Security Groups

A Security Group acts as a virtual firewall for your EC2 instances, managing both incoming and outgoing traffic.

As mentioned in my earlier post about creating an EC2 instance, Security Groups are important to know and think like this is firewall for your EC2 instance, controlling the flow of incoming and outgoing traffic.

Understanding these Security Groups is crucial, as they allow you to create rules that control the traffic. Each rule can either allow or deny traffic based on the IP Protocol. It's important to note that, by default, all incoming traffic is blocked, providing an initial layer of security.

Imagine our college with bouncers. These bouncers have a clear set of rules—they have to follow who's permitted to entry and who isn't. In Simple , if you have an ID card, you're in; without one, then access is denied. The bouncers strictly follow these guidelines.

They're like guardians at the gate, ensuring only those with valid Id's can entry. If anyone doesn't meet this specific requirement, they're blocked. The bouncers maintain a record of authorized guests, allowing them to move freely in and out as they meet the necessary criteria.

Think security is as a high priority task to secure our devices for additional security purpose you can add additional bouncers.

Security Group rules for different services and explain them in simple terms:

Type: SSH

Port Range: 22

Source: Usually, your own IP or a specific range of IPs. In simple Logging into server securely think like a special key to unlock your computer here for connecting purpose I will be using MobaXterm or you can use Putty and You can use terminal too.

HTTP : Hyper Test Transfer Protocol

Port Range : 80

source : 0.0.0.0/0 -> which means any IP Address

In Simple This rule lets your server receive and send regular web page requests.

HTTPS: Hypertext transfer Protocol

Type: HTTPS

Port Range : 443

source: 0.0.0.0/0 -> which means any IP Address

In Simple : Similar to HTTP, but this is for secure, encrypted communication.

FTP (File Transfer Protocol):

Type : FTP

Port Range : 21

source: Usually, your own IP or a specific range of IPs

Explanation: FTP is like a delivery service for files. This rule allows you to send and receive files to and from your server.

SMTP(Simple Mail Transfer Protocol)

Type: SMTP

Port Range: 25

Source: Usually, your own IP or a specific range of IPs.

Explanation: SMTP is like a service for emails. This rule allows your server to send out emails to others.

All Traffic (All Ports):

Type: All traffic

Port Range: All (0-65535)

Source: 0.0.0.0/0 (which means any IP address)

RDP (Remote Desktop Protocol):

Type: RDP

Port Range: 3389

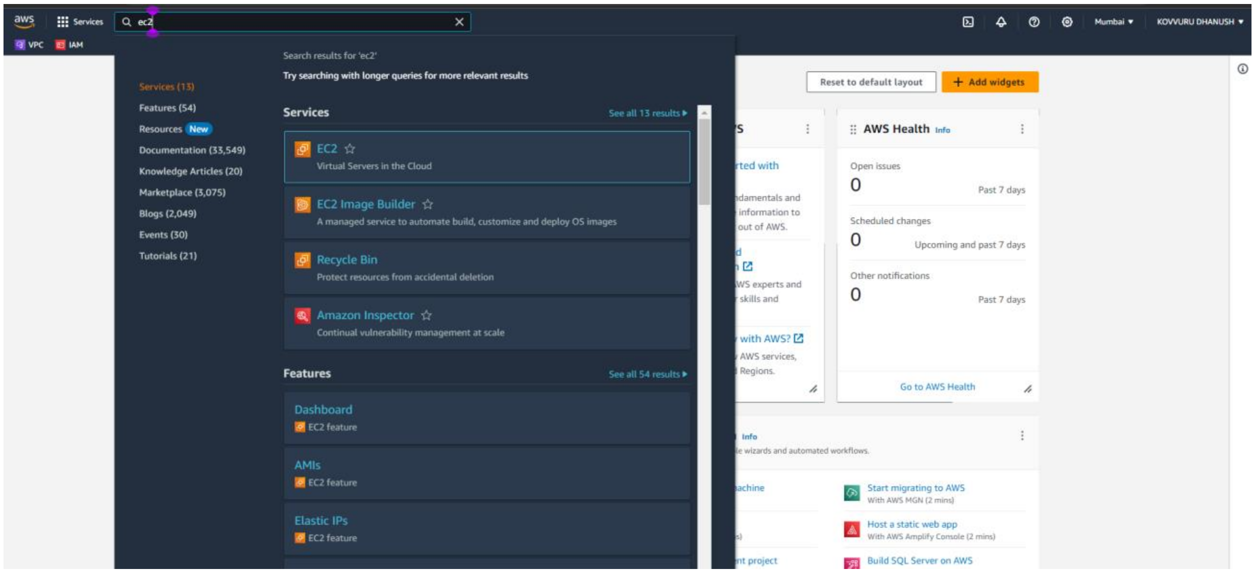
Source: Usually, your own IP or a specific range of IPs.

In Simple: This rule allows remote access to your Windows computer.

Custom Rules

Type: Custom (User-defined)

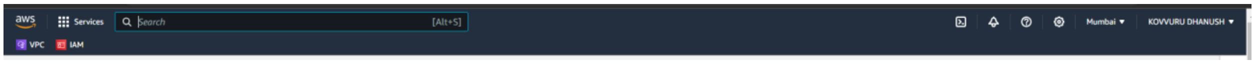
Port Range: You specify the port(s)



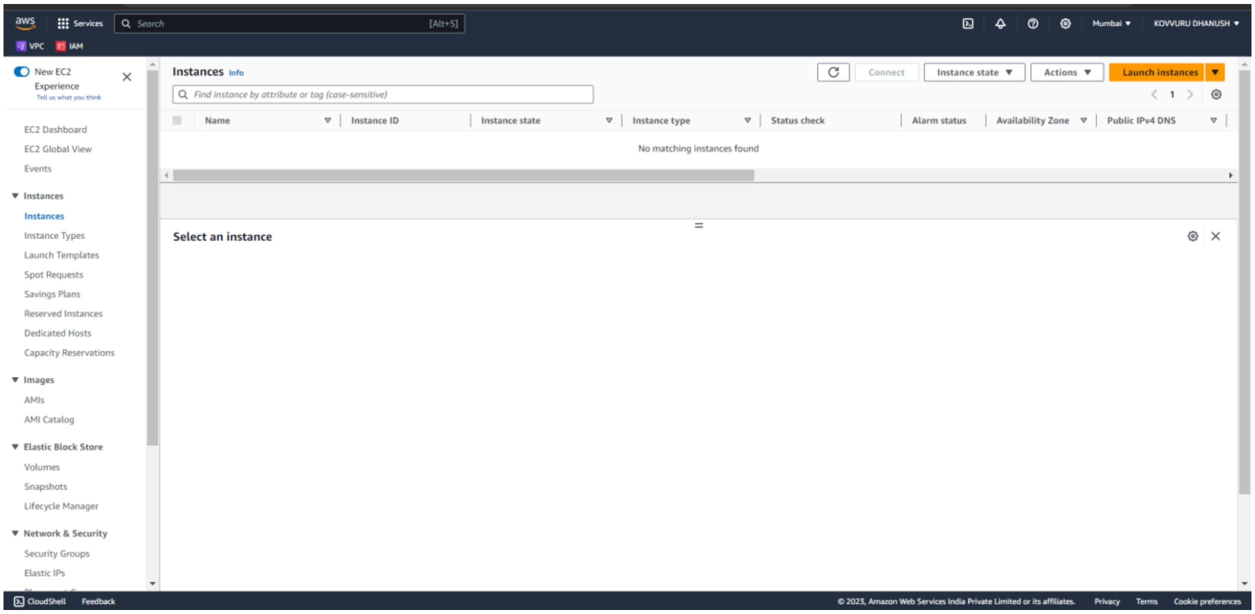
Search results for 'ec2'

Try searching with longer queries for more relevant results

In search bar type EC2.

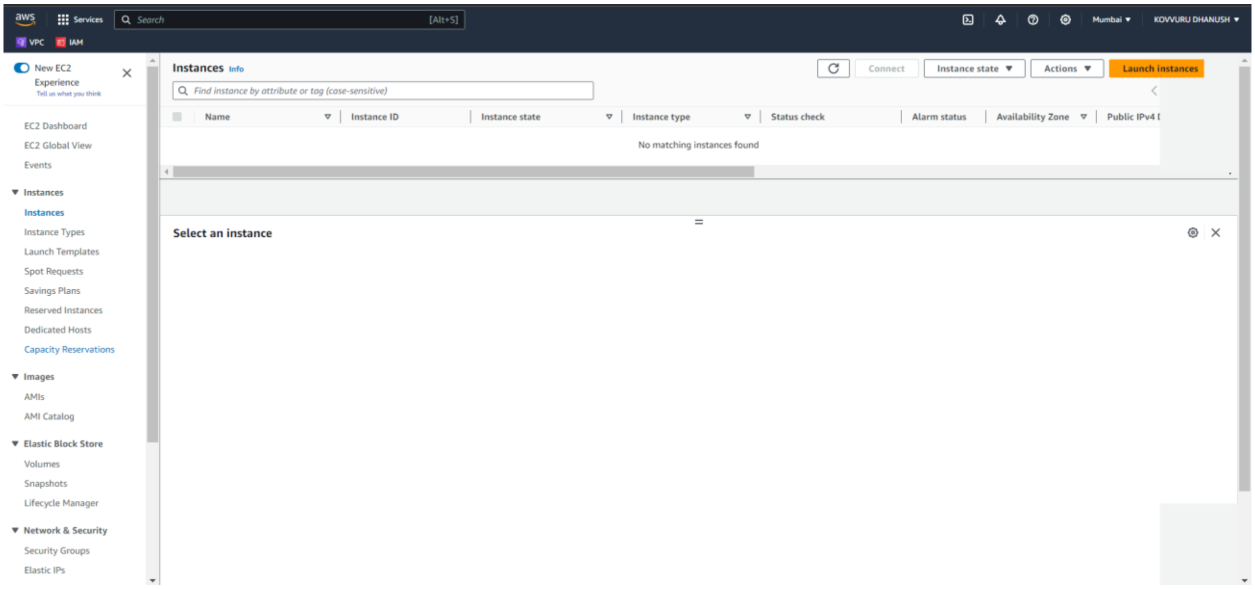


Here I’m choosing Mumbai.

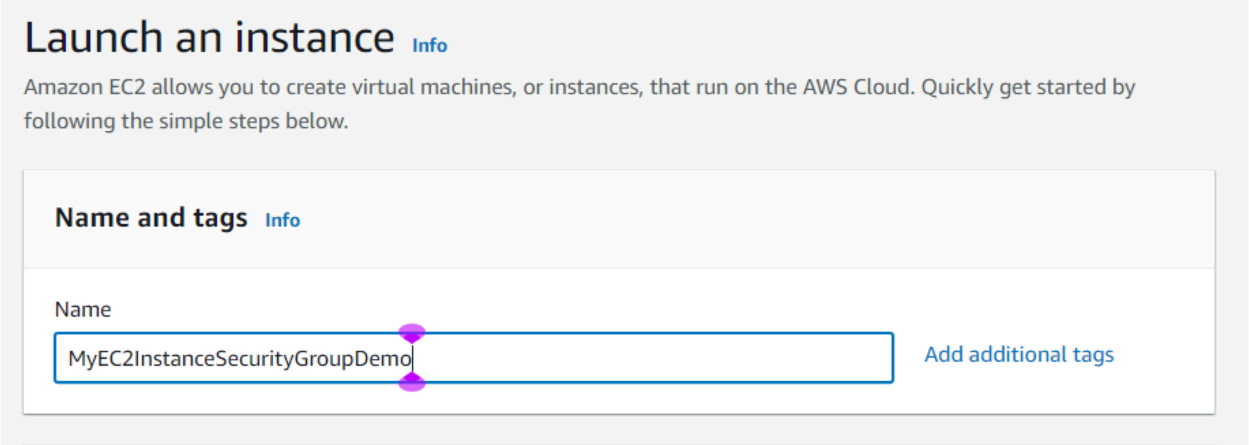


No matching instances found

In the left-hand side menu select Instances.



Click on launch 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.

