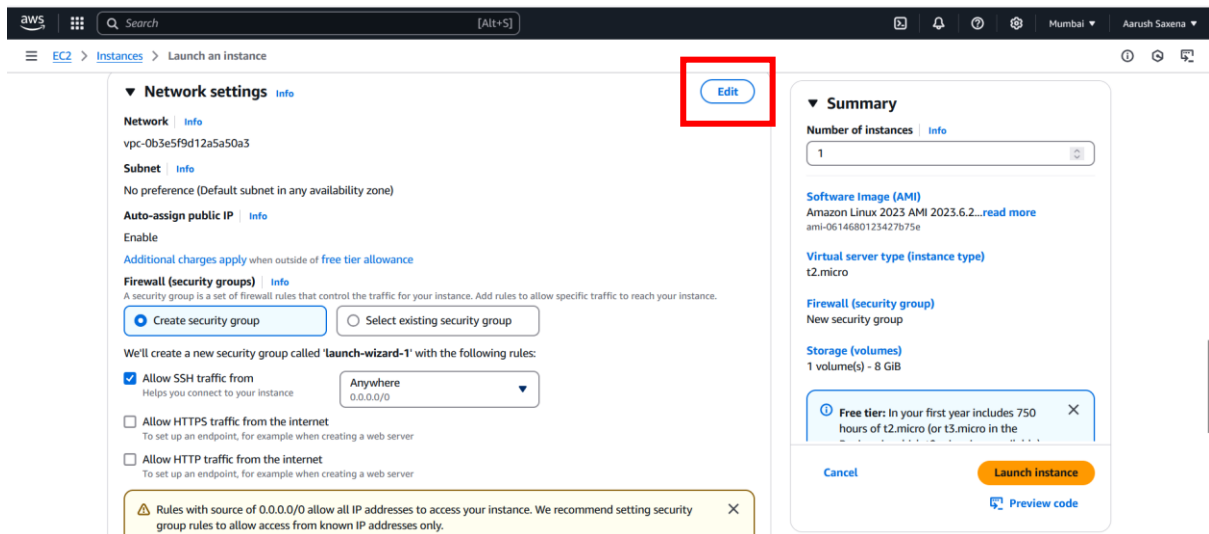


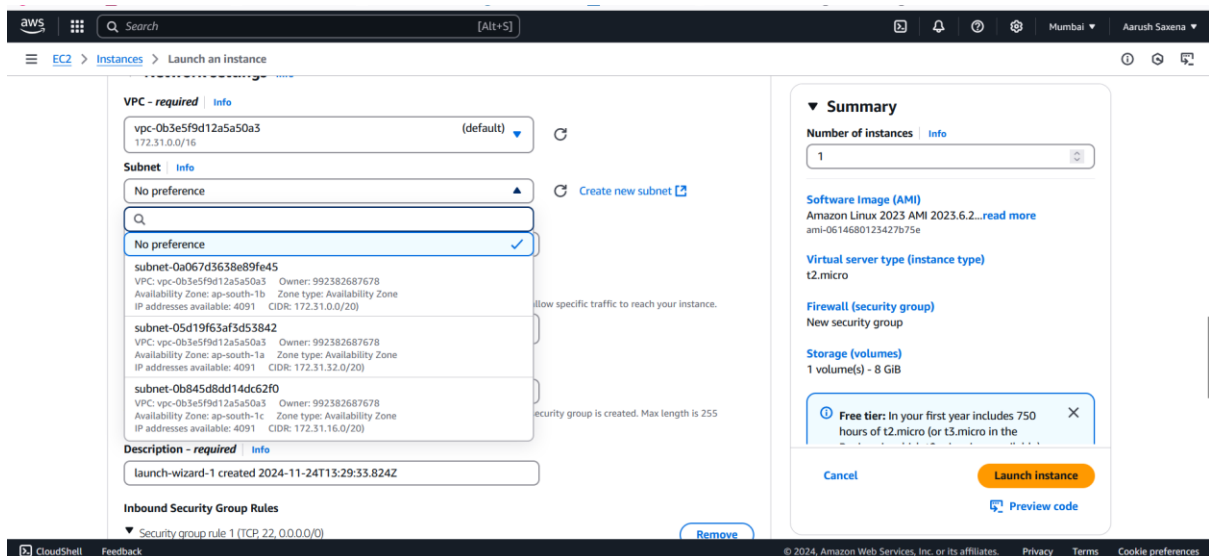
Elastic Load Balancer

Previous gen.(Classic Load Balancer)

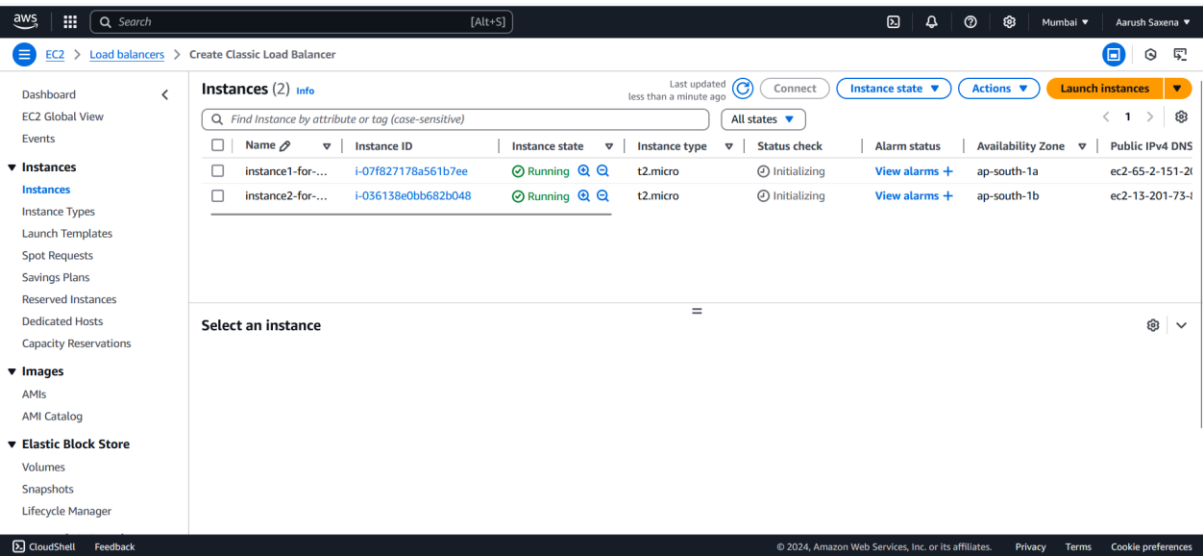
Step 1: log-in to your aws account and click on searchbar, search for EC2 click on it. On the left side click on Instances. And create approx 2-3 servers in different availability zones such as ap-south-1a and ap-south-1b from network settings and click on edit.



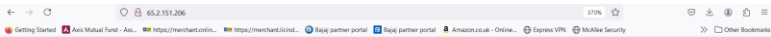
After clicking on edit click on subnets to define to create it in which availability zone.



We have created two servers in different availability zones.



Step 2: Now connect it and start the httpd server and on var/www/html path create a html file and denote which is server 1 and server 2 for increase readability.

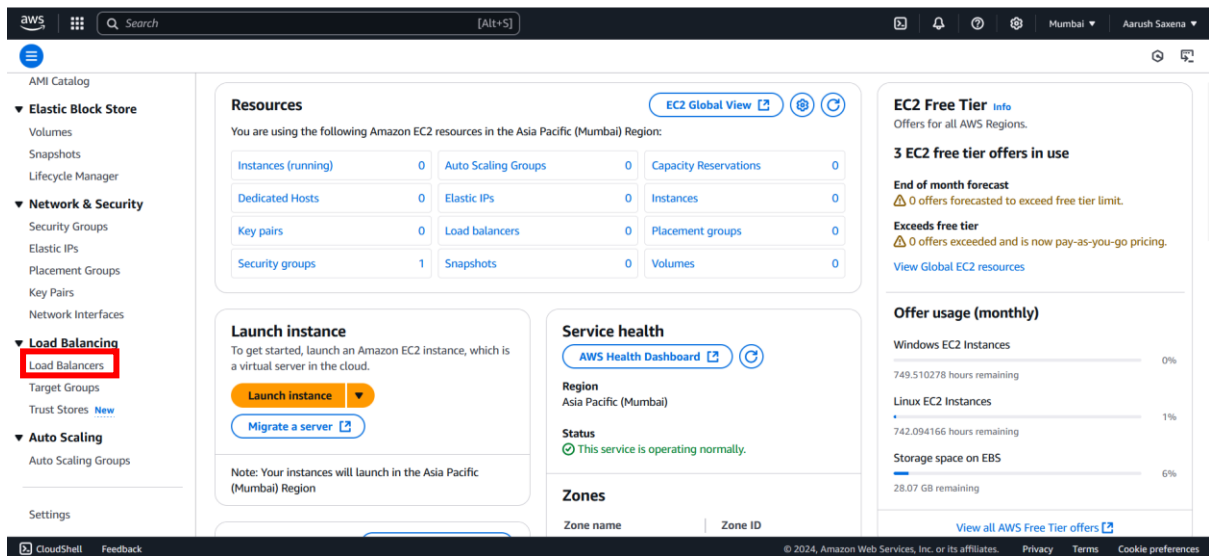


this is server1

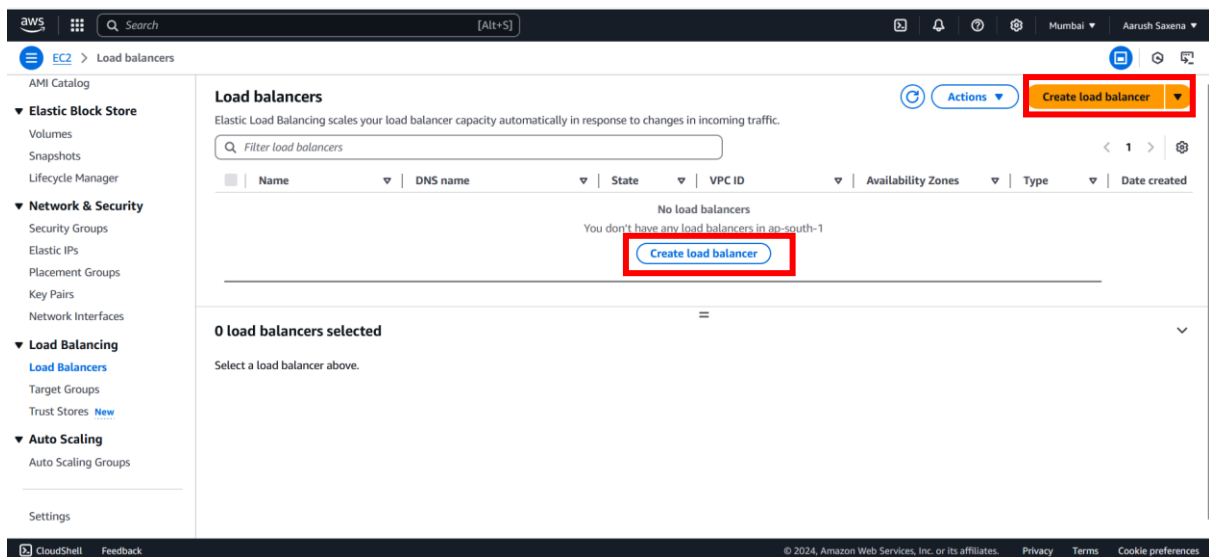


this is server2

Step 3 : On the left side scroll down and click on Load Balancers



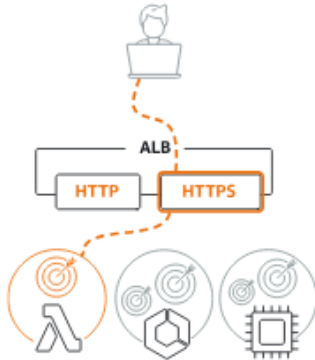
After clicking on it you can see window like this now click on create load balancer



After clicking on it you can see some types of load balancer in this pdf file we will discuss about previous generation load balancer.

Load balancer types

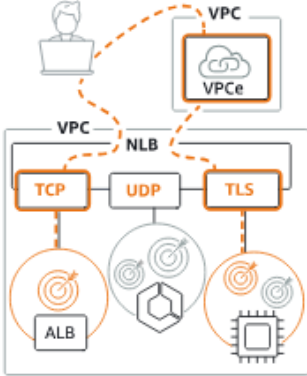
Application Load Balancer [Info](#)



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.

Create


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.

Create

Gateway Load Balancer [Info](#)

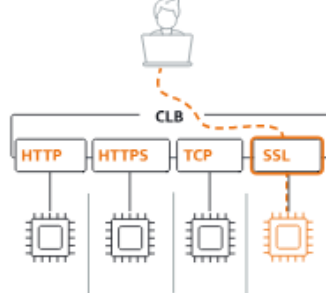


Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

▼ **Classic Load Balancer - previous generation**

Classic Load Balancer [Info](#)

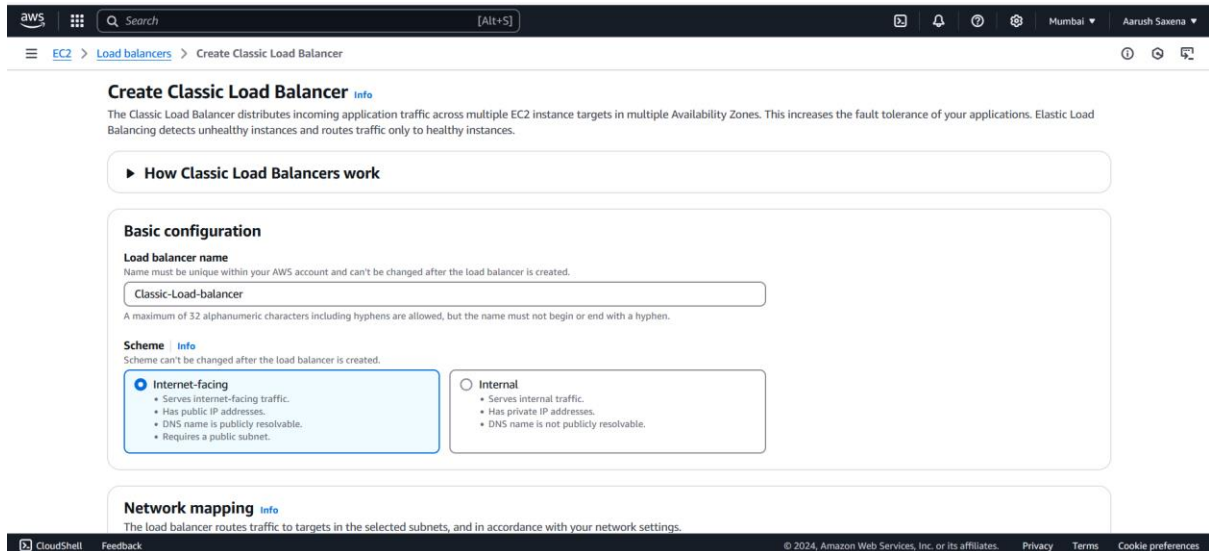


Choose a Classic Load Balancer when you have an existing application running in the EC2-Classic network.

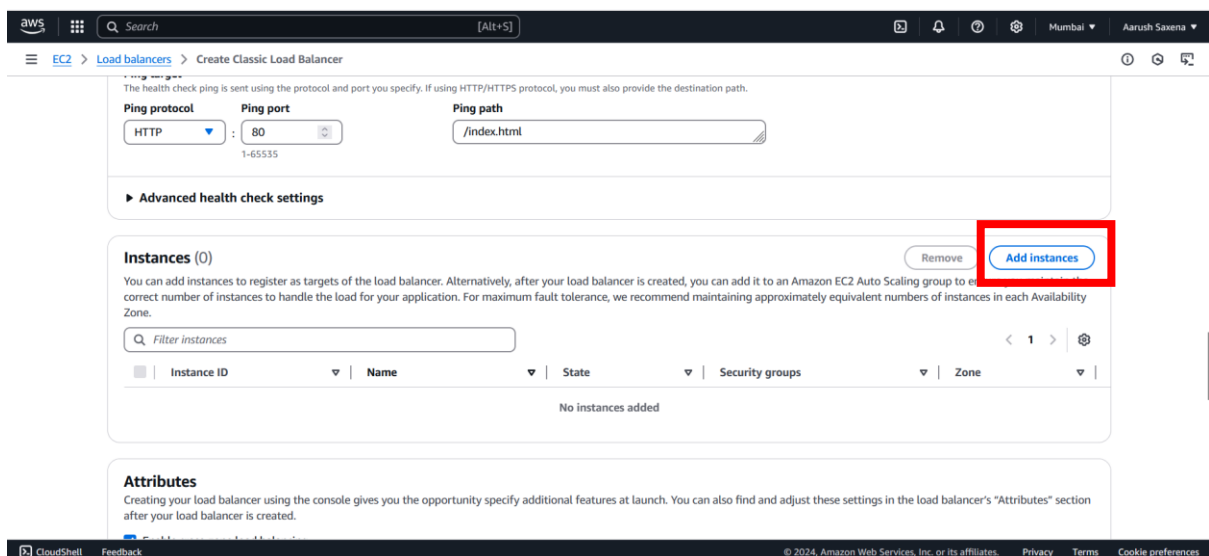
Create

Close

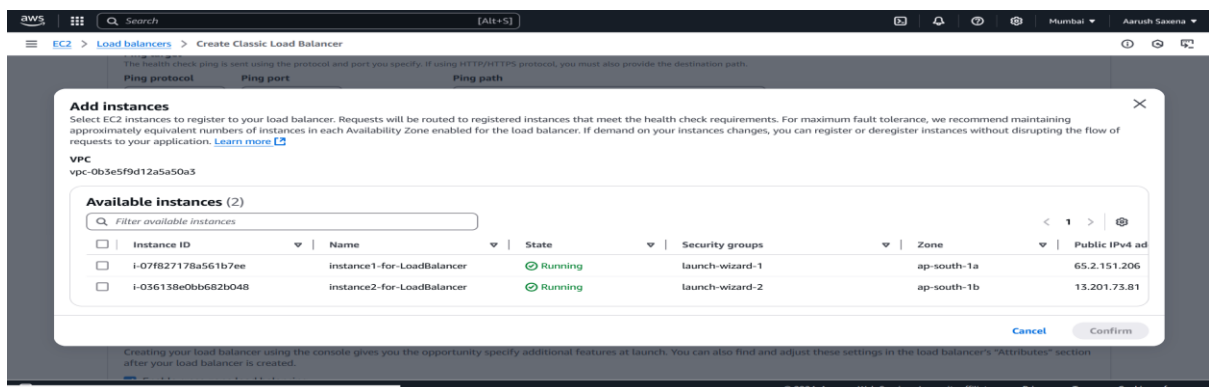
Step4: Click on Classic Load Balancer and click on create. Give a name to load balancer, scroll down and on network mapping select two availability zones in it and leave other settings to default settings.



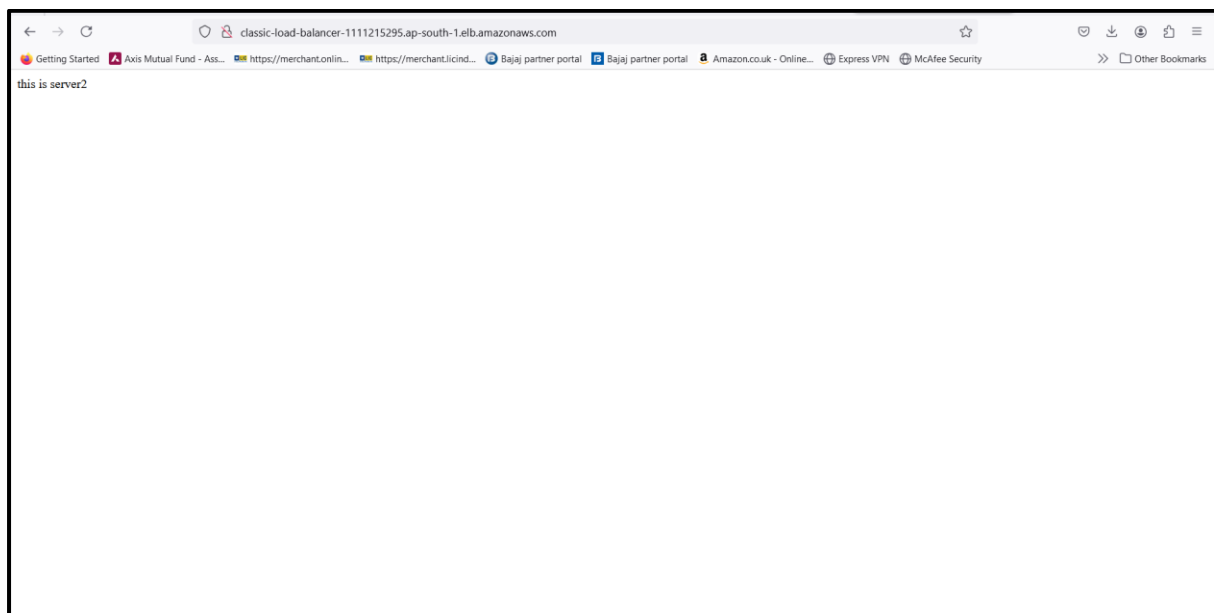
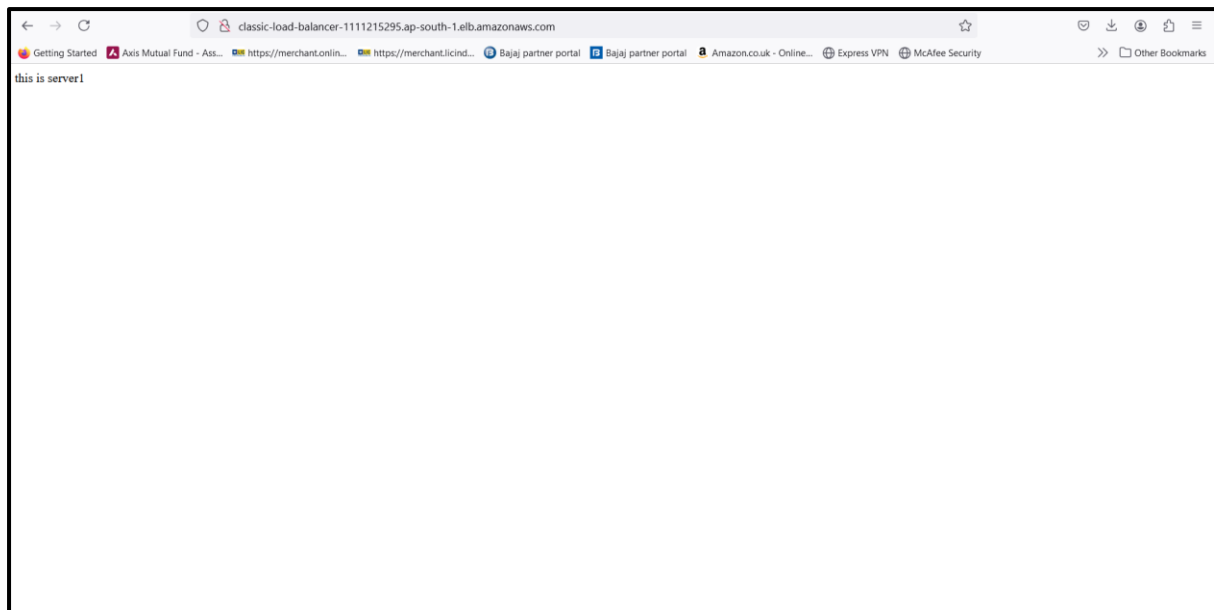
Scroll down and on Instances click on Add Instances



After clicking on it a window will appear that shows instances select both instances and click on confirm.



And now click on create load balancer.



From this approach you can see still you can access this data from hitting ip address of instance directly this is not a good approach.

Step 5: Go-to EC2 instance select the instance click on security under that you can see security groups click on it now click on edit inbound rules. Now delete all traffic rule and add a new rule with HTTP type and give source of classic load balancer.

aws [Search] [Alt+S] Mumbai Aarush Saxena

EC2 > Security Groups > sg-0c231074eb4168f4a - launch-wizard-1

Dashboard EC2 Global View Events

▼ Instances
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

sg-0c231074eb4168f4a - launch-wizard-1

Actions

Details

Security group name launch-wizard-1	Security group ID sg-0c231074eb4168f4a	Description launch-wizard-1 created 2024-11-24T13:33:53.456Z	VPC ID vpc-0b3e5f9d12a5a50a3
Owner 992382687678	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

Inbound rules (2) Manage tags Edit inbound rules

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-057f796fbfe24fe82	IPv4	SSH	TCP	22
-	sgr-01ecf03591b20a037	IPv4	All traffic	All	All

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

aws [Search] [Alt+S] Mumbai Aarush Saxena

EC2 > Security Groups > sg-0c231074eb4168f4a - launch-wizard-1 > Edit inbound rules

Edit inbound rules

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

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-057f796fbfe24fe82	SSH	TCP	22	Cus... 0.0.0.0/0	Delete
sgr-01ecf03591b20a037	All traffic	All	All	Cus...	Delete

Add rule

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.

Cancel Preview changes Save rules

Now give source id of classic load server and click on save rules.

aws [Search] [Alt+S] Mumbai Aarush Saxena

EC2 > Security Groups > sg-0c231074eb4168f4a - launch-wizard-1 > Edit inbound rules

Edit inbound rules

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

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-057f796fbfe24fe82	SSH	TCP	22	Cus... 0.0.0.0/0	Delete
-	HTTP	TCP	80	Cus... sg-0218bbebe69133f6b	Delete

Add rule

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.

Cancel Preview changes Save rules

To find this source id go to classic load balancer go to security a window will appear like this and on the top you can see source id

The screenshot shows the AWS Management Console interface. The browser address bar displays the URL: `https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#SecurityGroup:groupId=sg-0218bbebe69133f6b`. The console header shows the AWS logo and a search bar. The left-hand navigation pane includes sections for **Instances**, **Images**, and **Elastic Block Store**. The main content area is titled **sg-0218bbebe69133f6b - default** and contains a **Details** section with the following information:

Property	Value
Security group name	default
Security group ID	sg-0218bbebe69133f6b
Description	default VPC security group
VPC ID	vpc-0b3e5f9d12a5a50a3
Owner	992382687678
Inbound rules count	1 Permission entry
Outbound rules count	1 Permission entry

Below the details, there are tabs for **Inbound rules**, **Outbound rules**, **Sharing - new**, **VPC associations - new**, and **Tags**. The **Inbound rules** tab is active, showing a table with 1 rule:

Name	Security group rule ID	IP version	Type	Protocol	Port range
classic-load-balancer...	sgr-088a83df9681c3d14	IPv4	HTTP	TCP	80

The footer of the console shows the CloudShell icon, a feedback link, and the copyright notice: © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

Do the same with another instance.

Now you can see you cannot access the data while hitting ip directly.