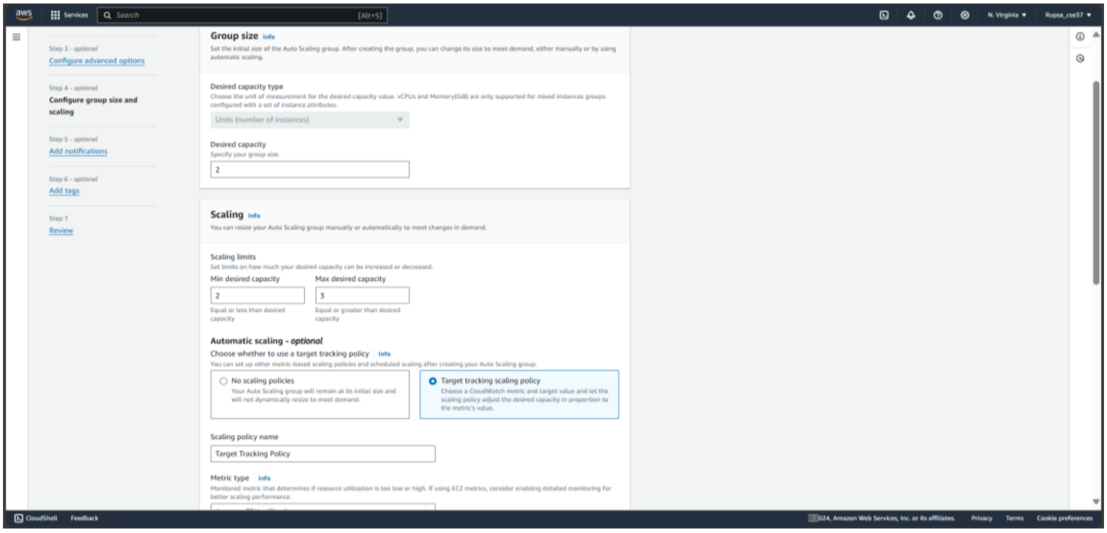
□ Enable group metrics collection within CloudWatch

Default instance warmup Info

The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

□ Enable default instance warmup

Cancel | Skip to review | Previous | Next



Step 3 - *optional*
Configure advanced options

Step 4 - *optional*
Configure group size and scaling

Step 5 - *optional*
Add notifications

Step 6 - *optional*
Add tags

Step 7
Review

Group size Info

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances) ▾

Desired capacity

Specify your group size.

2

Scaling Info

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity: 2 — Equal or less than desired capacity

Max desired capacity: 3 — Equal or greater than desired capacity

Automatic scaling - *optional*

Choose whether to use a target tracking policy Info

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

○ No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

● Target tracking scaling policy
Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

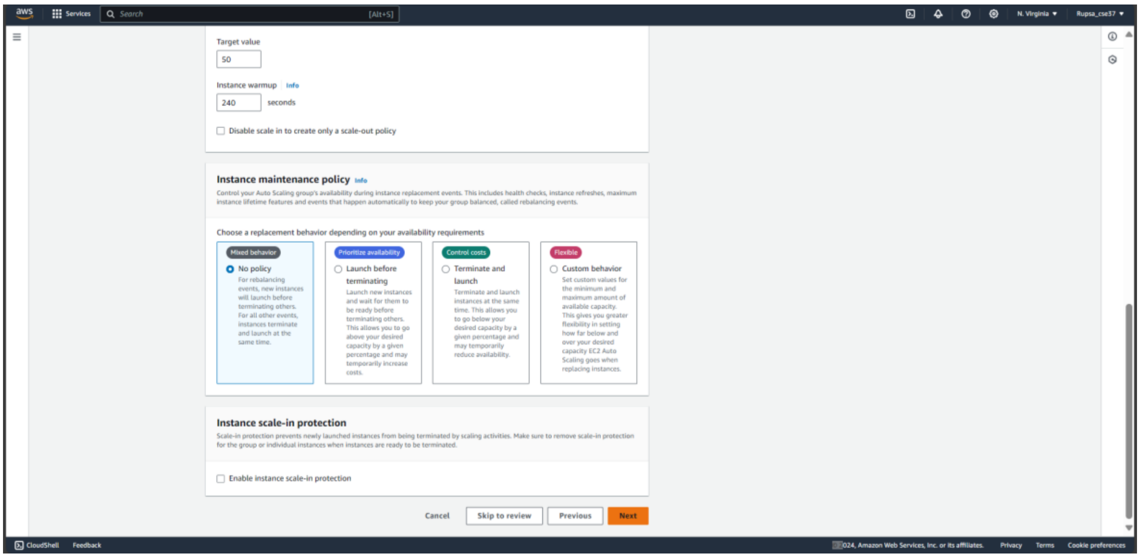
Scaling policy name

Target Tracking Policy

Metric type Info

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Click on “No policy” then on “Next”.