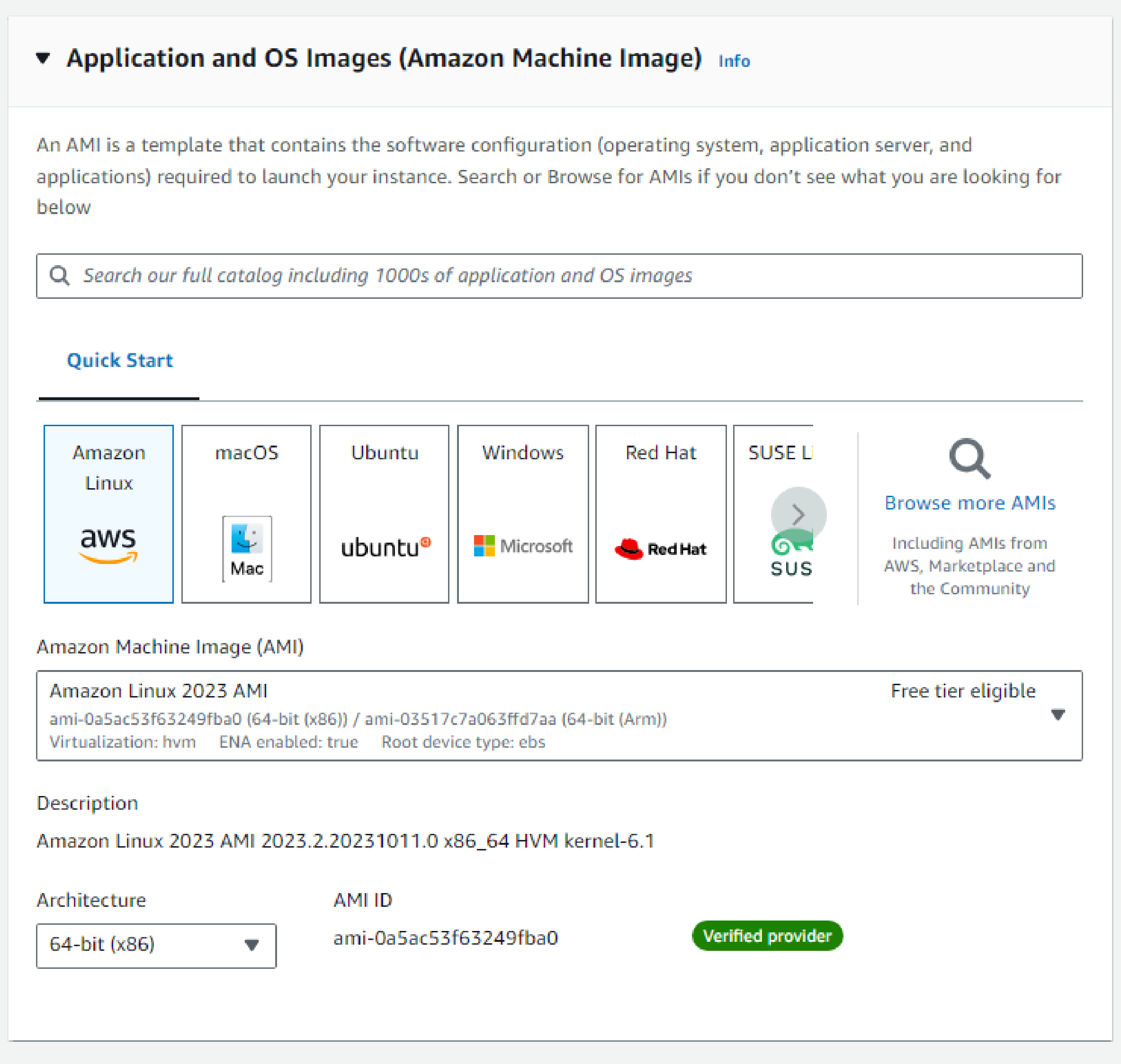
Name and tags Info

Name

MyEC2InstanceSecurityGroupDemo

Add additional tags

Here add your Instance Name.



▼ 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)

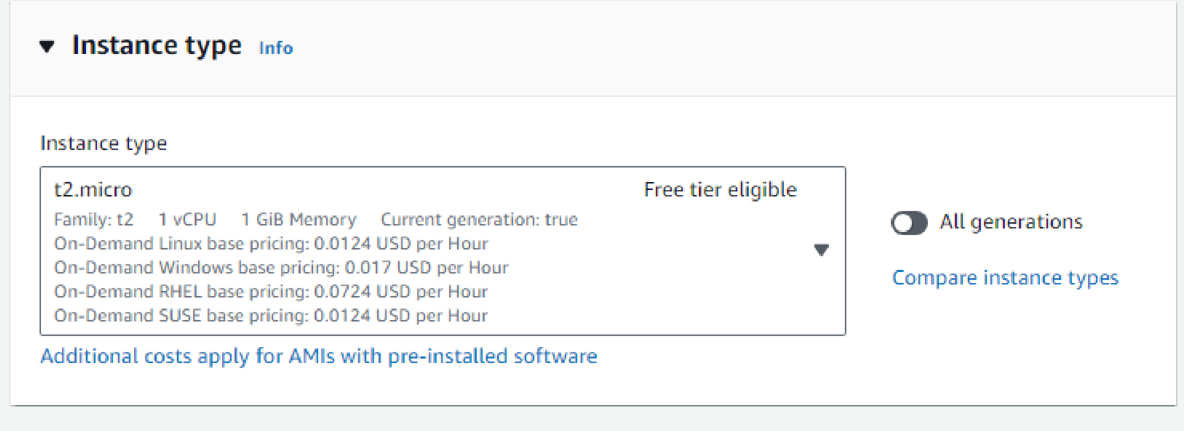
Amazon Linux 2023 AMI — Free tier eligible
ami-0a5ac53f63249fba0 (64-bit (x86)) / ami-03517c7a063ffd7aa (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.2.20231011.0 x86_64 HVM kernel-6.1

Architecture: 64-bit (x86)

AMI ID: ami-0a5ac53f63249fba0



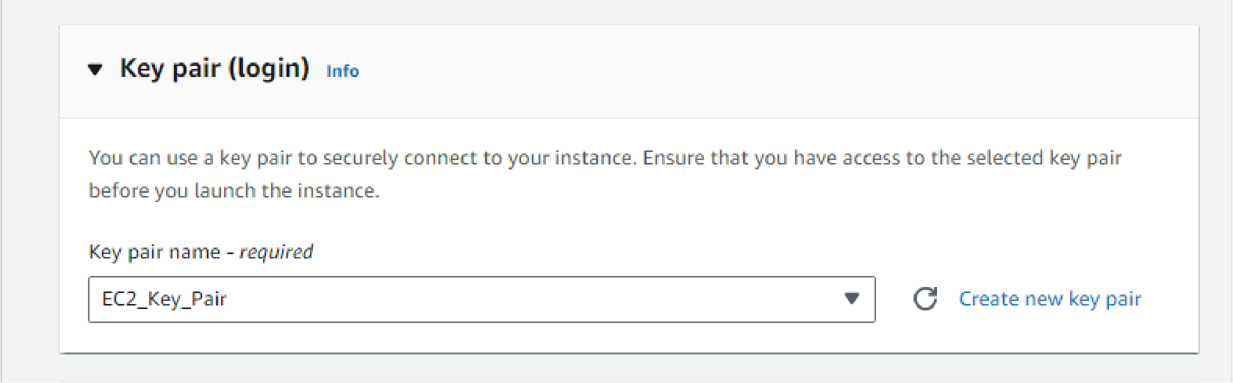
▼ Instance type Info

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: 0.0724 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

Additional costs apply for AMIs with pre-installed software

Here I'm using which is free tier eligible.



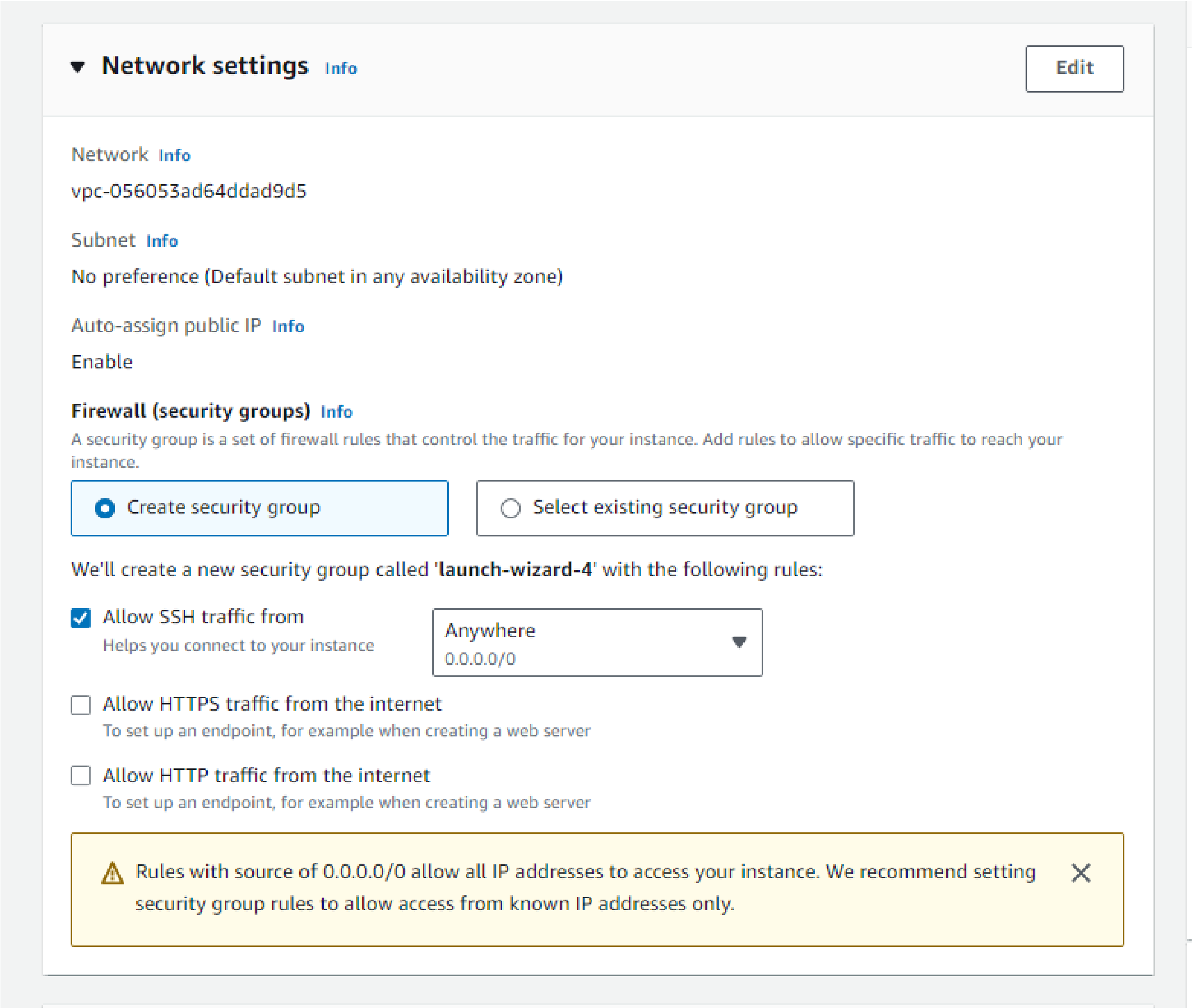
▼ Key pair (login) Info

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

Key pair name - *required*

EC2_Key_Pair ▼

Here I'm using existing key pair which I used in my previous post.



