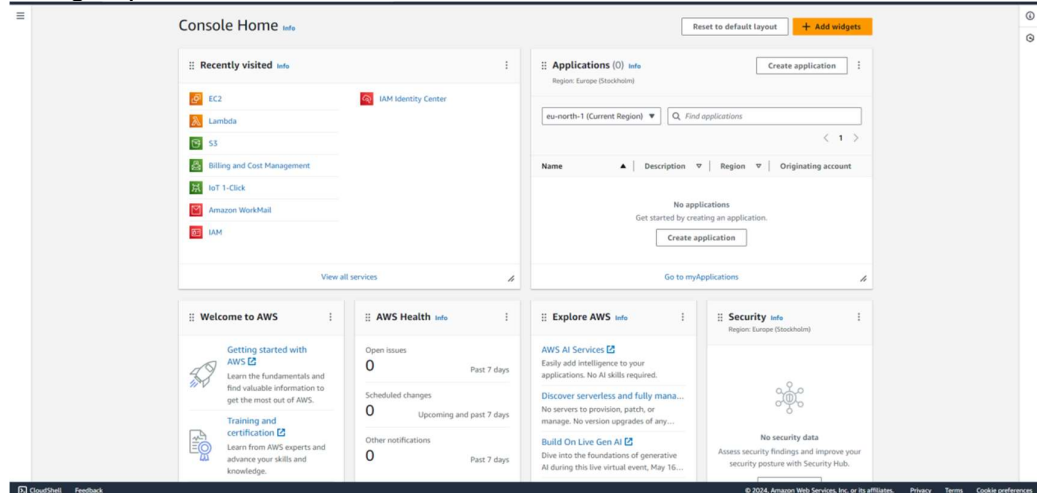


PROBLEM STATEMENT :

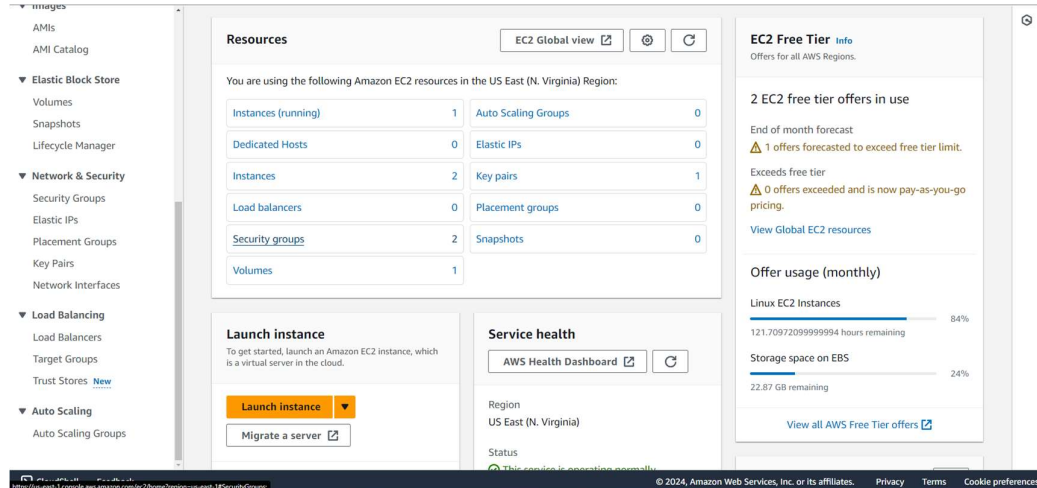
11) Build scaling plans in AWS that balance the load on different EC2 instances.

Steps to build scaling plans :

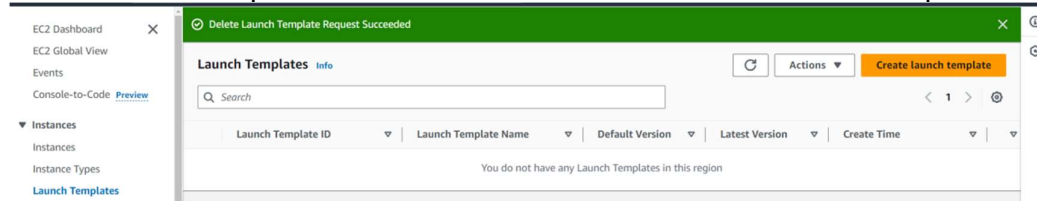
1. Sign up for an AWS account, search for 'EC2' then click on it.



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".

