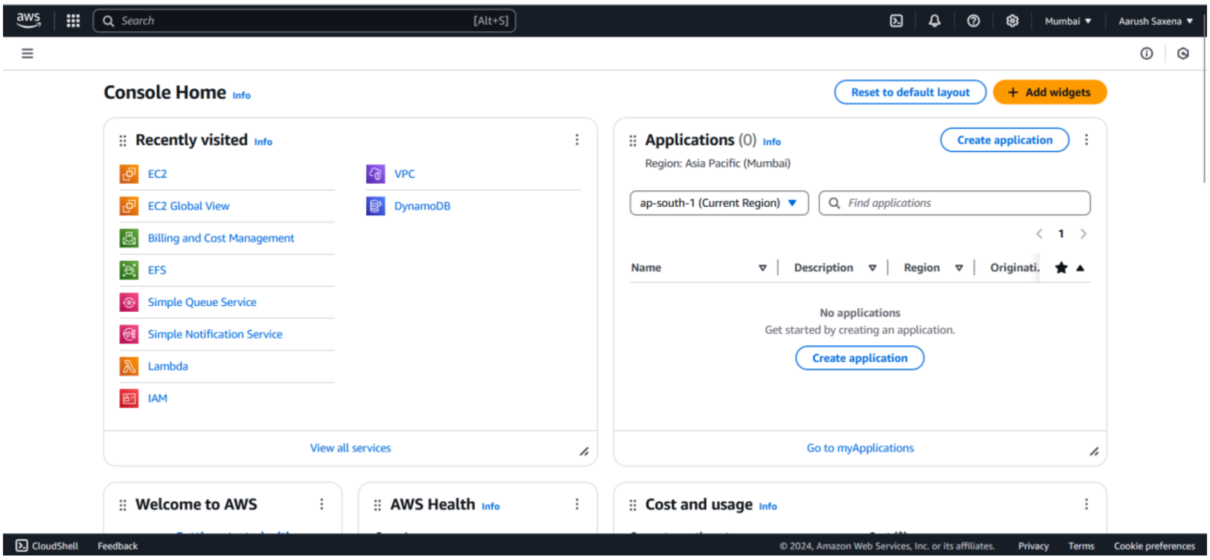
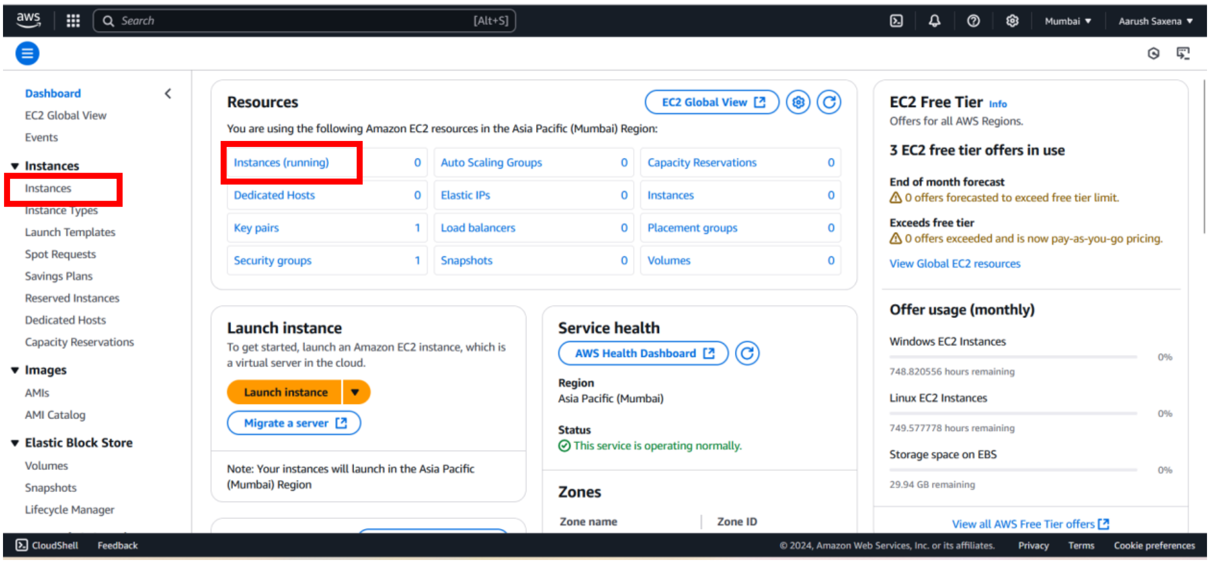
Load Balancer(Application Load Balancer)

Step1: Log-in to your amazon web service console and search for EC2 service.



No applications
Get started by creating an application.

You will see a console as shown in image given below click on instances and create instances.



You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

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

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

Note: Your instances will launch in the Asia Pacific (Mumbai) Region

Region
Asia Pacific (Mumbai)

Status
This service is operating normally.

Offers for all AWS Regions.

3 EC2 free tier offers in use

End of month forecast
0 offers forecasted to exceed free tier limit.

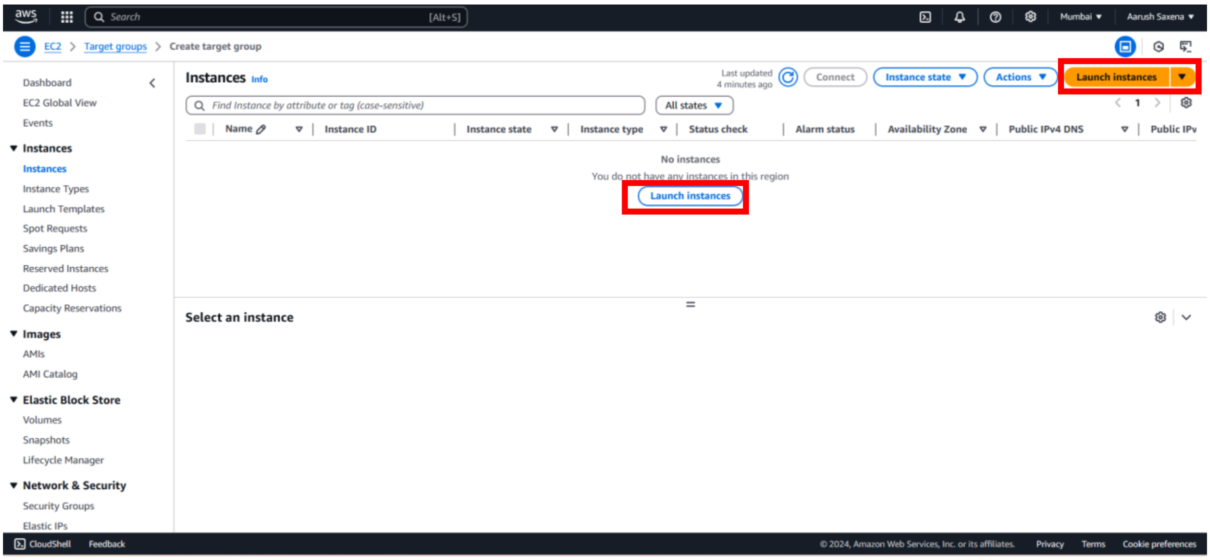
Exceeds free tier
0 offers exceeded and is now pay-as-you-go pricing.

Windows EC2 Instances 0%
748.820556 hours remaining

Linux EC2 Instances 0%
749.577778 hours remaining

Storage space on EBS 0%
29.94 GB remaining

click on launch instances. And type your instance name and select your AMI according to your requirements. Choose t2.micro or as per your requirement and allow http and https traffic.



Instances Info

Find Instance by attribute or tag (case-sensitive)

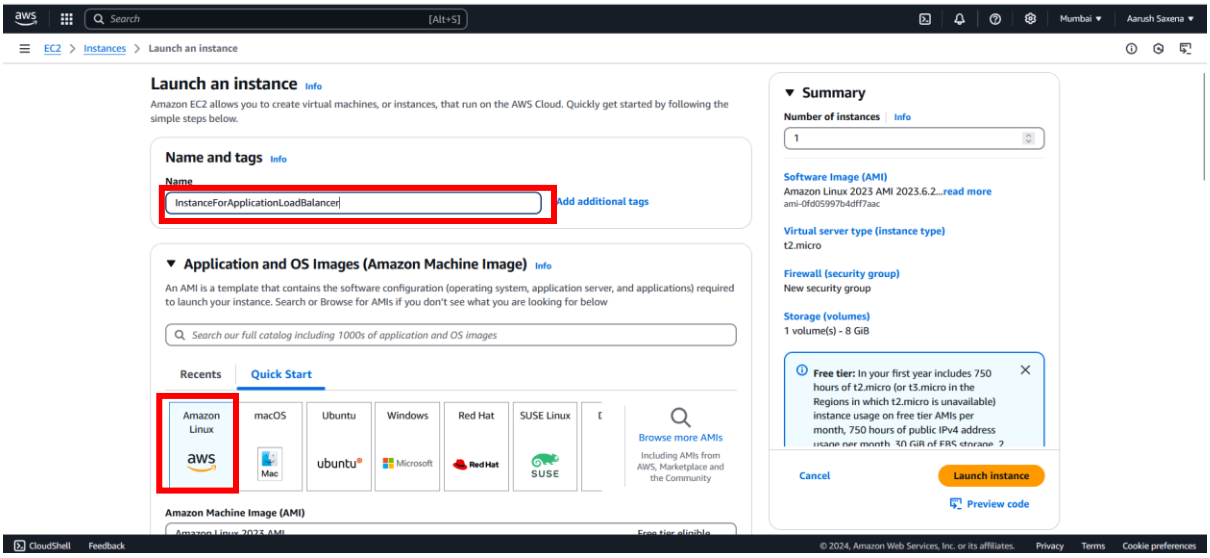
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv

No instances

You do not have any instances in this region

Launch instances

Select 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

InstanceForApplicationLoadBalancer

Add additional tags

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

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

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.6.2...read more

ami-0fd05997b4dff7aac

Virtual server type (instance type)

t2.micro

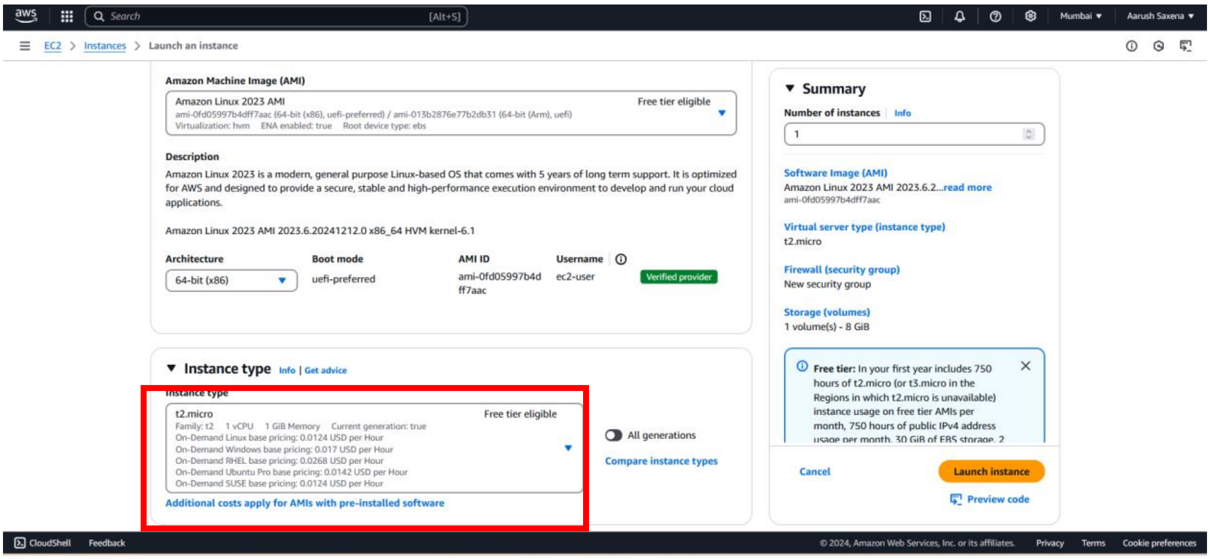
Firewall (security group)

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



Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible
ami-0fd05997b4dff7aac (64-bit (x86), uefi-preferred) / ami-013b2876e77b2db31 (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 2023.6.20241212.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Username
64-bit (x86)	uefi-preferred	ami-0fd05997b4dff7aac	ec2-user

Instance type Info | Get advice

Instance type

t2.micro Free tier eligible
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

Additional costs apply for AMIs with pre-installed software

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.6.2...read more

ami-0fd05997b4dff7aac

Virtual server type (instance type)

t2.micro

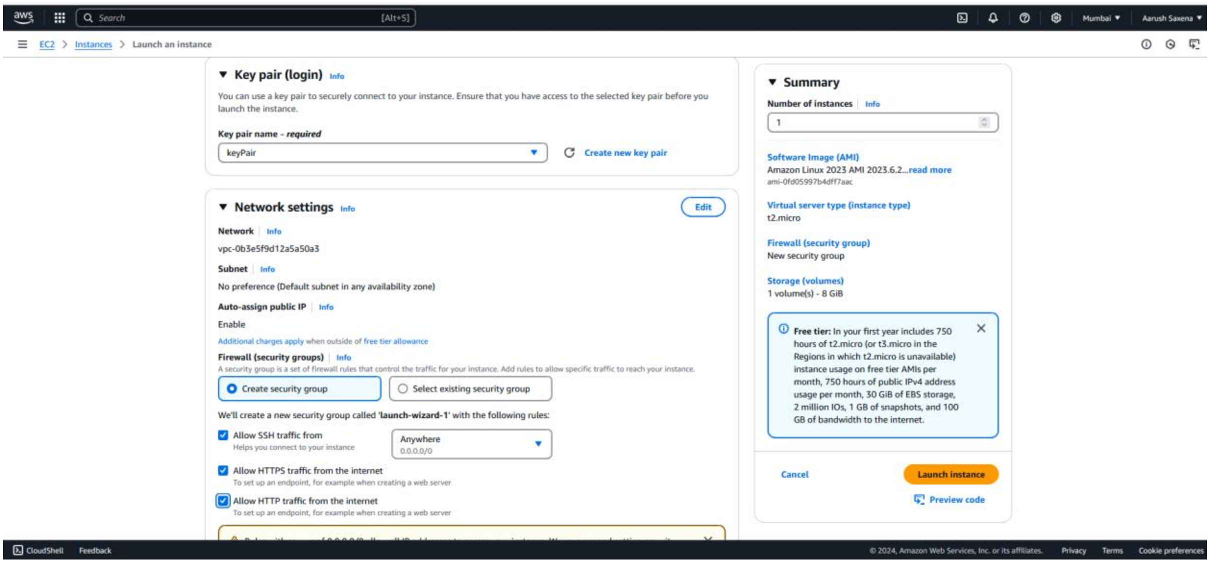
Firewall (security group)

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



▼ Key pair (login)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

keyPair ▼

▼ Network settings

Network

vpc-0b3e5f9d12a5a50a3

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-1**' with the following rules:

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

▼ Summary

Number of instances

1

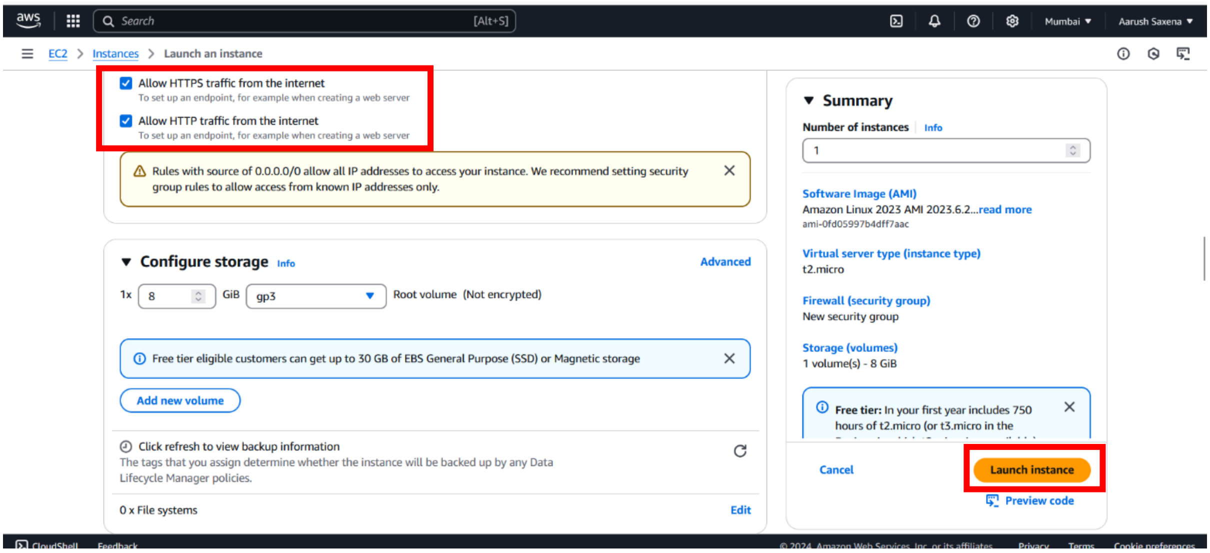
Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0fd05997b4dff7aac

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 bandwidth to the internet.



☑ 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

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

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

▼ Summary

Number of instances

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0fd05997b4dff7aac

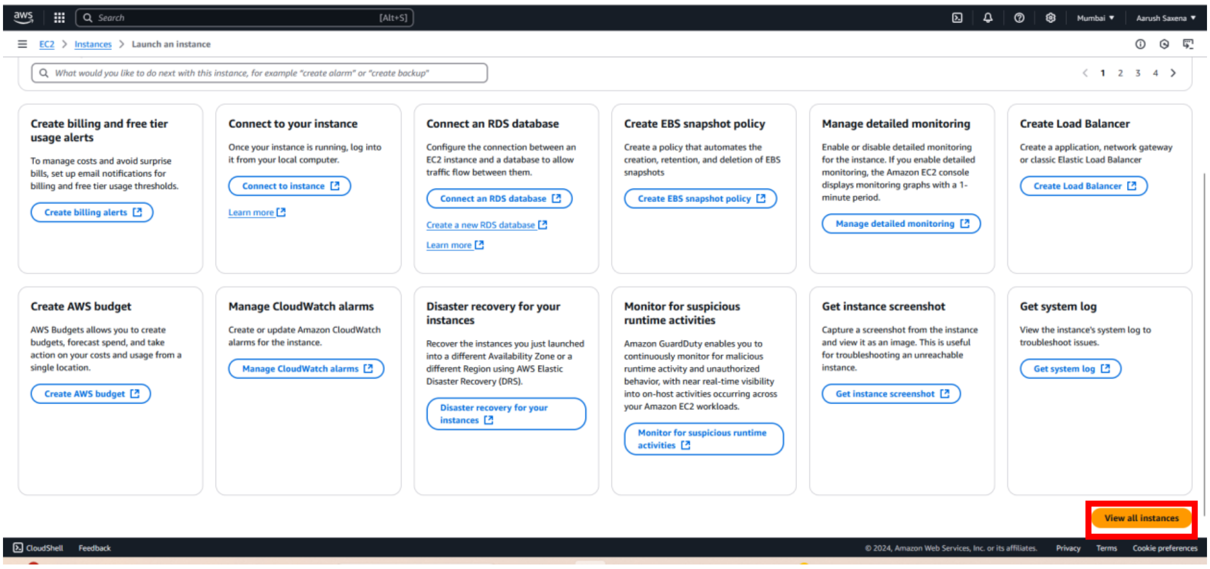
Virtual server type (instance type)
t2.micro

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

after that click on launch instance a window will appear to see your instances click on view all instances.



What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Connect to your instance
Once your instance is running, log into it from your local computer.

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots

Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer

Create AWS budget
AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.

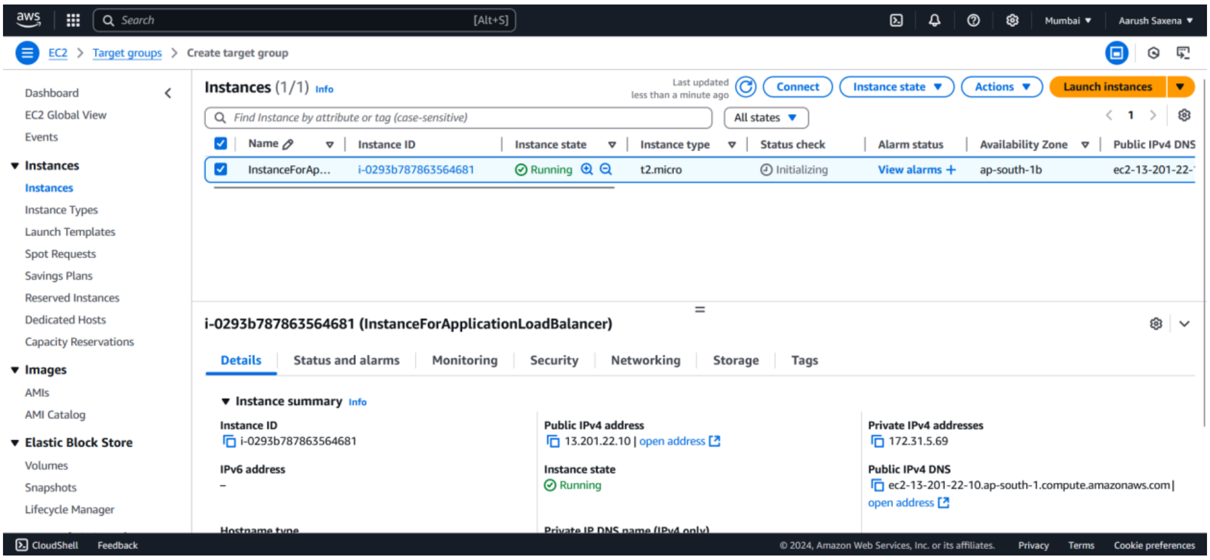
Disaster recovery for your instances
Recover the instances you just launched into a different Availability Zone or a different Region using AWS Elastic Disaster Recovery (DRS).