▼ Network settings Info

Network Info

vpc-056053ad64ddad9d5

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

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.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-4**' with the following rules:

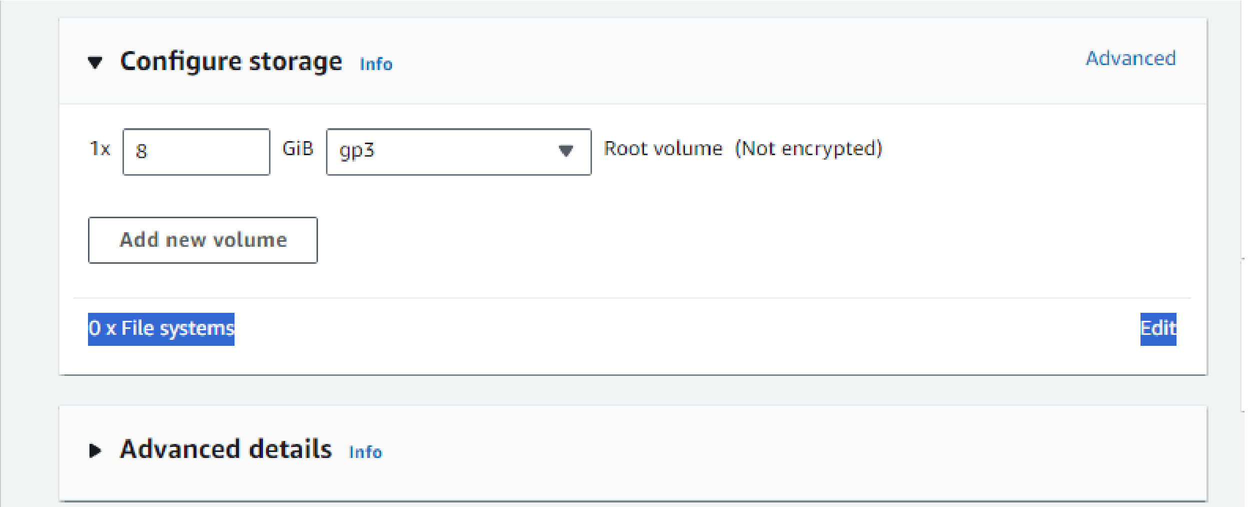
☑ Allow SSH traffic from — Anywhere 0.0.0.0/0 ▼
Helps you connect to your instance

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

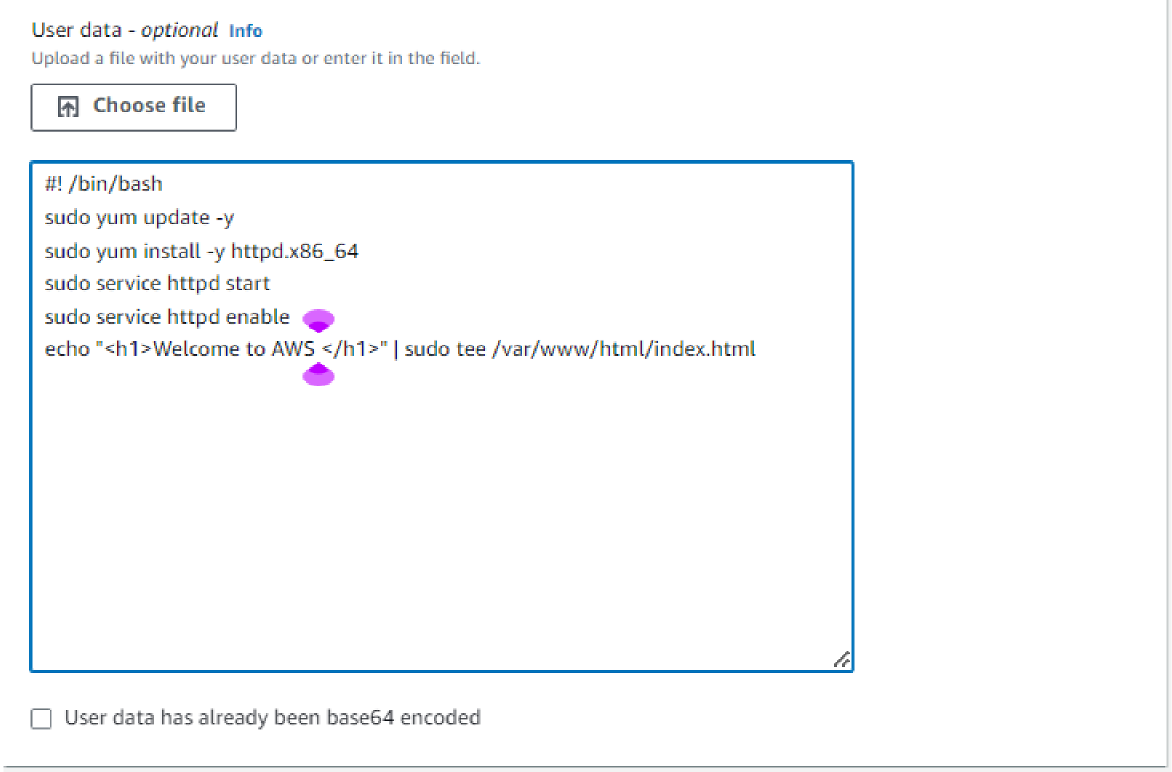
☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ 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.

Here I'm allowing SSH.



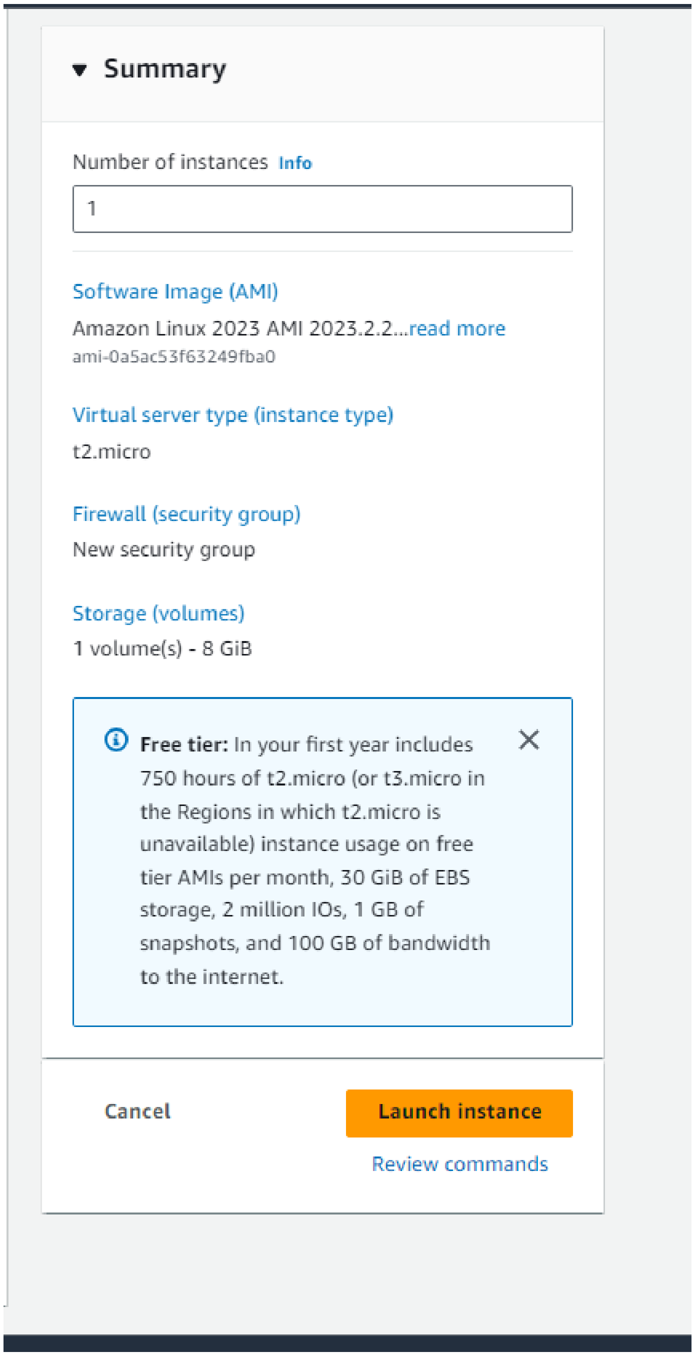
Click on advance details.


User data - *optional* Info
Upload a file with your user data or enter it in the field.
Choose file

```
#! /bin/bash
sudo yum update -y
sudo yum install -y httpd.x86_64
sudo service httpd start
sudo service httpd enable
echo "<h1>Welcome to AWS </h1>" | sudo tee /var/www/html/index.html
```

□ User data has already been base64 encoded

Add this user data.



▼ Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.2.2...read more

ami-0a5ac53f63249fba0

Virtual server type (instance type)

t2.micro

Firewall (security group)

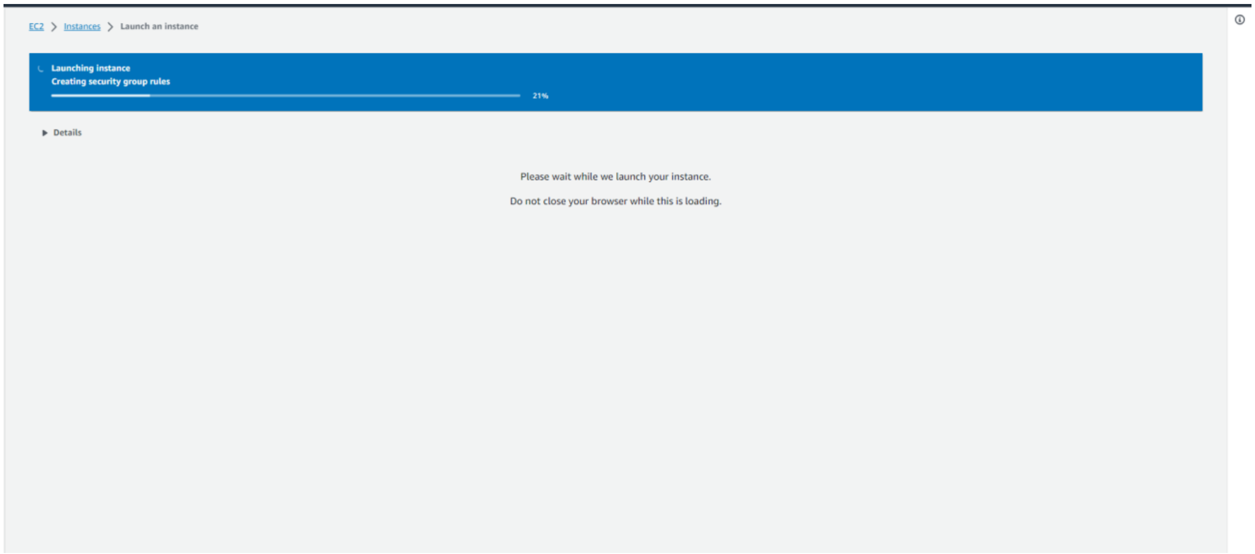
New security group

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, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Now click on launch instance.



EC2 > Instances > Launch an instance

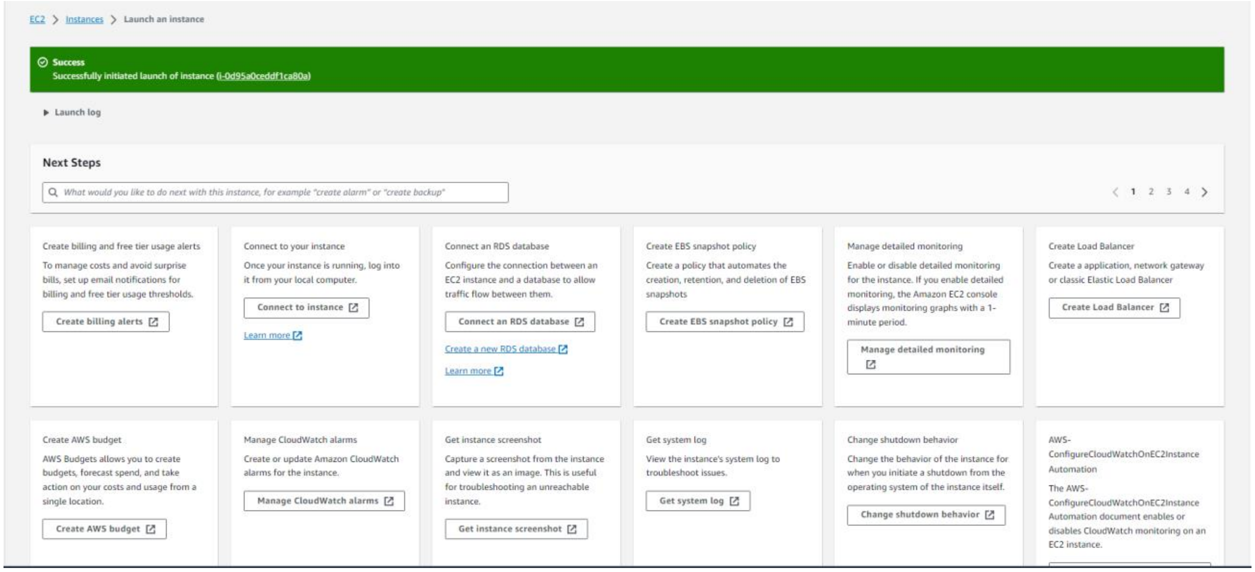
Launching instance
Creating security group rules
21%

Details

Please wait while we launch your instance.

Do not close your browser while this is loading.

It will take some time to create .



EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0d95a0ceddf1ca80a)

Launch log

Next Steps

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

< 1 2 3 4 >

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.
Create billing alerts

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

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

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

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.
Manage detailed monitoring

Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer
Create 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.
Create AWS budget

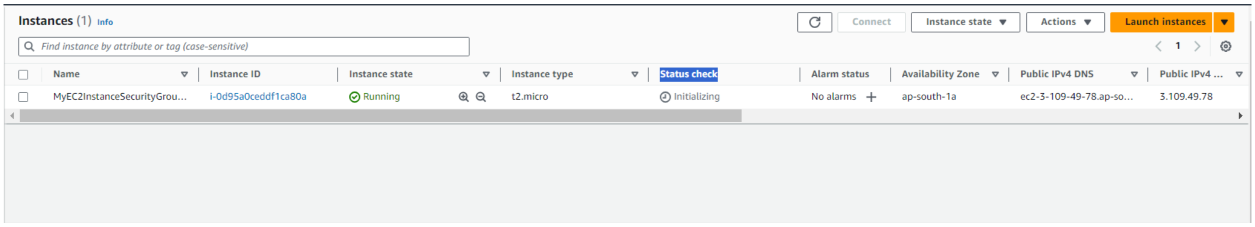
Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.
Manage CloudWatch alarms

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

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

Change shutdown behavior
Change the behavior of the instance for when you initiate a shutdown from the operating system of the instance itself.
Change shutdown behavior

AWS-ConfigureCloudWatchOnEC2Instance Automation
The AWS-ConfigureCloudWatchOnEC2Instance Automation document enables or disables CloudWatch monitoring on an EC2 instance.

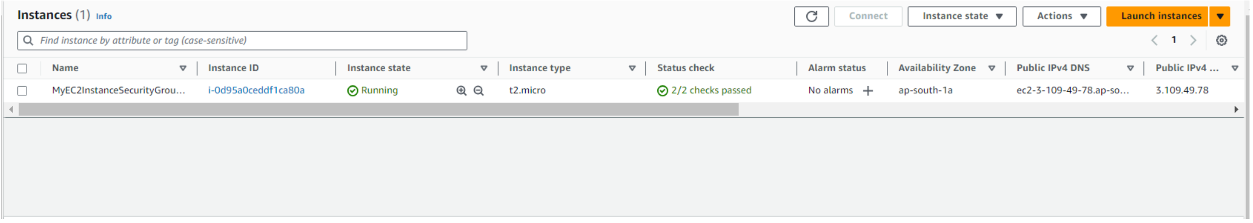


Instances (1) Info

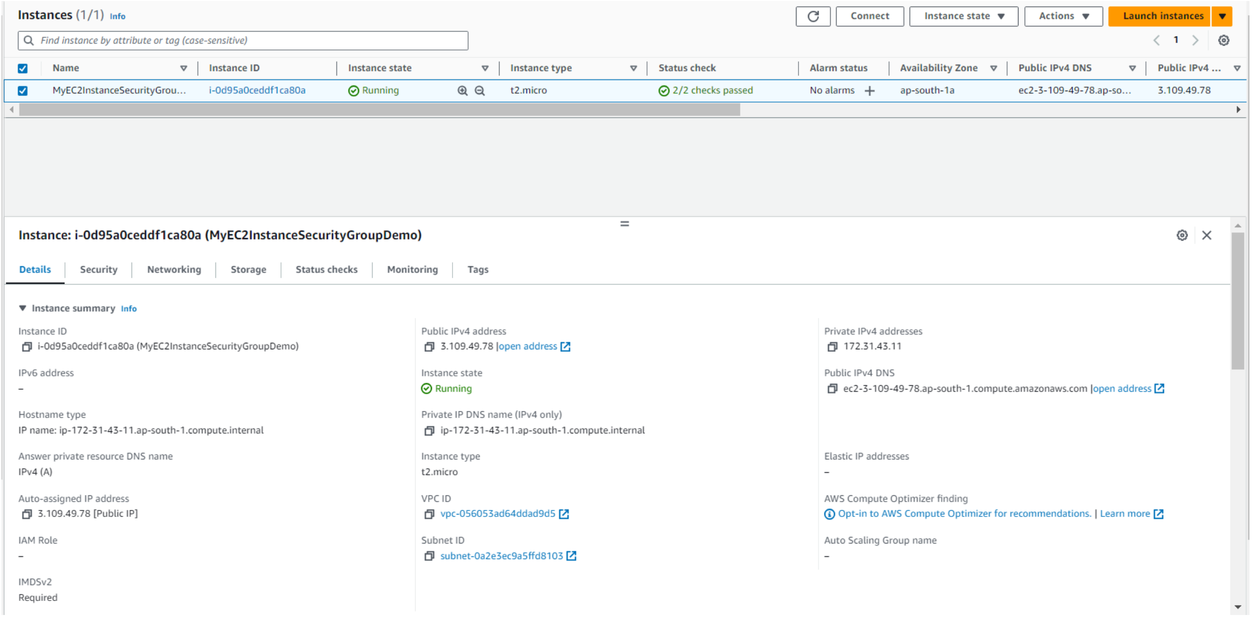
Find instance by attribute or tag (case-sensitive)

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
□	MyEC2InstanceSecurityGrou...	i-0d95a0ceddf1ca80a	Running	t2.micro	Initializing	No alarms +	ap-south-1a	ec2-3-109-49-78.ap-so...	3.109.49.78

It's initializing wait till 2/2 status check passed.



□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
□	MyEC2InstanceSecurityGrou...	i-0d95a0ceddf1ca80a	Running	t2.micro	2/2 checks passed	No alarms +	ap-south-1a	ec2-3-109-49-78.ap-so...	3.109.49.78



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
☑	MyEC2InstanceSecurityGrou...	i-0d95a0ceddf1ca80a	Running	t2.micro	2/2 checks passed	No alarms +	ap-south-1a	ec2-3-109-49-78.ap-so...	3.109.49.78

Instance: i-0d95a0ceddf1ca80a (MyEC2InstanceSecurityGroupDemo)

▼ Instance summary Info

Instance ID
i-0d95a0ceddf1ca80a (MyEC2InstanceSecurityGroupDemo)

IPv6 address
–

Hostname type
IP name: ip-172-31-43-11.ap-south-1.compute.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
3.109.49.78 [Public IP]

IAM Role
–

IMDSv2
Required

Public IPv4 address
3.109.49.78 |open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-43-11.ap-south-1.compute.internal

Instance type
t2.micro

VPC ID
vpc-056053ad64ddad9d5

Subnet ID
subnet-0a2e3ec9a5ffd8103

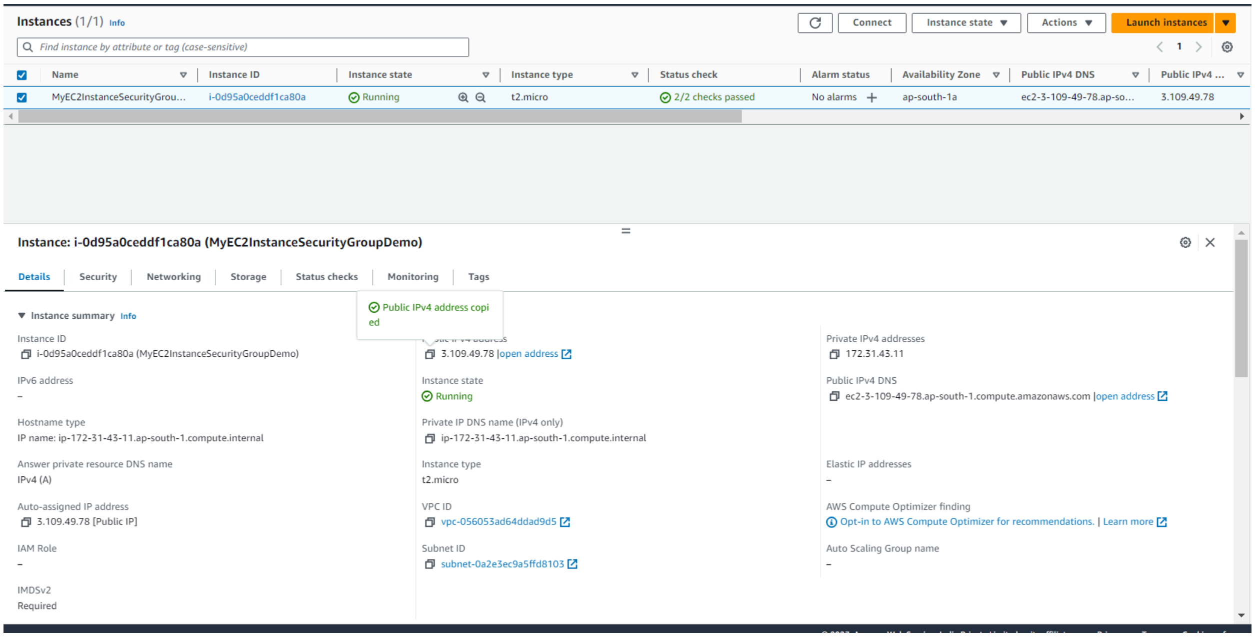
Private IPv4 addresses
172.31.43.11

Public IPv4 DNS
ec2-3-109-49-78.ap-south-1.compute.amazonaws.com |open address

Elastic IP addresses
–

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
☑	MyEC2InstanceSecurityGrou...	i-0d95a0ceddf1ca80a	Running	t2.micro	2/2 checks passed	No alarms +	ap-south-1a	ec2-3-109-49-78.ap-so...	3.109.49.78

Instance: i-0d95a0ceddf1ca80a (MyEC2InstanceSecurityGroupDemo)

▼ Instance summary Info

Public IPv4 address copied

Instance ID
i-0d95a0ceddf1ca80a (MyEC2InstanceSecurityGroupDemo)

IPv6 address
–

Hostname type
IP name: ip-172-31-43-11.ap-south-1.compute.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
3.109.49.78 [Public IP]

IAM Role
–

IMDSv2
Required

Public IPv4 address
3.109.49.78 |open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-43-11.ap-south-1.compute.internal

Instance type
t2.micro

VPC ID
vpc-056053ad64ddad9d5

Subnet ID
subnet-0a2e3ec9a5ffd8103

Private IPv4 addresses
172.31.43.11

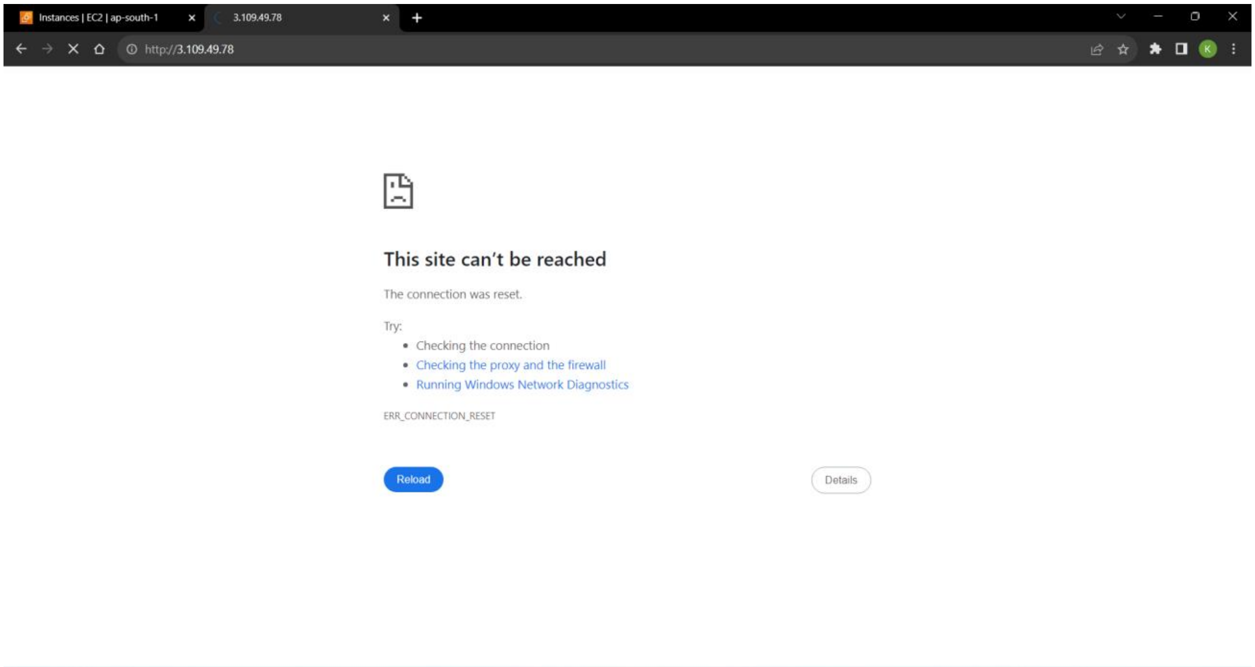
Public IPv4 DNS
ec2-3-109-49-78.ap-south-1.compute.amazonaws.com |open address

Elastic IP addresses
–

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–

Copy this pubic Ip and paste it on a new tab.