Target value

50

Instance warmup Info

240 seconds

□ Disable scale in to create only a scale-out policy

Instance maintenance policy Info

Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.

Choose a replacement behavior depending on your availability requirements

Mixed behavior
● No policy
For rebalancing events, new instances will launch before terminating others. For all other events, instances terminate and launch at the same time.

Prioritize availability
○ Launch before terminating
Launch new instances and wait for them to be ready before terminating others. This allows you to go above your desired capacity by a given percentage and may temporarily increase costs.

Control costs
○ Terminate and launch
Terminate and launch instances at the same time. This allows you to go below your desired capacity by a given percentage and may temporarily reduce availability.

Flexible
○ Custom behavior
Set custom values for the minimum and maximum amount of available capacity. This gives you greater flexibility in setting how far below and over your desired capacity EC2 Auto Scaling goes when replacing instances.

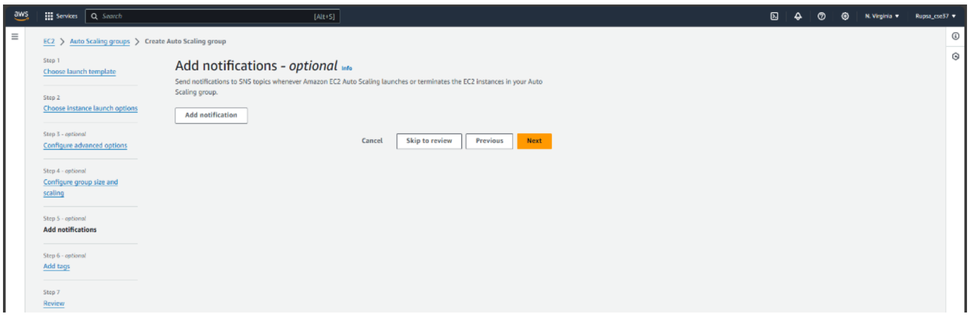
Instance scale-in protection

Scale-in protection prevents newly launched instances from being terminated by scaling activities. Make sure to remove scale-in protection for the group or individual instances when instances are ready to be terminated.

□ Enable instance scale-in protection

Cancel | Skip to review | Previous | Next

Click on “Next”.



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template

Step 2
Choose instance launch options

Step 3 - optional
Configure advanced options

Step 4 - optional
Configure group size and scaling

Step 5 - optional
Add notifications

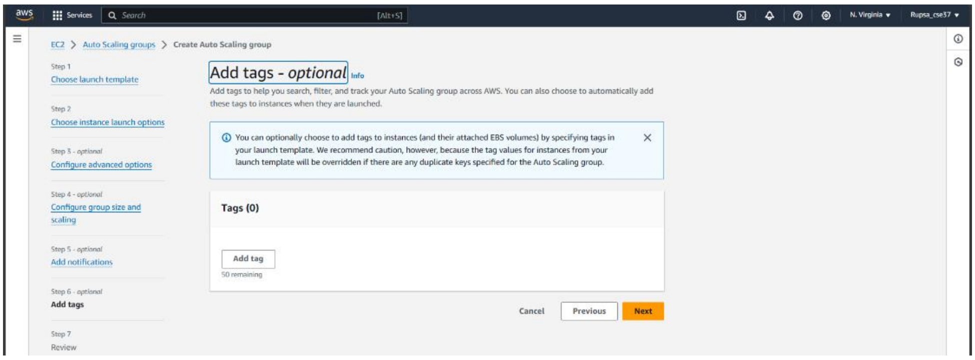
Step 6 - optional
Add tags

Step 7
Review

Add notifications - *optional* Info

Send notifications to SNS topics whenever Amazon EC2 Auto Scaling launches or terminates the EC2 instances in your Auto Scaling group.

Click on “Next”.