5. Under "Create launch template", give the following details.

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

Linux

aws Mac ubuntu Microsoft Red Hat SUSI

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-04b70fa74e45c3917 (64-bit (x86)) / ami-0eac975a54dfee8cb (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

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

Architecture
64-bit (x86)

AMI ID
ami-04b70fa74e45c3917

Verified provider

▼ 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

Cancel Create launch template

▼ Instance type Info | Get advice Advanced

Instance type
t2.micro
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

Free tier eligible

All generations

Compare instance types

select the key pair & the existing security group.

Before you launch the instance.

Key pair name
arijit111

Create new key pair

▼ Network settings Info

Subnet Info
Don't include in launch template
When you specify a subnet, a network interface is automatically added to your template.

Create new subnet

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

Select existing security group

Create security group

Security groups Info
Select security groups

arisec1 sg-07f884cd38f16ef90
VPC: vpc-09a4d91ecdeb1748

Compare security group rules

► 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)
arisec1

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”

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
sudo apt-get update
sudo apt-get install -y nginx
systemctl start nginx
systemctl enable nginx
sudo apt-get install -y git
curl -SL https://deb.nodesource.com/setup_16.x | sudo -E bash -
sudo apt-get install -y nodejs
git clone https://github.com/arijit-giorno/repo3.git
cd repo3
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

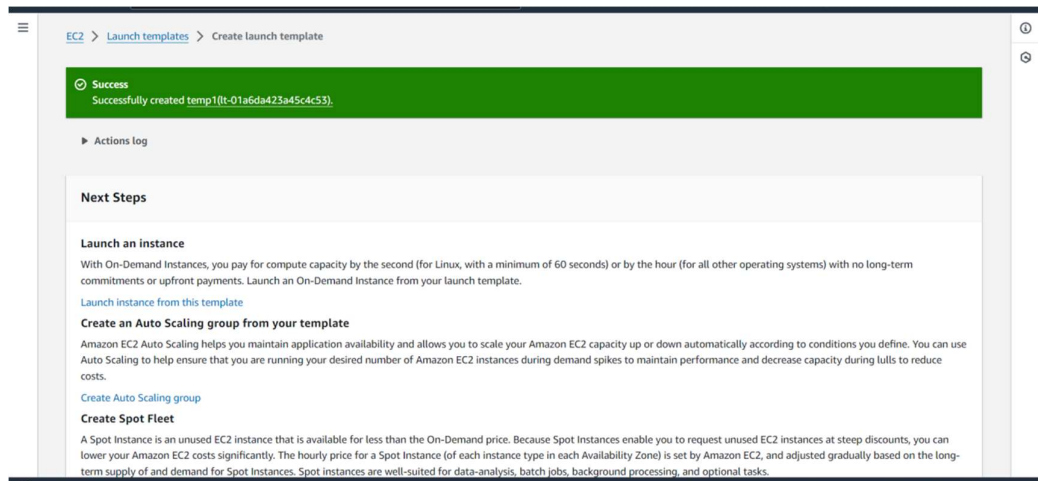
Virtual server type (instance type)
t2.micro