This site can't be reached

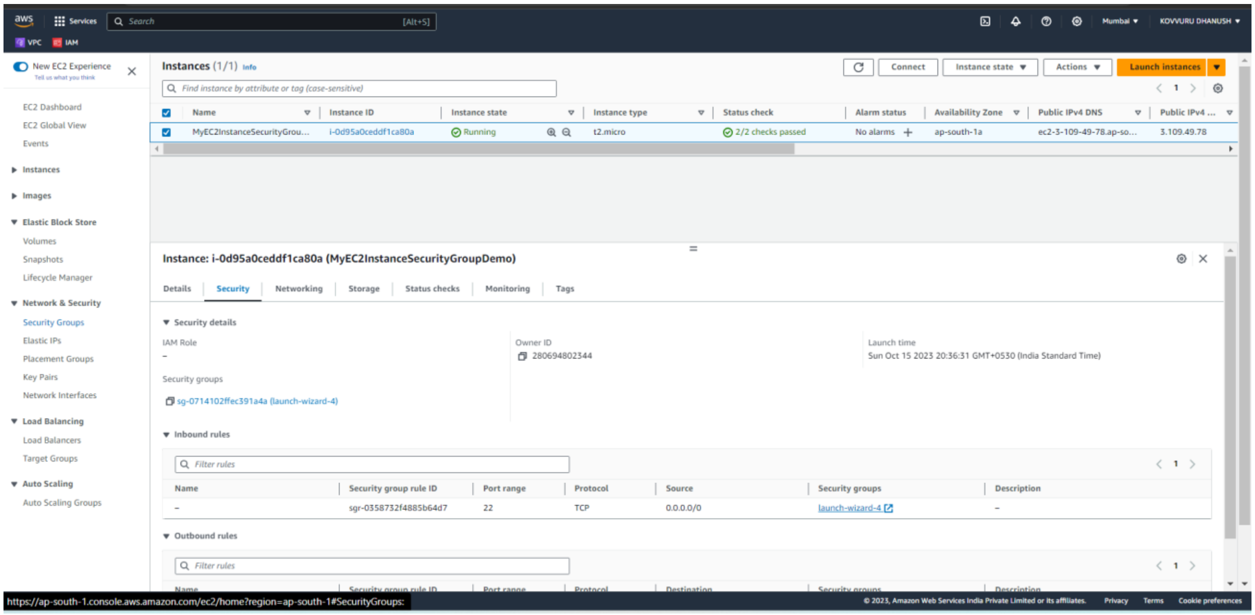
The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET

You will get like this.



Instances (1/1) 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 IPv4 ...
☑	MyEC2InstanceSecurityGrou...	i-0d95a0ceddf1ca80a	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms +	ap-south-1a	ec2-3-109-49-78.ap-so...	3.109.49.78

Instance: i-0d95a0ceddf1ca80a (MyEC2InstanceSecurityGroupDemo)

Security details

IAM Role
–

Owner ID
280694802344

Launch time
Sun Oct 15 2023 20:36:31 GMT+0530 (India Standard Time)

Security groups
sg-0714102ffec391a4a (launch-wizard-4)

Inbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
–	sgr-0358732f4885b64d7	22	TCP	0.0.0.0/0	launch-wizard-4	–

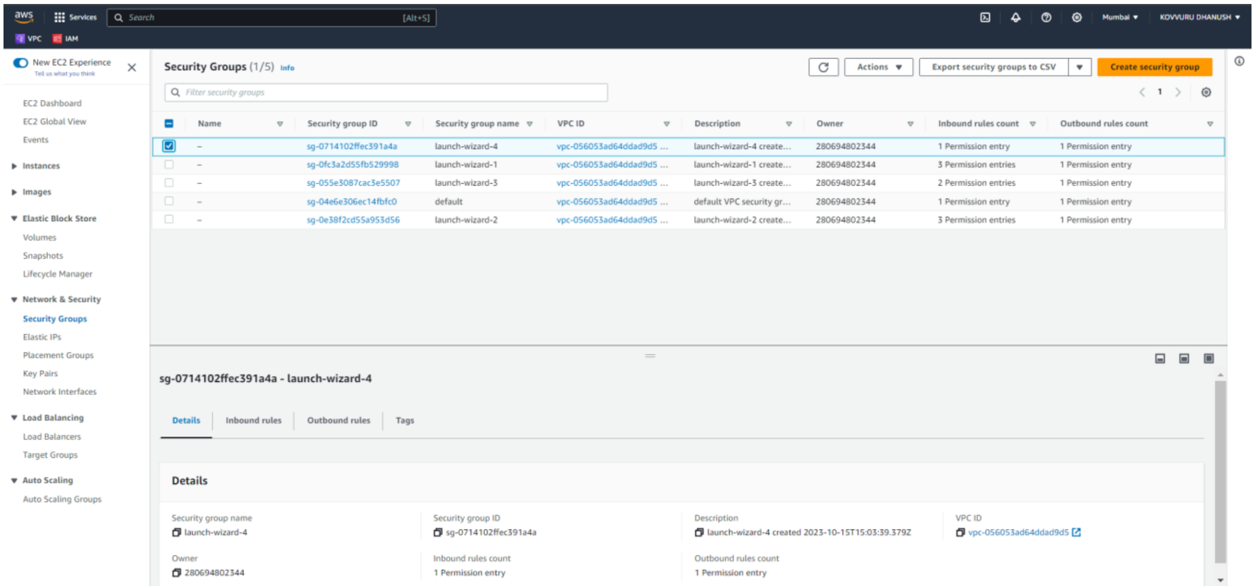
Outbound rules

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description

https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#SecurityGroups:

© 2023, Amazon Web Services India Private Limited or its affiliates.

In the left-hand menu select Security Groups.



Security Groups (1/5) Info

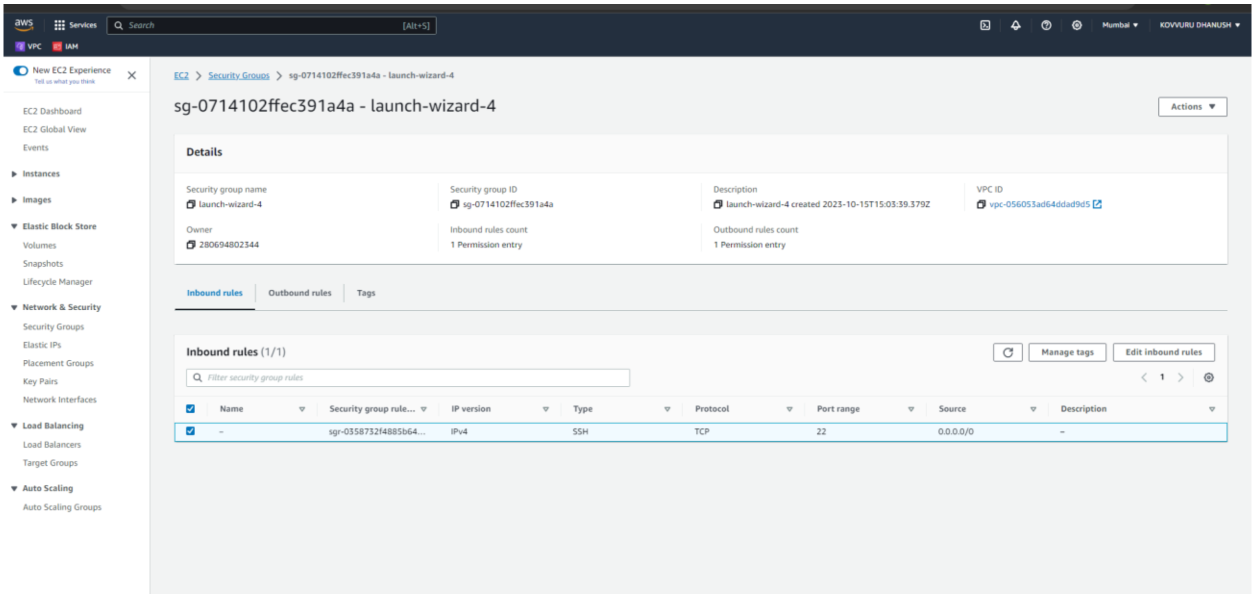
☐	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
☑	–	sg-0714102ffec391a4a	launch-wizard-4	vpc-056053ad64ddad9d5 ...	launch-wizard-4 create...	280694802344	1 Permission entry	1 Permission entry
☐	–	sg-0fc3a2d55fb529998	launch-wizard-1	vpc-056053ad64ddad9d5 ...	launch-wizard-1 create...	280694802344	3 Permission entries	1 Permission entry
☐	–	sg-055e3087cac3e5507	launch-wizard-3	vpc-056053ad64ddad9d5 ...	launch-wizard-3 create...	280694802344	2 Permission entries	1 Permission entry
☐	–	sg-04e6e306ec14fbfc0	default	vpc-056053ad64ddad9d5 ...	default VPC security gr...	280694802344	1 Permission entry	1 Permission entry
☐	–	sg-0e38f2cd55a953d56	launch-wizard-2	vpc-056053ad64ddad9d5 ...	launch-wizard-2 create...	280694802344	3 Permission entries	1 Permission entry

sg-0714102ffec391a4a - launch-wizard-4

Details

Security group name: launch-wizard-4
Security group ID: sg-0714102ffec391a4a
Description: launch-wizard-4 created 2023-10-15T15:03:39.379Z
VPC ID: vpc-056053ad64ddad9d5
Owner: 280694802344
Inbound rules count: 1 Permission entry
Outbound rules count: 1 Permission entry

Here in my case Launch-wizard-4.



sg-0714102ffec391a4a - launch-wizard-4

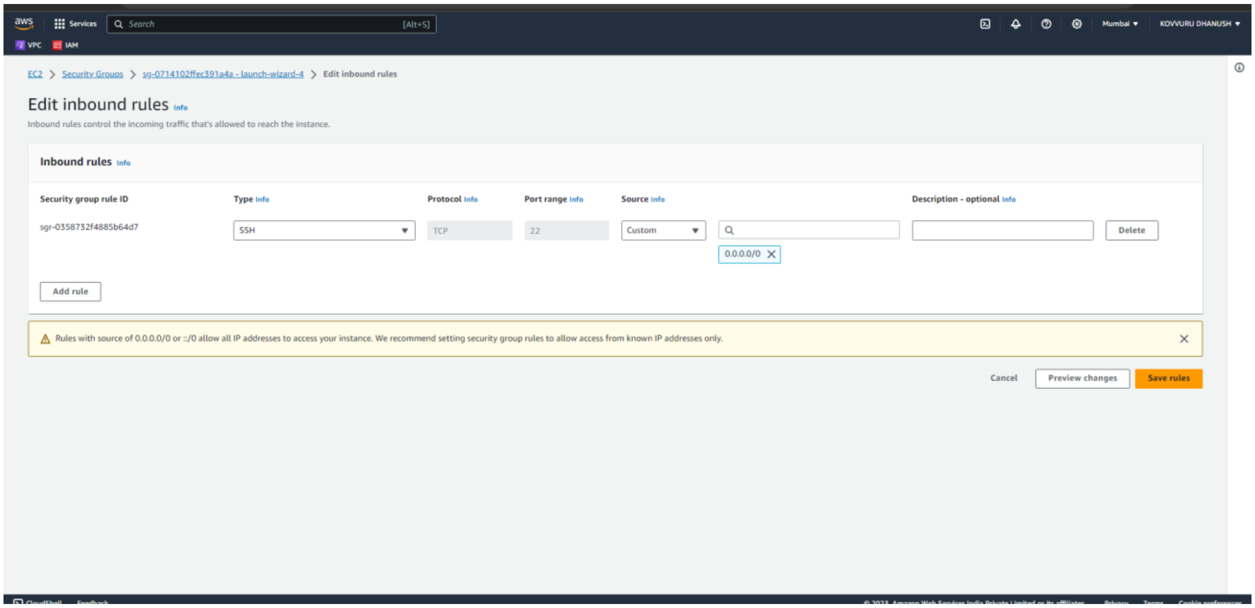
Details

Security group name: launch-wizard-4
Security group ID: sg-0714102ffec391a4a
Description: launch-wizard-4 created 2023-10-15T15:03:39.379Z
VPC ID: vpc-056053ad64ddad9d5
Owner: 280694802344
Inbound rules count: 1 Permission entry
Outbound rules count: 1 Permission entry

Inbound rules (1/1)

☑	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☑	–	sgr-0358732f4885b64...	IPv4	SSH	TCP	22	0.0.0.0/0	–

Now click on edit inbound rules.



Edit inbound rules Info

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

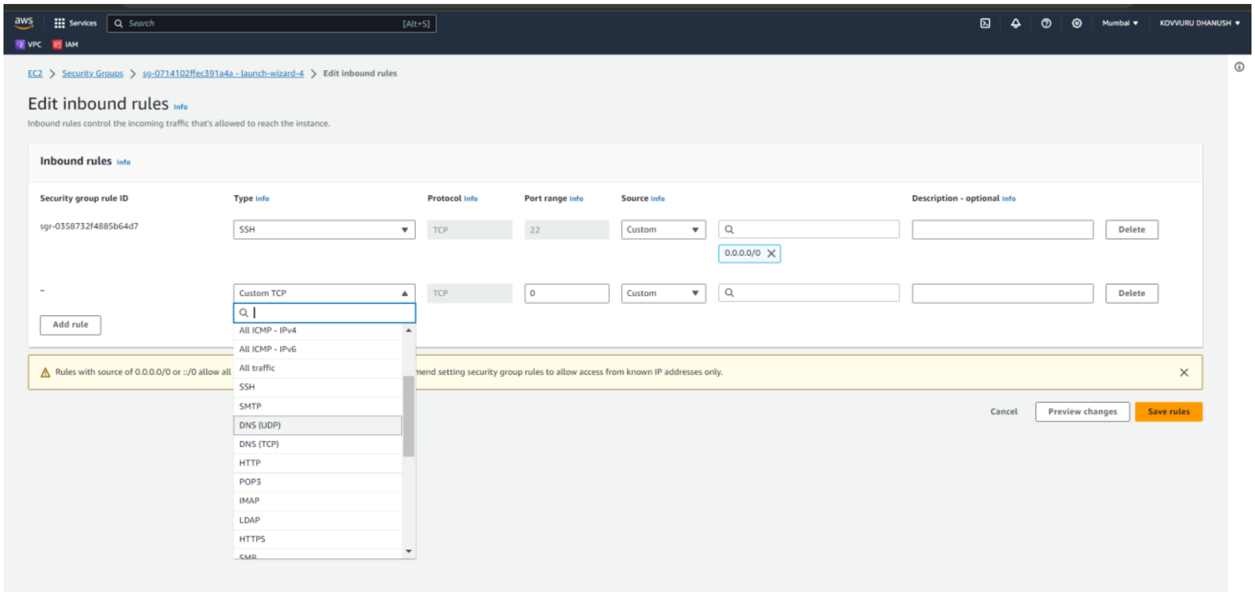
Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0358732f4885b64d7	SSH	TCP	22	Custom	0.0.0.0/0		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.

Now click on add rule.

Here if you observe I mentioned few protocols right here I'm adding HTTP protocol as of now to see it's working or not.



Edit inbound rules Info

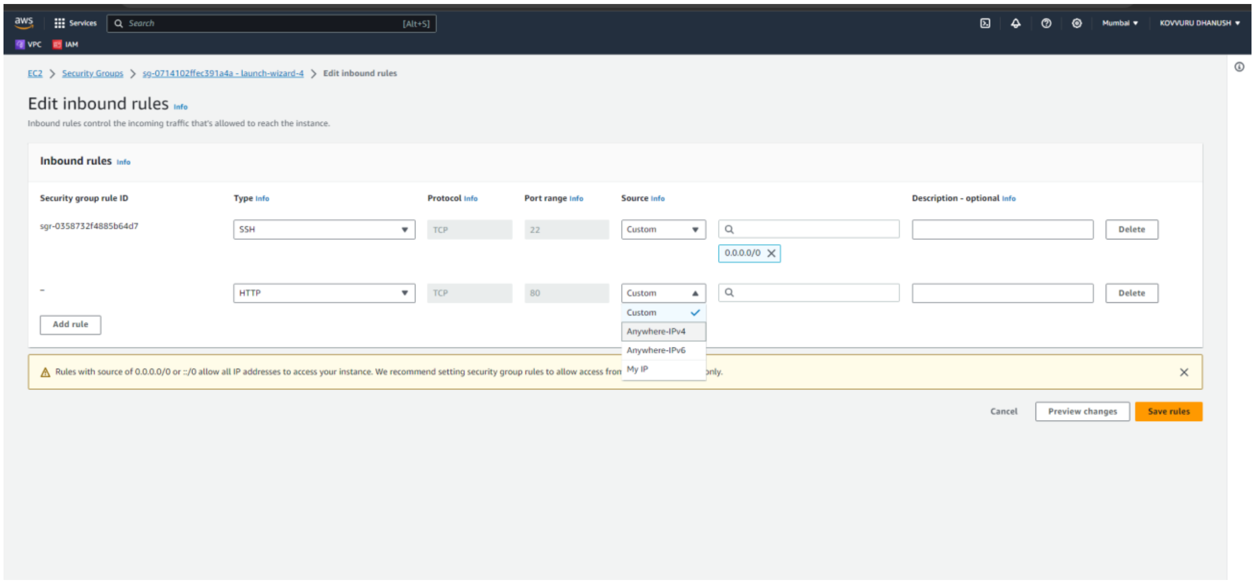
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0358732f4885b64d7	SSH	TCP	22	Custom	0.0.0.0/0		Delete
-	Custom TCP	TCP	0	Custom			Delete

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

Now click on HTTP.



EC2 > Security Groups > sg-0714102ffec391a4a - launch-wizard-4 > Edit inbound rules

Edit inbound rules Info

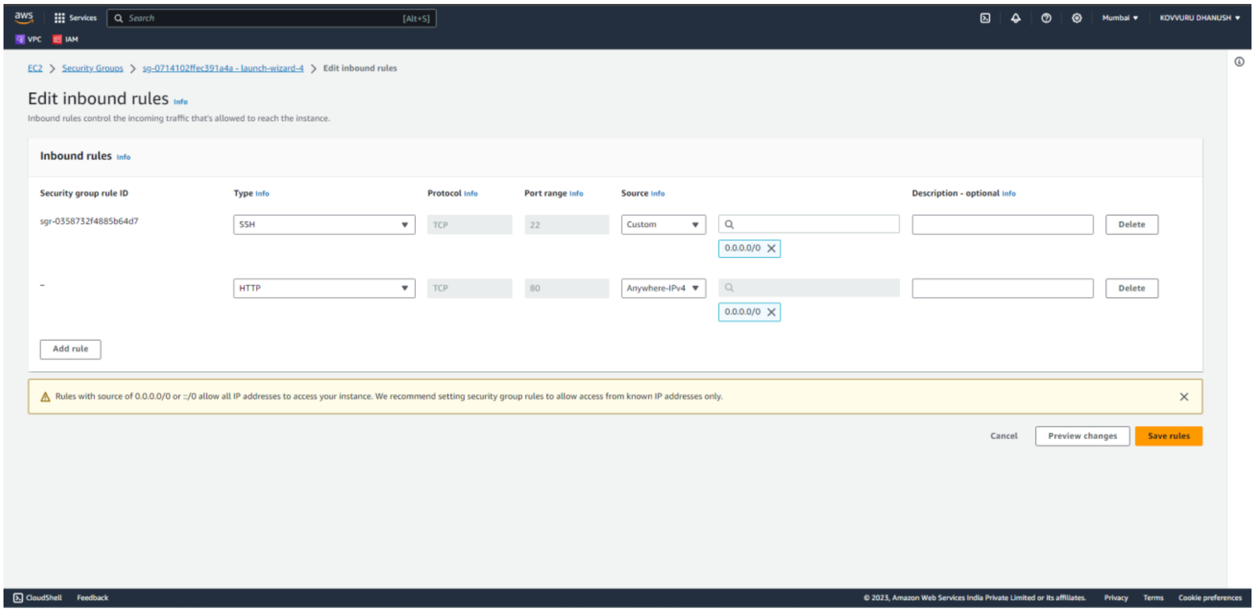
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-0358732f4885b64d7	SSH	TCP	22	Custom	0.0.0.0/0	
-	HTTP	TCP	80	Custom		

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 fron ... only.

Now click on IPV4 Anywhere.



EC2 > Security Groups > sg-0714102ffec391a4a - launch-wizard-4 > Edit inbound rules

Edit inbound rules Info

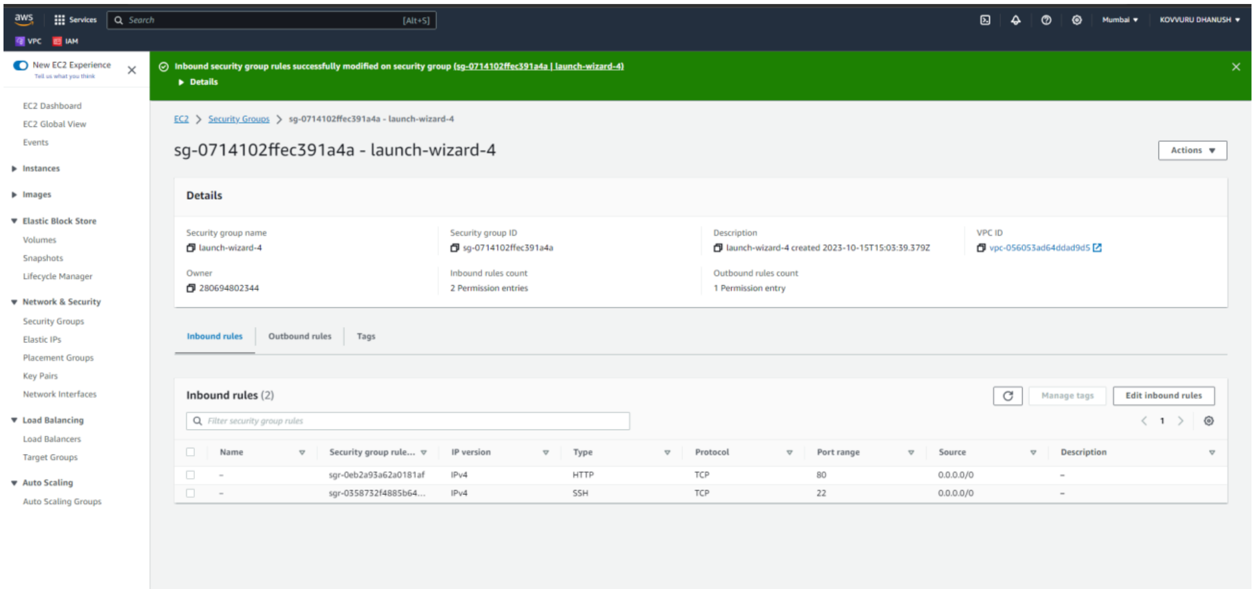
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-0358732f4885b64d7	SSH	TCP	22	Custom	0.0.0.0/0	
-	HTTP	TCP	80	Anywhere-IPv4	0.0.0.0/0	

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.

Now click on save rules.



Inbound security group rules successfully modified on security group (sg-0714102ffec391a4a | launch-wizard-4)

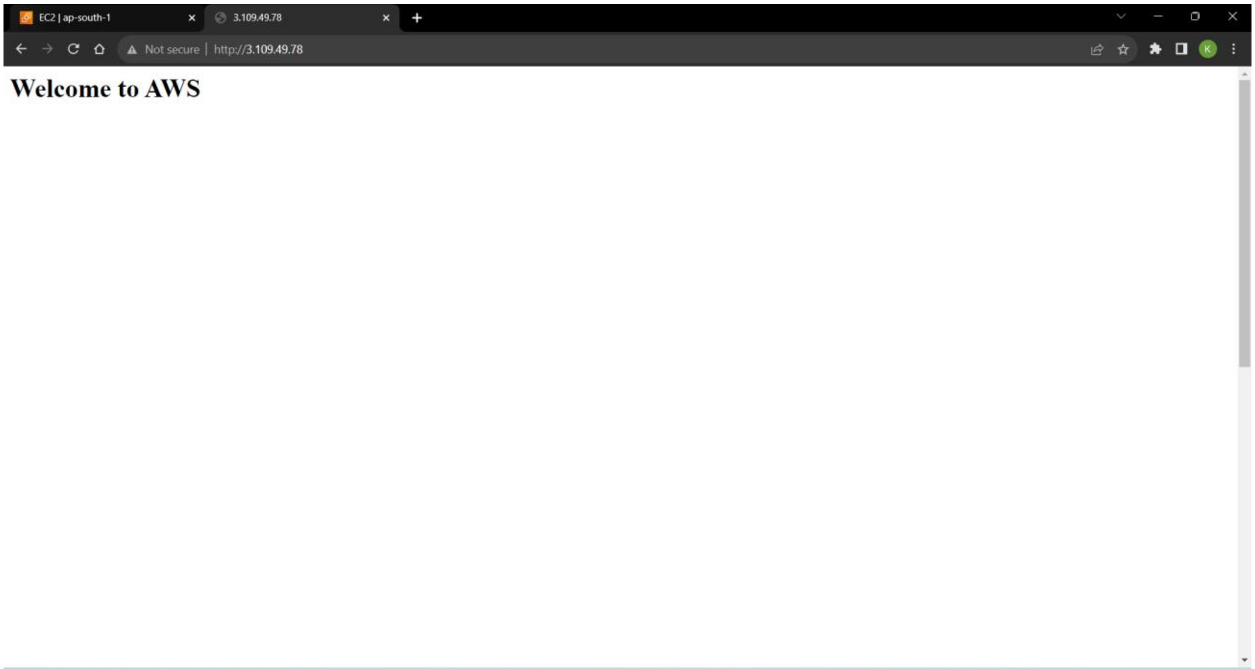
sg-0714102ffec391a4a - launch-wizard-4

Details

Security group name: launch-wizard-4
Security group ID: sg-0714102ffec391a4a
Description: launch-wizard-4 created 2023-10-15T15:03:39.379Z
VPC ID: vpc-056053ad64ddad9d5
Owner: 280694802344
Inbound rules count: 2 Permission entries
Outbound rules count: 1 Permission entry

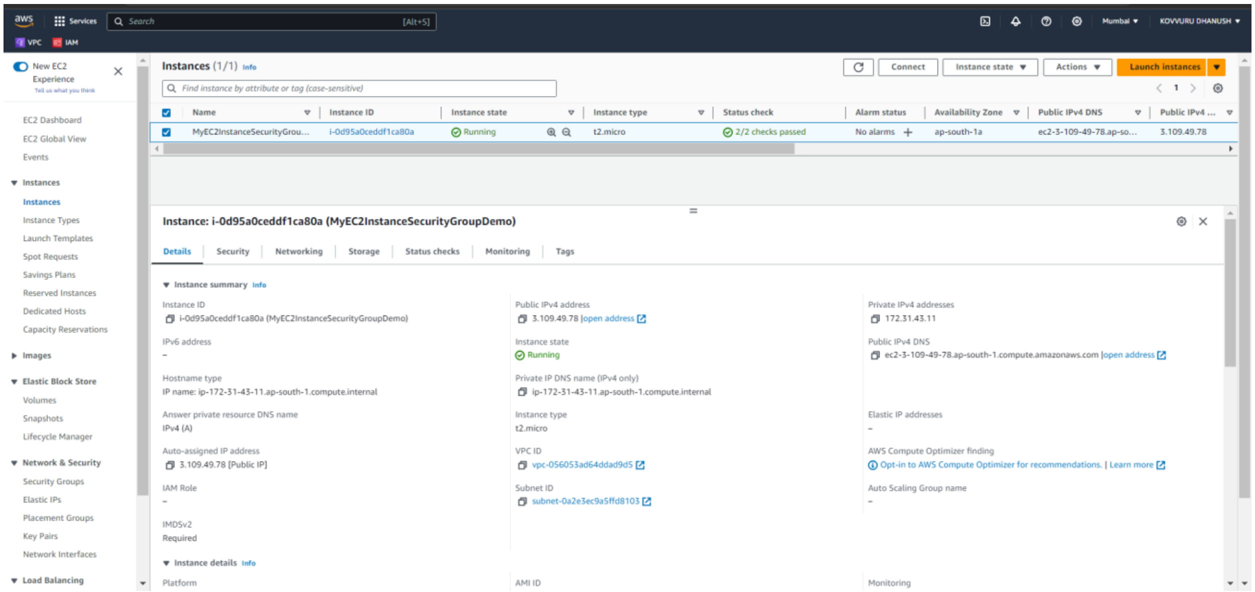
Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
–	sgr-0eb2a93a62a0181af	IPv4	HTTP	TCP	80	0.0.0.0/0	–
–	sgr-0358732f4885b64...	IPv4	SSH	TCP	22	0.0.0.0/0	–



Welcome to AWS

See when I refresh the page, I got the output mean HTTP helping to access this page.



Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
☑	MyEC2InstanceSecurityGrou...	i-0d95a0ceddf1ca80a	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	ec2-3-109-49-78.ap-so...	3.109.49.78

Instance: i-0d95a0ceddf1ca80a (MyEC2InstanceSecurityGroupDemo)

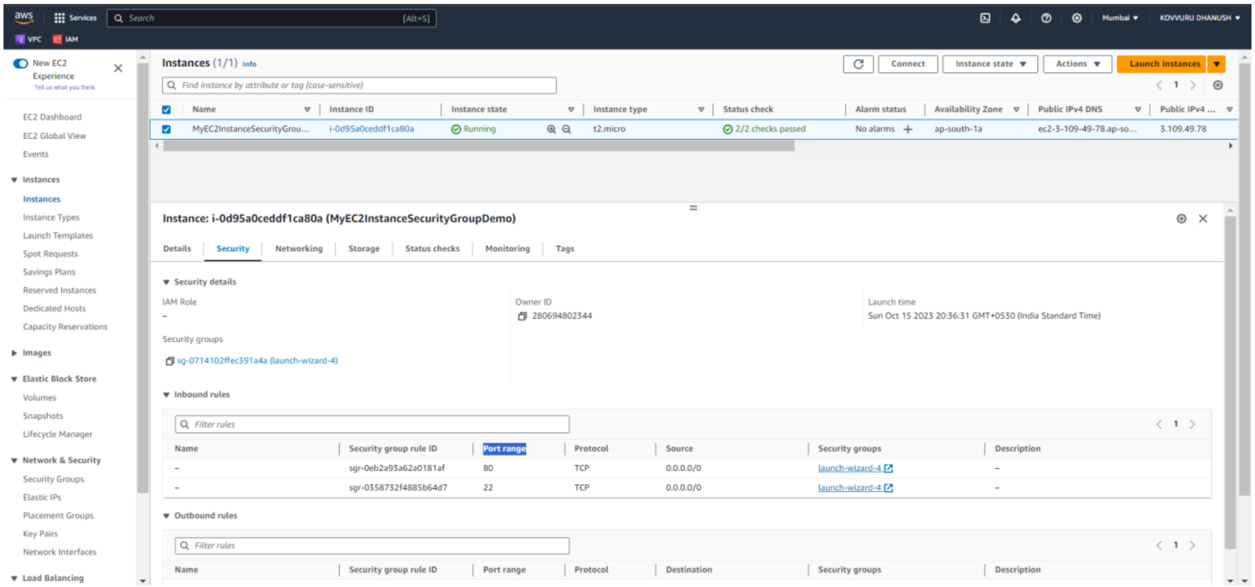
Instance summary Info

Instance ID: i-0d95a0ceddf1ca80a (MyEC2InstanceSecurityGroupDemo)
Public IPv4 address: 3.109.49.78 |open address
Private IPv4 addresses: 172.31.43.11
IPv6 address: –
Instance state: Running
Public IPv4 DNS: ec2-3-109-49-78.ap-south-1.compute.amazonaws.com |open address
Hostname type: IP name: ip-172-31-43-11.ap-south-1.compute.internal
Private IP DNS name (IPv4 only): ip-172-31-43-11.ap-south-1.compute.internal
Answer private resource DNS name: IPv4 (A)
Instance type: t2.micro
Elastic IP addresses: –
Auto-assigned IP address: 3.109.49.78 [Public IP]
VPC ID: vpc-056053ad64ddad9d5
AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role: –
Subnet ID: subnet-0a2e3ec9a5ffd8103
Auto Scaling Group name: –
IMDSv2: Required

Instance details Info

Platform
AMI ID
Monitoring

Click on security.



Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
☑	MyEC2InstanceSecurityGrou...	i-0d95a0ceddf1ca80a	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	ec2-3-109-49-78.ap-so...	3.109.49.78

Instance: i-0d95a0ceddf1ca80a (MyEC2InstanceSecurityGroupDemo)

Security details

IAM Role: –
Owner ID: 280694802344
Launch time: Sun Oct 15 2023 20:36:31 GMT+0530 (India Standard Time)
Security groups: sg-0714102ffec391a4a (launch-wizard-4)

Inbound rules

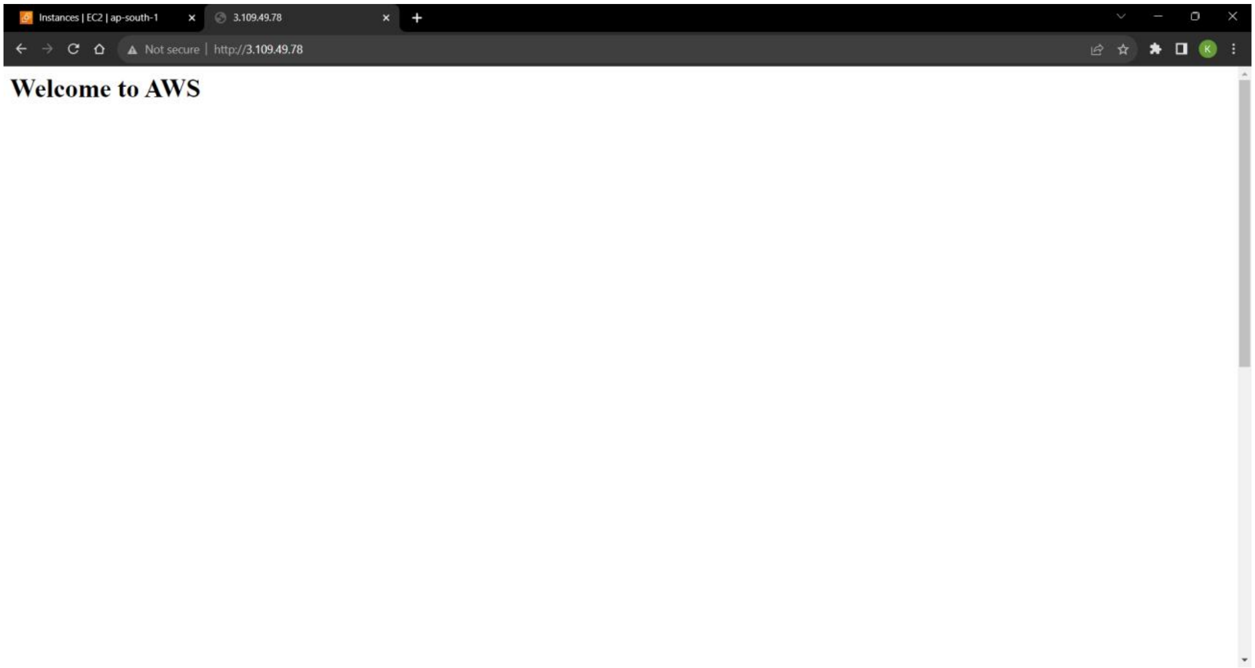
Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
–	sgr-0eb2a93a62a0181af	80	TCP	0.0.0.0/0	launch-wizard-4	–
–	sgr-0358732f4885b64d7	22	TCP	0.0.0.0/0	launch-wizard-4	–