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template

Step 2
Choose instance launch options

Step 3 - optional
Configure advanced options

Step 4 - optional
Configure group size and scaling

Step 5 - optional
Add notifications

Step 6 - optional
Add tags

Step 7
Review

Add tags - *optional* Info

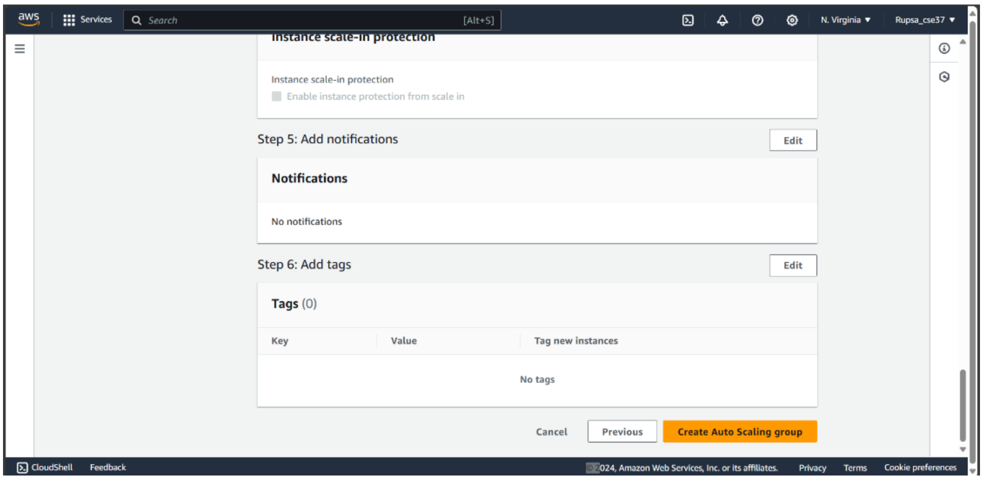
Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched.

You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group.

Tags (0)

50 remaining

Click on “Create Auto Scaling group”.



Instance scale-in protection

Instance scale-in protection
□ Enable instance protection from scale in

Step 5: Add notifications

Notifications

No notifications

Step 6: Add tags

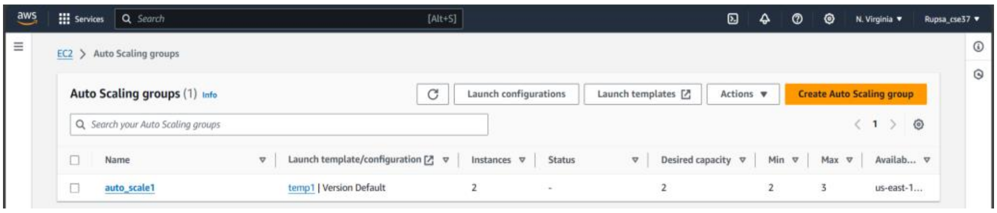
Tags (0)

Key	Value	Tag new instances

No tags

Edit
Edit
Cancel
Previous
Create Auto Scaling group
CloudShell
Feedback
024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

9. Auto scaling group is successfully created.

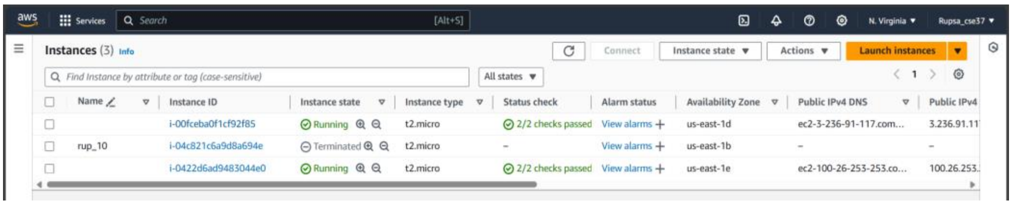


EC2 > Auto Scaling groups

Auto Scaling groups (1) Info

□	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availab...
□	auto_scale1	temp1 | Version Default	2	-	2	2	3	us-east-1...