Monitor for suspicious runtime activities
Amazon GuardDuty enables you to continuously monitor for malicious runtime activity and unauthorized behavior, with near real-time visibility into on-host activities occurring across your Amazon EC2 workloads.

Get instance screenshot
Capture a screenshot from the instance and view it as an image. This is useful for troubleshooting an unreachable instance.

Get system log
View the instance's system log to troubleshoot issues.

Now as shown in image given below you can see our instances has been created now create another instances with same steps.



Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	InstanceForAp…	i-0293b787863564681	Running	t2.micro	Initializing	View alarms +	ap-south-1b	ec2-13-201-22-

i-0293b787863564681 (InstanceForApplicationLoadBalancer)

▼ Instance summary Info

Instance ID
i-0293b787863564681

Public IPv4 address
13.201.22.10 | open address

Private IPv4 addresses
172.31.5.69

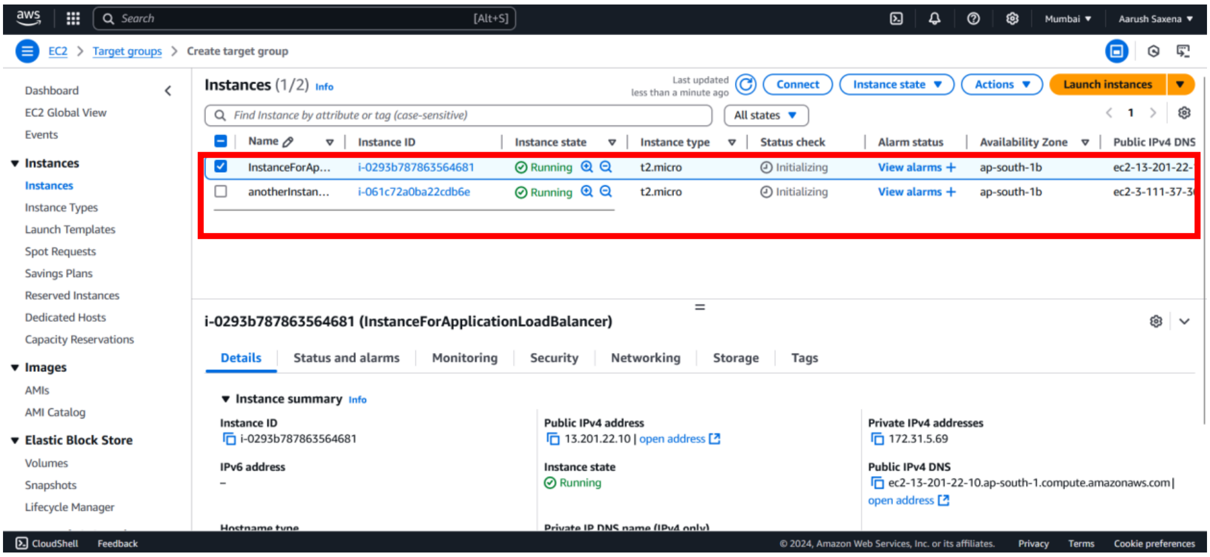
IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-13-201-22-10.ap-south-1.compute.amazonaws.com | open address

Hostname type

Private IP DNS name (IPv4 only)



Instances (1/2) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	InstanceForAp…	i-0293b787863564681	Running	t2.micro	Initializing	View alarms +	ap-south-1b	ec2-13-201-22-
☐	anotherInstan…	i-061c72a0ba22cdb6e	Running	t2.micro	Initializing	View alarms +	ap-south-1b	ec2-3-111-37-3

i-0293b787863564681 (InstanceForApplicationLoadBalancer)

▼ Instance summary Info

Instance ID
i-0293b787863564681

Public IPv4 address
13.201.22.10 | open address

Private IPv4 addresses
172.31.5.69

IPv6 address
–

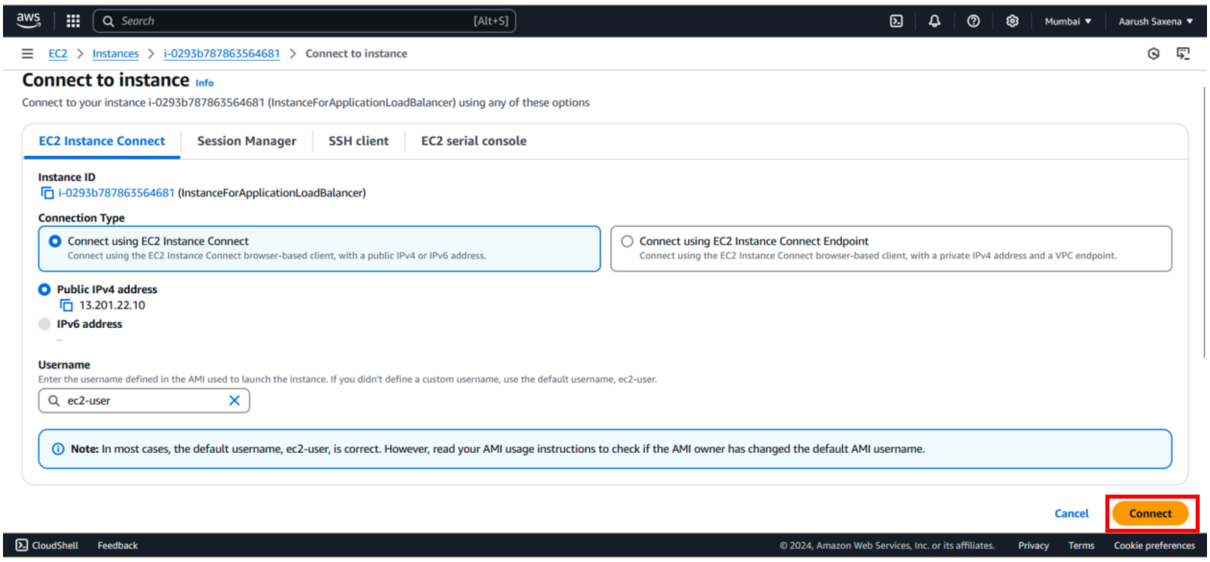
Instance state
Running

Public IPv4 DNS
ec2-13-201-22-10.ap-south-1.compute.amazonaws.com | open address

Hostname type

Private IP DNS name (IPv4 only)

Select the instances one by one and click on connect button a window will appear as shown in image given below click on connect.



Connect to instance Info

Connect to your instance i-0293b787863564681 (InstanceForApplicationLoadBalancer) using any of these options

Instance ID
i-0293b787863564681 (InstanceForApplicationLoadBalancer)

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
13.201.22.10

○ 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.

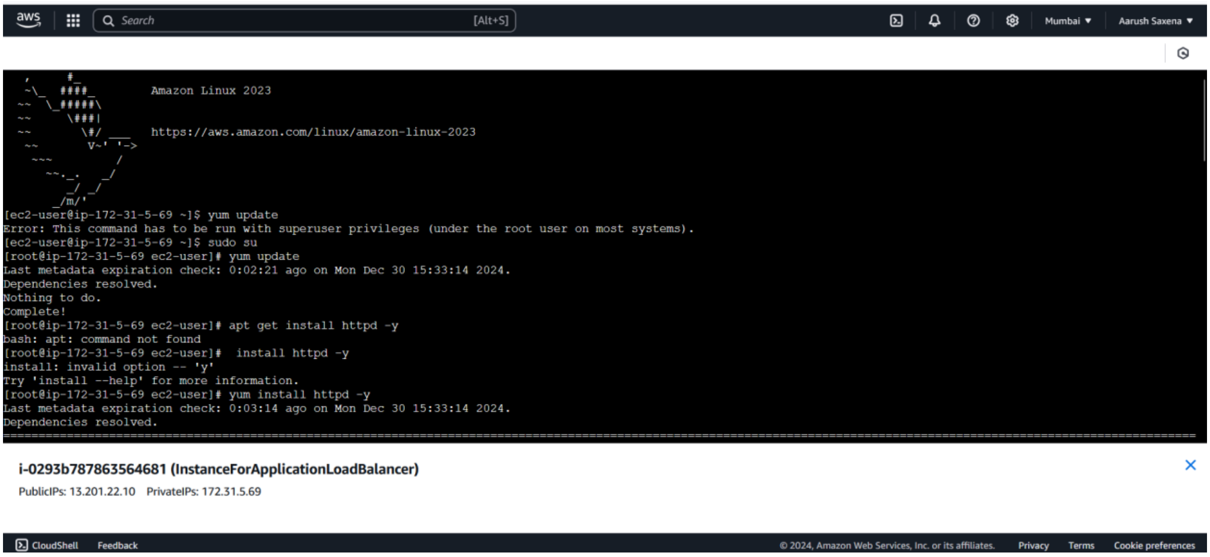
ec2-user

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.