Outbound rules

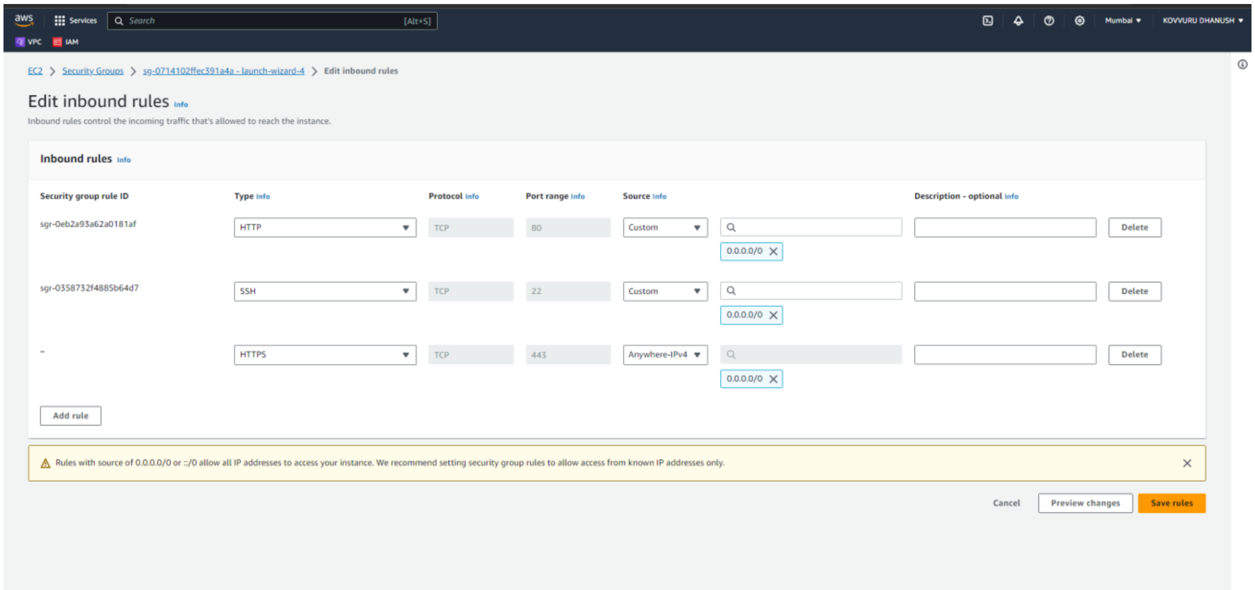
Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description

Check the port range here we are using SSH and HTTP.

For secure and encrypt communication you can add HTTPS the way we added HTTP.



Welcome to AWS



aws
Services
Search
[Alt+S]
Mumbai ▾
KOVVURU DHANUSH ▾
VPC
IAM
EC2 > Security Groups > sg-0714102ffec391a4a - launch-wizard-4 > Edit inbound rules

Edit inbound rules Info

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

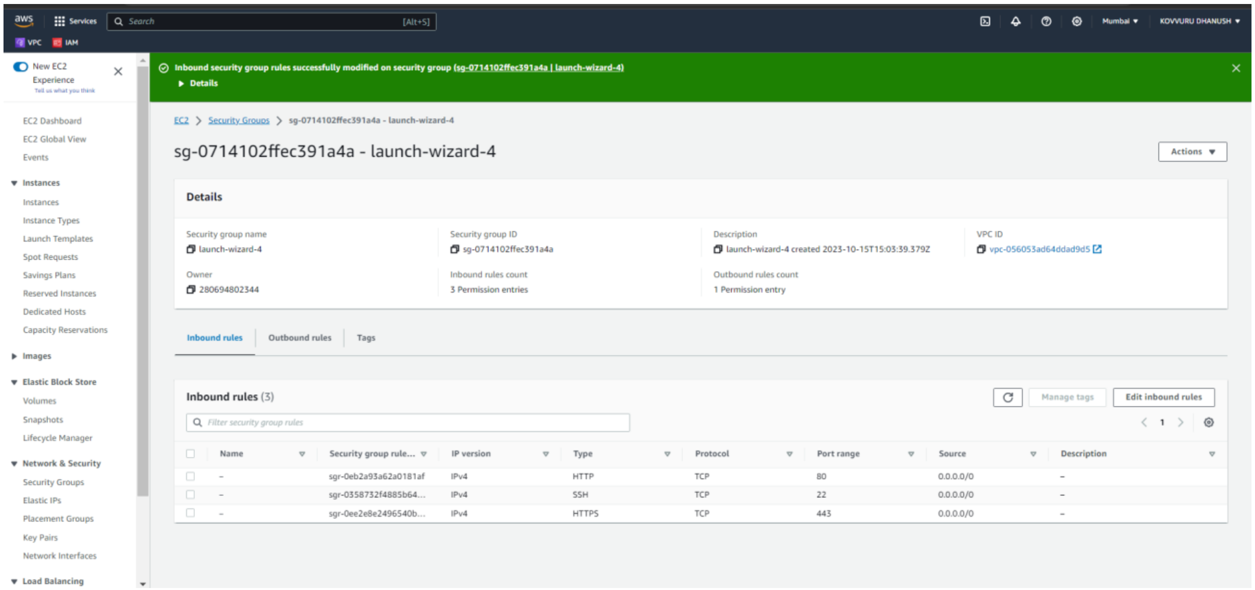
Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0eb2a93a62a0181af	HTTP ▾	TCP	80	Custom ▾	0.0.0.0/0 ✕		Delete
sgr-0358732f4885b64d7	SSH ▾	TCP	22	Custom ▾	0.0.0.0/0 ✕		Delete
-	HTTPS ▾	TCP	443	Anywhere-IPv4 ▾	0.0.0.0/0 ✕		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.

Now I'm adding HTTPS we will check now.

After adding click on save rule.



Inbound security group rules successfully modified on security group (sg-0714102ffec391a4a | launch-wizard-4)

▸ Details

EC2 > Security Groups > sg-0714102ffec391a4a - launch-wizard-4

sg-0714102ffec391a4a - launch-wizard-4

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-4	sg-0714102ffec391a4a	launch-wizard-4 created 2023-10-15T15:03:39.379Z	vpc-056053ad64ddad9d5
Owner	**Inbound rules count**	**Outbound rules count**	
280694802344	3 Permission entries	1 Permission entry	

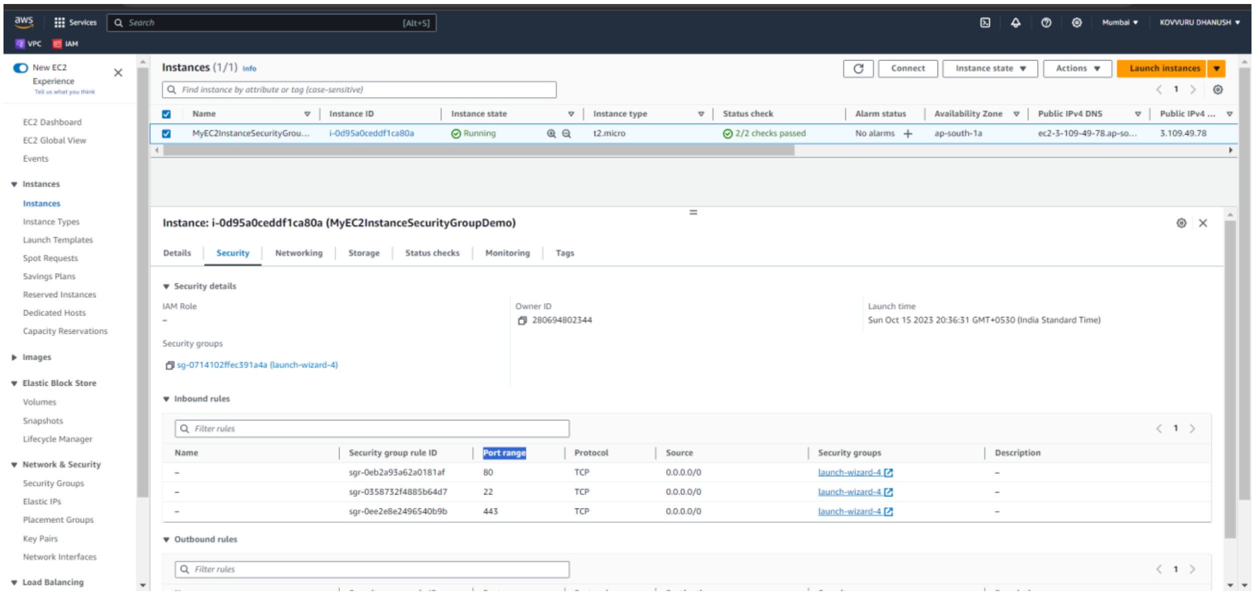
Inbound rules | Outbound rules | Tags

Inbound rules (3)

Filter security group rules

□	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-0eb2a93a62a0181af	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-0358732f4885b64...	IPv4	SSH	TCP	22	0.0.0.0/0	–
□	–	sgr-0ee2e8e2496540b...	IPv4	HTTPS	TCP	443	0.0.0.0/0	–

Inbound security group rules successfully modified on security group.



Instances (1/1) 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 IPv4 ...
☑	MyEC2InstanceSecurityGrou...	i-0d95a0ceddf1ca80a	Running	t2.micro	2/2 checks passed	No alarms +	ap-south-1a	ec2-3-109-49-78.ap-so...	3.109.49.78

Instance: i-0d95a0ceddf1ca80a (MyEC2InstanceSecurityGroupDemo)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

▾ Security details

IAM Role	Owner ID	Launch time
–	280694802344	Sun Oct 15 2023 20:36:31 GMT+0530 (India Standard Time)

Security groups

sg-0714102ffec391a4a (launch-wizard-4)

▾ Inbound rules

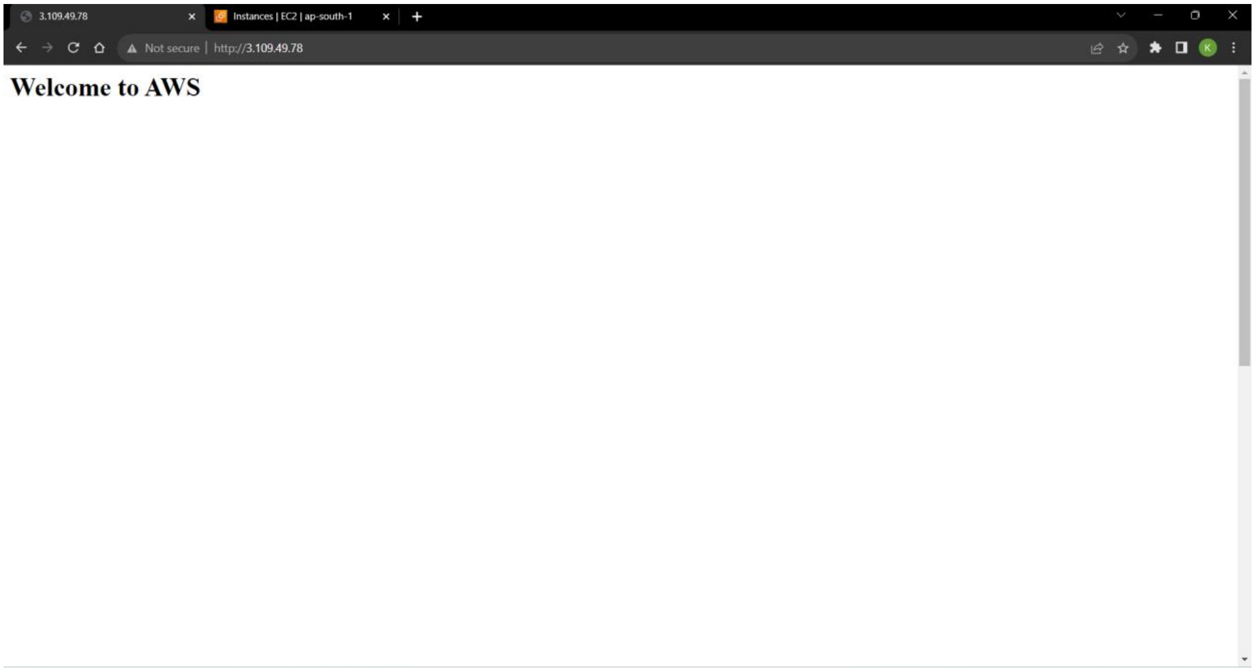
Filter rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
–	sgr-0eb2a93a62a0181af	80	TCP	0.0.0.0/0	launch-wizard-4	–
–	sgr-0358732f4885b64d7	22	TCP	0.0.0.0/0	launch-wizard-4	–
–	sgr-0ee2e8e2496540b9b	443	TCP	0.0.0.0/0	launch-wizard-4	–

▾ Outbound rules

Filter rules

See HTTPS Protocol was added here.



Welcome to AWS

See we can access securely.

THANK YOU