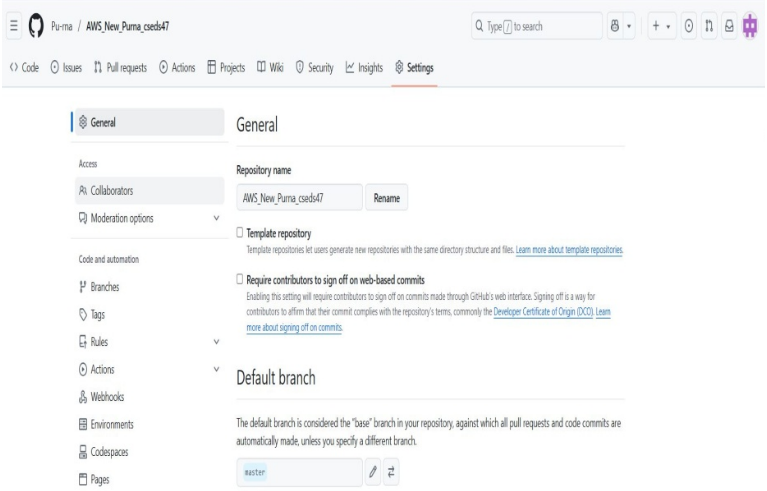
ASSIGNMENT 11: Build scaling plans in AWS that balance the load on different EC2 instances.

STEP 1 :- Check if your **GitHub Repository** is **public or not** . For that Login to your GitHub Account and then select your Repository and then go to **Setting** and **navigate** to **Danger Zone** and check your **Repository Visibility.**



Pu-rna / AWS_New_Purna_cseds47

Type / to search

General

Repository name

AWS_New_Purna_cseds47 Rename

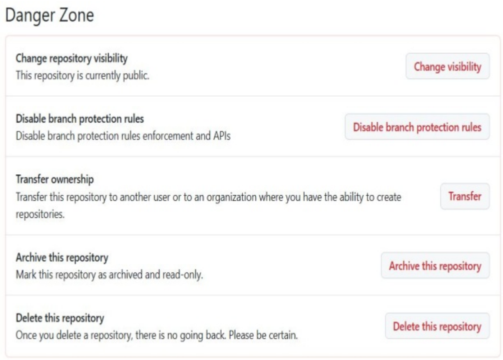
□ Template repository
Template repositories let users generate new repositories with the same directory structure and files. Learn more about template repositories.

□ Require contributors to sign off on web-based commits
Enabling this setting will require contributors to sign off on commits made through GitHub's web interface. Signing off is a way for contributors to affirm that their commit complies with the repository's terms, commonly the Developer Certificate of Origin (DCO). Learn more about signing off on commits.

Default branch

The default branch is considered the "base" branch in your repository, against which all pull requests and code commits are automatically made, unless you specify a different branch.

master



Danger Zone

Change repository visibility
This repository is currently public. Change visibility

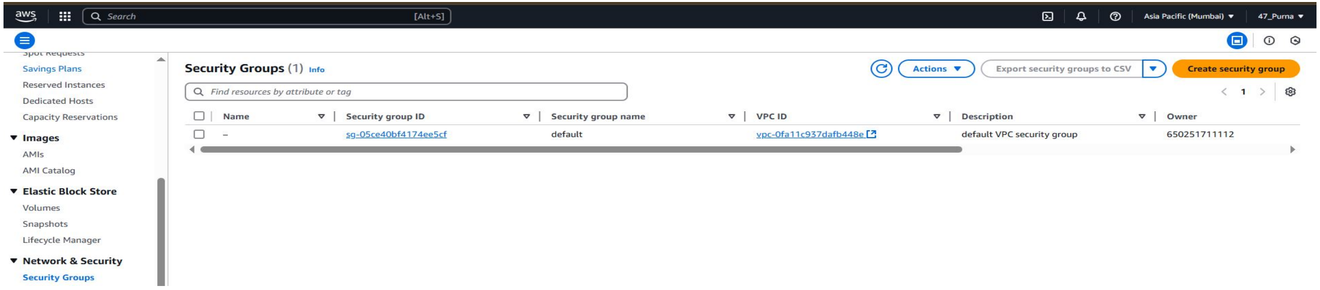
Disable branch protection rules
Disable branch protection rules enforcement and APIs Disable branch protection rules

Transfer ownership
Transfer this repository to another user or to an organization where you have the ability to create repositories. Transfer

Archive this repository
Mark this repository as archived and read-only. Archive this repository

Delete this repository
Once you delete a repository, there is no going back. Please be certain. Delete this repository

STEP 2 :- Login to your AWS Account and click on **EC2** and go to **Security Groups** and click on **Create Security Group**.

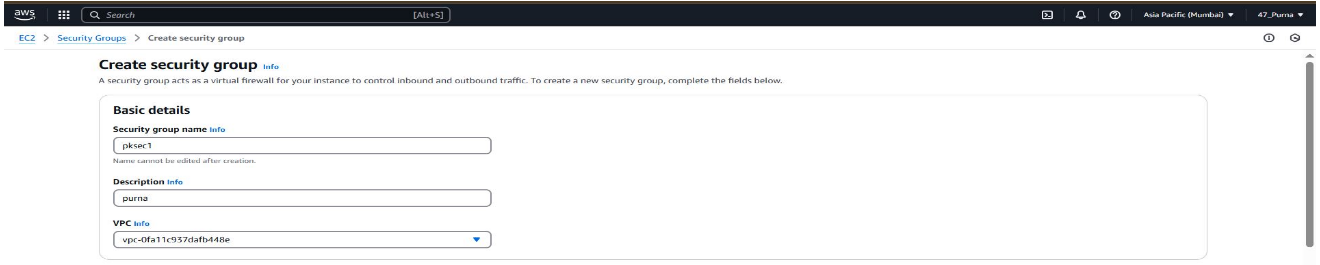


Security Groups (1) Info

Find resources by attribute or tag

□	Name	Security group ID	Security group name	VPC ID	Description	Owner
□	–	sg-05ce40bf4174ee5cf	default	vpc-0fa11c937dafb448e	default VPC security group	650251711112

>> Give the **Security Group Name and Description** and the click on **Add Rules of Inbound Rules.**



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.

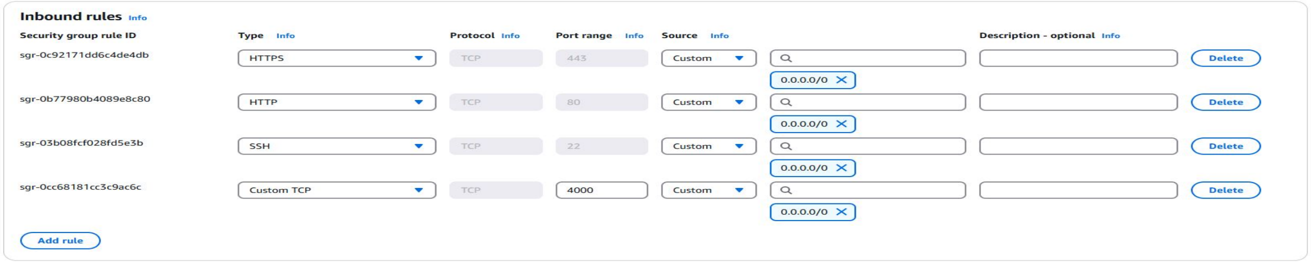
Basic details

Security group name Info: pksec1
Name cannot be edited after creation.

Description Info: purna

VPC Info: vpc-0fa11c937dafb448e

>> Add SSH , HTTP , HTTPS and CUSTOM TCP Type Rules as Given below.

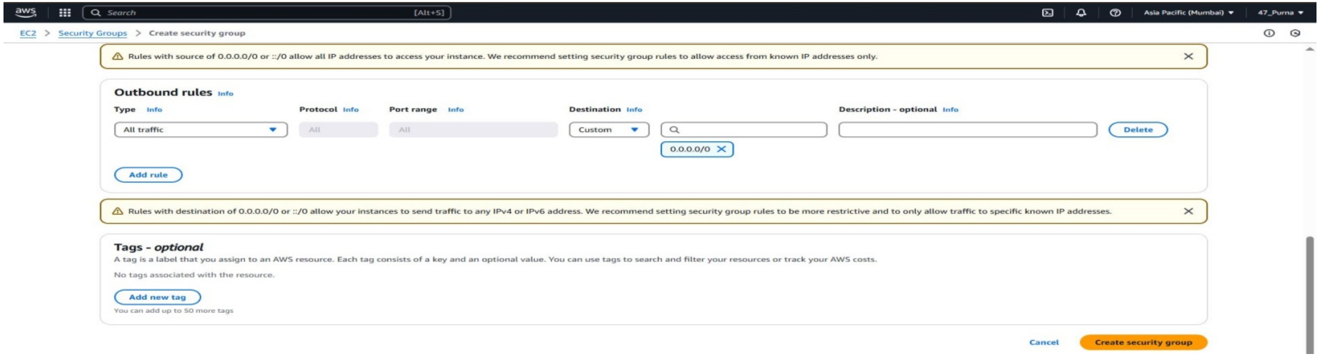


Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional	
sgr-0c92171dd6c4de4db	HTTPS	TCP	443	Custom	0.0.0.0/0		Delete
sgr-0b77980b4089e8c80	HTTP	TCP	80	Custom	0.0.0.0/0		Delete
sgr-03b08fcf028fd5e3b	SSH	TCP	22	Custom	0.0.0.0/0		Delete
sgr-0cc68181cc3c9ac6c	Custom TCP	TCP	4000	Custom	0.0.0.0/0		Delete

Add rule

>> Click on **CREATE Security Group**.