You can see our aws linux has been connected now type some commands to shown in our html page

Commands are :-

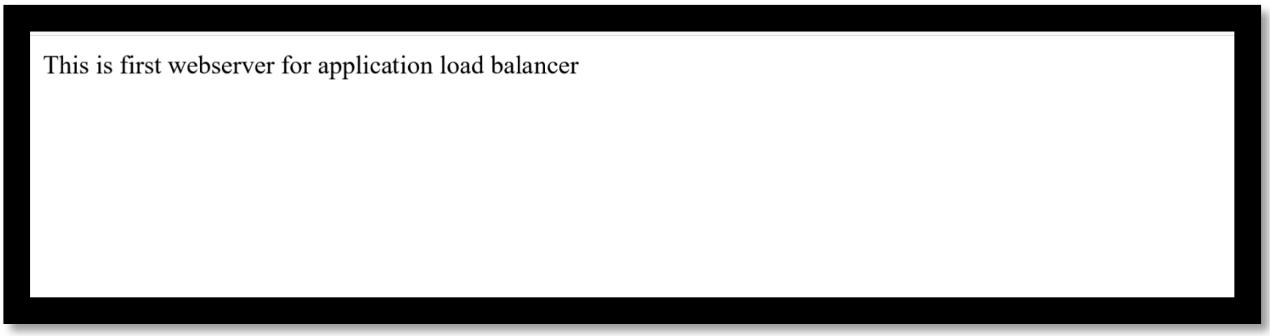
1. sudo su
2. yum update
3. yum install httpd -y
4. systemctl start httpd
5. systemctl status httpd
6. cd /var/www/html
7. echo “this is first webserver” > index.html (type command as your wish)



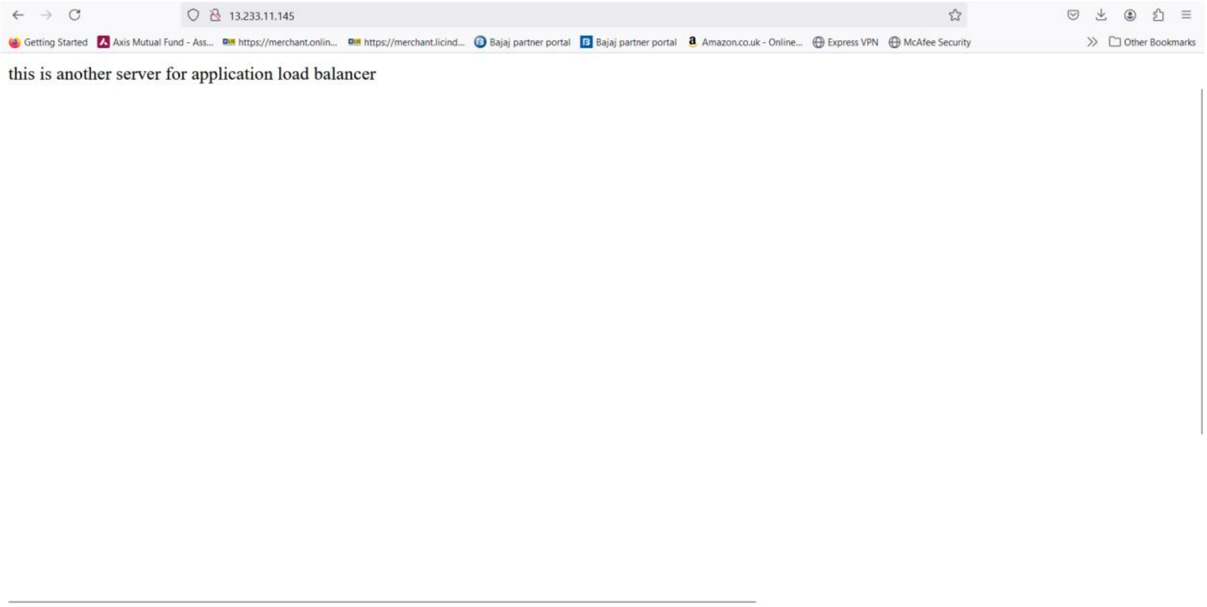
```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-5-69 ~]$ yum update
Error: This command has to be run with superuser privileges (under the root user on most systems).
[ec2-user@ip-172-31-5-69 ~]$ sudo su
[root@ip-172-31-5-69 ec2-user]# yum update
Last metadata expiration check: 0:02:21 ago on Mon Dec 30 15:33:14 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-172-31-5-69 ec2-user]# apt get install httpd -y
bash: apt: command not found
[root@ip-172-31-5-69 ec2-user]#  install httpd -y
install: invalid option -- 'y'
Try 'install --help' for more information.
[root@ip-172-31-5-69 ec2-user]# yum install httpd -y
Last metadata expiration check: 0:03:14 ago on Mon Dec 30 15:33:14 2024.
Dependencies resolved.
================================================================================
```

i-0293b787863564681 (InstanceForApplicationLoadBalancer)

PublicIPs: 13.201.22.10 PrivateIPs: 172.31.5.69

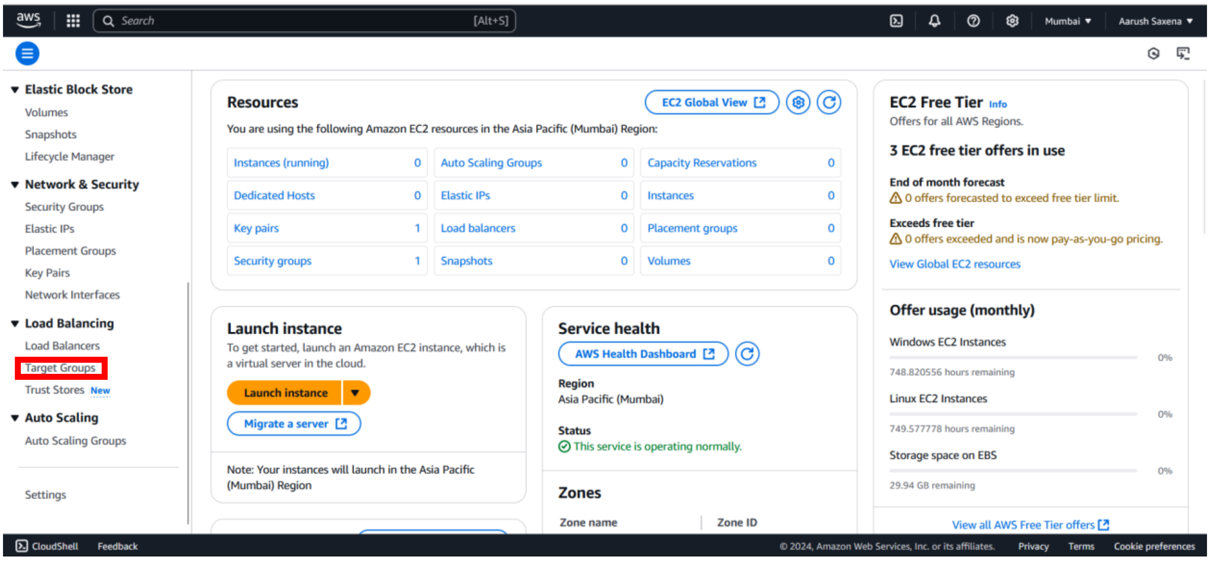


This is first webserver for application load balancer



this is another server for application load balancer

Step2: Now to create Load Balancer we need to create Target groups, we make target groups so that we can transfer traffic to specified targets(servers) and helps to monitor on it easily or easily to maintain.



Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

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

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 Asia Pacific (Mumbai) Region

Service health

Region
Asia Pacific (Mumbai)

Status
This service is operating normally.

Zones

Zone name | Zone ID

EC2 Free Tier Info

Offers for all AWS Regions.

3 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.

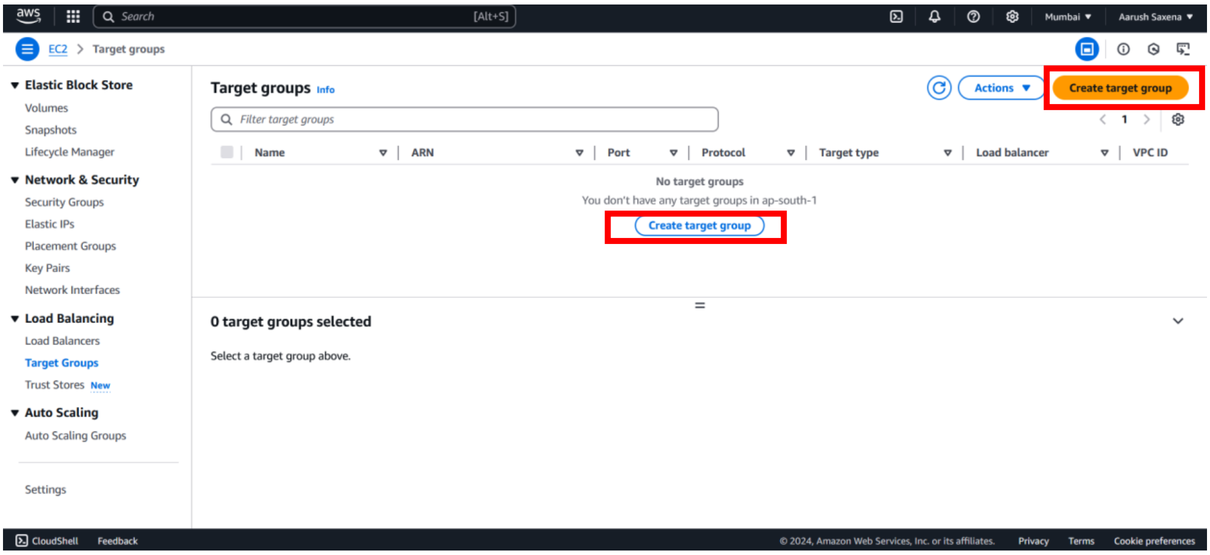
Offer usage (monthly)

Windows EC2 Instances 0%
748.820556 hours remaining

Linux EC2 Instances 0%
749.577778 hours remaining

Storage space on EBS 0%
29.94 GB remaining

Click on Create target group



No target groups

You don't have any target groups in ap-south-1

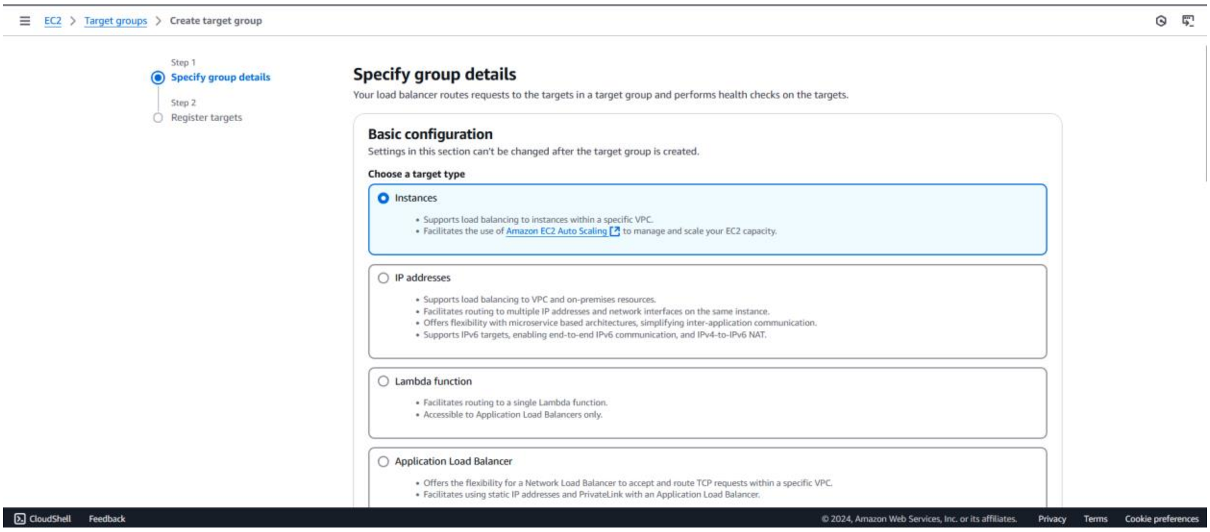
Create target group

0 target groups selected

Select a target group above.