Firewall (security group)
arisec1

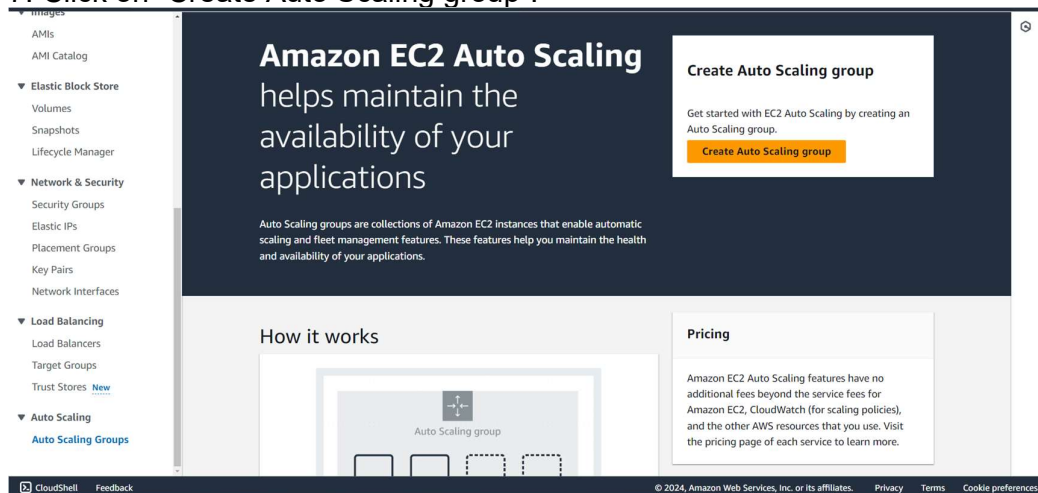
Storage (volumes)
1 volume(s) - 8 GiB

Cancel Create launch template

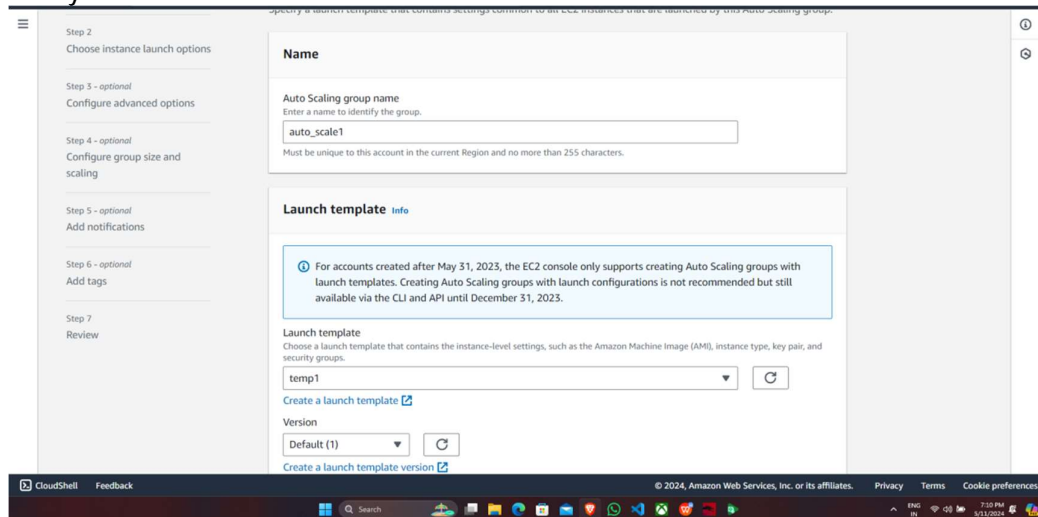
6. Template has successfully created & now click on “Auto Scaling Groups”.



7. Click on “Create Auto Scaling group”.



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



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

Step 7

Review

For most applications, you can use multiple Availability Zones and let EL2 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-09a4d91ecdeb1748

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-010a308380597c99d

172.31.0.0/20

Default

us-east-1b | subnet-003a41e659d765a8d

172.31.80.0/20

Default

us-east-1c | subnet-008c3f1e363d537f9

172.31.16.0/20

Default

us-east-1d | subnet-04cc6d7da722e2de2

172.31.32.0/20

Default

us-east-1e | subnet-07f512007ec0122fd

172.31.48.0/20

Default

us-east-1f | subnet-03b28ecf45d0993fb

172.31.64.0/20

Default

Create a subnet

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

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

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

Click on “No VPC Lattice service”.In “Health checks”, click on the checkbox

us-east-1f

subnet-03b28ecf45d0993fb

us-east-1d

subnet-04cc6d7da722e2de2

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	auto1-1 HTTP

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.

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.

250

seconds

Additional settings

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

“Turn on Elastic load ...” Then click on “Next”.

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

Info

Choose whether to use a target tracking policy

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

50

CloudShell

Feedback

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

Privacy

Terms

Cookie preferences

Click on “No policy” then on “Next”. Click on “Next”.