EC2 > Security Groups > Create security group

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

Outbound rules Info

Type	Protocol	Port range	Destination		Description - optional	
All traffic	All	All	Custom	0.0.0.0/0		Delete

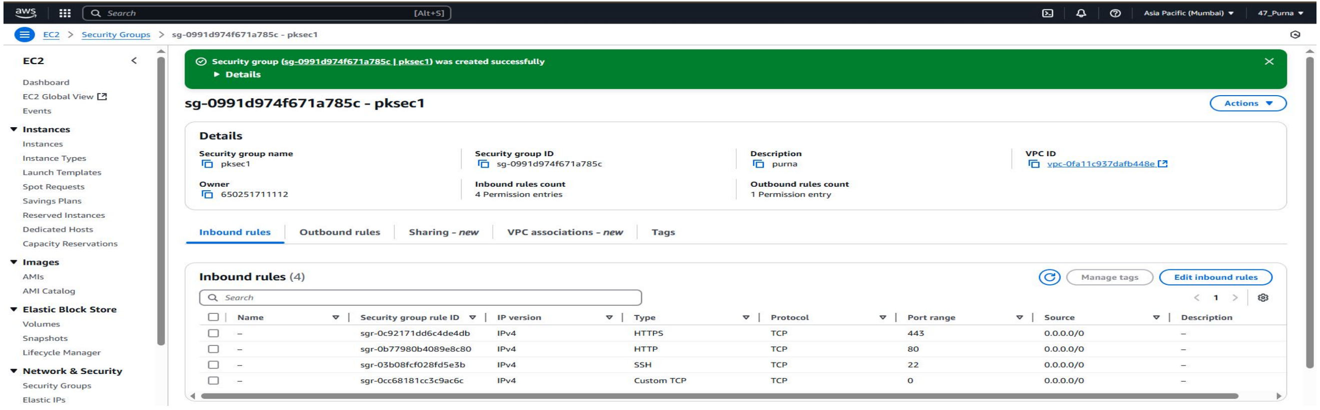
Add rule

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

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.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags

Cancel Create security group

>> And the Security Group is successfully created.



Security group (sg-0991d974f671a785c | pksec1) was created successfully

▸ Details

sg-0991d974f671a785c - pksec1

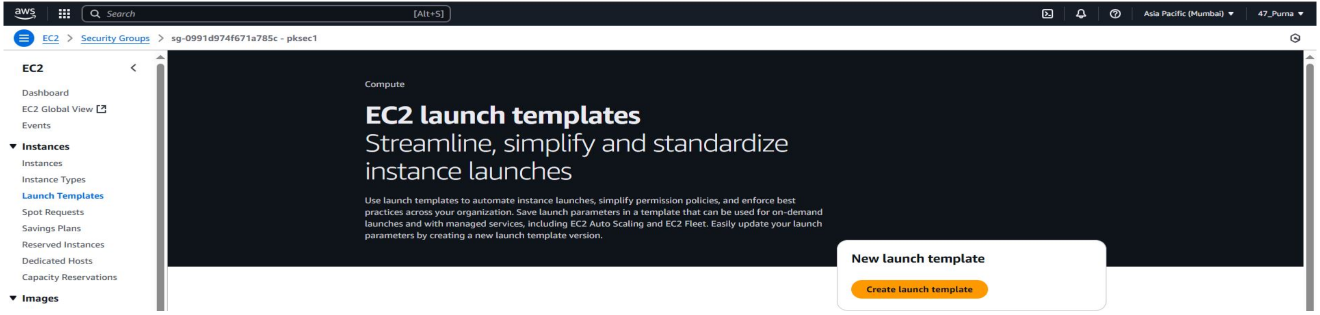
Details

Security group name pksec1	**Security group ID** sg-0991d974f671a785c	**Description** purna	**VPC ID** vpc-0fa11c937dafb448e
Owner 650251711112	**Inbound rules count** 4 Permission entries	**Outbound rules count** 1 Permission entry	

Inbound rules (4)

□	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-0c92171dd6c4de4db	IPv4	HTTPS	TCP	443	0.0.0.0/0	–
□	–	sgr-0b77980b4089e8c80	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-03b08fcf028fd5e3b	IPv4	SSH	TCP	22	0.0.0.0/0	–
□	–	sgr-0cc68181cc3c9ac6c	IPv4	Custom TCP	TCP	0	0.0.0.0/0	–

STEP 3 :- Then go to **Launch Template** and click on **Create Launch Template.**



Compute

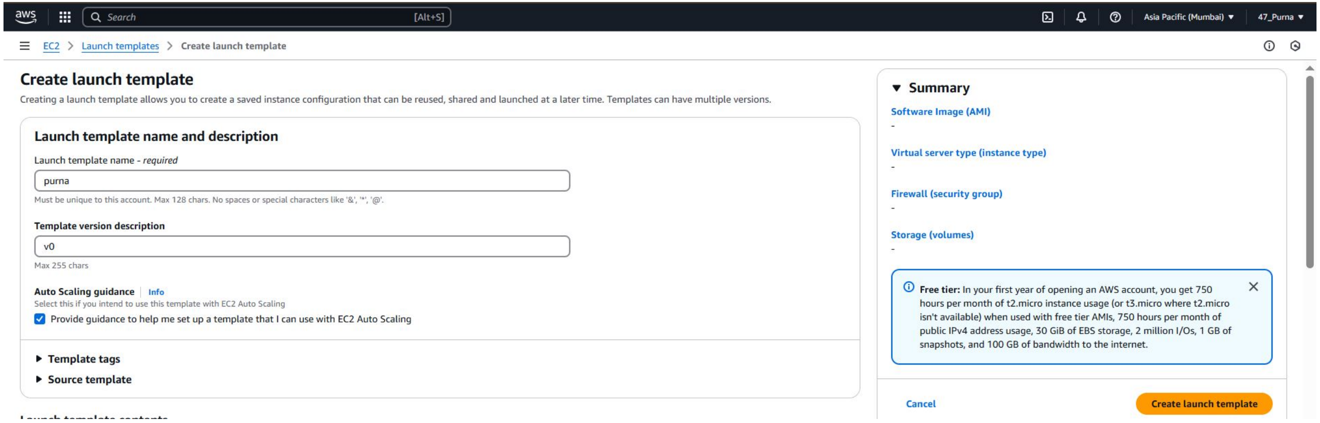
EC2 launch templates

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

STEP 4:- Give your **Template name** and **version description** and **select Auto Scaling guidance**.



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*

purna

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

Template version description

v0

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

▾ **Summary**

Software Image (AMI)
-

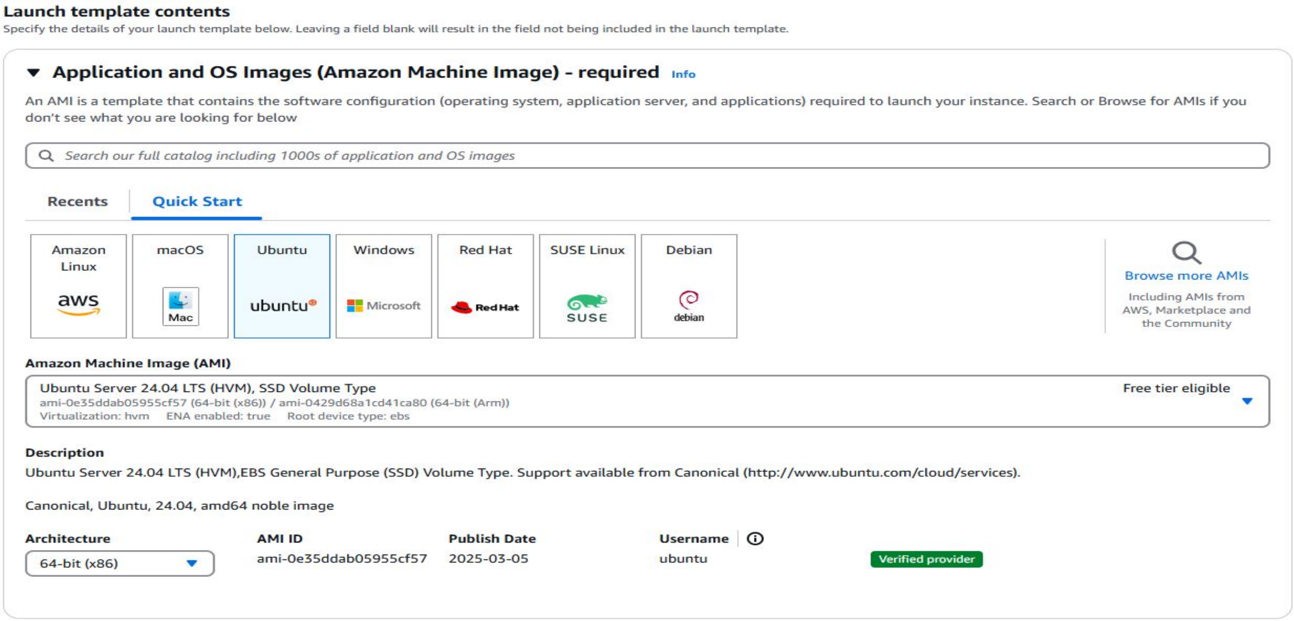
Virtual server type (instance type)
-

Firewall (security group)
-

Storage (volumes)
-

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

>> Select **Ubuntu in Quickstart**



Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▾ **Application and OS Images (Amazon Machine Image) - required** Info

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

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

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0e35ddab05955cf57 (64-bit (x86)) / ami-0429d68a1cd41ca80 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs
Free tier eligible