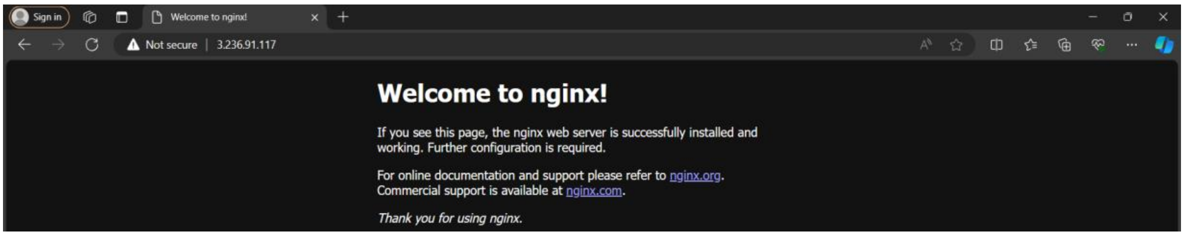
10. Now go to “Instance” and check for running instances with no name and then click on any one of the instance ID & copy the “Public IPv4 address”.



Instances (3) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
□		i-00fceba0f1cf92f85	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1d	ec2-3-236-91-117.com...	3.236.91.11
□	rup_10	i-04c821c6a9d8a694e	Terminated	t2.micro	-	View alarms +	us-east-1b	-	-
□		i-0422d6ad9483044e0	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1e	ec2-100-26-253-253.co...	100.26.253.

11. Paste the address in a new Window.



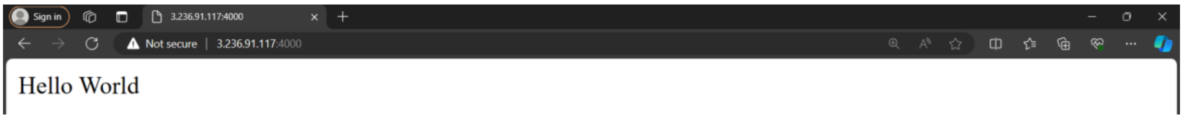
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

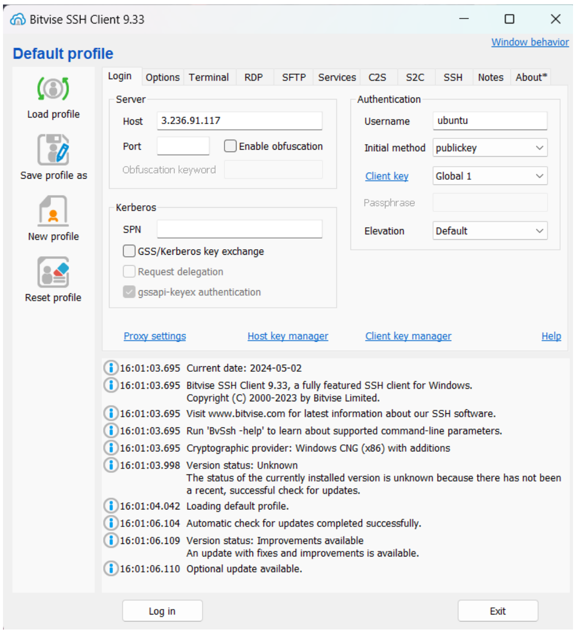
Thank you for using nginx.

12. Now add ":4000" at the end of the IPv4 address and press enter.



Hello World

13. Then copy the address of any one of the instance & paste in the host of the "Bitvise SSH Client" then click on "Client key Manager".



Server

Host: 3.236.91.117

Port:

□ Enable obfuscation

Obfuscation keyword:

Kerberos

SPN:

□ GSS/Kerberos key exchange

□ Request delegation

☑ gssapi-keyex authentication

Authentication

Username: ubuntu

Initial method: publickey

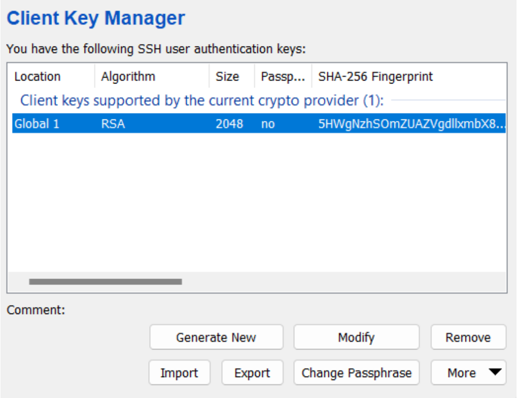
Client key: Global 1

Passphrase:

Elevation: Default

```
16:01:03.695  Current date: 2024-05-02
16:01:03.695  Bitvise SSH Client 9.33, a fully featured SSH client for Windows.
              Copyright (C) 2000-2023 by Bitvise Limited.
16:01:03.695  Visit www.bitvise.com for latest information about our SSH software.
16:01:03.695  Run 'BvSsh -help' to learn about supported command-line parameters.
16:01:03.695  Cryptographic provider: Windows CNG (x86) with additions
16:01:03.998  Version status: Unknown
              The status of the currently installed version is unknown because there has not been
              a recent, successful check for updates.
16:01:04.042  Loading default profile.
16:01:06.104  Automatic check for updates completed successfully.
16:01:06.109  Version status: Improvements available
              An update with fixes and improvements is available.
16:01:06.110  Optional update available.
```

14. Then import the key & click on "Log in".



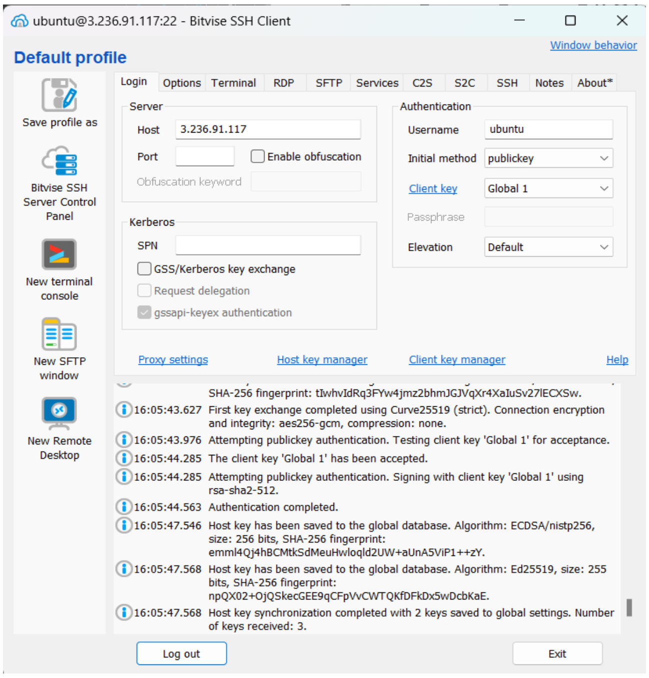
Client Key Manager

You have the following SSH user authentication keys:

Location	Algorithm	Size	Passp...	SHA-256 Fingerprint
Client keys supported by the current crypto provider (1):				
Global 1	RSA	2048	no	5HWgNzhSOmZUAZVgdllxmbX8...

Comment:

15. The “Log out” came means that is is successfully logged in.



ubuntu@3.236.91.117:22 - Bitvise SSH Client

Default profile

Server

Host: 3.236.91.117

Port:

☐ Enable obfuscation

Obfuscation keyword:

Kerberos

SPN:

☐ GSS/Kerberos key exchange

☐ Request delegation

☑ gssapi-keyex authentication

Authentication

Username: ubuntu

Initial method: publickey

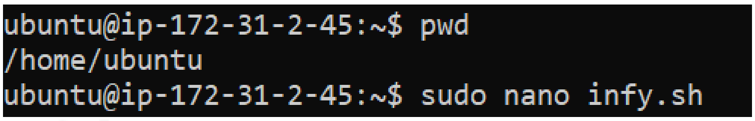
Client key: Global 1

Passphrase:

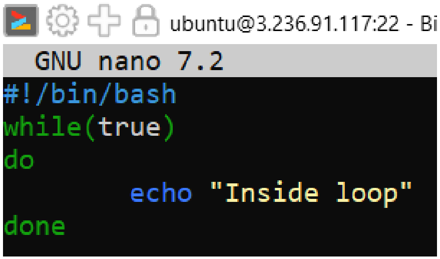
Elevation: Default

```
                SHA-256 fingerprint: tIwhvIdRq3FYw4jmz2bhmJGJVqXr4XaIuSv27lECXSw.
16:05:43.627  First key exchange completed using Curve25519 (strict). Connection encryption
              and integrity: aes256-gcm, compression: none.
16:05:43.976  Attempting publickey authentication. Testing client key 'Global 1' for acceptance.
16:05:44.285  The client key 'Global 1' has been accepted.
16:05:44.285  Attempting publickey authentication. Signing with client key 'Global 1' using
              rsa-sha2-512.
16:05:44.563  Authentication completed.
16:05:47.546  Host key has been saved to the global database. Algorithm: ECDSA/nistp256,
              size: 256 bits, SHA-256 fingerprint:
              emml4Qj4hBCMtkSdMeuHwloqld2UW+aUnA5ViP1++zY.
16:05:47.568  Host key has been saved to the global database. Algorithm: Ed25519, size: 255
              bits, SHA-256 fingerprint:
              npQX02+OjQSkecGEE9qCFpVvCWTQKfDFkDx5wDcbKaE.
16:05:47.568  Host key synchronization completed with 2 keys saved to global settings. Number
              of keys received: 3.
```