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

CloudShell

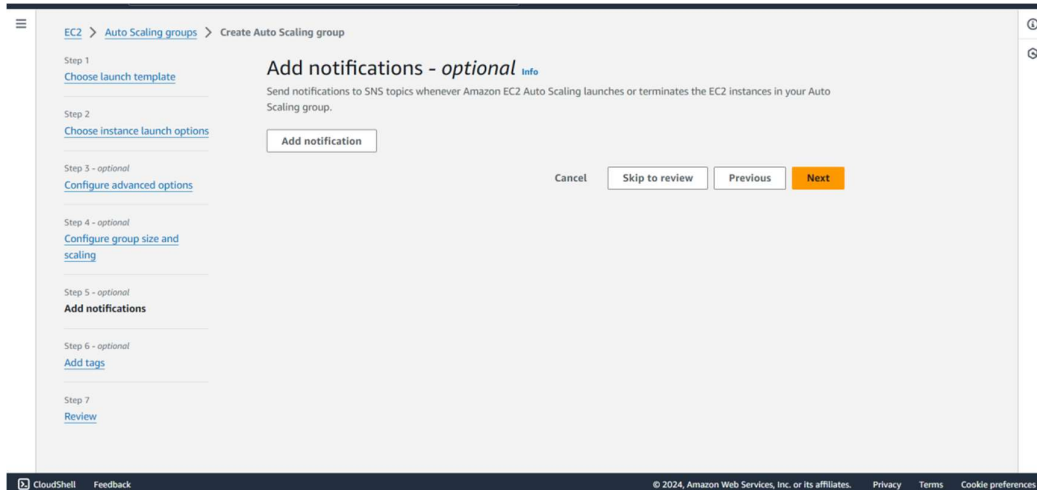
Feedback

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

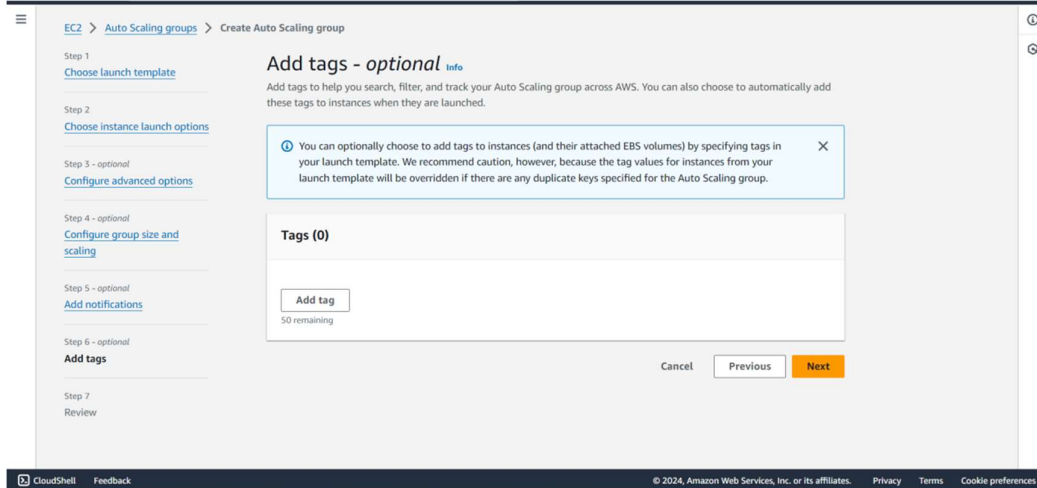
Privacy

Terms

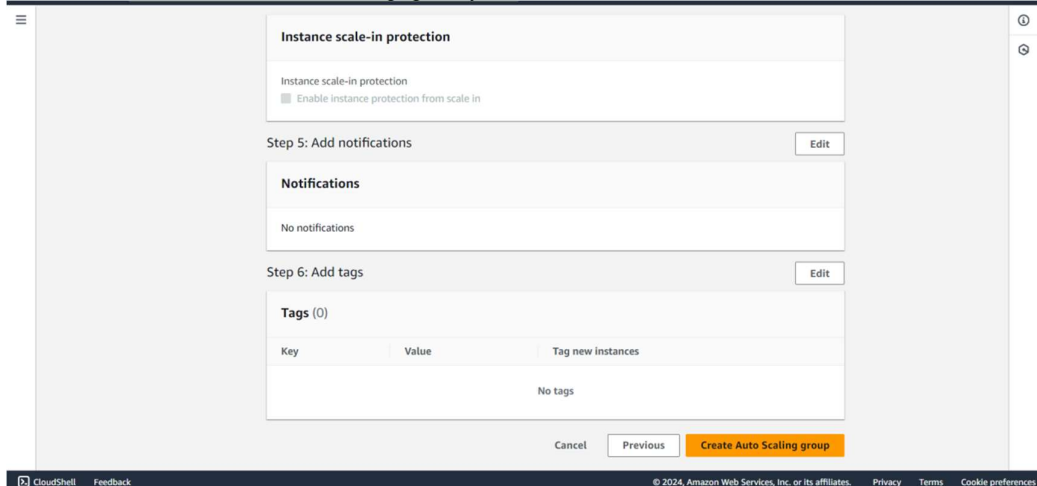
Cookie preferences



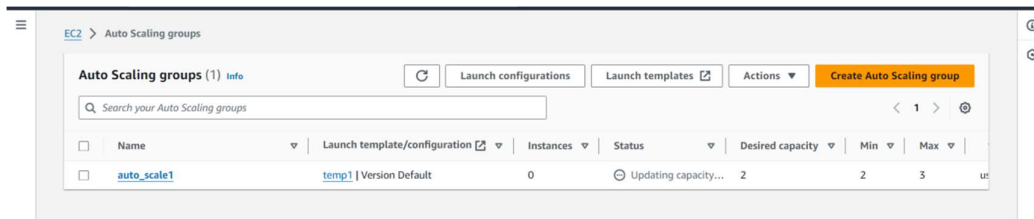