After clicking on it you have to choose target groups on which you have to apply it and access it.

Give name to your target group



Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section can't be changed after the target group is created.

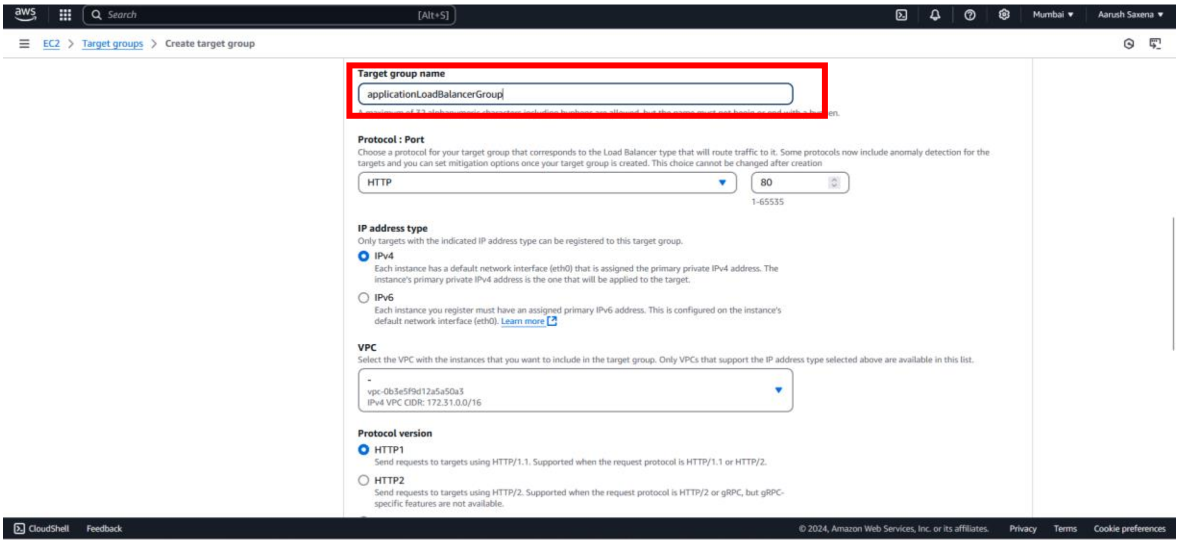
Choose a target type

● Instances
- Supports load balancing to instances within a specific VPC.
- Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity.

○ IP addresses
- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

○ Lambda function
- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

○ Application Load Balancer
- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.



Target group name

applicationLoadBalancerGroup

[illegible] en.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP ▾ | 80

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

● IPv4
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

○ IPv6
Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). Learn more

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

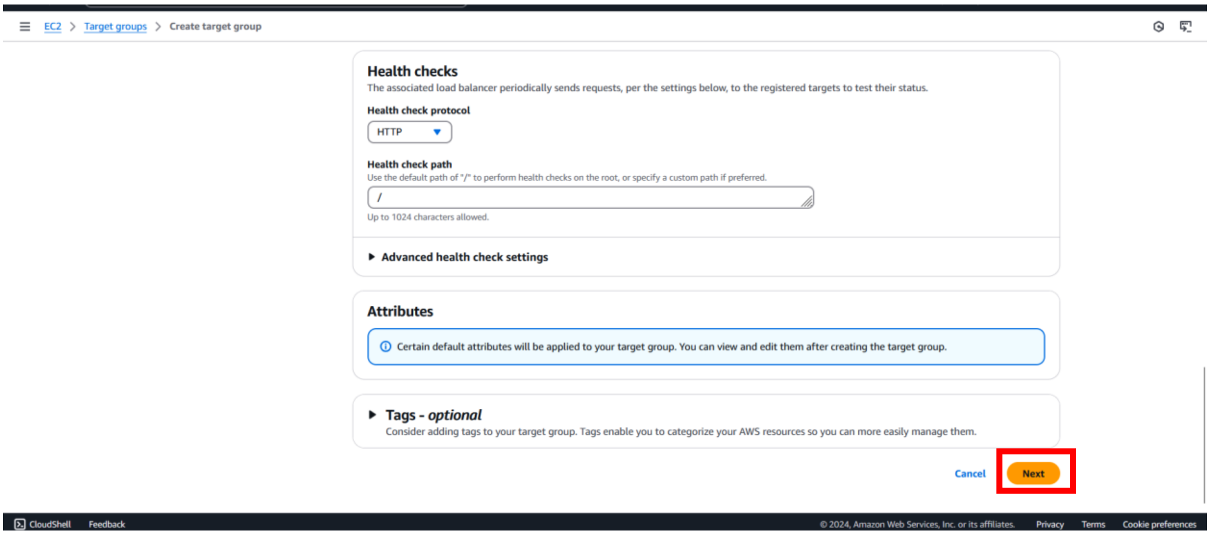
-
vpc-0b3e5f9d12a5a50a3
IPv4 VPC CIDR: 172.31.0.0/16

Protocol version

● HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

○ HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

Leave everything to default settings and click on next.



Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

HTTP ▾

Health check path

Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

▸ Advanced health check settings

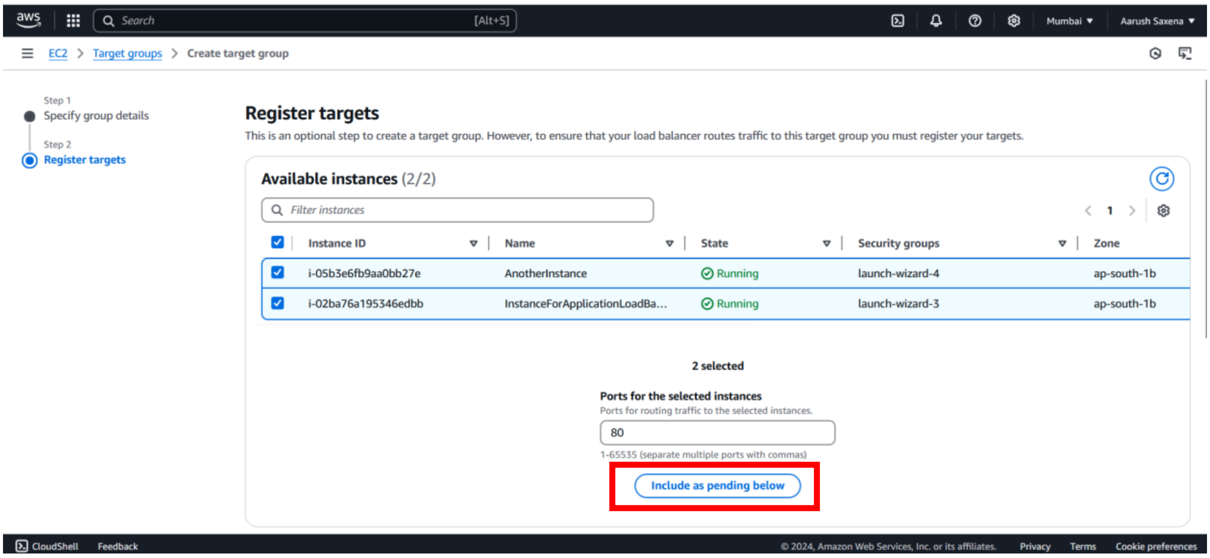
Attributes

Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

▸ **Tags - *optional***

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

Select the instances and click on include as pending below.



Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2/2)

Filter instances

☑	Instance ID	Name	State	Security groups	Zone
☑	i-05b3e6fb9aa0bb27e	AnotherInstance	✓ Running	launch-wizard-4	ap-south-1b
☑	i-02ba76a195346edbb	InstanceForApplicationLoadBa...	✓ Running	launch-wizard-3	ap-south-1b

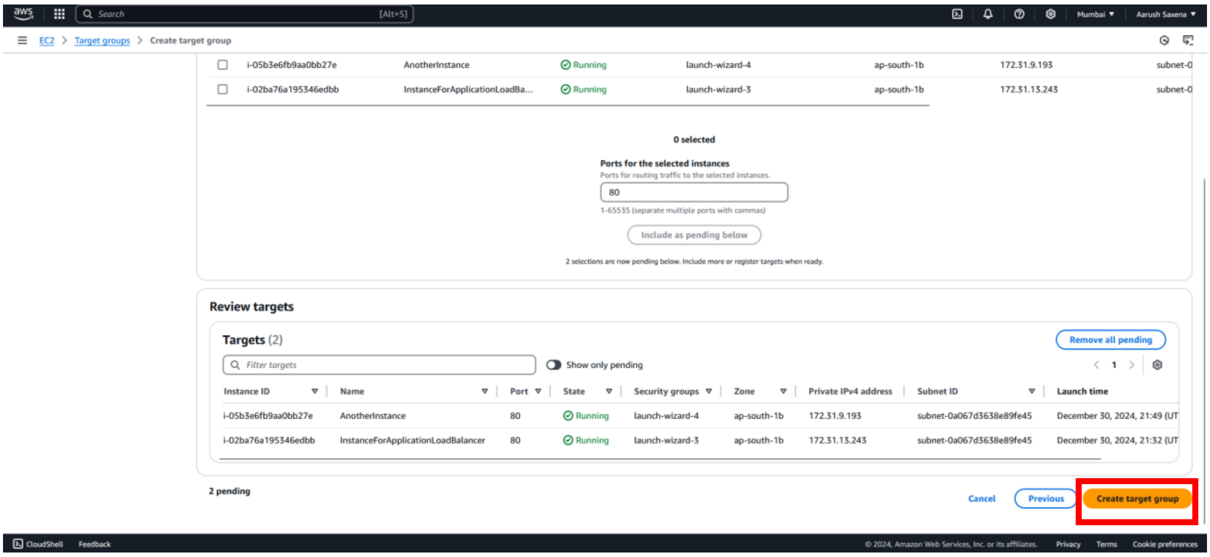
2 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)



□	i-05b3e6fb9aa0bb27e	AnotherInstance	✓ Running	launch-wizard-4	ap-south-1b	172.31.9.193
□	i-02ba76a195346edbb	InstanceForApplicationLoadBa...	✓ Running	launch-wizard-3	ap-south-1b	172.31.13.243

0 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)

2 selections are now pending below. Include more or register targets when ready.

Review targets

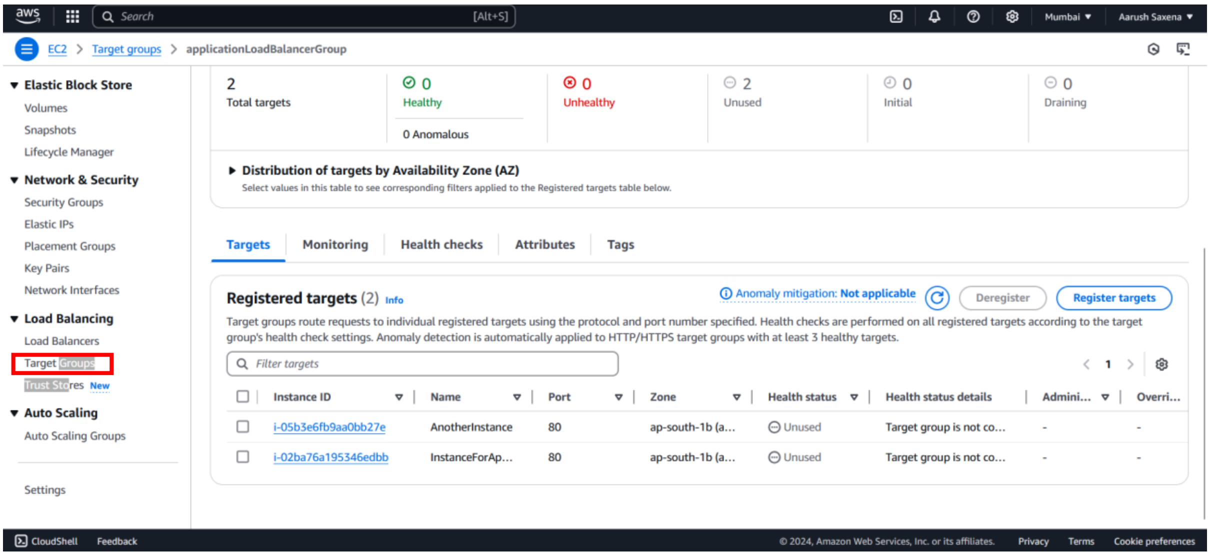
Targets (2)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-05b3e6fb9aa0bb27e	AnotherInstance	80	✓ Running	launch-wizard-4	ap-south-1b	172.31.9.193	subnet-0a067d3638e89fe45	December 30, 2024, 21:49 (UT
i-02ba76a195346edbb	InstanceForApplicationLoadBalancer	80	✓ Running	launch-wizard-3	ap-south-1b	172.31.13.243	subnet-0a067d3638e89fe45	December 30, 2024, 21:32 (UT

2 pending

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

Click on create target group and you will see console as given below.



2	⊘ 0	⊗ 0	⊖ 2	⊖ 0	⊖ 0
Total targets	Healthy	Unhealthy	Unused	Initial	Draining
	0 Anomalous				

▸ Distribution of targets by Availability Zone (AZ)
Select values in this table to see corresponding filters applied to the Registered targets table below.

Registered targets (2) Info

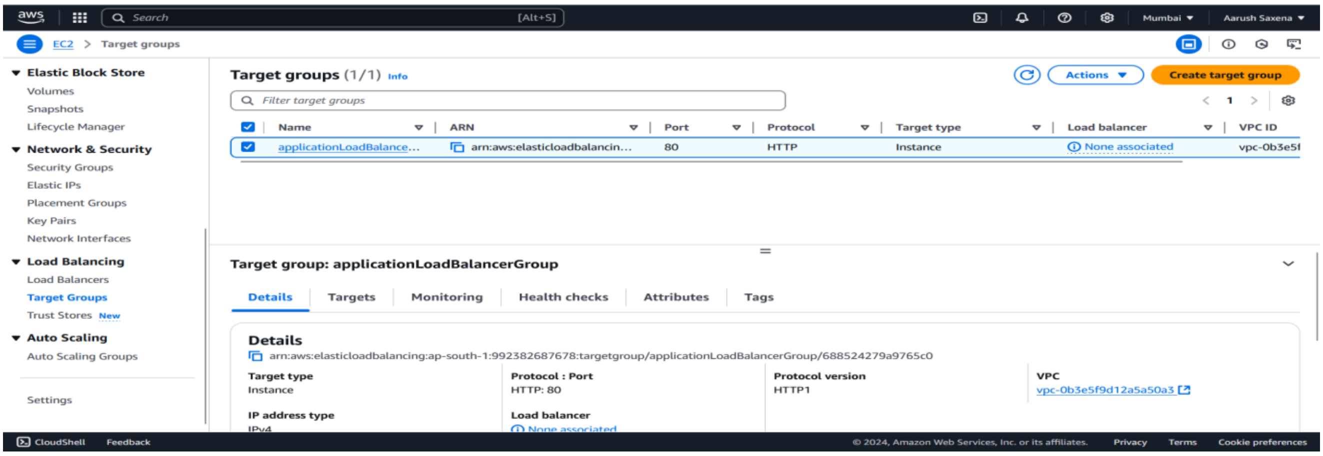
Anomaly mitigation: Not applicable

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

□	Instance ID	Name	Port	Zone	Health status	Health status details	Admini...	Overri...
□	i-05b3e6fb9aa0bb27e	AnotherInstance	80	ap-south-1b (a...	⊖ Unused	Target group is not co...	-	-
□	i-02ba76a195346edbb	InstanceForAp...	80	ap-south-1b (a...	⊖ Unused	Target group is not co...	-	-

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

After clicking on target groups you can see target groups has been created



Target groups (1/1) Info

☑	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
☑	applicationLoadBalance...	arn:aws:elasticloadbalancin...	80	HTTP	Instance	None associated	vpc-0b3e5f

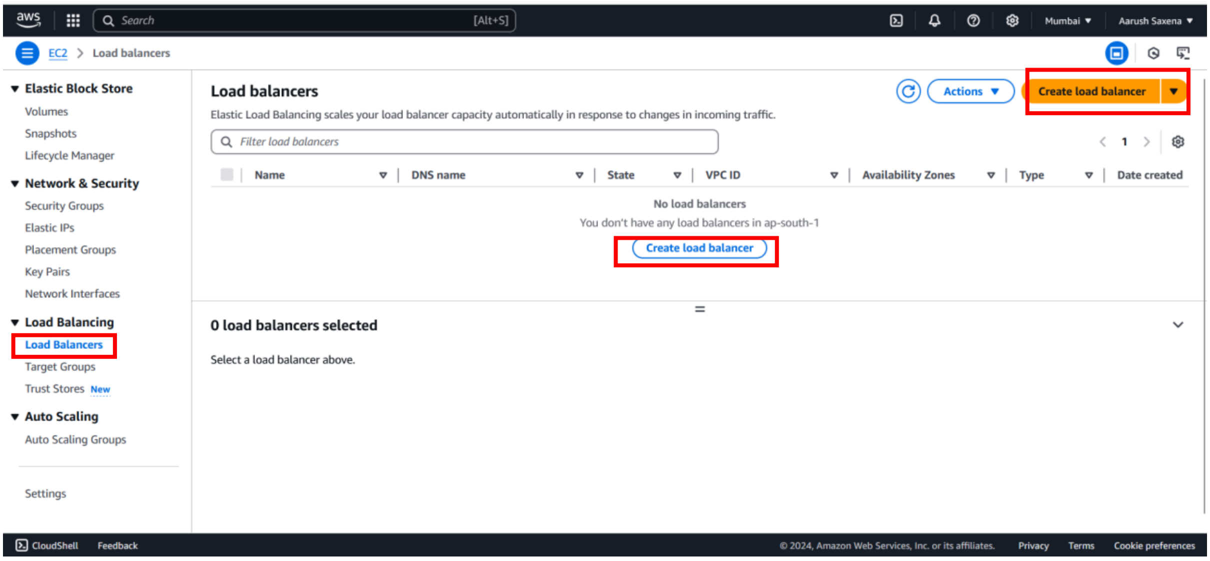
Target group: applicationLoadBalancerGroup

Details
arn:aws:elasticloadbalancing:ap-south-1:992382687678:targetgroup/applicationLoadBalancerGroup/688524279a9765c0

Target type	Protocol : Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-0b3e5f9d12a5a50a3
IP address type	Load balancer		
IPv4	None associated		

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

Step3: Click on Load Balancers and create load balancer click on it



▾ Elastic Block Store
- Volumes
- Snapshots
- Lifecycle Manager

▾ Network & Security
- Security Groups
- Elastic IPs
- Placement Groups
- Key Pairs
- Network Interfaces

▾ Load Balancing
- Load Balancers
- Target Groups
- Trust Stores New

▾ Auto Scaling
- Auto Scaling Groups

Settings

Load balancers

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created

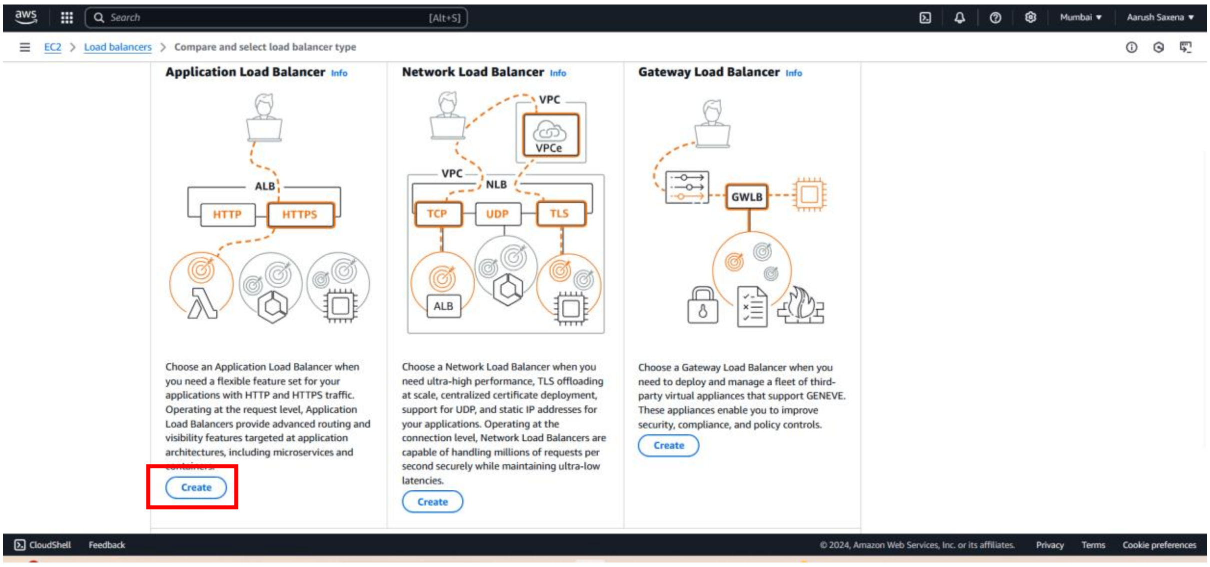
No load balancers

You don't have any load balancers in ap-south-1

0 load balancers selected

Select a load balancer above.

After clicking on it choose application load balancer and click on create.



Application Load Balancer Info

Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Network Load Balancer Info

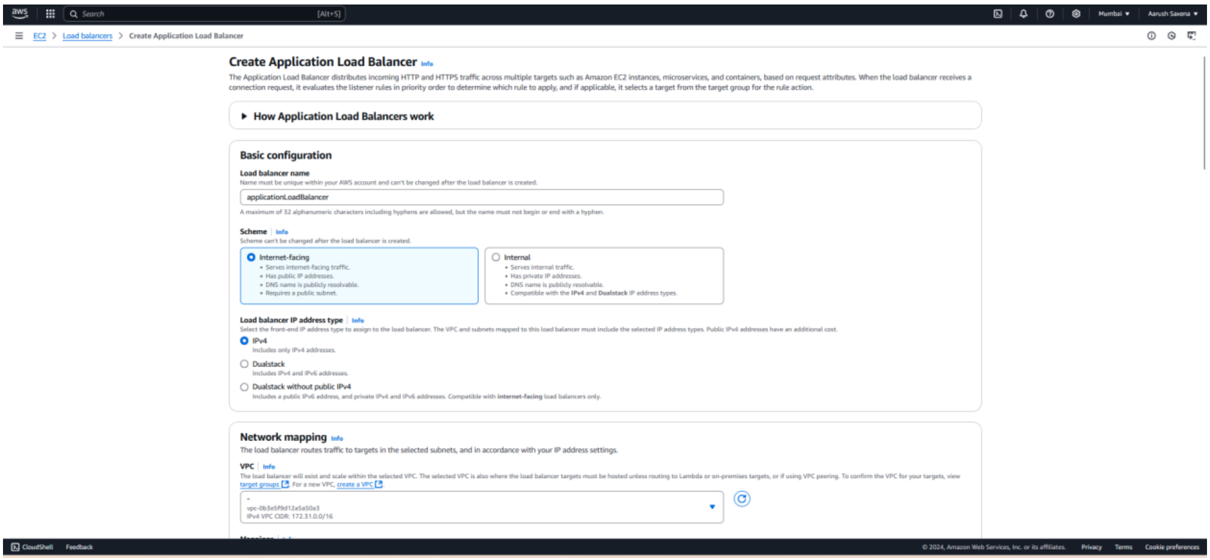
Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Gateway Load Balancer Info

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

After clicking on it fill the steps as shown in image given below.

As first give load balancer name and choose internet facing and leave everything to default settings and click on create Load balancer.



EC2 > Load balancers > Create Application Load Balancer

Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▸ How Application Load Balancers work

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
applicationLoadBalancer
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme Info
Scheme can't be changed after the load balancer is created.

● Internet-facing
- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

○ Internal
- Serves internal traffic.
- Has private IP addresses.
- DNS name is publicly resolvable.
- Compatible with the **IPv4** and **Dualstack** IP address types.

Load balancer IP address type Info
Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

● IPv4
Includes only IPv4 addresses.

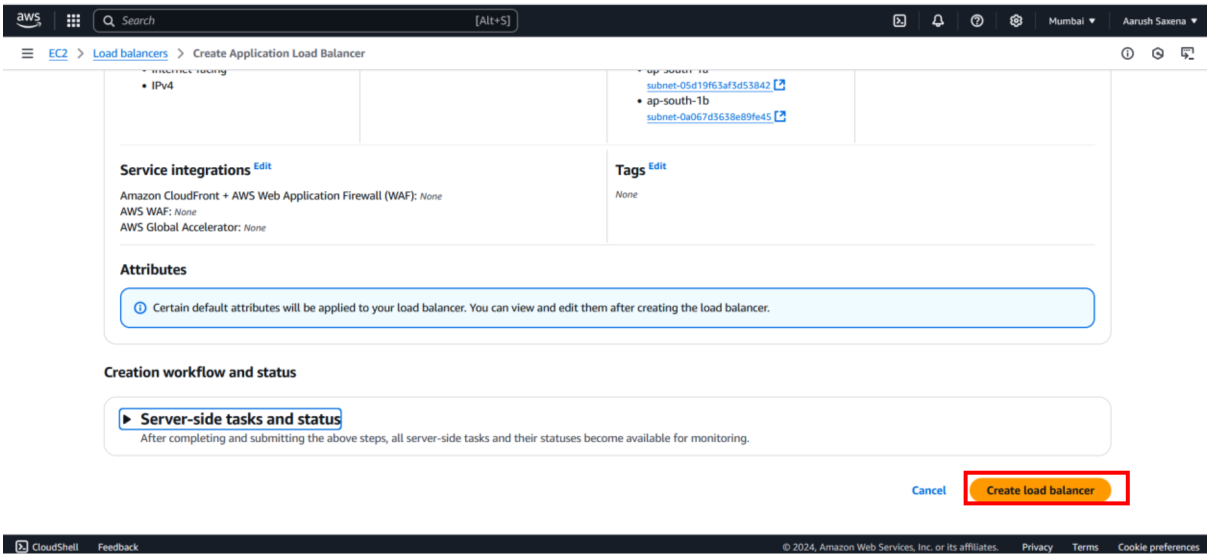
○ Dualstack
Includes IPv4 and IPv6 addresses.

○ Dualstack without public IPv4
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

Network mapping Info
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC Info
The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view target groups. For a new VPC, create a VPC.

-
vpc-0b3e5f9d12a5a50a3
IPv4 VPC CIDR: 172.31.0.0/16



EC2 > Load balancers > Create Application Load Balancer

- IPv4

subnet-05d19f63af3d53842
- ap-south-1b
subnet-0a067d3638e89fe45

Service integrations Edit

Amazon CloudFront + AWS Web Application Firewall (WAF): *None*
AWS WAF: *None*
AWS Global Accelerator: *None*

Tags Edit

None

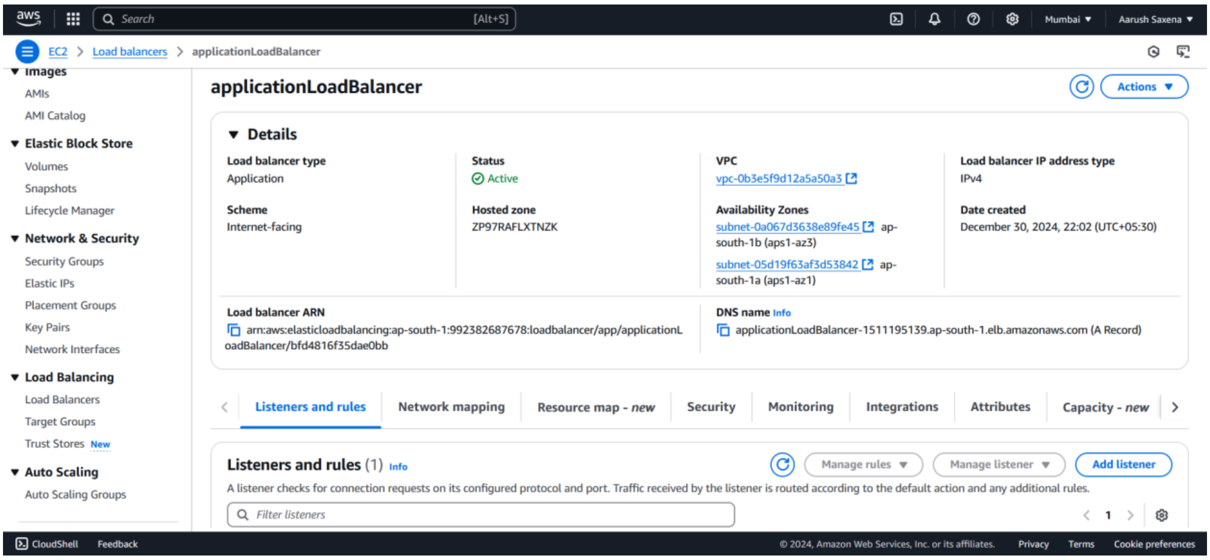
Attributes

Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Creation workflow and status

▸ **Server-side tasks and status**
After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.

Copy the dns name and paste it to the web, you will see that you can acess the web through it.



EC2 > Load balancers > applicationLoadBalancer

applicationLoadBalancer

▾ **Details**

Load balancer type
Application

Status
Active

VPC
vpc-0b3e5f9d12a5a50a3

Load balancer IP address type
IPv4

Scheme
Internet-facing

Hosted zone
ZP97RAFLXTNZK

Availability Zones
subnet-0a067d3638e89fe45 ap-south-1b (aps1-az3)
subnet-05d19f63af3d53842 ap-south-1a (aps1-az1)

Date created
December 30, 2024, 22:02 (UTC+05:30)

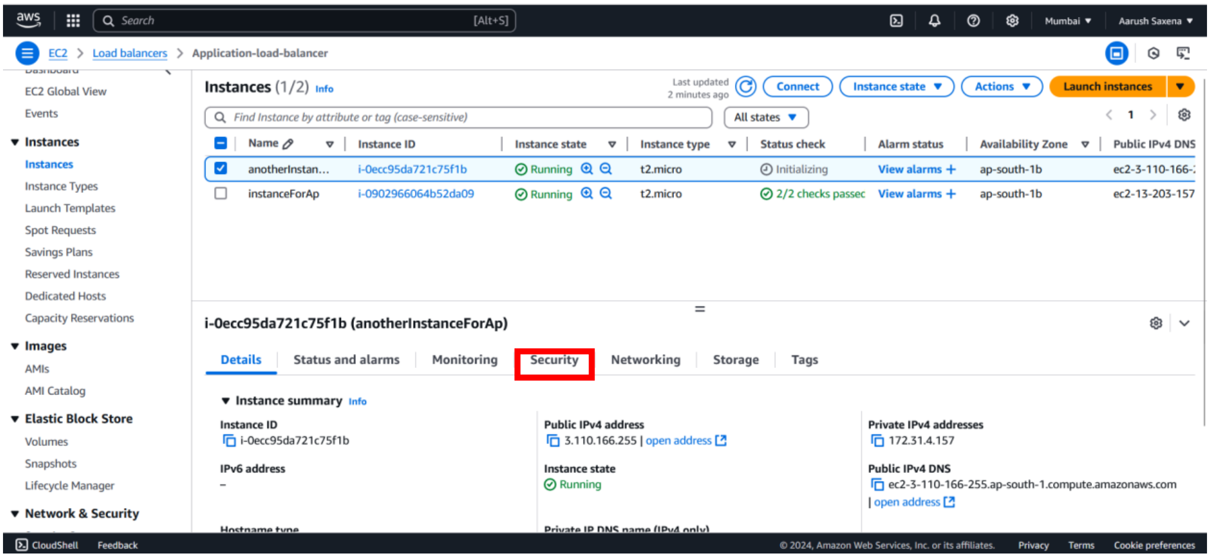
Load balancer ARN
arn:aws:elasticloadbalancing:ap-south-1:992382687678:loadbalancer/app/applicationLoadBalancer/bfd4816f35dae0bb

DNS name Info
applicationLoadBalancer-1511195139.ap-south-1.elb.amazonaws.com (A Record)

Listeners and rules (1) Info

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

But now we get a problem that we can acess the web through ec2 public ip and through application load balancer dns name to remove this problem we need to change the security group settings of EC2.



Instances (1/2) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	anotherInstan...	i-0ecc95da721c75f1b	Running	t2.micro	Initializing	View alarms +	ap-south-1b	ec2-3-110-166-:
☐	instanceForAp	i-0902966064b52da09	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1b	ec2-13-203-157

i-0ecc95da721c75f1b (anotherInstanceForAp)

▼ Instance summary Info

Instance ID
i-0ecc95da721c75f1b

Public IPv4 address
3.110.166.255 | open address

Private IPv4 addresses
172.31.4.157

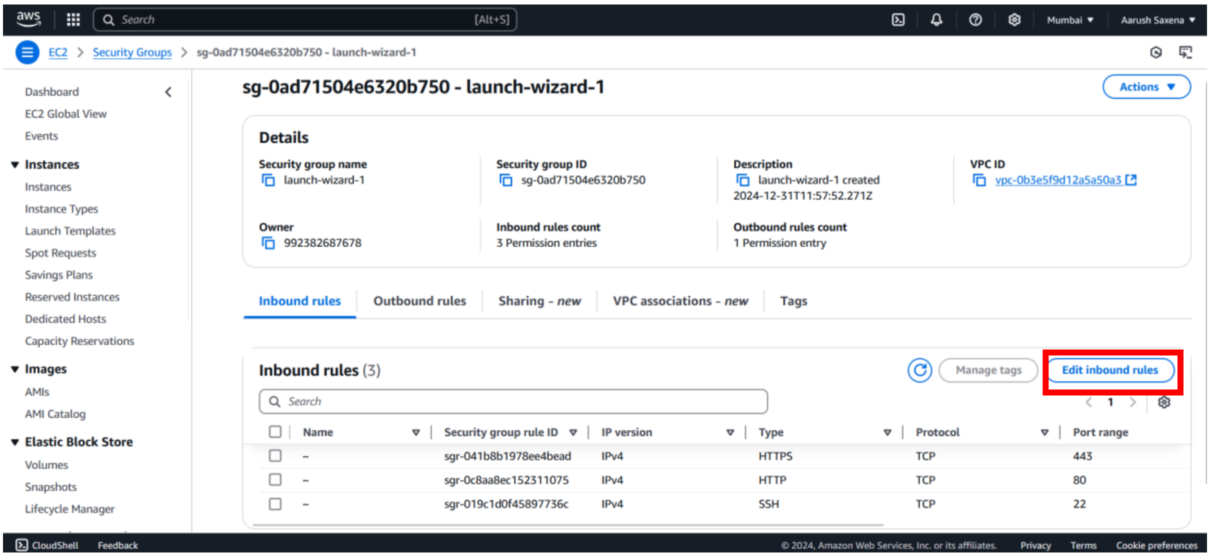
IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-3-110-166-255.ap-south-1.compute.amazonaws.com | open address

Hostname type

Private IP DNS name (IPv4 only)



sg-0ad71504e6320b750 - launch-wizard-1

Details

Security group name
launch-wizard-1

Security group ID
sg-0ad71504e6320b750

Description
launch-wizard-1 created 2024-12-31T11:57:52.271Z

VPC ID
vpc-0b3e5f9d12a5a50a3

Owner
992382687678

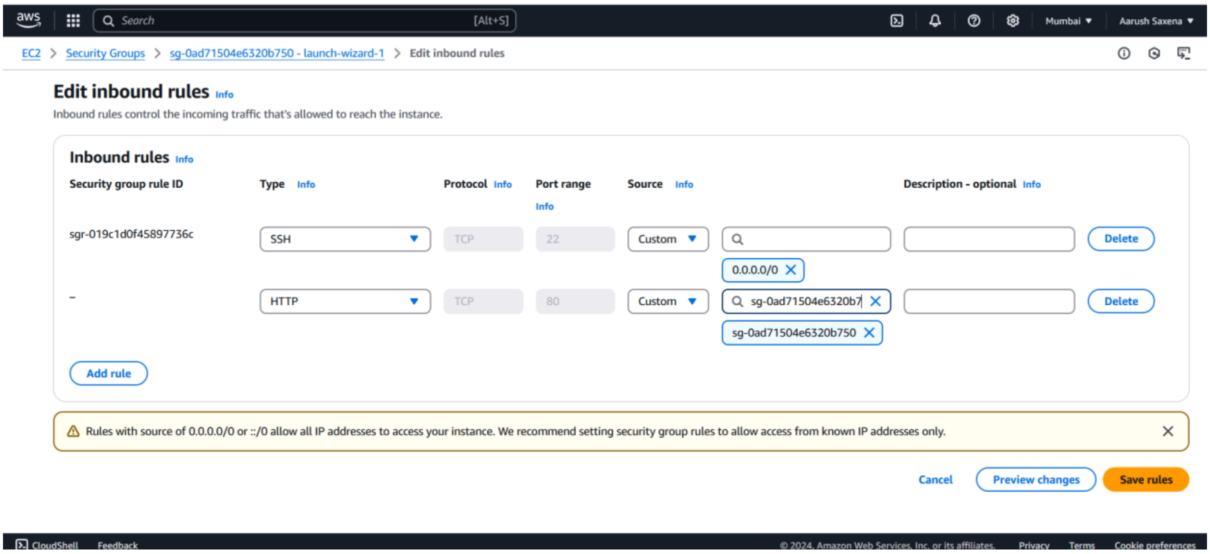
Inbound rules count
3 Permission entries

Outbound rules count
1 Permission entry

Inbound rules (3)

☐	Name	Security group rule ID	IP version	Type	Protocol	Port range
☐	–	sgr-041b8b1978ee4bead	IPv4	HTTPS	TCP	443
☐	–	sgr-0c8aa8ec152311075	IPv4	HTTP	TCP	80
☐	–	sgr-019c1d0f45897736c	IPv4	SSH	TCP	22

Delete the old rules and add new rule with load balancer security group so that data can be access through load balancer.



aws
Search [Alt+S]
Mumbai ▼
Aarush Saxena ▼
EC2 > Security Groups > sg-0ad71504e6320b750 - launch-wizard-1 > Edit inbound rules

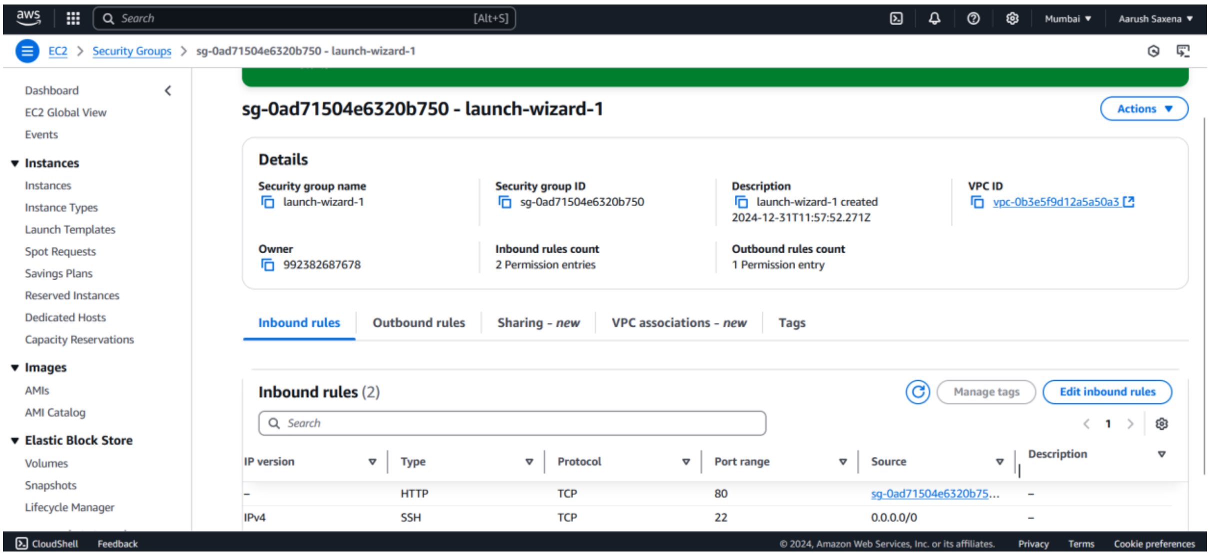
Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-019c1d0f45897736c	SSH	TCP	22	Custom	0.0.0.0/0		Delete
–	HTTP	TCP	80	Custom	sg-0ad71504e6320b7 sg-0ad71504e6320b750		Delete

⚠ 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.



sg-0ad71504e6320b750 - launch-wizard-1

Details

Security group name: launch-wizard-1

Security group ID: sg-0ad71504e6320b750

Description: launch-wizard-1 created 2024-12-31T11:57:52.271Z

VPC ID: vpc-0b3e5f9d12a5a50a3

Owner: 992382687678

Inbound rules count: 2 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules (2)

IP version	Type	Protocol	Port range	Source	Description
–	HTTP	TCP	80	sg-0ad71504e6320b75...	–
IPv4	SSH	TCP	22	0.0.0.0/0	–

Do the same for other instances.