16. Now in “New terminal console” and type the following commands.

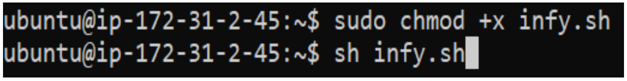


```
ubuntu@ip-172-31-2-45:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-2-45:~$ sudo nano infy.sh
```

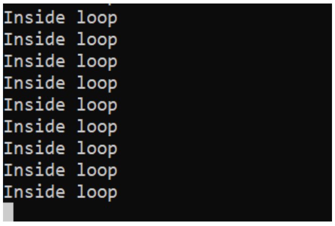


ubuntu@3.236.91.117:22 - Bi

```
 GNU nano 7.2
#!/bin/bash
while(true)
do
        echo "Inside loop"
done
```

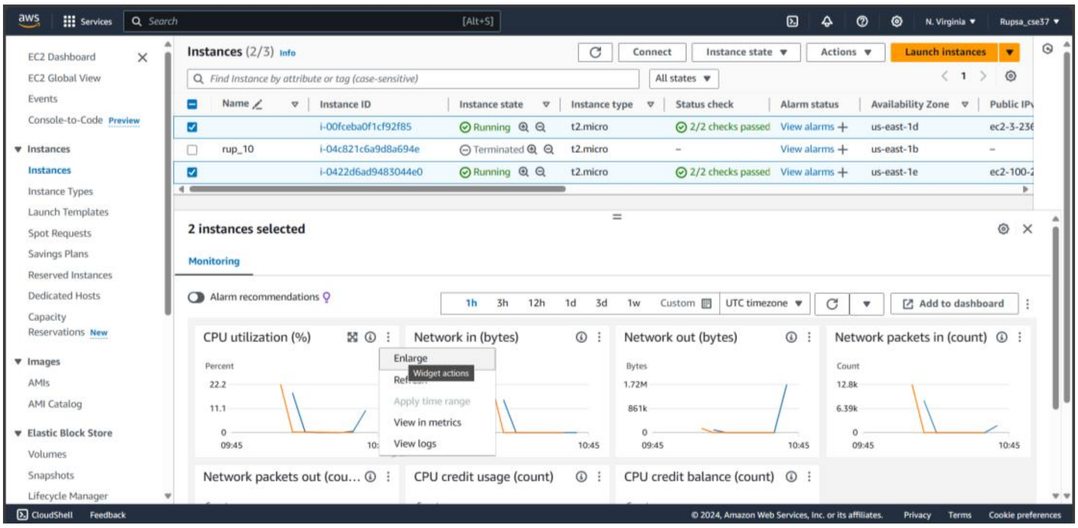


```
ubuntu@ip-172-31-2-45:~$ sudo chmod +x infy.sh
ubuntu@ip-172-31-2-45:~$ sh infy.sh
```



```
Inside loop
Inside loop
Inside loop
Inside loop
Inside loop
Inside loop
Inside loop
Inside loop
Inside loop
```

17. Now In Instances select both the unnamed instances & click on 'Enlarge'.

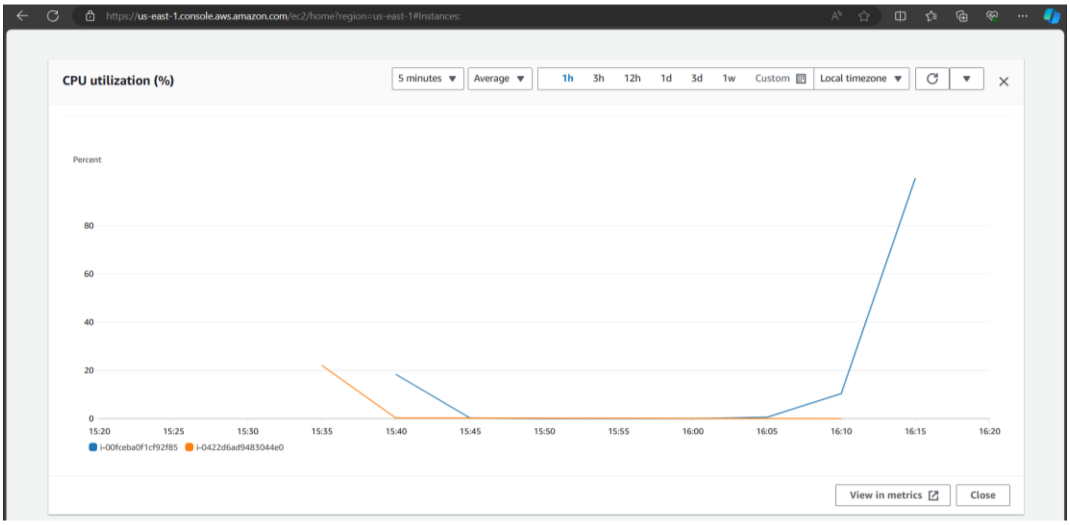


Instances (2/3)

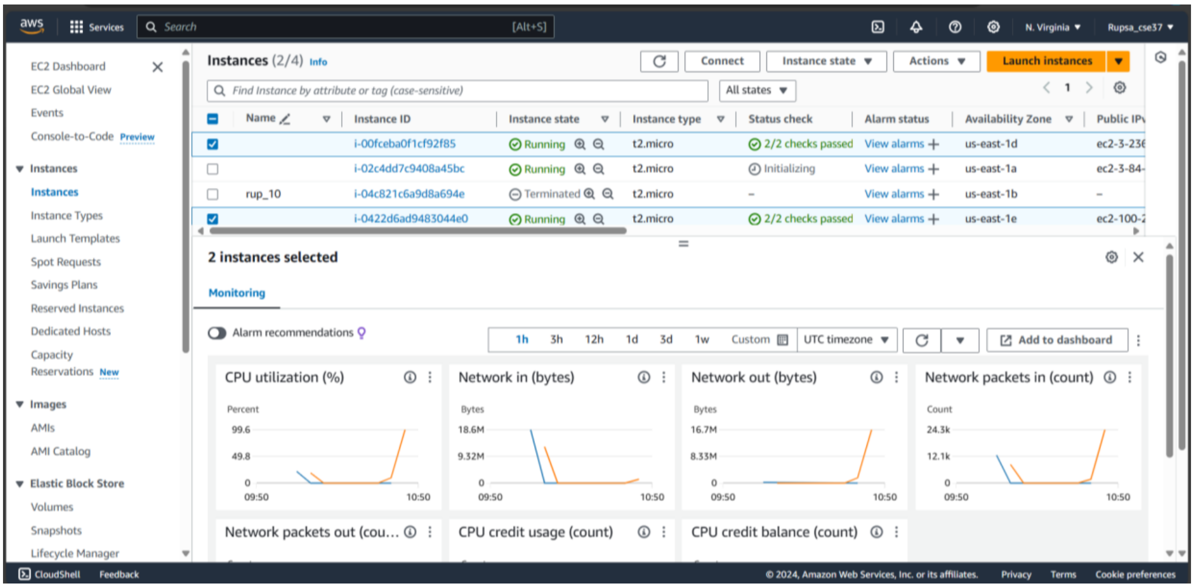
☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv
☑		i-00fceba0f1cf92f85	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1d	ec2-3-23€
□	rup_10	i-04c821c6a9d8a694e	Terminated	t2.micro	–	View alarms +	us-east-1b	–
☑		i-0422d6ad9483044e0	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1e	ec2-100-2

2 instances selected

18. Here, we see the graph of CPU utilization(%) & select "Local timezone".



19. Here, we see that two instances are running along with the initialization of the third instance.



Instances (2/4) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv
☑		i-00fceba0f1cf92f85	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1d	ec2-3-23€
☐		i-02c4dd7c9408a45bc	Running	t2.micro	Initializing	View alarms +	us-east-1a	ec2-3-84-
☐	rup_10	i-04c821c6a9d8a694e	Terminated	t2.micro	–	View alarms +	us-east-1b	–
☑		i-0422d6ad9483044e0	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1e	ec2-100-2

2 instances selected

Monitoring