Click on “Next”.



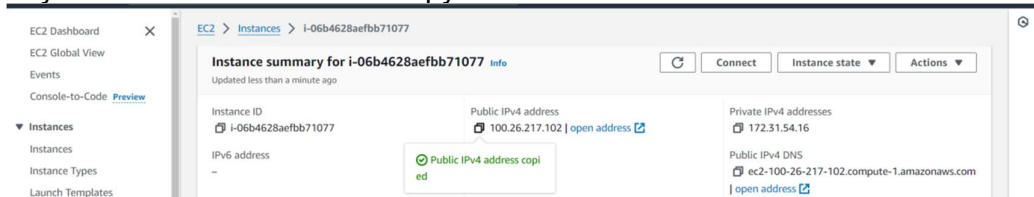
Click on “Create Auto Scaling group”.



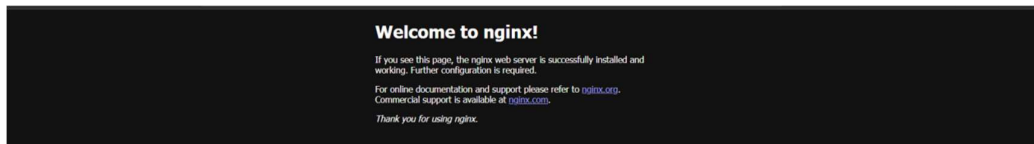
9. Auto scaling group is successfully created.



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



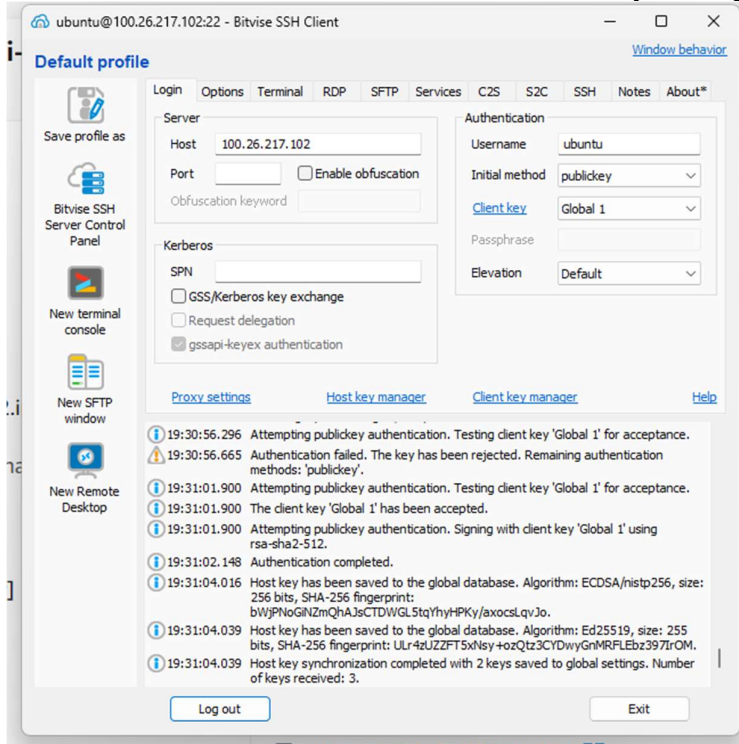
11. Paste the address in a new Window.