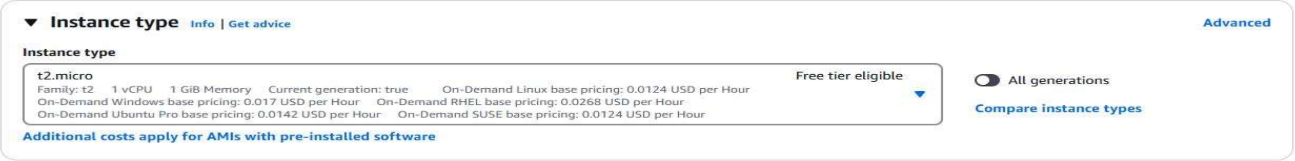
Description

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

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture	AMI ID	Publish Date	Username
64-bit (x86)	ami-0e35ddab05955cf57	2025-03-05	ubuntu

>> Select **t2.micro** as Instance type and create or select a **key pair.**

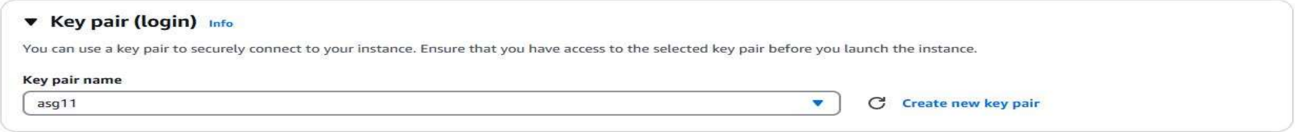


▼ Instance type Info | Get advice
Advanced

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour On-Demand SUSE base pricing: 0.0124 USD per Hour
Free tier eligible

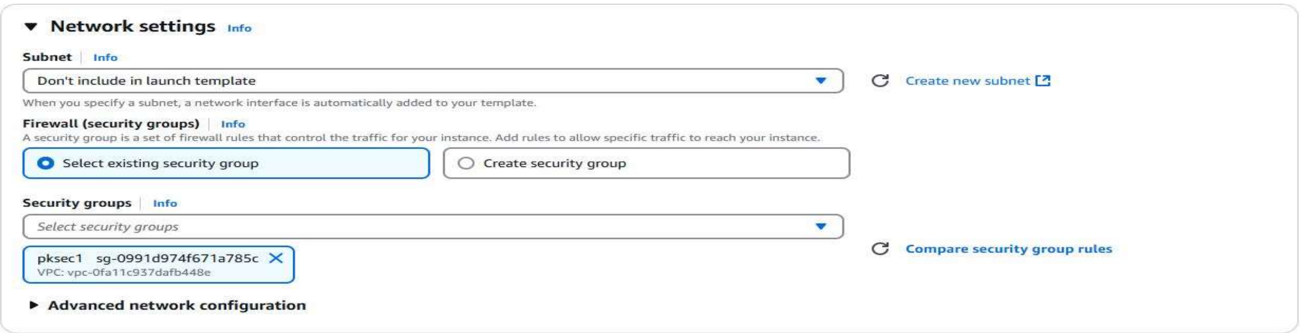
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software



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: asg11

>> Select the **Security group** you created.



Subnet: Don't include in launch template

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

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.

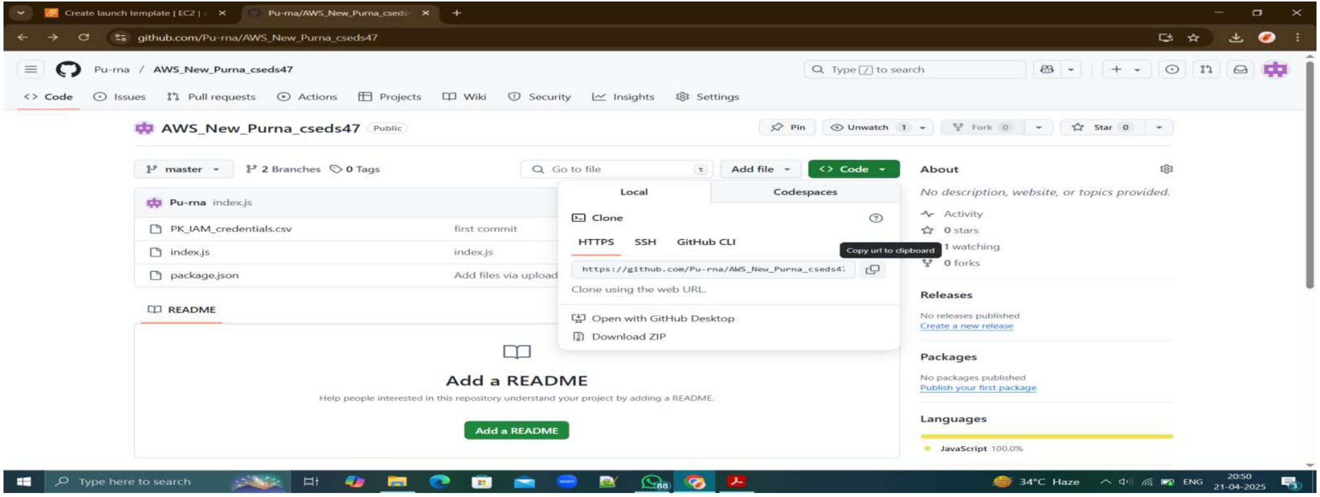
● Select existing security group ○ Create security group

Security groups: Select security groups

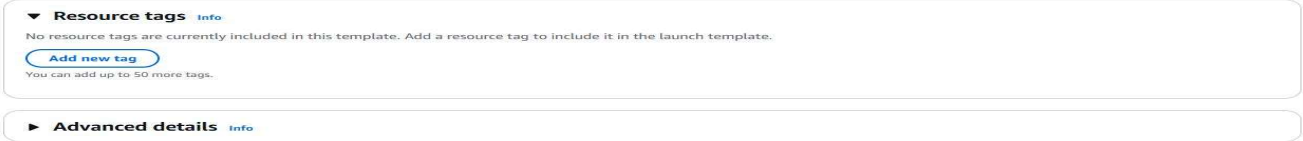
pksec1 sg-0991d974f671a785c ✕
VPC: vpc-0fa11c937dafb448e

Compare security group rules
▶ Advanced network configuration

>> Then go to your Github Repository and copy the address .



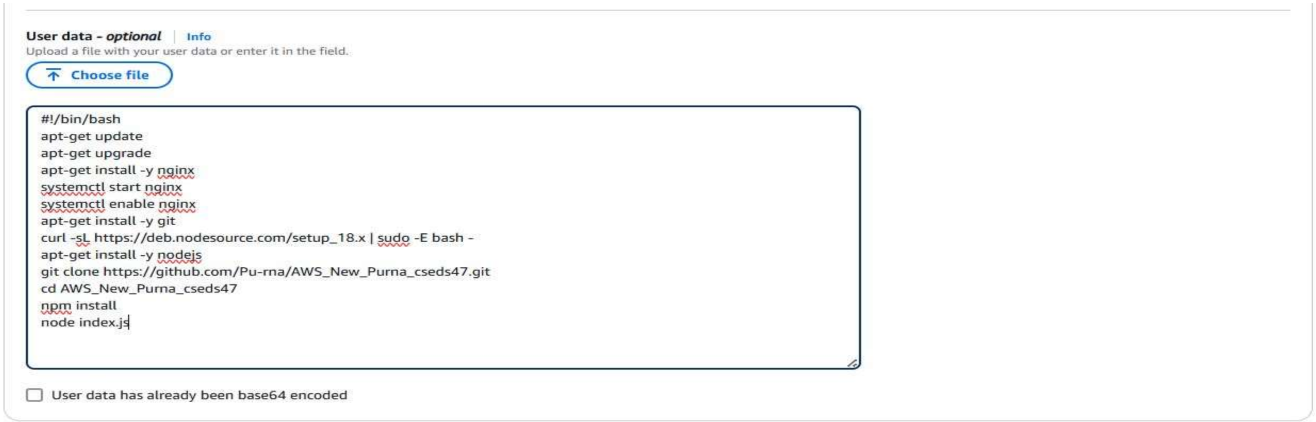
>> then again move to the template creation and click on **Advanced Details.**



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

You can add up to 50 more tags.

>> write the command line as written below and add your Repository link in Git Clone <Repository Link>



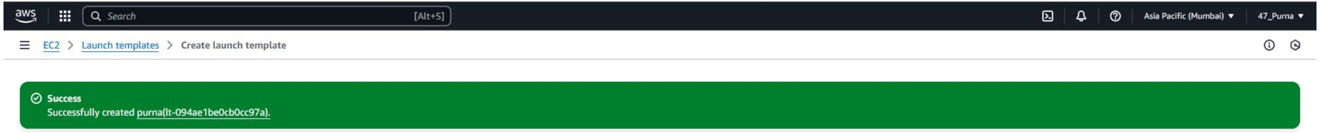
User data - *optional* Info

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

```
#!/bin/bash
apt-get update
apt-get upgrade
apt-get install -y nginx
systemctl start nginx
systemctl enable nginx
apt-get install -y git
curl -sL https://deb.nodesource.com/setup_18.x | sudo -E bash -
apt-get install -y nodejs
git clone https://github.com/Pu-rna/AWS_New_Purna_cseds47.git
cd AWS_New_Purna_cseds47
npm install
node index.js
```

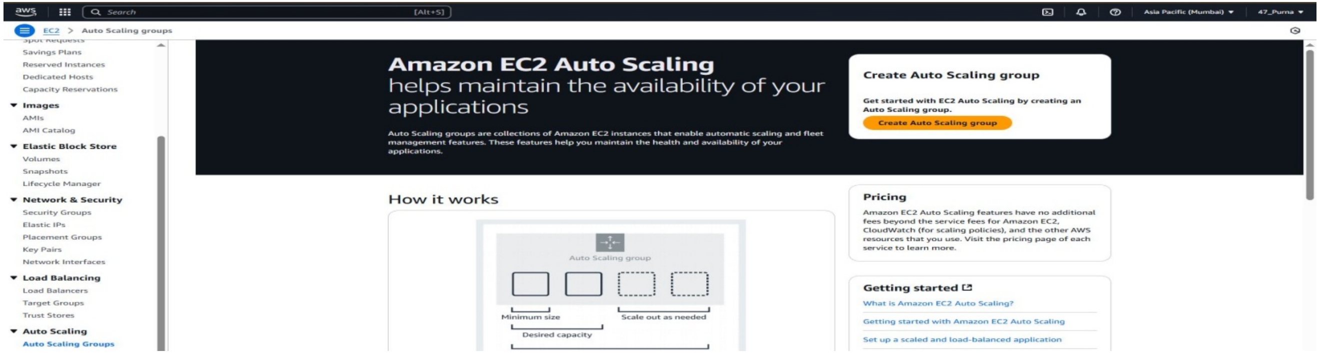
□ User data has already been base64 encoded

>> Your Template is created successfully.



Success
Successfully created purna(lt-094ae1be0cb0cc97a).

STEP 5:- Click on **Auto Scaling Groups** and then click on **Create Auto Scaling groups**.



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.

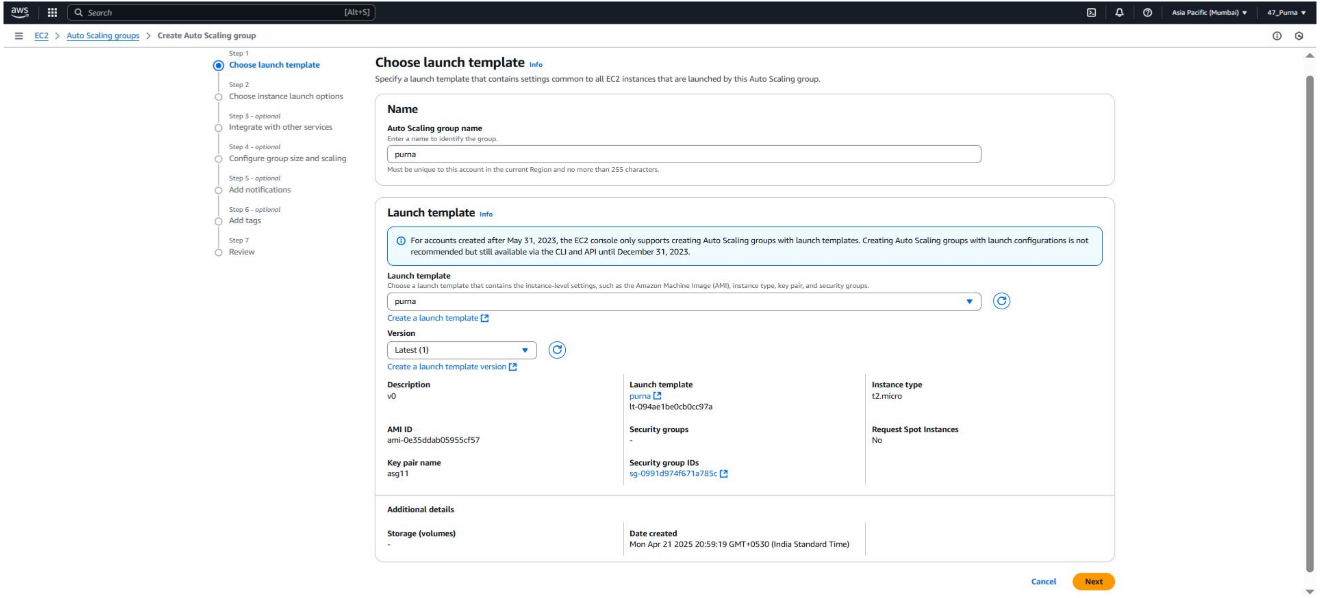
How it works

Pricing

Amazon EC2 Auto Scaling features have no additional fees beyond the service fees for Amazon EC2, CloudWatch (for scaling policies), and the other AWS resources that you use. Visit the pricing page of each service to learn more.

Getting started

>> Give a name and select your desired Template and Give the version as Latest (1) and click on Next.



Choose launch template

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

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

Launch template

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.
purna ▾

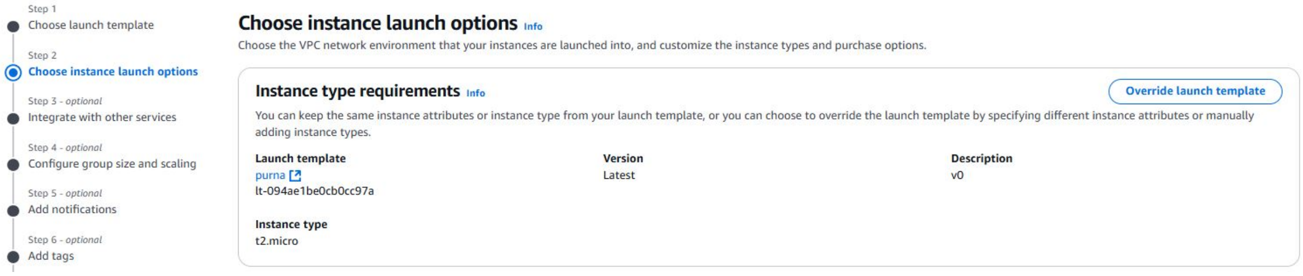
Version
Latest (1) ▾

Description	Launch template	Instance type
v0	purna lt-094ae1be0cb0cc97a	t2.micro
AMI ID	**Security groups**	**Request Spot Instances**
ami-0e35ddab05955cf57	-	No
Key pair name	**Security group IDs**	
asg11	sg-0991d974f671a785c	

Additional details

Storage (volumes)	Date created
-	Mon Apr 21 2025 20:59:19 GMT+0530 (India Standard Time)

>> In step 2 click on Override launch template under Choose instance launch options.



Choose instance launch options

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

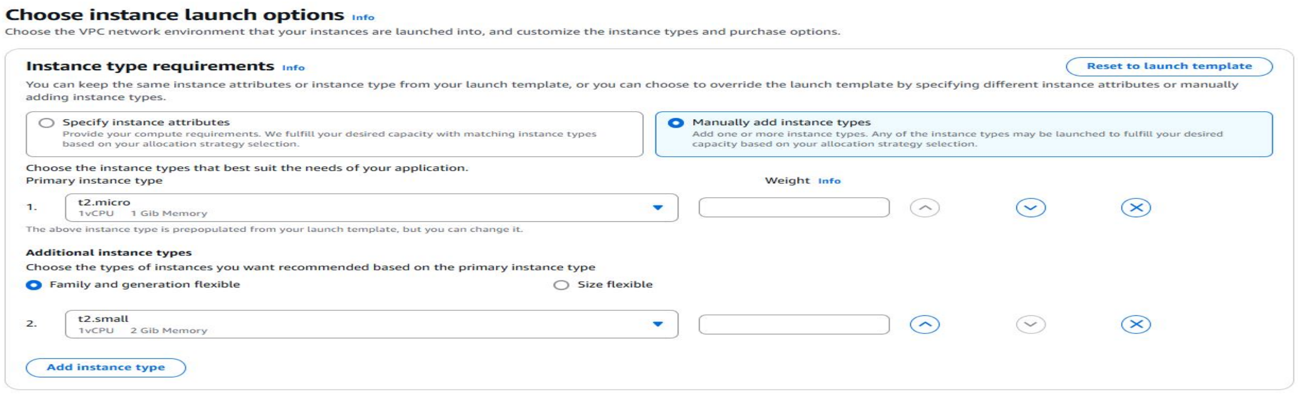
Instance type requirements

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Launch template	Version	Description
purna lt-094ae1be0cb0cc97a	Latest	v0

Instance type
t2.micro

>> Select the Manual add Instance type.



Choose instance launch options

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

Instance type requirements

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

○ Specify instance attributes
Provide your compute requirements. We fulfill your desired capacity with matching instance types based on your allocation strategy selection.

● Manually add instance types
Add one or more instance types. Any of the instance types may be launched to fulfill your desired capacity based on your allocation strategy selection.

Choose the instance types that best suit the needs of your application.

Primary instance type | Weight

1. t2.micro ▾ 1vCPU 1 GiB Memory

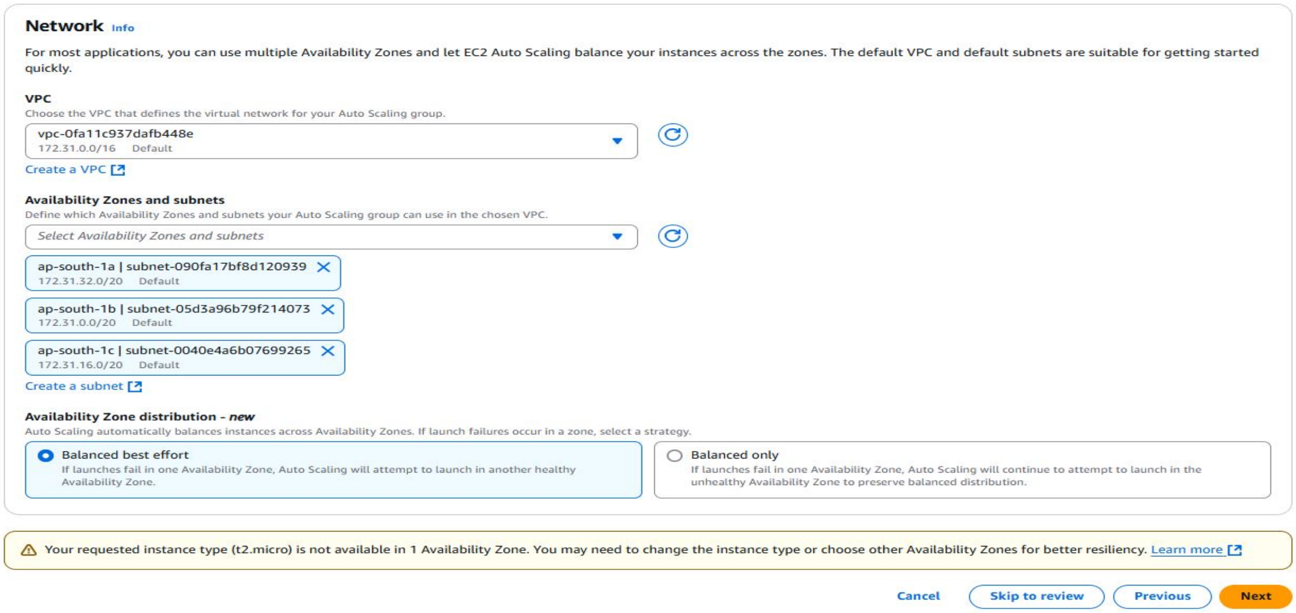
The above instance type is prepopulated from your launch template, but you can change it.

Additional instance types
Choose the types of instances you want recommended based on the primary instance type

● Family and generation flexible ○ Size flexible

2. t2.small ▾ 1vCPU 2 GiB Memory

>>In Network region Select the Three Available Zones as servers and click on next.



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-0fa11c937dafb448e
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

- ap-south-1a | subnet-090fa17bf8d120939 — 172.31.32.0/20 Default
- ap-south-1b | subnet-05d3a96b79f214073 — 172.31.0.0/20 Default
- ap-south-1c | subnet-0040e4a6b07699265 — 172.31.16.0/20 Default

Create a subnet

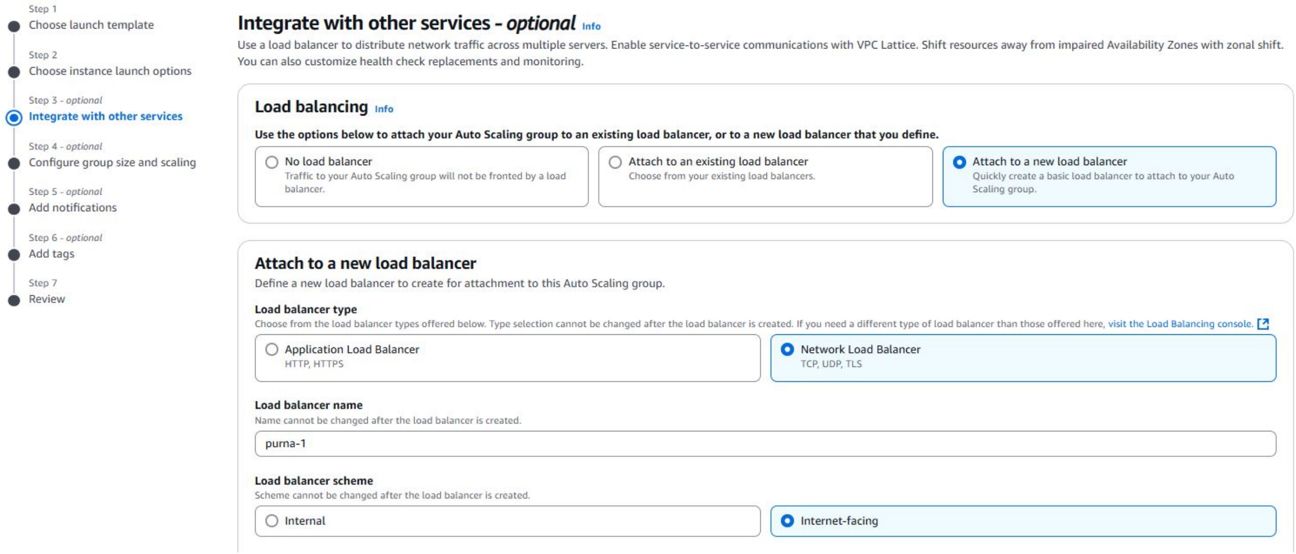
Availability Zone distribution - *new*
Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

● Balanced best effort
If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.

○ Balanced only
If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

⚠ Your requested instance type (t2.micro) is not available in 1 Availability Zone. You may need to change the instance type or choose other Availability Zones for better resiliency. Learn more

>> Select Attach a new load balancer and then select Network load balancer and then select Internet Facing.



Integrate with other services - *optional* Info

Use a load balancer to distribute network traffic across multiple servers. Enable service-to-service communications with VPC Lattice. Shift resources away from impaired Availability Zones with zonal shift. You can also customize health check replacements and monitoring.

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

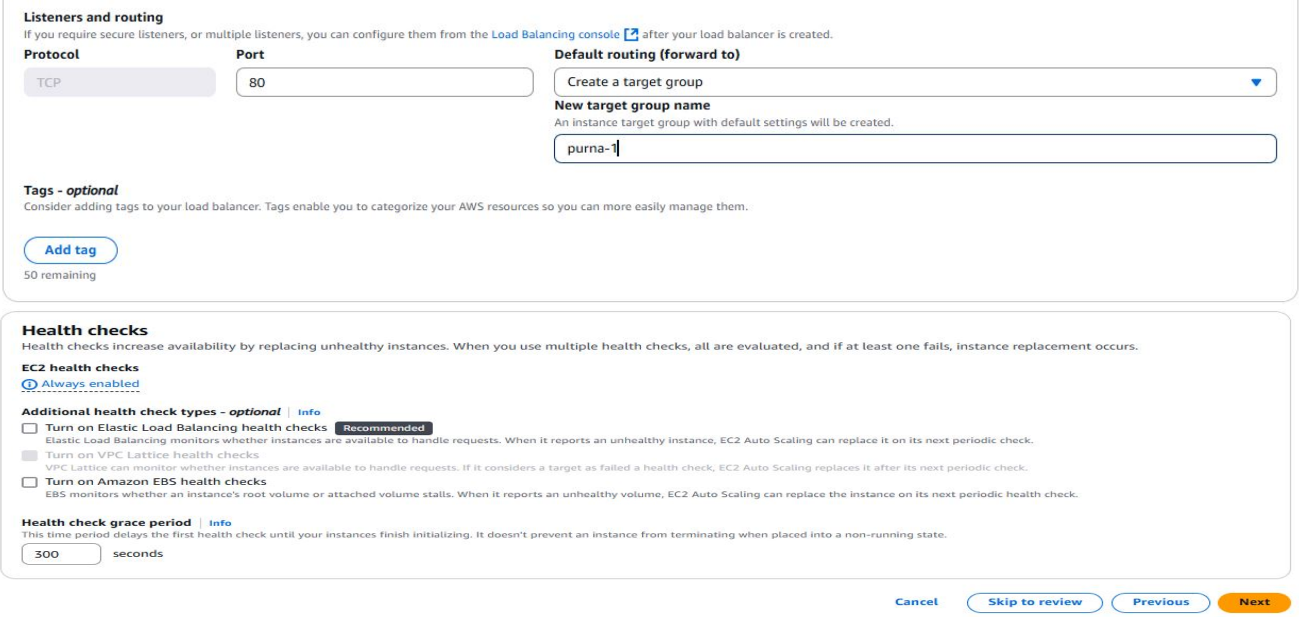
Load balancer name
Name cannot be changed after the load balancer is created.
purna-1

Load balancer scheme
Scheme cannot be changed after the load balancer is created.

○ Internal

● Internet-facing

>> click on Create Target Group and select a target group name and then click on next



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)
TCP	80	Create a target group

New target group name
An instance target group with default settings will be created.
purna-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

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

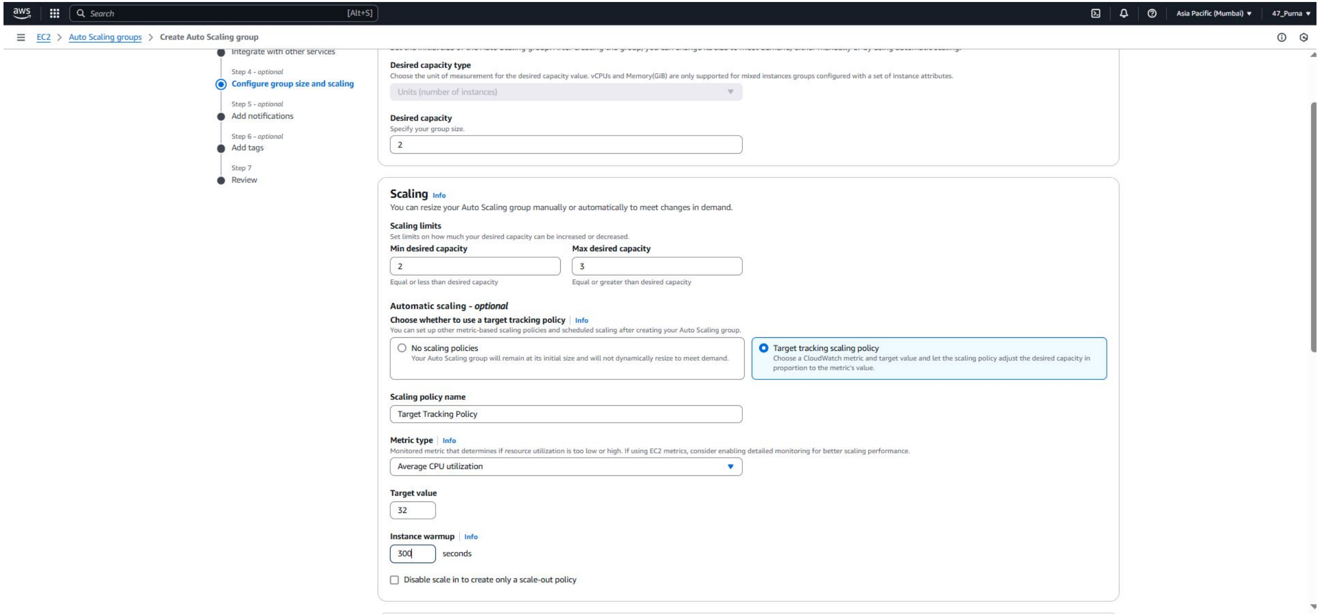
□ Turn on Elastic Load Balancing health checks Recommended
Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.

□ 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.

□ Turn on Amazon EBS health checks
EBS monitors whether an instance's root volume or attached volume stalls. When it reports an unhealthy volume, EC2 Auto Scaling can replace the instance on its next periodic health 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.
300 seconds

>> Now select your Desired capacity , Min desired and max desired capacity and then select Target Tracking Scaling capacity. Give the Target Value and give Instance Warmup and then click on Next.



EC2 > Auto Scaling groups > Create Auto Scaling group

- Integrate with other services
- Step 4 - *optional* — **Configure group size and scaling**
- Step 5 - *optional* — Add notifications
- Step 6 - *optional* — Add tags
- Step 7 — Review

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	Max desired capacity
2	3
Equal or less than desired capacity	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

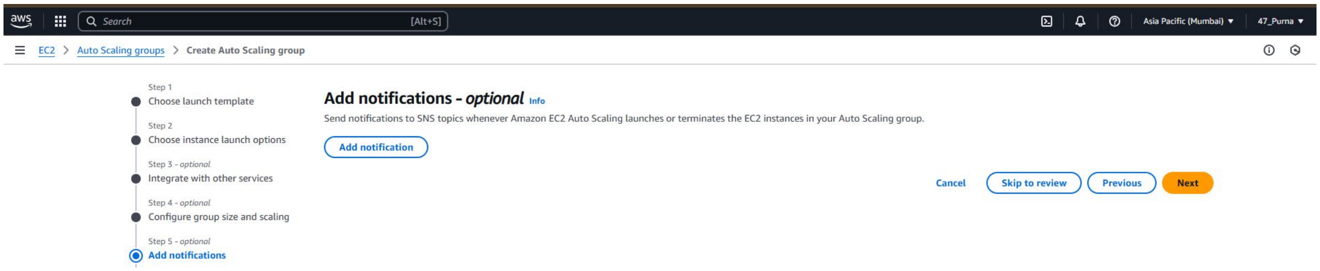
Metric type | Info
Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.
Average CPU utilization

Target value
32

Instance warmup | Info
300 seconds

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

>>click on NEXT

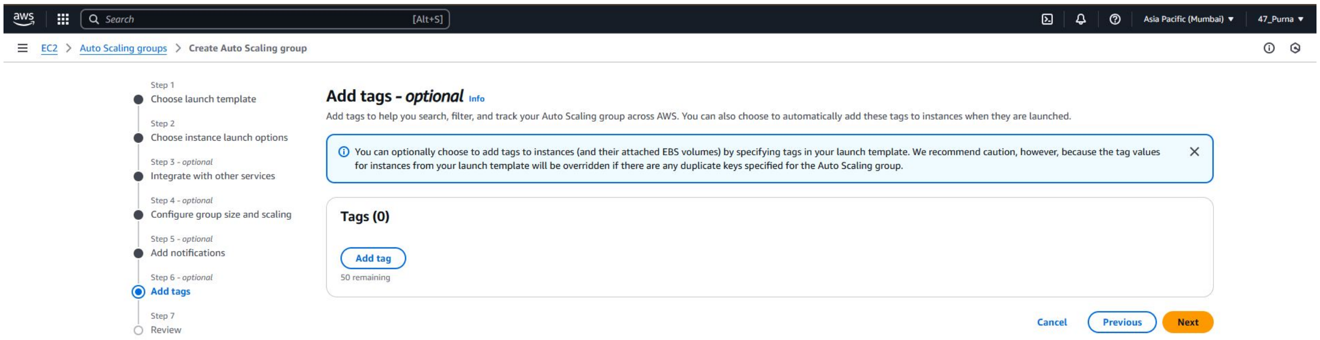


EC2 > Auto Scaling groups > Create Auto Scaling group

- Step 1 — Choose launch template
- Step 2 — Choose instance launch options
- Step 3 - *optional* — Integrate with other services
- Step 4 - *optional* — Configure group size and scaling
- Step 5 - *optional* — **Add notifications**

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

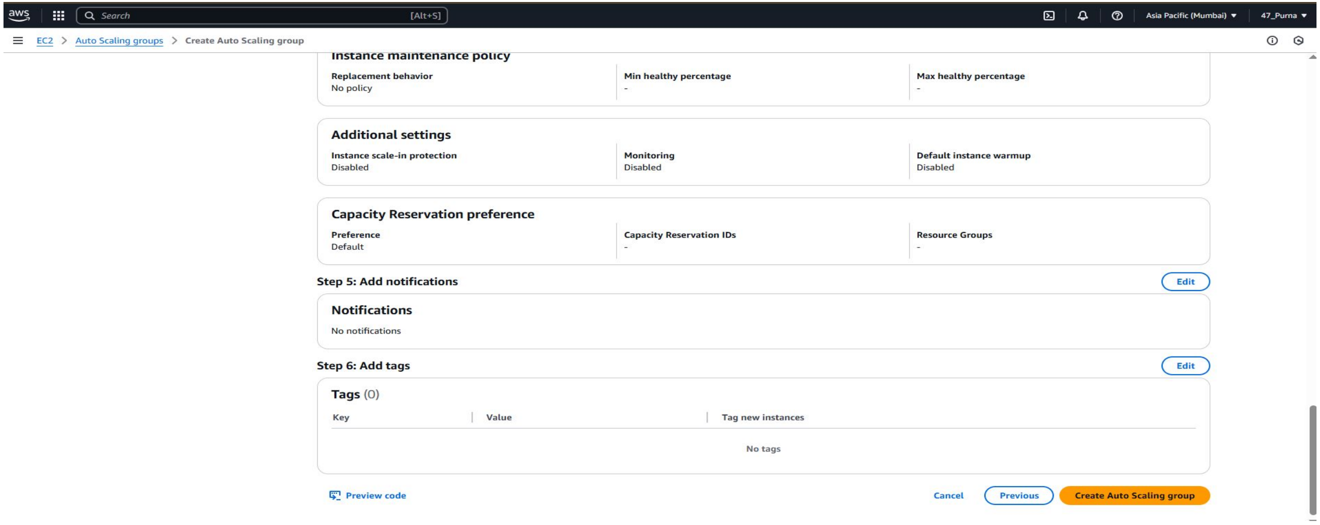
- Step 1 — Choose launch template
- Step 2 — Choose instance launch options
- Step 3 - *optional* — Integrate with other services
- Step 4 - *optional* — Configure group size and scaling
- Step 5 - *optional* — Add notifications
- Step 6 - *optional* — **Add tags**
- Step 7 — Review

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)
Add tag
50 remaining

>>click on Create Auto Scaling Group.



EC2 > Auto Scaling groups > Create Auto Scaling group

Instance maintenance policy

Replacement behavior	Min healthy percentage	Max healthy percentage
No policy	-	-

Additional settings

Instance scale-in protection	Monitoring	Default instance warmup
Disabled	Disabled	Disabled

Capacity Reservation preference

Preference	Capacity Reservation IDs	Resource Groups
Default	-	-

Step 5: Add notifications

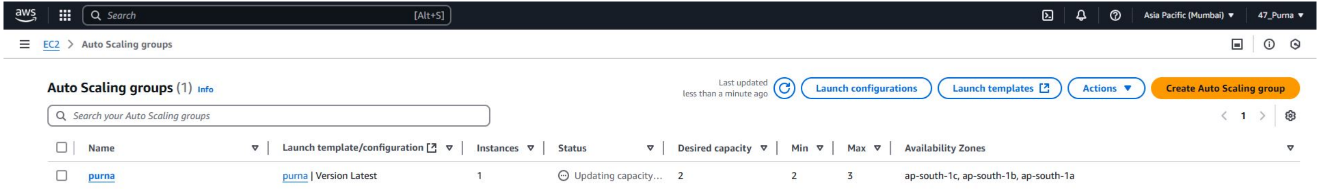
Notifications
No notifications

Step 6: Add tags

Tags (0)

Key	Value	Tag new instances
No tags		

>> And your Auto Scaling Group is Created Successfully.

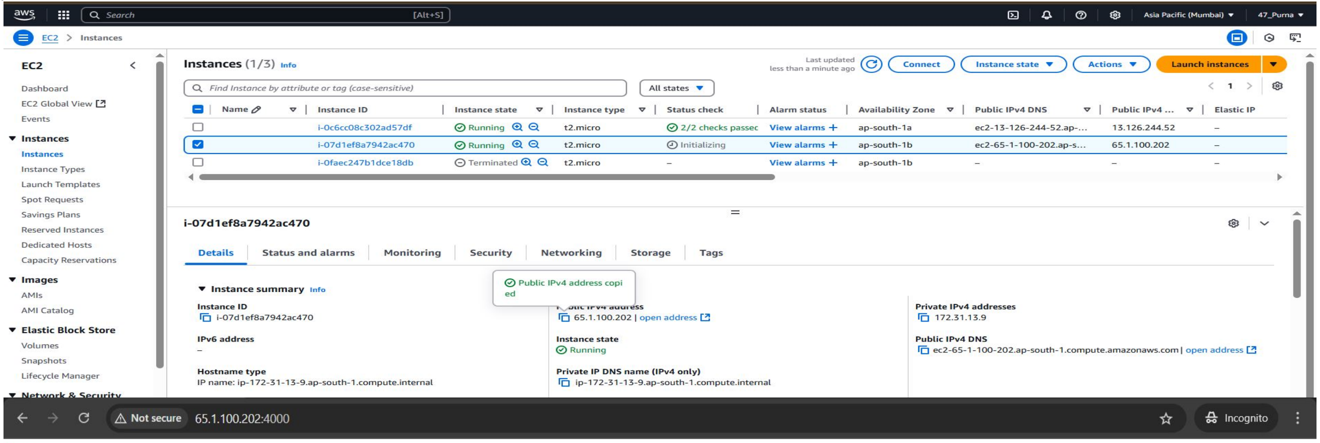

EC2 > Auto Scaling groups
Launch configurations
Launch templates
Actions
Create Auto Scaling group
Search your Auto Scaling groups

Auto Scaling groups (1) Info

Last updated less than a minute ago

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
purna	purna | Version Latest	1	Updating capacity...	2	2	3	ap-south-1c, ap-south-1b, ap-south-1a

STEP 5:- As you can see the Instances are automatically created if you will delete one instance then the 3rd one will automatically generated as 3 servers are given. Now any one Instance and Copy its IPV4 address and paste it in Incognito website with port number(IP Address : 4000).



Instances (1/3) Info

Last updated less than a minute ago

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
	i-0c6cc08c302ad57df	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1a	ec2-13-126-244-52.ap-...	13.126.244.52	–
	i-07d1ef8a7942ac470	Running	t2.micro	Initializing	View alarms +	ap-south-1b	ec2-65-1-100-202.ap-s...	65.1.100.202	–
	i-0faec247b1dce18db	Terminated	t2.micro	–	View alarms +	ap-south-1b	–	–	–

i-07d1ef8a7942ac470

Instance summary Info

Public IPv4 address copied

Instance ID: i-07d1ef8a7942ac470

Public IPv4 address: 65.1.100.202 | open address

Private IPv4 addresses: 172.31.13.9

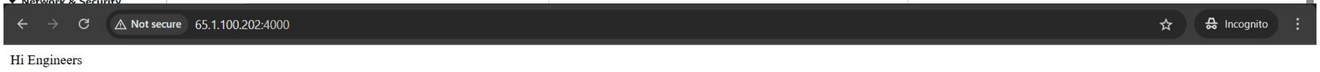
IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-65-1-100-202.ap-south-1.compute.amazonaws.com | open address

Hostname type: IP name: ip-172-31-13-9.ap-south-1.compute.internal

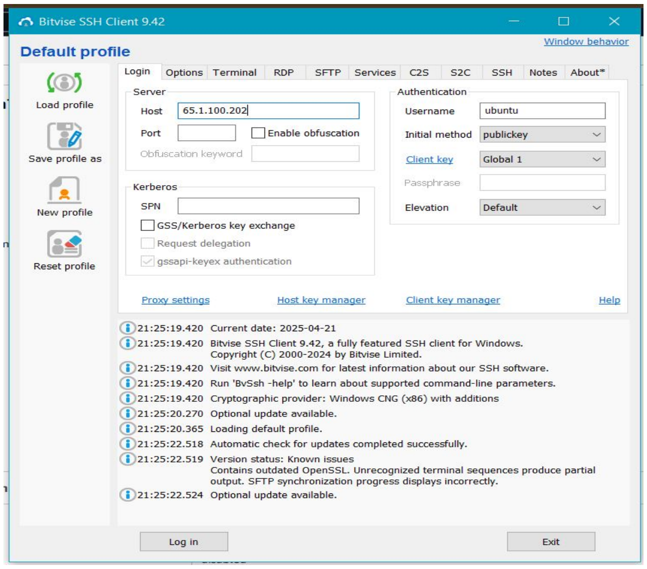
Private IP DNS name (IPv4 only): ip-172-31-13-9.ap-south-1.compute.internal



65.1.100.202:4000

Hi Engineers

STEP 7:- Paste the address in Bitvise Server and give the required field of username ,Initial method and Client key then click on LOG IN and go to the New Terminal.



Server

Host: 65.1.100.202

Port:

□ Enable obfuscation

Obfuscation keyword

Kerberos

SPN

□ GSS/Kerberos key exchange

□ Request delegation

☑ gssapi-keyex authentication

Authentication

Username: ubuntu

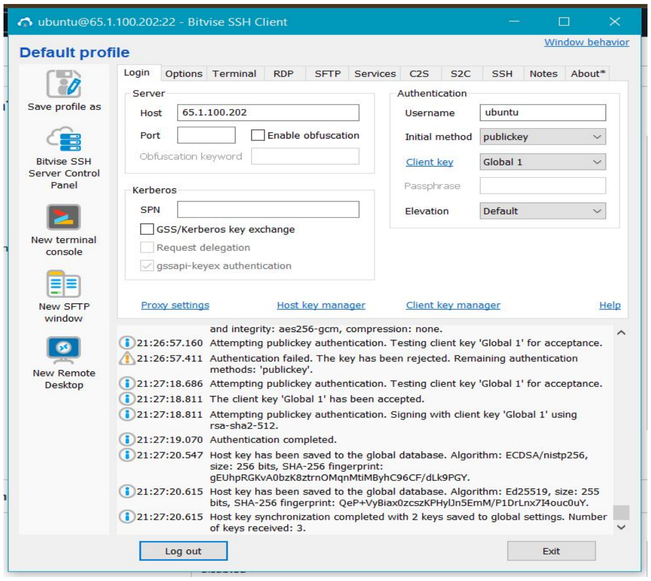
Initial method: publickey

Client key: Global 1

Passphrase

Elevation: Default

```
21:25:19.420 Current date: 2025-04-21
21:25:19.420 Bitvise SSH Client 9.42, a fully featured SSH client for Windows.
             Copyright (C) 2000-2024 by Bitvise Limited.
21:25:19.420 Visit www.bitvise.com for latest information about our SSH software.
21:25:19.420 Run 'BvSsh -help' to learn about supported command-line parameters.
21:25:19.420 Cryptographic provider: Windows CNG (x86) with additions
21:25:20.270 Optional update available.
21:25:20.365 Loading default profile.
21:25:22.518 Automatic check for updates completed successfully.
21:25:22.519 Version status: Known issues
             Contains outdated OpenSSL. Unrecognized terminal sequences produce partial
             output. SFTP synchronization progress displays incorrectly.
21:25:22.524 Optional update available.
```



Server

Host: 65.1.100.202

Port:

□ Enable obfuscation

Obfuscation keyword

Kerberos

SPN

□ GSS/Kerberos key exchange

□ Request delegation

☑ gssapi-keyex authentication

Authentication

Username: ubuntu

Initial method: publickey

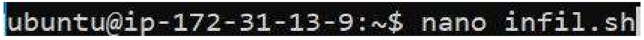
Client key: Global 1

Passphrase

Elevation: Default

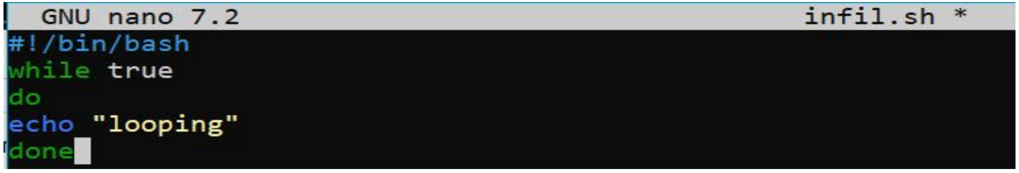
```
             and integrity: aes256-gcm, compression: none.
21:26:57.160 Attempting publickey authentication. Testing client key 'Global 1' for acceptance.
21:26:57.411 Authentication failed. The key has been rejected. Remaining authentication
             methods: 'publickey'.
21:27:18.686 Attempting publickey authentication. Testing client key 'Global 1' for acceptance.
21:27:18.811 The client key 'Global 1' has been accepted.
21:27:18.811 Attempting publickey authentication. Signing with client key 'Global 1' using
             rsa-sha2-512.
21:27:19.070 Authentication completed.
21:27:20.547 Host key has been saved to the global database. Algorithm: ECDSA/nistp256,
             size: 256 bits, SHA-256 fingerprint:
             gEUhpRGKvA0bzK8ztrnOMqnMtiMByhC96CF/dLk9PGY.
21:27:20.615 Host key has been saved to the global database. Algorithm: Ed25519, size: 255
             bits, SHA-256 fingerprint: QeP+VyBiax0zcszKPHylJn5EmM/P1DrLnx7I4ouc0uY.
21:27:20.615 Host key synchronization completed with 2 keys saved to global settings. Number
             of keys received: 3.
```

>> Then write the following command in terminal to open a shell file.



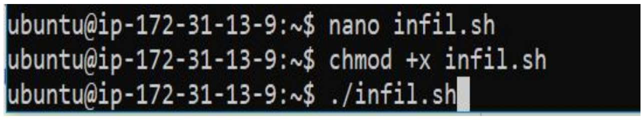
```
ubuntu@ip-172-31-13-9:~$ nano infil.sh
```

>> Then write the following code in the shell file.

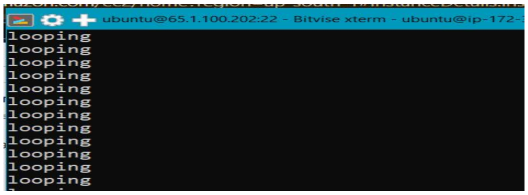


```
 GNU nano 7.2                                 infil.sh *
#!/bin/bash
while true
do
echo "looping"
done
```

>> Compile and run the File Using the following command.

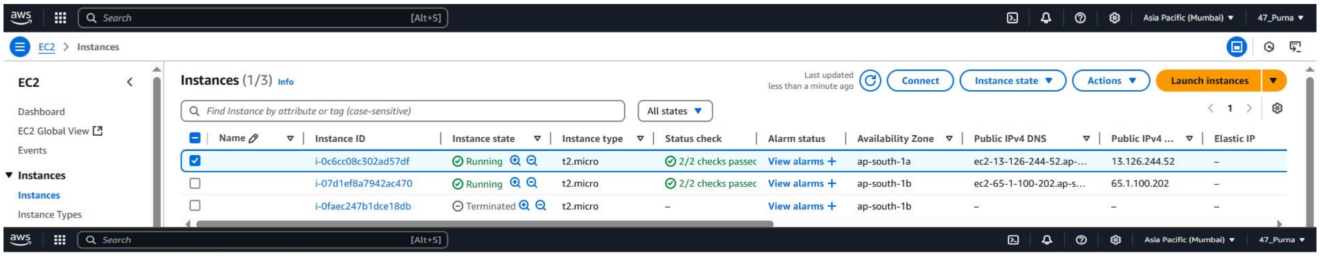


```
ubuntu@ip-172-31-13-9:~$ nano infil.sh
ubuntu@ip-172-31-13-9:~$ chmod +x infil.sh
ubuntu@ip-172-31-13-9:~$ ./infil.sh
```



```
looping
looping
looping
looping
looping
looping
looping
looping
looping
looping
looping
looping
```

STEP 6:- Select other Instance and click on Connect.



EC2 > Instances

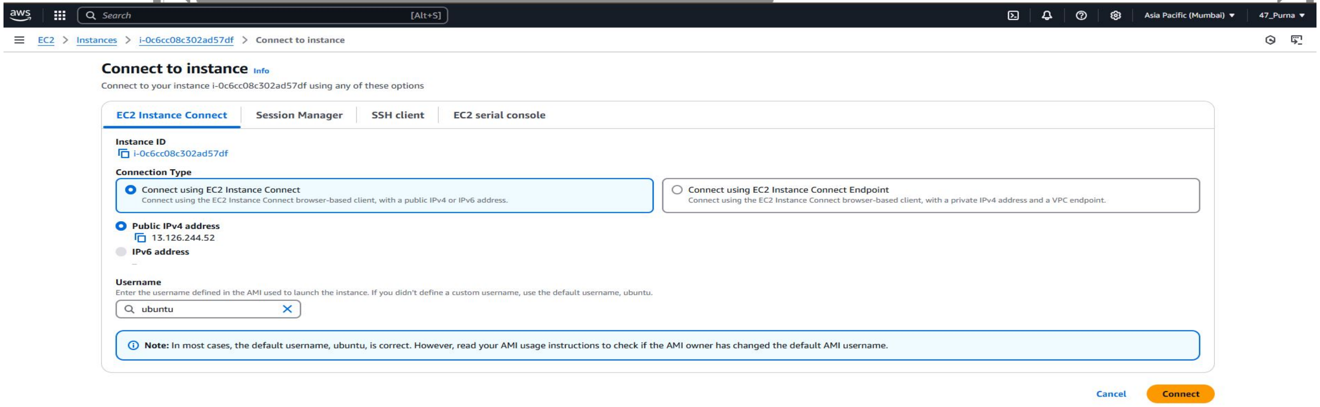
Instances (1/3) Info

Last updated less than a minute ago

Connect | Instance state ▼ | Actions ▼ | Launch instances ▼

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

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☑		i-0c6cc08c302ad57df	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1a	ec2-13-126-244-52.ap-...	13.126.244.52	–
□		i-07d1ef8a7942ac470	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1b	ec2-65-1-100-202.ap-s...	65.1.100.202	–
□		i-0faec247b1dce18db	Terminated	t2.micro	–	View alarms +	ap-south-1b	–	–	–



EC2 > Instances > i-0c6cc08c302ad57df > Connect to instance

Connect to instance Info

Connect to your instance i-0c6cc08c302ad57df using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID
i-0c6cc08c302ad57df

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.

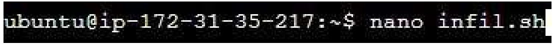
● Public IPv4 address
13.126.244.52
○ IPv6 address

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, ubuntu.
ubuntu

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

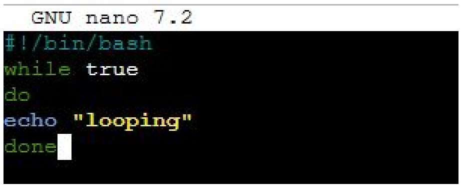
Cancel | Connect

>> Then write the following command in terminal to open a shell file.



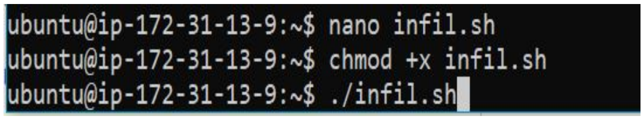
```
ubuntu@ip-172-31-35-217:~$ nano infil.sh
```

>> Then write the following code in the shell file.

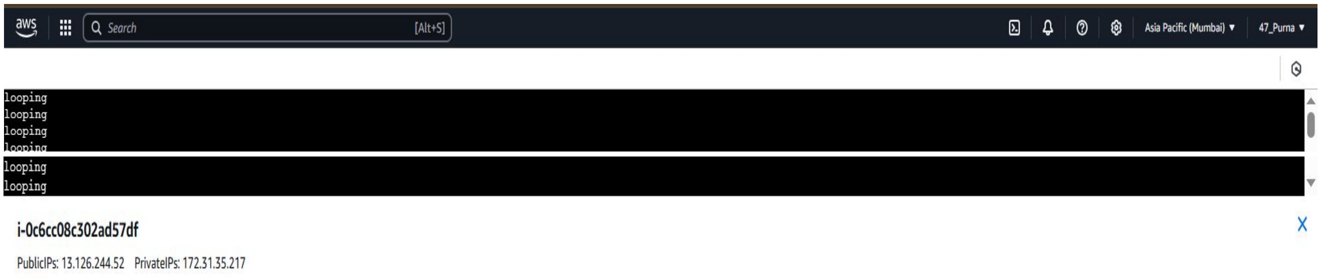


```
  GNU nano 7.2
#!/bin/bash
while true
do
echo "looping"
done
```

>> Compile and run the File Using the following command.



```
ubuntu@ip-172-31-13-9:~$ nano infil.sh
ubuntu@ip-172-31-13-9:~$ chmod +x infil.sh
ubuntu@ip-172-31-13-9:~$ ./infil.sh
```

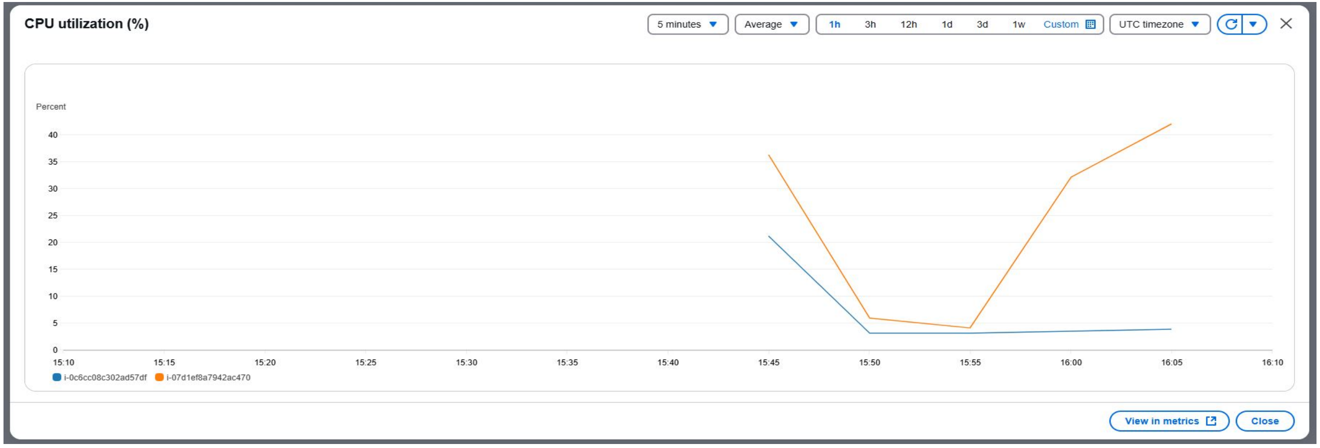


```
looping
looping
looping
looping
looping
looping
```

i-0c6cc08c302ad57df

PublicIPs: 13.126.244.52 PrivateIPs: 172.31.35.217

>> Then click on both the instances and you can see the graph of both processes CPU UTILISATION.



CPU utilization (%)
5 minutes ▼
Average ▼
1h
3h
12h
1d
3d
1w
Custom
UTC timezone ▼
Percent
15:10
15:15
15:20
15:25
15:30
15:35
15:40
15:45
15:50
15:55
16:00
16:05
16:10
i-0c6cc08c302ad57df
i-07d1ef8a7942ac470
View in metrics
Close