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



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



14. Then import the key & click on “Log in”.

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

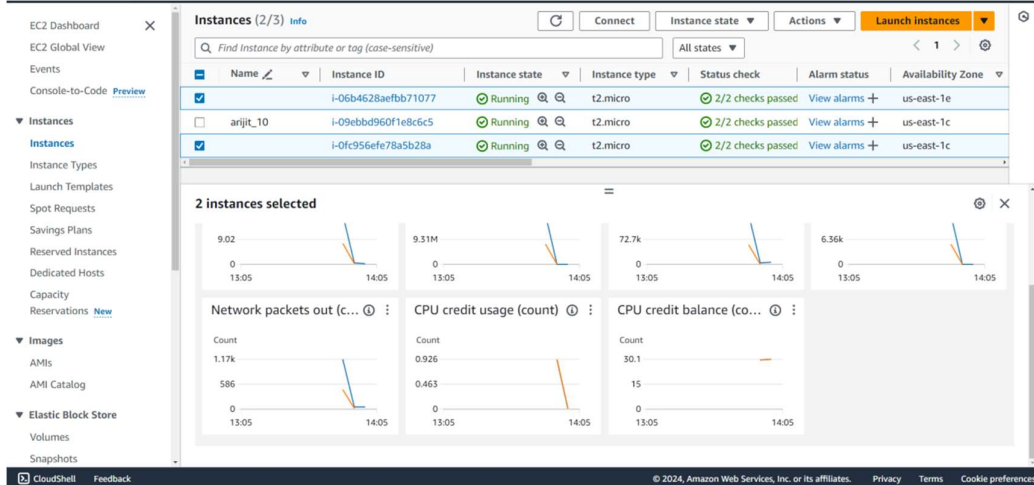
16. Now in “New terminal console and type the following commands.


```
See "man sudo_root" for details.

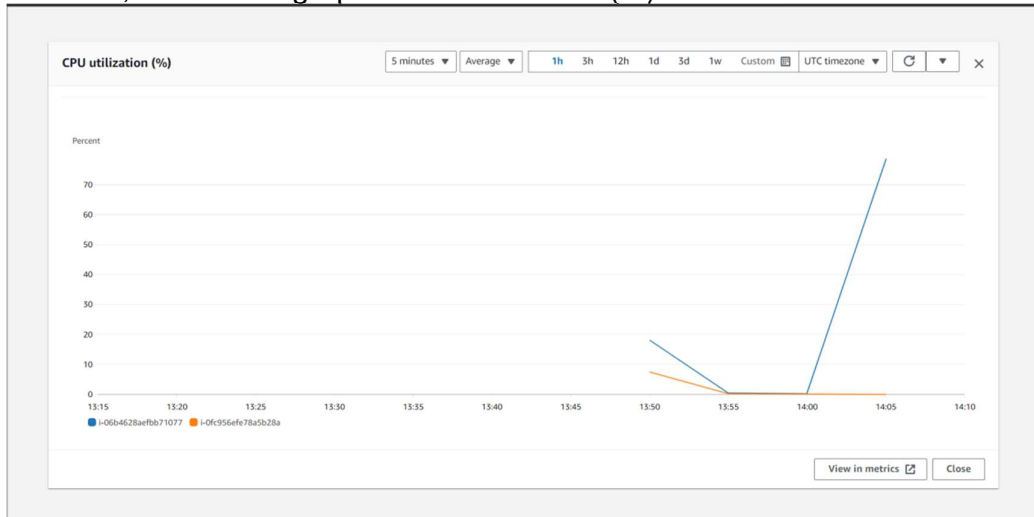
ubuntu@ip-172-31-54-16:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-54-16:~$ sudo nano infy.sh

GNU nano 7.2 infy.s
while(true)
do
    echo"inf loop"
done
```

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



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.

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity

Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Instances (2/3)

Find Instance by attribute or tag (case-sensitive)

All states

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/>		i-06b4628aefbb71077	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1e	ec2-100-
<input type="checkbox"/>	arijit_10	i-09ebbd960f1e8c6c5	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c	ec2-23-2
<input checked="" type="checkbox"/>		i-0fc956efe78a5b28a	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1c	ec2-3-85

2 instances selected

Monitoring

Alarm recommendations

1h 3h 12h 1d 3d 1w Custom UTC timezone

CPU utilization (%)

Percent

18 9.02 0 13:05 14:05

Network in (bytes)

Bytes

18.6M 9.31M 0 13:05 14:05

Network out (bytes)

Bytes

145k 72.7k 0 13:05 14:05

Network packets in (count)

Count

12.7k 6.36k 0 13:05 14:05

Network packets out (count)

Count

0 0 0 13:05 14:05

CPU credit usage (count)

Count

0 0 0 13:05 14:05

CPU credit balance (count)

Count

0 0 0 13:05 14:05

Add to dashboard

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences