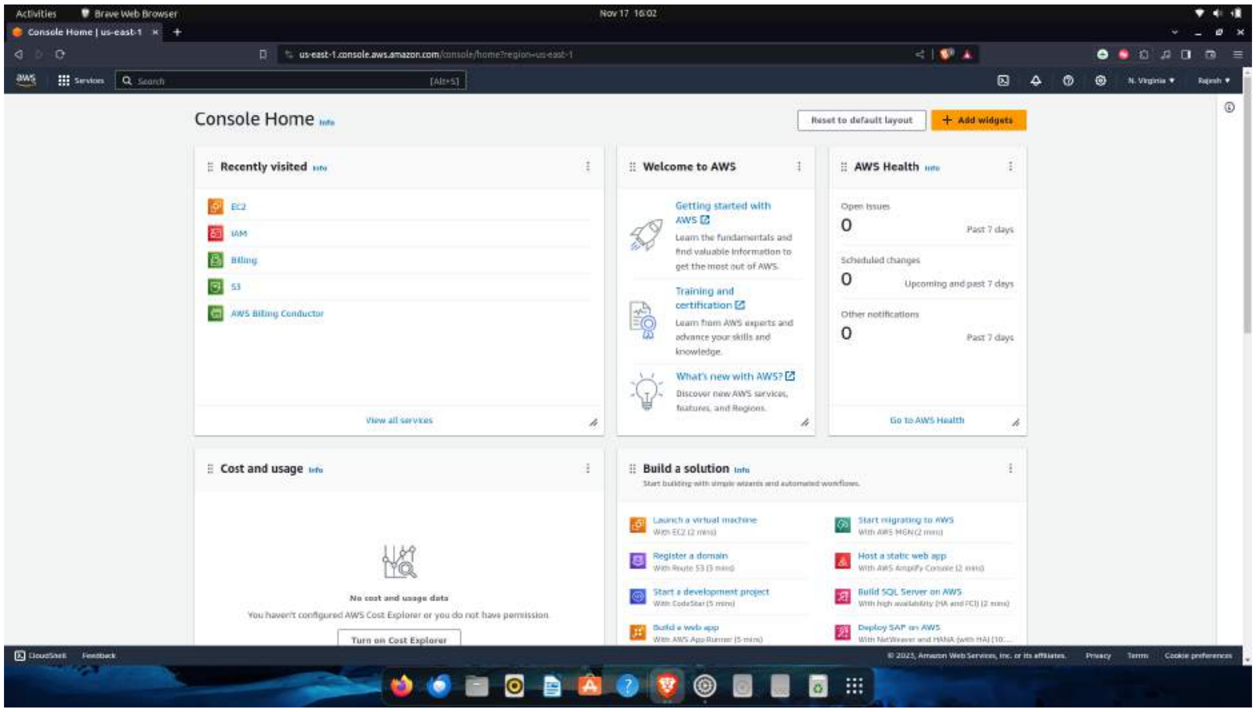
Rajesh's blog

Running a Python Server in a Secured VPC

Follow these steps to implement a python server in a secured vpc along that you will gain a good knowledge about working with NACLs and Security Groups.

Step 1: Open your AWS Account



Learn the fundamentals and find valuable information to get the most out of AWS.

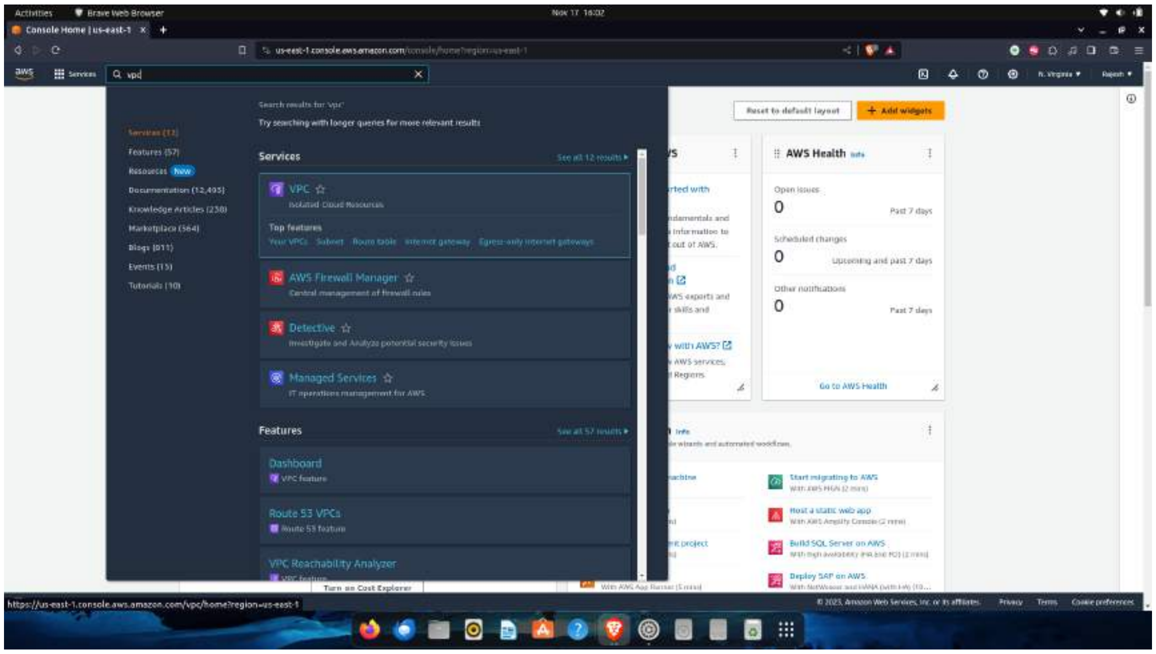
Learn from AWS experts and advance your skills and knowledge.

Discover new AWS services, features, and Regions.

Start building with simple wizards and automated workflows.

You haven't configured AWS Cost Explorer or you do not have permission.

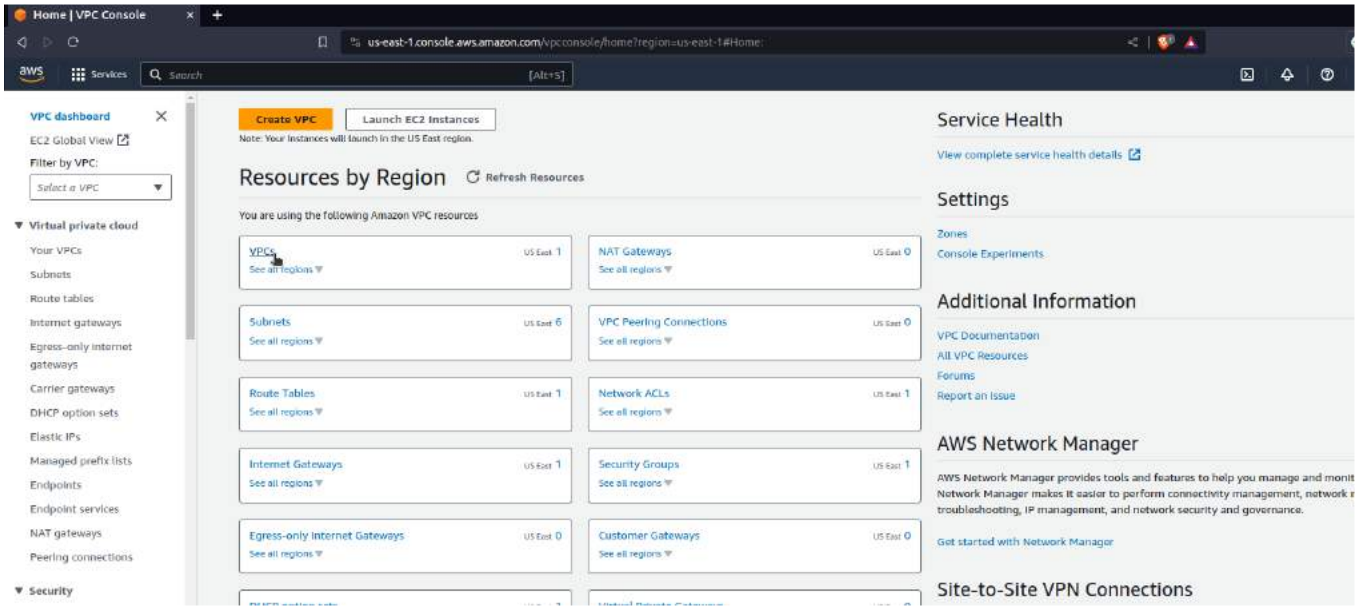
Step 2: Search for VPC in console and click on vpc



Search results for 'vpc'

Try searching with longer queries for more relevant results

Step 3: Click on VPCs



Note: Your instances will launch in the US East region.

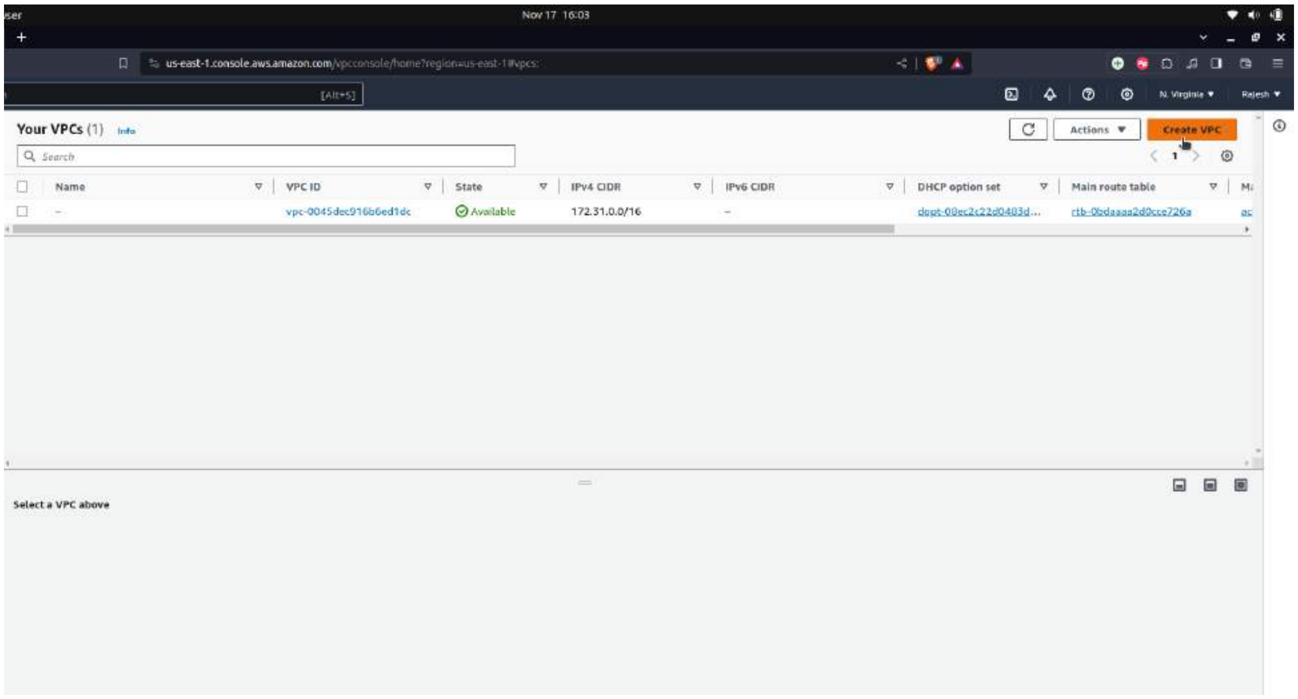
Resources by Region

You are using the following Amazon VPC resources

VPCs	US East 1	NAT Gateways	US East 0
Subnets	US East 6	VPC Peering Connections	US East 0
Route Tables	US East 1	Network ACLs	US East 1
Internet Gateways	US East 1	Security Groups	US East 1
Egress-only Internet Gateways	US East 0	Customer Gateways	US East 0

AWS Network Manager provides tools and features to help you manage and monit Network Manager makes it easier to perform connectivity management, network troubleshooting, IP management, and network security and governance.

Step 4: Click on create VPC



Your VPCs (1) Info

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	M
–	vpc-0045dec916b6ed1dc	Available	172.31.0.0/16	–	dopt-08ec2c22d0403d...	rtb-0bdaaaa2d0cce726a	ac

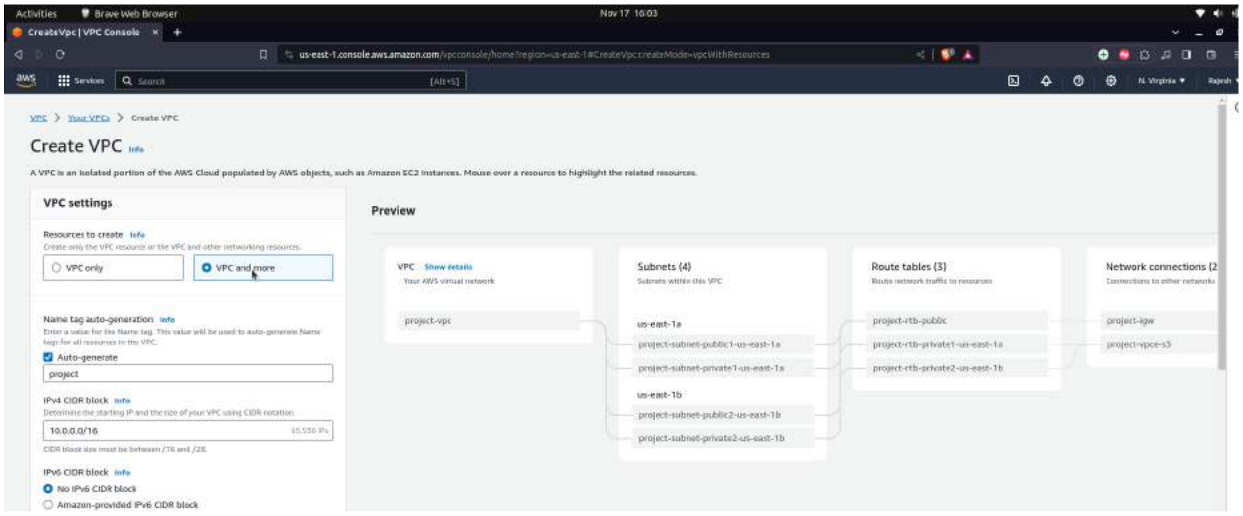
Select a VPC above

Nov 17 16:03
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#vpcs:
[Alt+S]
N. Virginia
Rajesh
Actions
Create VPC
Search

Step 5: Choose VPC and more

When we choose vpc and more ,AWS will create subnets and Route Table for us.please observe

the preview to gain more understanding.



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only [✓ VPC and more]

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
[✓] Auto-generate
project

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
[✓ No IPv6 CIDR block]
Amazon-provided IPv6 CIDR block

Preview

VPC Show details
Your AWS virtual network
project-vpc

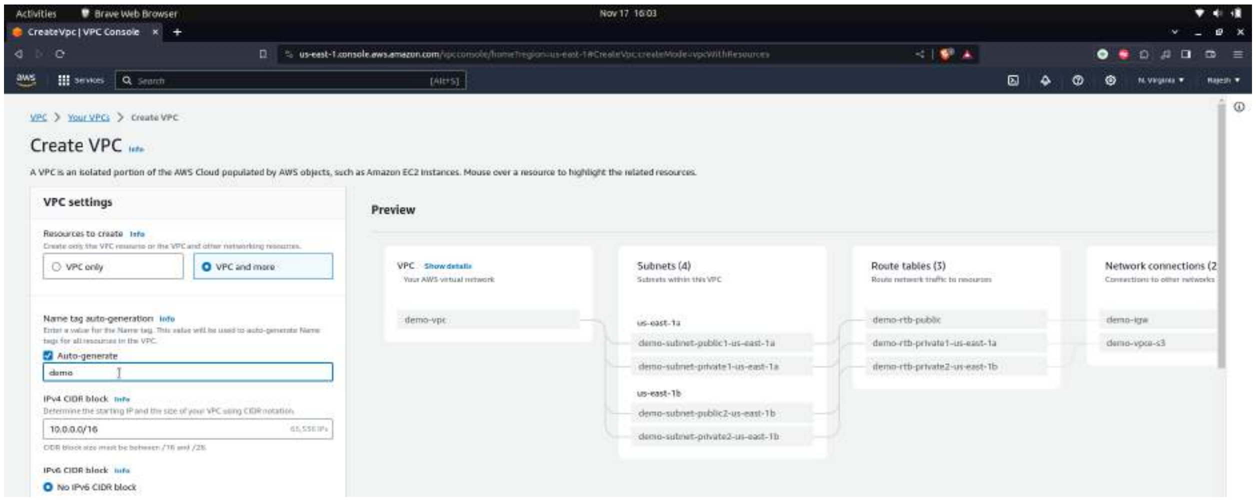
Subnets (4)
Subnets within this VPC
us-east-1a
project-subnet-public1-us-east-1a
project-subnet-private1-us-east-1a
us-east-1b
project-subnet-public2-us-east-1b
project-subnet-private2-us-east-1b

Route tables (3)
Route network traffic to resources
project-rtb-public
project-rtb-private1-us-east-1a
project-rtb-private2-us-east-1b

Network connections (2
Connections to other networks
project-igw
project-vpce-s3

Activities
Brave Web Browser
CreateVpc | VPC Console
Nov 17 16:03
us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpc:createMode=vpcWithResources
Services
Search
[Alt+S]
N. Virginia
Rajesh

Step 6: Enter you vpc name,for now i will go with demo


Activities   Brave Web Browser   Nov 17 16:03

CreateVpc | VPC Console

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateVpc:createMode=vpcWithResources

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only [✓ VPC and more]

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
[✓] Auto-generate
demo

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16   65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
[✓ No IPv6 CIDR block]

Preview

VPC Show details
Your AWS virtual network
demo-vpc

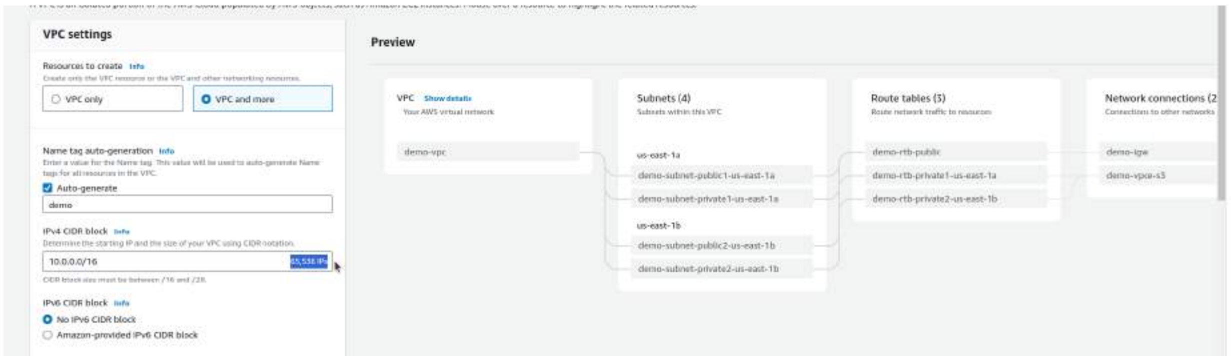
Subnets (4)
Subnets within this VPC
us-east-1a
demo-subnet-public1-us-east-1a
demo-subnet-private1-us-east-1a
us-east-1b
demo-subnet-public2-us-east-1b
demo-subnet-private2-us-east-1b

Route tables (3)
Route network traffic to resources
demo-rtb-public
demo-rtb-private1-us-east-1a
demo-rtb-private2-us-east-1b

Network connections (2
Connections to other networks
demo-igw
demo-vpce-s3

Step 7: you can choose a range of IP addresses for your VPC

For now I am leaving default range


VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only [✓ VPC and more]

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
[✓] Auto-generate
demo

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16   65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
[✓ No IPv6 CIDR block]
Amazon-provided IPv6 CIDR block

Preview

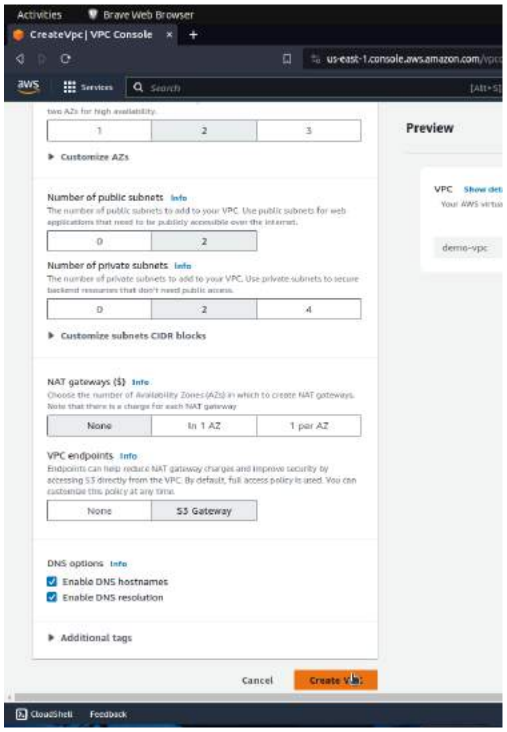
VPC Show details
Your AWS virtual network
demo-vpc

Subnets (4)
Subnets within this VPC
us-east-1a
demo-subnet-public1-us-east-1a
demo-subnet-private1-us-east-1a
us-east-1b
demo-subnet-public2-us-east-1b
demo-subnet-private2-us-east-1b

Route tables (3)
Route network traffic to resources
demo-rtb-public
demo-rtb-private1-us-east-1a
demo-rtb-private2-us-east-1b

Network connections (2
Connections to other networks
demo-igw
demo-vpce-s3

Step 8: Selecting AZ,public private subnets,NAT Gateway and VPC endpoints


Number of public subnets: [✓ 2]

Number of private subnets: [✓ 2]

NAT gateways ($): [✓ None]

VPC endpoints: [✓ S3 Gateway]

DNS options: ☑ Enable DNS hostnames ☑ Enable DNS resolution

You can select the number of availability zones you

Want to have your vpc.

You can set the count of subnets you want in public

As well as private

In this project I don’t want to interact with the NAT gateway.

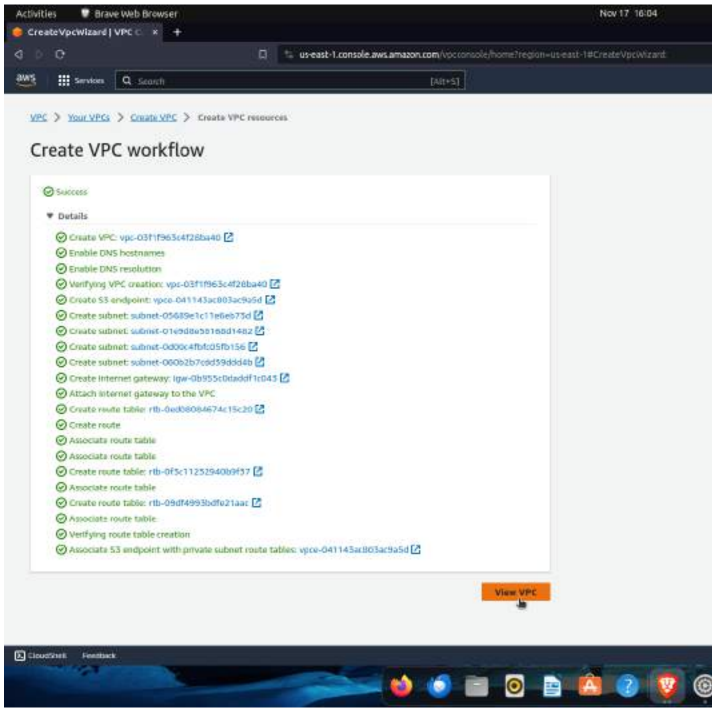
I am leaving it default.

In VPC endpoints you can choose any one either None

Or S3 Gateway.

After all click on **createVPC**

Step 9: creating vpc


Create VPC workflow

Success

Details

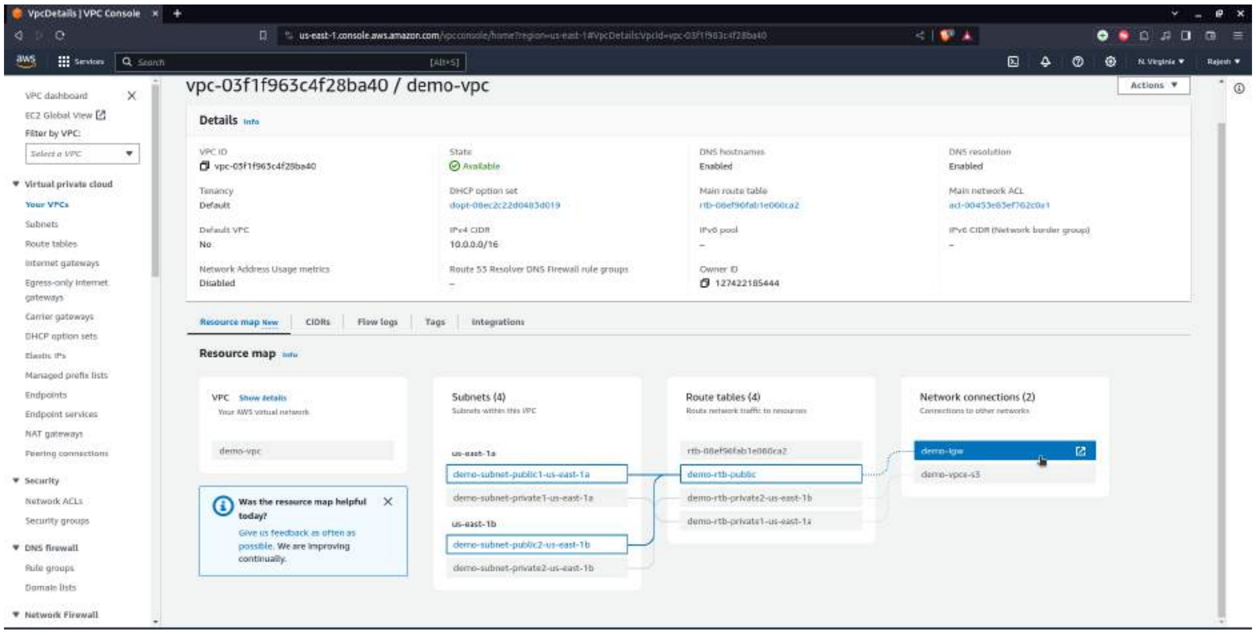
- Create VPC: vpc-03f1f963c4f28ba40
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: vpc-03f1f963c4f28ba40
- Create S3 endpoint: vpce-041143ac803ac9a5d
- Create subnet: subnet-05689e1c11e6eb73d
- Create subnet: subnet-01e9d8e58168d1482
- Create subnet: subnet-0d00c4fbfc05fb156
- Create subnet: subnet-060b2b7c9d39ddd4b
- Create internet gateway: igw-0b955c0daddf1c043
- Attach internet gateway to the VPC
- Create route table: rtb-0ed08084674c15c20
- Create route
- Associate route table
- Associate route table
- Create route table: rtb-0f5c11252940b9f37
- Associate route table
- Create route table: rtb-09df4993bdfe21aac
- Associate route table
- Verifying route table creation
- Associate S3 endpoint with private subnet route tables: vpce-041143ac803ac9a5d

Observe how VPC is creating.

After all is done. Click on view VPC

Step 10: Observe the Resource map diagram

Looking into the diagram you can identify how logically it is connecting.



vpc-03f1f963c4f28ba40 / demo-vpc

Details

VPC ID vpc-03f1f963c4f28ba40	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-08ec2c22d0483d019	Main route table rtb-08ef96fab1e060ca2	Main network ACL acl-00453e83ef762c0a1
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –	IPv6 CIDR (Network border group) –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 127422185444	

Resource map

VPC Show details
Your AWS virtual network
demo-vpc

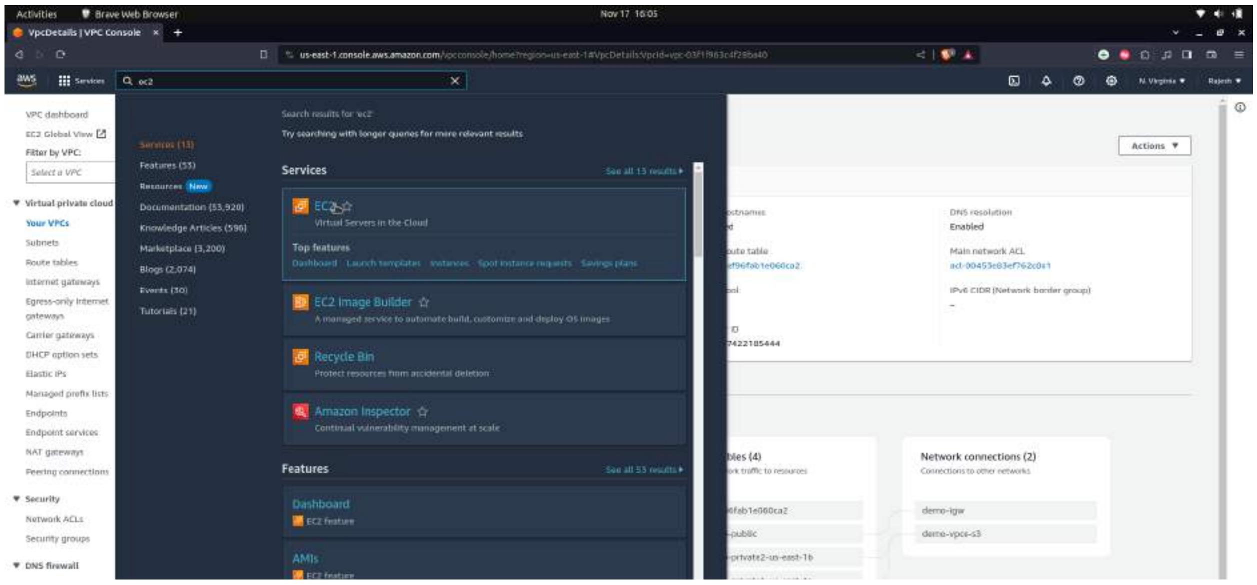
Subnets (4)
Subnets within this VPC
us-east-1a
demo-subnet-public1-us-east-1a
demo-subnet-private1-us-east-1a
us-east-1b
demo-subnet-public2-us-east-1b
demo-subnet-private2-us-east-1b

Route tables (4)
Route network traffic to resources
rtb-08ef96fab1e060ca2
demo-rtb-public
demo-rtb-private2-us-east-1b
demo-rtb-private1-us-east-1a

Network connections (2)
Connections to other networks
demo-igw
demo-vpce-s3

Was the resource map helpful today?
Give us feedback as often as possible. We are improving continually.

Step 11: Open Ec2



ec2

Search results for 'ec2'

Try searching with longer queries for more relevant results

Services

EC2
Virtual Servers in the Cloud
Top features
Dashboard Launch templates Instances Spot Instance requests Savings plans

EC2 Image Builder
A managed service to automate build, customize and deploy OS images

Recycle Bin
Protect resources from accidental deletion

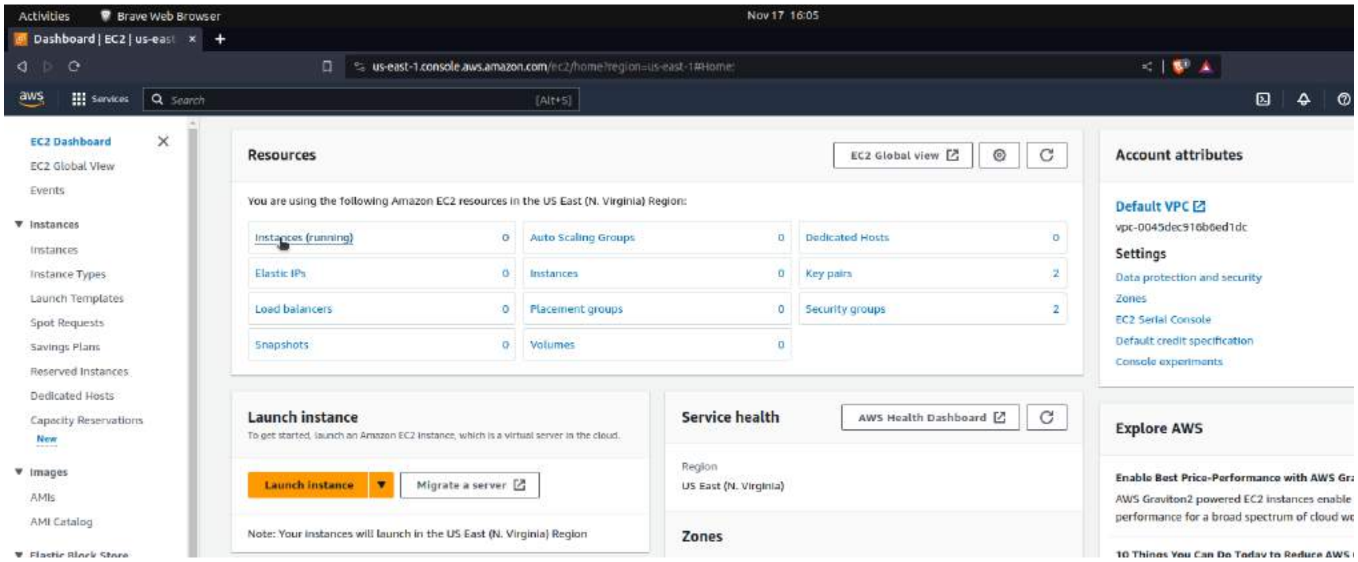
Amazon Inspector
Continual vulnerability management at scale

Features

Dashboard
EC2 feature

AMIs
EC2 feature

Step 12:Click on Instances Running



You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	2
Load balancers	0	Placement groups	0	Security groups	2
Snapshots	0	Volumes	0		

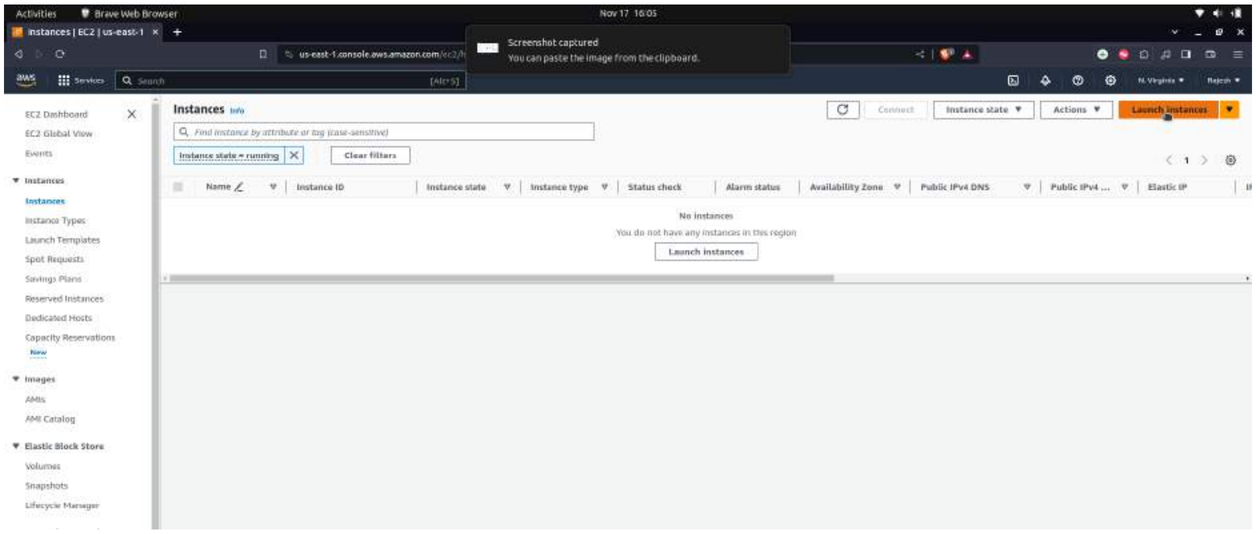
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the US East (N. Virginia) Region

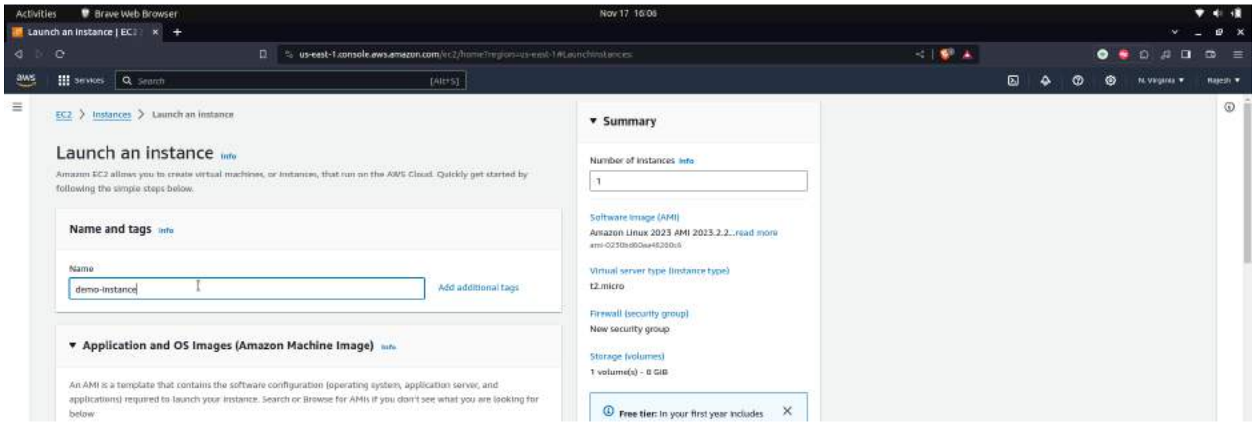
Enable Best Price-Performance with AWS Gra
AWS Graviton2 powered EC2 instances enable
performance for a broad spectrum of cloud wo

10 Things You Can Do Today to Reduce AWS

Step 13: Click on Launch Instance



Step 14:Provide Ec2 Instance Name(demo-Instance)


EC2 > Instances > Launch an instance

Launch an instance

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

Name: demo-instance

Application and OS Images (Amazon Machine Image)

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

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.2.2...read more

Virtual server type (instance type): t2.micro

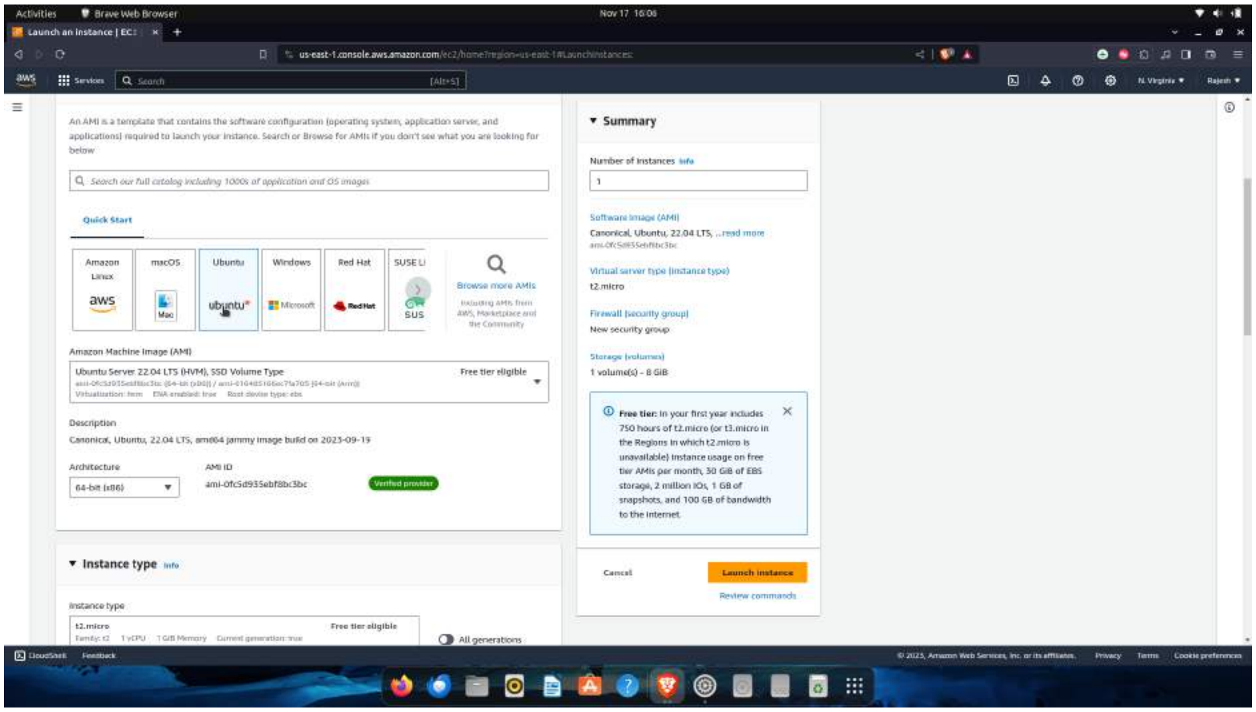
Firewall (security group): New security group

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

Free tier: In your first year includes

Step 15:choose ubuntu os

But you can choose your familiar os


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

Amazon Machine Image (AMI): Ubuntu Server 22.04 LTS (HVM), SSD Volume Type — Free tier eligible

Description: Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-09-19

Architecture: 64-bit (x86)

AMI ID: ami-0fc5d935ebf8bc3bc — Verified provider

Instance type: t2.micro — Free tier eligible

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 22.04 LTS, ...read more

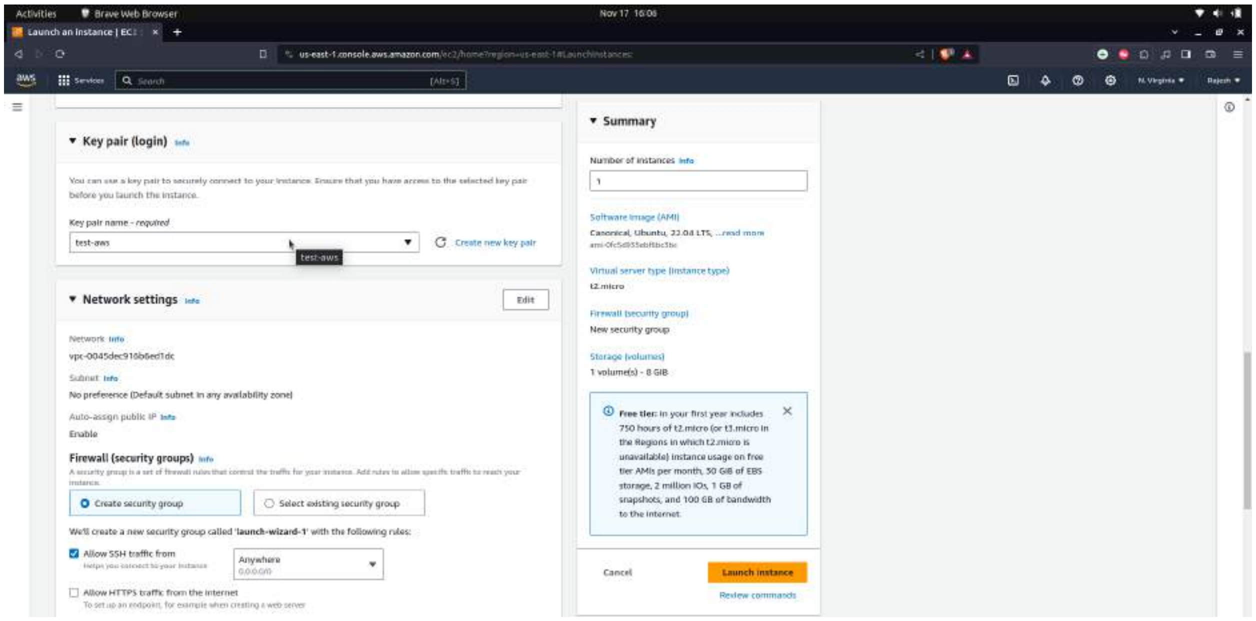
Virtual server type (instance type): t2.micro

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

Step 16:Select key-pair



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*: test-aws

Network settings

Network: vpc-0045dec916b6ed1dc

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enable

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

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 22.04 LTS, ...read more

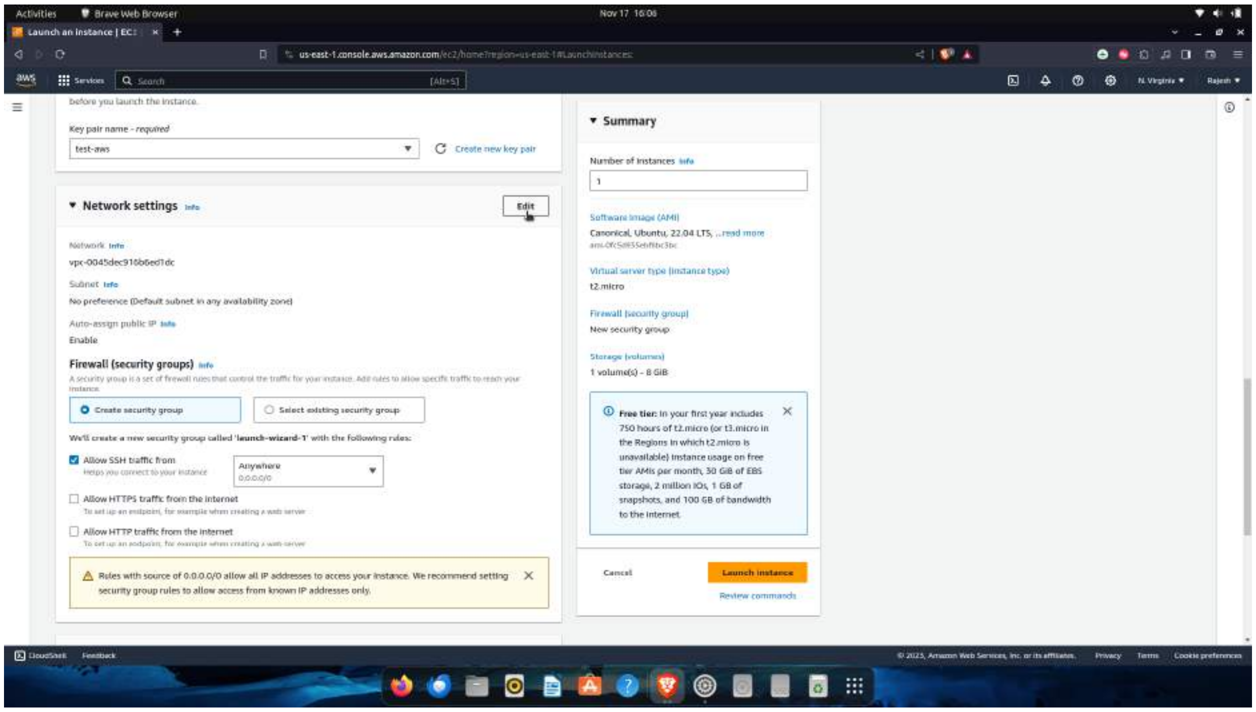
Virtual server type (instance type): t2.micro

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.

Step 17:Click Edit in Networking settings



before you launch the instance.

Key pair name - *required*: test-aws

Network settings

Network: vpc-0045dec916b6ed1dc

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enable

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

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.

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 22.04 LTS, ...read more

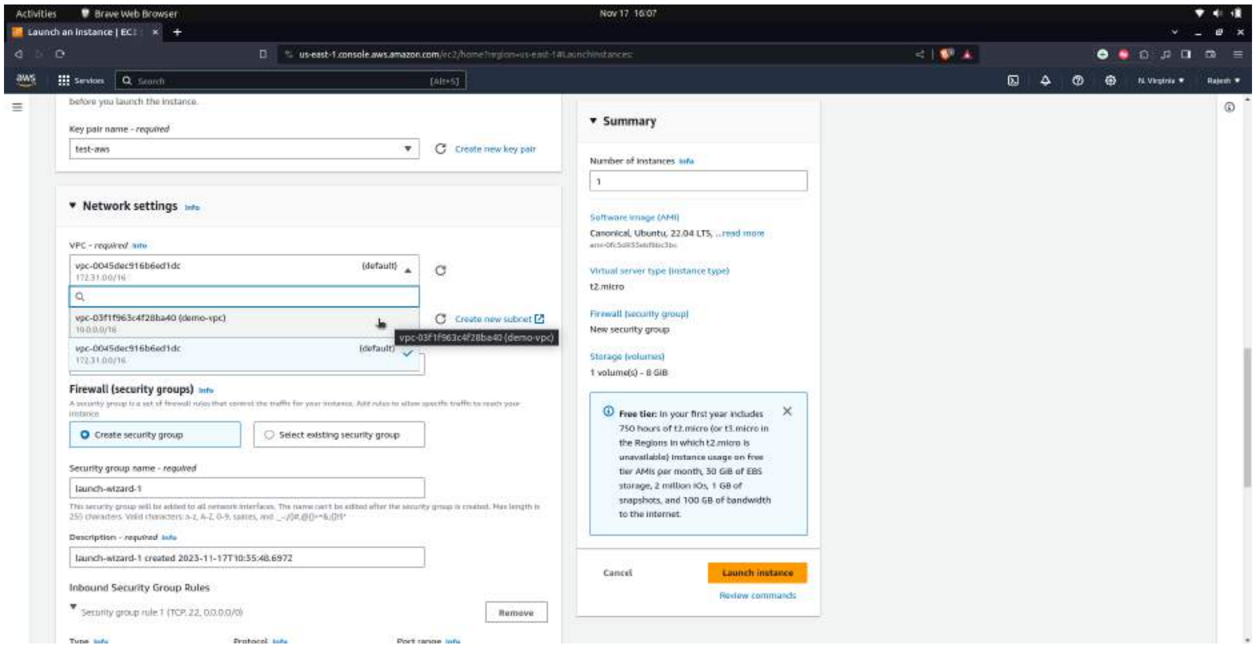
Virtual server type (instance type): t2.micro

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.

Step 18:Select our created demo vpc


Key pair name - required: test-aws

Network settings

VPC - required: vpc-0045dec916b6ed1dc (default) 172.31.0.0/16

vpc-03f1f963c4f28ba40 (demo-vpc) 10.0.0.0/16

vpc-0045dec916b6ed1dc (default) 172.31.0.0/16

Firewall (security groups): Create security group

Security group name - required: launch-wizard-1

Description - required: launch-wizard-1 created 2023-11-17T10:35:48.697Z

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 0.0.0.0/0)

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 22.04 LTS, ...read more

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

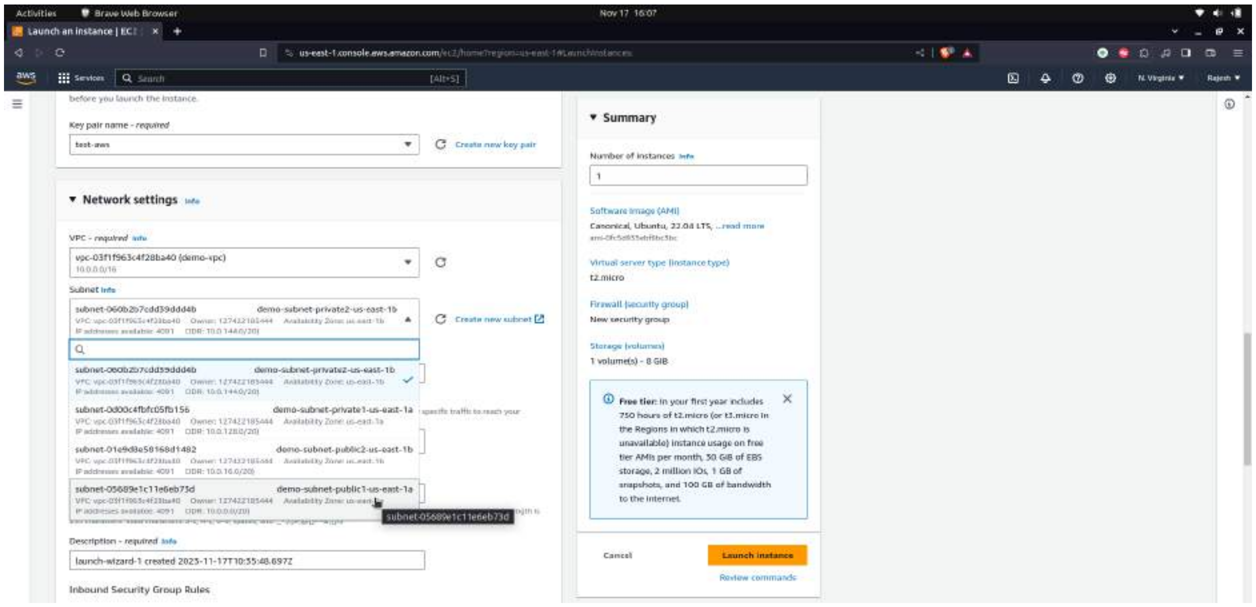
Storage (volumes): 1 volume(s) - 8 GiB

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.

Step 19:Select Subnet

Choose demo-subnet-public1-us-east-1a.In this project I don’t want to deal with load balancers

And other topics.Go with the public subnet in your availability zone.


VPC - required: vpc-03f1f963c4f28ba40 (demo-vpc) 10.0.0.0/16

Subnet

subnet-060b2b7cdd39ddd4b demo-subnet-private2-us-east-1b

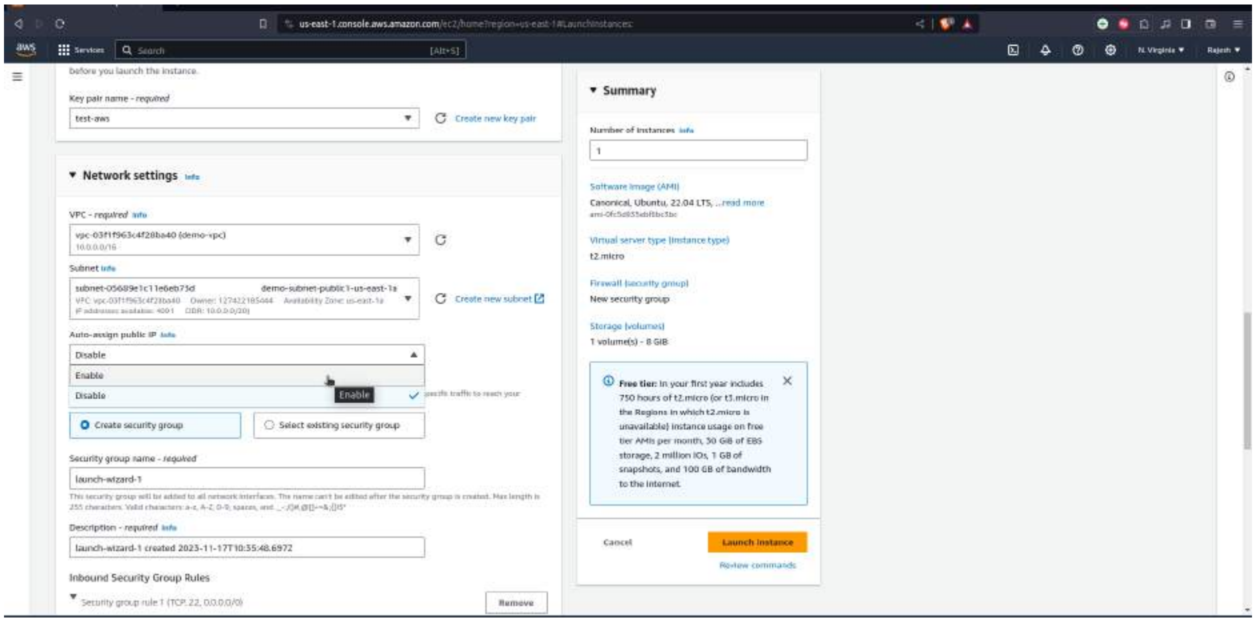
subnet-0d00c4fbfc05fb156 demo-subnet-private1-us-east-1a

subnet-01e9d8e58168d1482 demo-subnet-public2-us-east-1b

subnet-05689e1c11e6eb73d demo-subnet-public1-us-east-1a

Description - required: launch-wizard-1 created 2023-11-17T10:35:48.697Z

Step 20:Enable Auto-assign public IP



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

before you launch the instance.

Key pair name - *required*
test-aws

Network settings

VPC - *required*
vpc-03f1f963c4f28ba40 (demo-vpc)
10.0.0.0/16

Subnet
subnet-05689e1c11e6eb73d demo-subnet-public1-us-east-1a
VPC: vpc-03f1f963c4f28ba40 Owner: 127422185444 Availability Zone: us-east-1a
IP addresses available: 4091 CIDR: 10.0.0.0/20)

Auto-assign public IP
Disable
Enable
Disable

Create security group | Select existing security group

Security group name - *required*
launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#,@[]+=&;{}!$*

Description - *required*
launch-wizard-1 created 2023-11-17T10:35:48.697Z

Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)

Summary

Number of instances
1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0fc5d935ebf8bc3bc

Virtual server type (instance type)
t2.micro

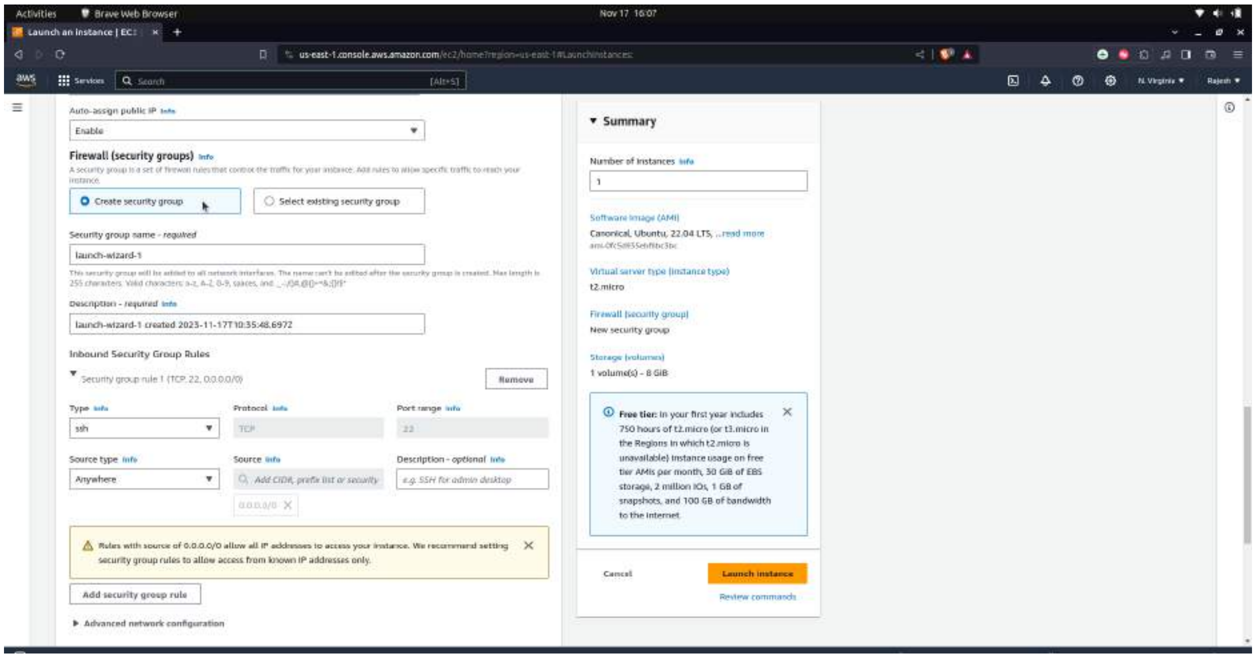
Firewall (security group)
New security group

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.

Step 21:Select create security group

AWS will automatically create the security group for you then you can manage it



Launch an instance | EC2

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

Auto-assign public IP
Enable

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

Security group name - *required*
launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#,@[]+=&;{}!$*

Description - *required*
launch-wizard-1 created 2023-11-17T10:35:48.697Z

Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type	Protocol	Port range
ssh	TCP	22

Source type	Source	Description - optional
Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

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.

Add security group rule

Advanced network configuration

Summary

Number of instances
1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0fc5d935ebf8bc3bc

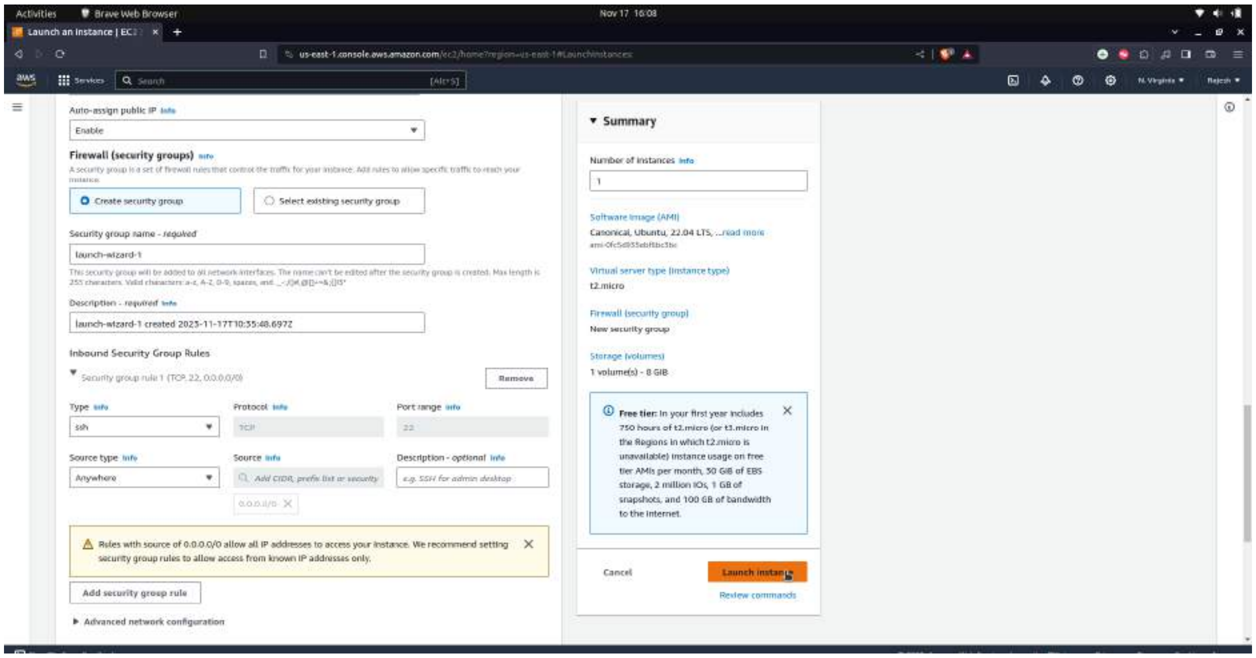
Virtual server type (instance type)
t2.micro

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.

Step 22:Click on Launch Instance



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

Security group name - *required*

launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

launch-wizard-1 created 2023-11-17T10:35:48.697Z

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type: ssh	Protocol: TCP	Port range: 22
Source type: Anywhere	Source: 0.0.0.0/0	Description - *optional*: e.g. SSH for admin desktop

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.

Add security group rule

Advanced network configuration

Summary

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more

ami-0fc5d935ebf8bc3bc

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

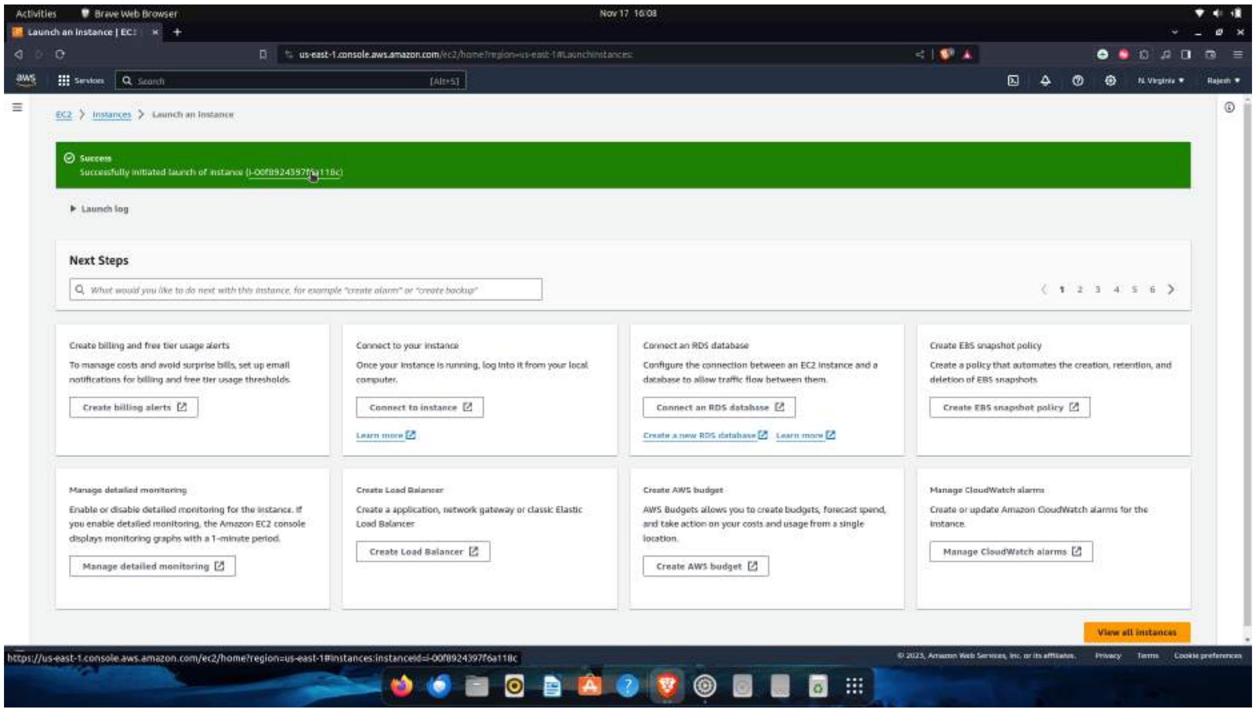
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

Review commands

Step 23:After creating open your Instance



EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-00f8924397f6a118c)

Launch log

Next Steps

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.

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

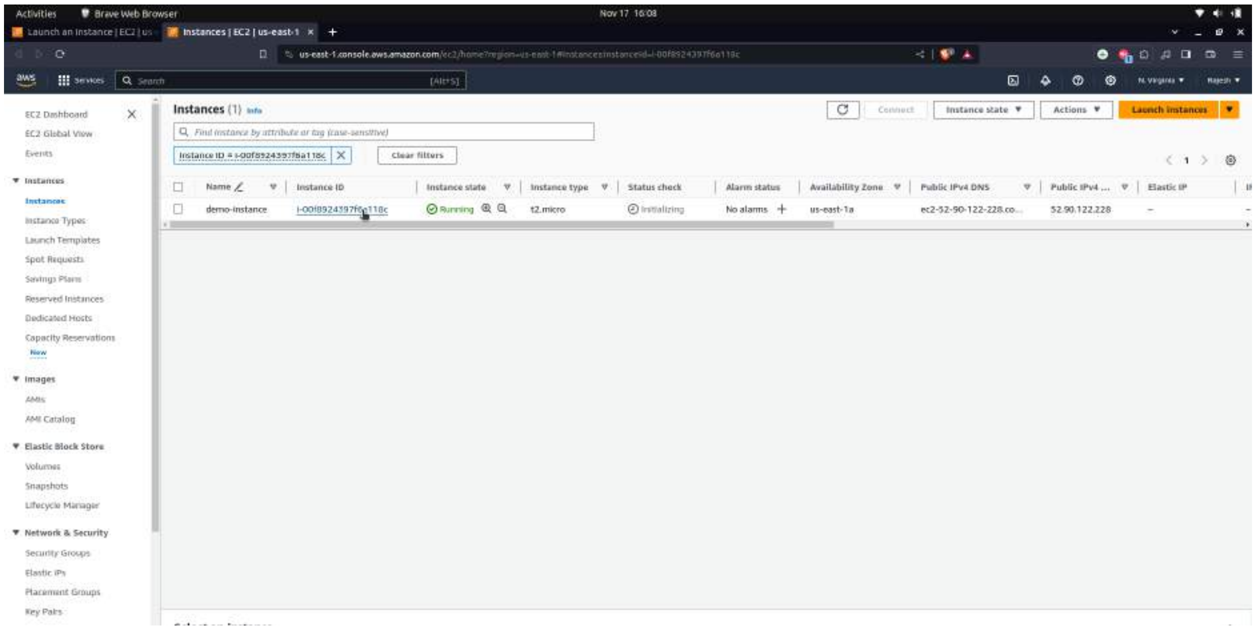
Create or update Amazon CloudWatch alarms for the instance.

Manage CloudWatch alarms

View all instances

https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:instanceId=i-00f8924397f6a118c

Step 24:Click on your Instance ID

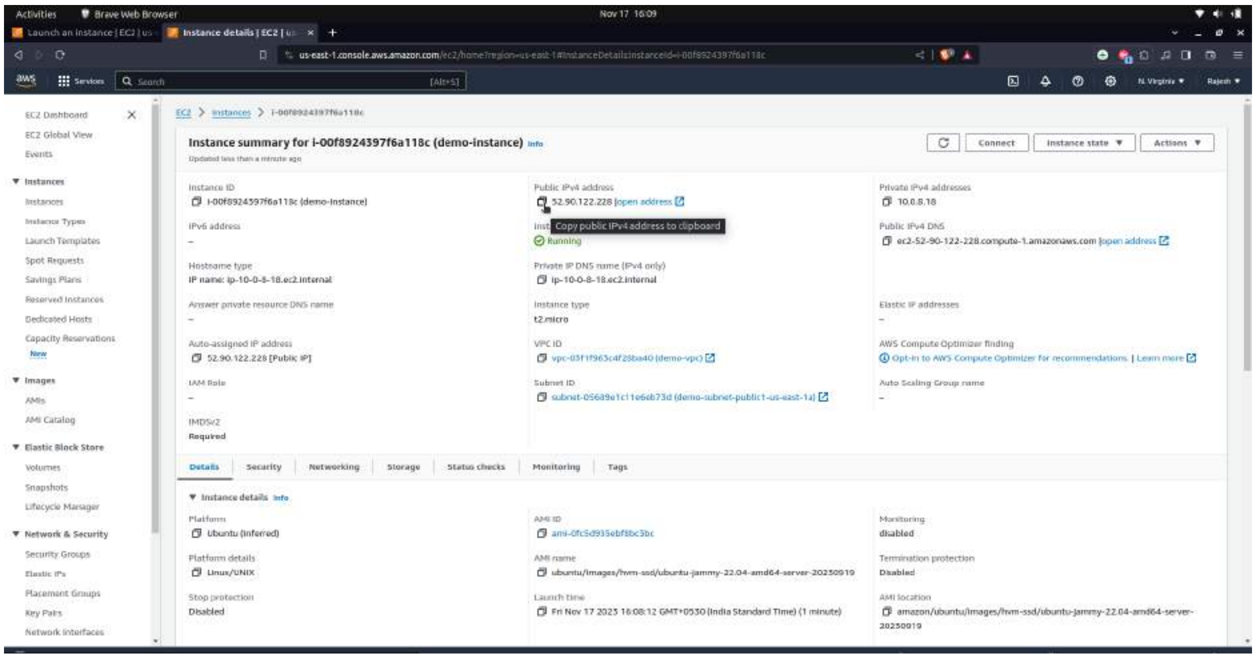


Instances (1)

Instance ID = i-00f8924397f6a118c

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
demo-instance	i-00f8924397f6a118c	Running	t2.micro	Initializing	No alarms	us-east-1a	ec2-52-90-122-228.co...	52.90.122.228	–

Step 25:Copy your Instance public IP address



Instance summary for i-00f8924397f6a118c (demo-instance)

Updated less than a minute ago

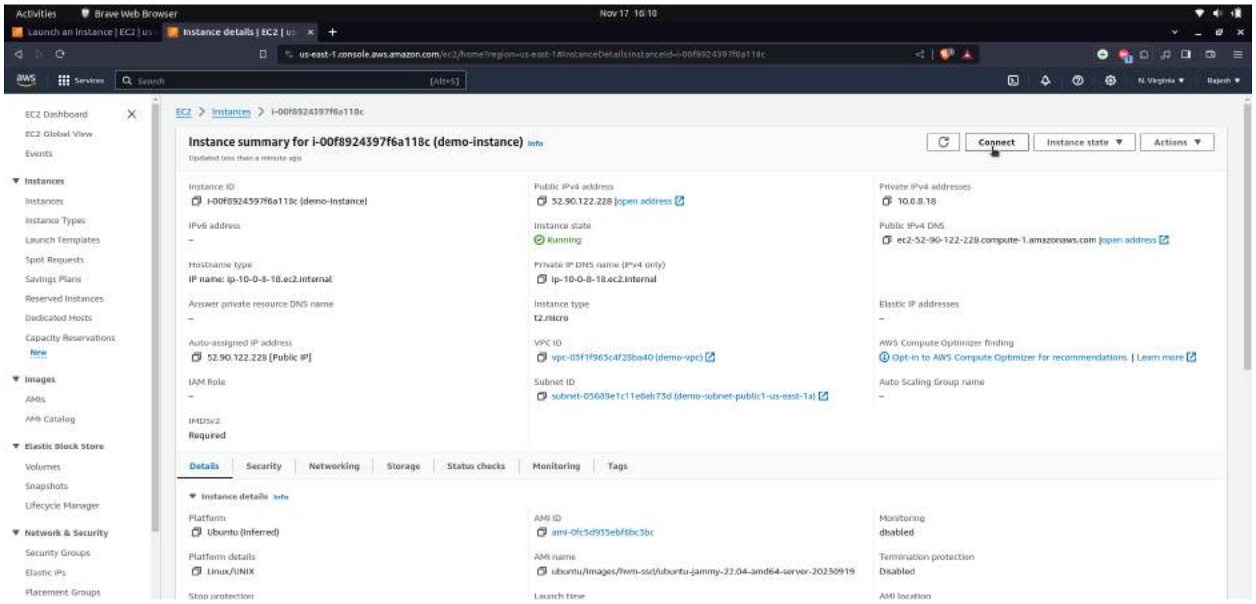
Instance ID: i-00f8924397f6a118c (demo-instance)	Public IPv4 address: 52.90.122.228 |open address	Private IPv4 addresses: 10.0.8.18
IPv6 address: –	Instance state: Running	Public IPv4 DNS: ec2-52-90-122-228.compute-1.amazonaws.com |open address
Hostname type: IP name: ip-10-0-8-18.ec2.internal	Private IP DNS name (IPv4 only): ip-10-0-8-18.ec2.internal	
Answer private resource DNS name: –	Instance type: t2.micro	Elastic IP addresses: –
Auto-assigned IP address: 52.90.122.228 [Public IP]	VPC ID: vpc-03f1f963c4f28ba40 (demo-vpc)	AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role: –	Subnet ID: subnet-05689e1c11e6eb73d (demo-subnet-public1-us-east-1a)	Auto Scaling Group name: –
IMDSv2: Required		

Copy public IPv4 address to clipboard

Instance details

Platform: Ubuntu (Inferred)	AMI ID: ami-0fc5d935ebf8bc3bc	Monitoring: disabled
Platform details: Linux/UNIX	AMI name: ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20230919	Termination protection: Disabled
Stop protection: Disabled	Launch time: Fri Nov 17 2023 16:08:12 GMT+0530 (India Standard Time) (1 minute)	AMI location: amazon/ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20230919

Step 26:Click on Connect



EC2 > Instances > i-00f8924397f6a118c

Instance summary for i-00f8924397f6a118c (demo-instance)

Updated less than a minute ago

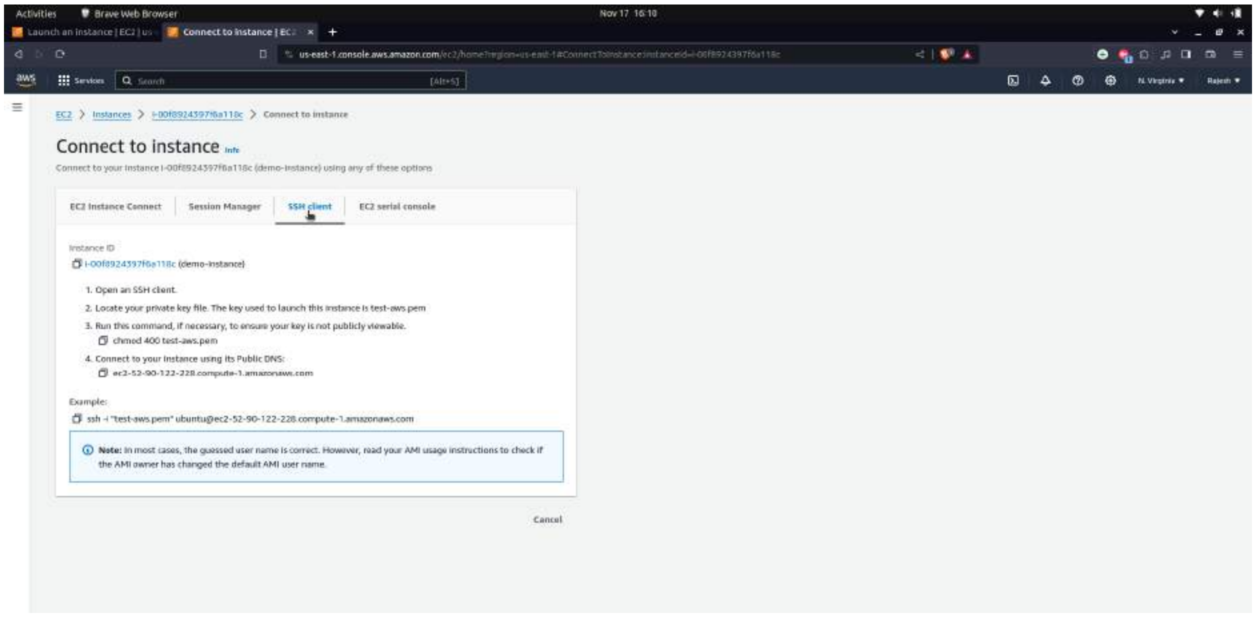
Instance ID: i-00f8924597f6a118c (demo-instance)	Public IPv4 address: 52.90.122.228 | open address	Private IPv4 addresses: 10.0.8.18
IPv6 address: –	Instance state: Running	Public IPv4 DNS: ec2-52-90-122-228.compute-1.amazonaws.com | open address
Hostname type: IP name: ip-10-0-8-18.ec2.internal	Private IP DNS name (IPv4 only): ip-10-0-8-18.ec2.internal	
Answer private resource DNS name: –	Instance type: t2.micro	Elastic IP addresses: –
Auto-assigned IP address: 52.90.122.228 [Public IP]	VPC ID: vpc-03f1f963c4f28ba40 (demo-vpc)	AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role: –	Subnet ID: subnet-05689e1c11e6eb73d (demo-subnet-public1-us-east-1a)	Auto Scaling Group name: –
IMDSv2: Required		

Instance details

Platform: Ubuntu (Inferred)	AMI ID: ami-0fc5d935ebf8bc3bc	Monitoring: disabled
Platform details: Linux/UNIX	AMI name: ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20230919	Termination protection: Disabled
Stop protection	Launch time	AMI location

Step 27: Click on SSH client

Follow the given steps to connect your ec2 instance through terminal.let's go.



EC2 > Instances > i-00f8924397f6a118c > Connect to instance

Connect to instance

Connect to your instance i-00f8924397f6a118c (demo-instance) using any of these options

Instance ID

i-00f8924397f6a118c (demo-instance)

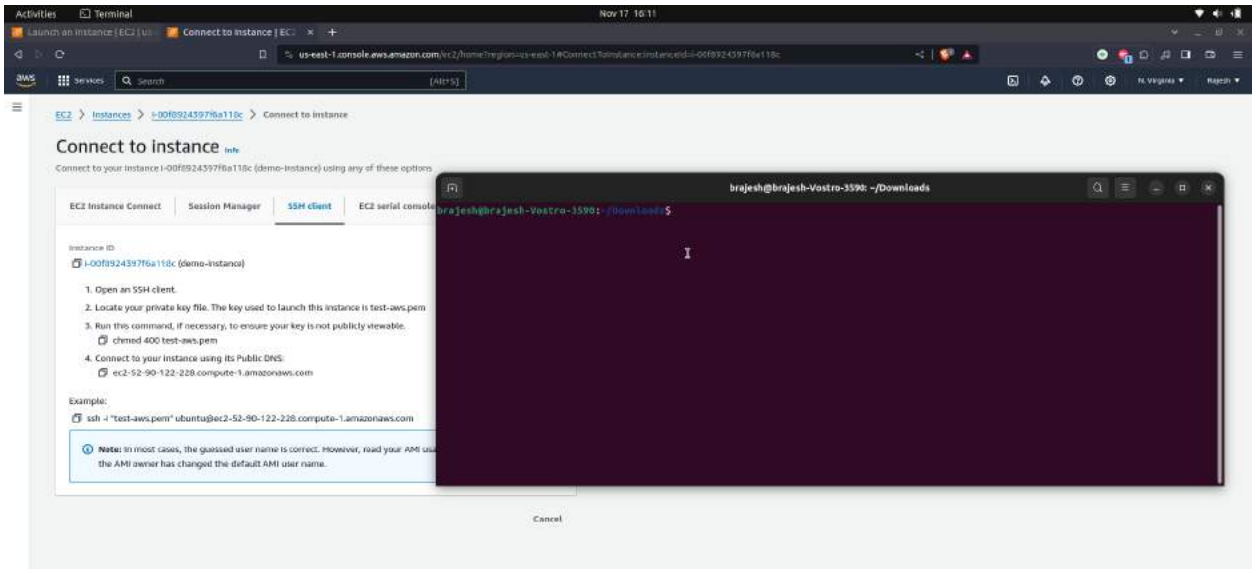
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is test-aws.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   ```
   chmod 400 test-aws.pem
   ```
4. Connect to your instance using its Public DNS:
   ec2-52-90-122-228.compute-1.amazonaws.com

Example:

```
ssh -i "test-aws.pem" ubuntu@ec2-52-90-122-228.compute-1.amazonaws.com
```

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

Step 28: Open your Terminal



EC2 > Instances > i-00f8924397f6a118c > Connect to instance

Connect to instance Info

Connect to your instance i-00f8924397f6a118c (demo-instance) using any of these options

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

Instance ID

i-00f8924397f6a118c (demo-instance)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is test-aws.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 test-aws.pem
4. Connect to your instance using its Public DNS:
   ec2-52-90-122-228.compute-1.amazonaws.com

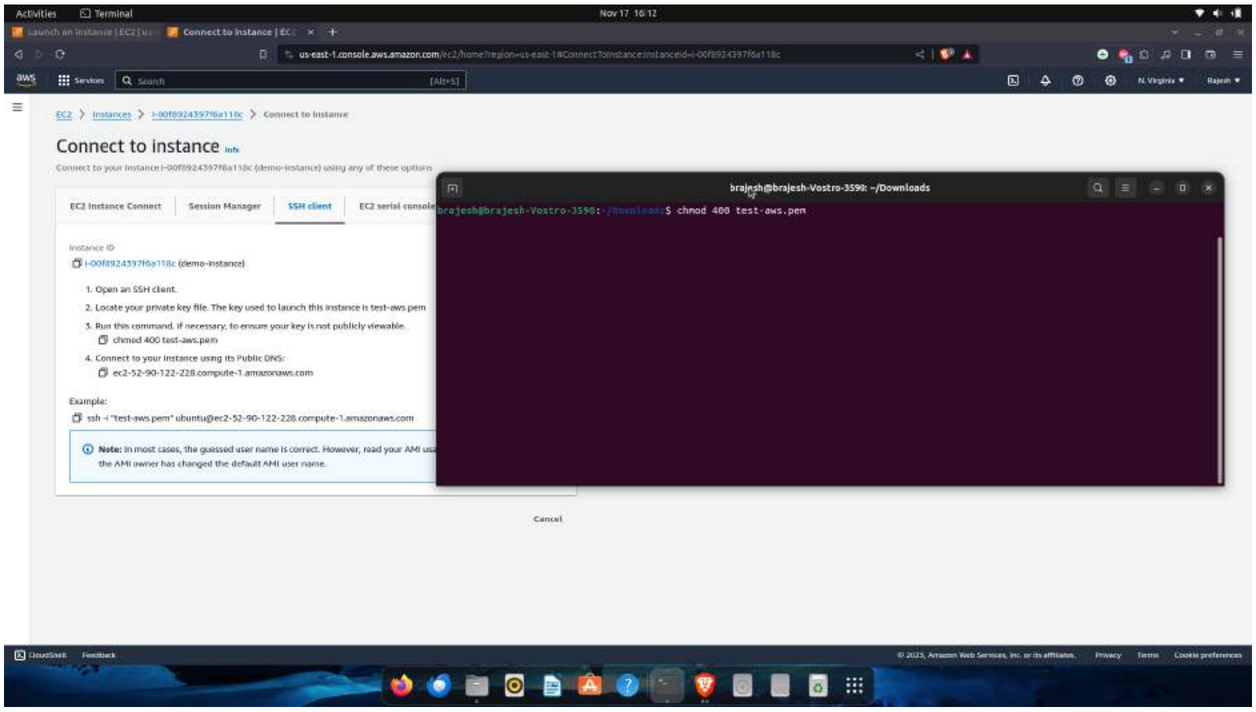
Example:

ssh -i "test-aws.pem" ubuntu@ec2-52-90-122-228.compute-1.amazonaws.com

Note: In most cases, the guessed user name is correct. However, read your AMI us… the AMI owner has changed the default AMI user name.

```
brajesh@brajesh-Vostro-3590:~/Downloads$
```

Step 29: Provide 400 permission to your .pem file



EC2 > Instances > i-00f8924397f6a118c > Connect to instance

Connect to instance Info

Connect to your instance i-00f8924397f6a118c (demo-instance) using any of these options

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

Instance ID

i-00f8924397f6a118c (demo-instance)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is test-aws.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 test-aws.pem
4. Connect to your instance using its Public DNS:
   ec2-52-90-122-228.compute-1.amazonaws.com

Example:

ssh -i "test-aws.pem" ubuntu@ec2-52-90-122-228.compute-1.amazonaws.com

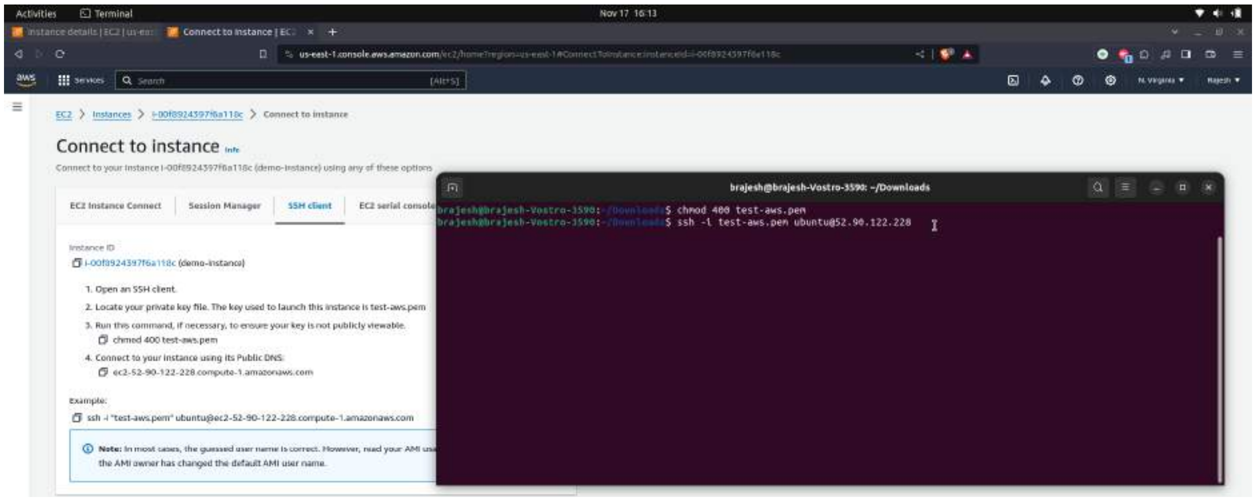
Note: In most cases, the guessed user name is correct. However, read your AMI us… the AMI owner has changed the default AMI user name.

```
brajesh@brajesh-Vostro-3590:~/Downloads$ chmod 400 test-aws.pem
```

Step 30: run ssh command to connect

Run this command : **ssh -i test-aws.pem ubuntu@ipaddress**

Replace ip address with your instance public ip address.



Connect to instance

Connect to your instance i-00f8924397f6a118c (demo-instance) using any of these options

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

Instance ID

i-00f8924397f6a118c (demo-instance)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is test-aws.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 test-aws.pem
4. Connect to your instance using its Public DNS:
   ec2-52-90-122-228.compute-1.amazonaws.com

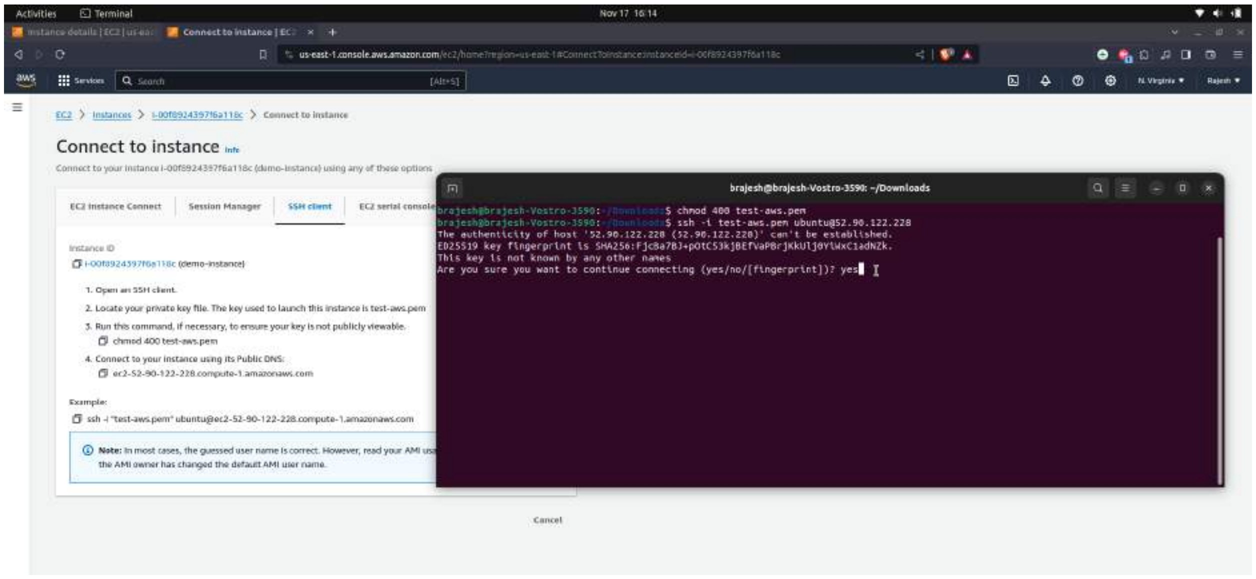
Example:

ssh -i "test-aws.pem" ubuntu@ec2-52-90-122-228.compute-1.amazonaws.com

Note: In most cases, the guessed user name is correct. However, read your AMI usa… the AMI owner has changed the default AMI user name.

```
brajesh@brajesh-Vostro-3590:~/Downloads$ chmod 400 test-aws.pem
brajesh@brajesh-Vostro-3590:~/Downloads$ ssh -i test-aws.pem ubuntu@52.90.122.228
```

Step 31: Type yes

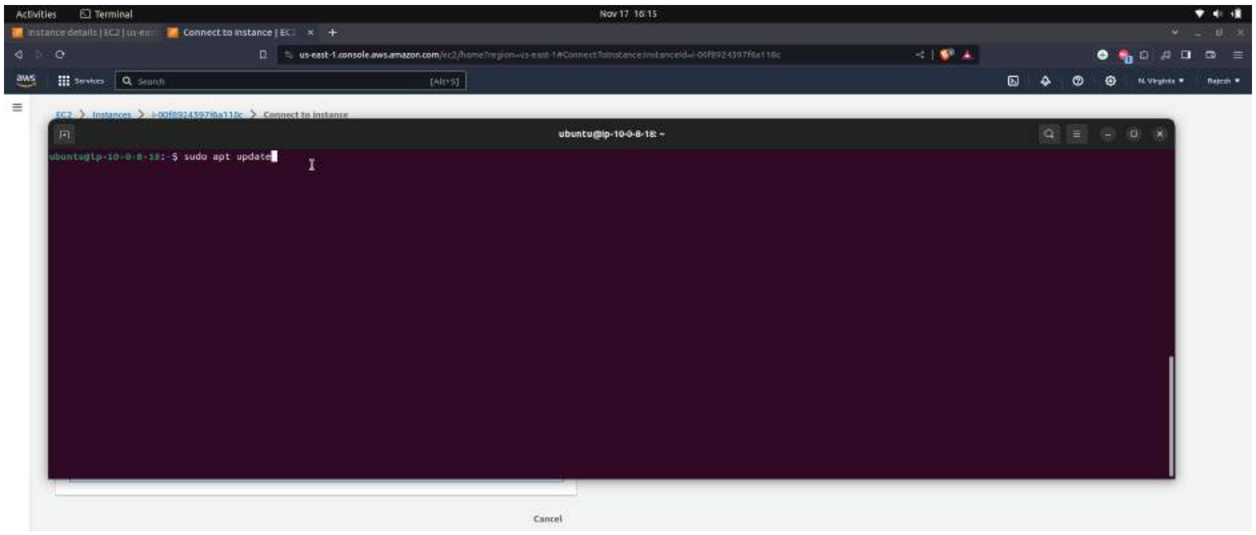


```
brajesh@brajesh-Vostro-3590:~/Downloads$ chmod 400 test-aws.pem
brajesh@brajesh-Vostro-3590:~/Downloads$ ssh -i test-aws.pem ubuntu@52.90.122.228
The authenticity of host '52.90.122.228 (52.90.122.228)' can't be established.
ED25519 key fingerprint is SHA256:FjcBa7BJ+pOtC53kjBEfVaPBrjKkUlj0YlWxC1adNZk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Step 32:Best practice to update your instance

After successfully connecting to your instance.

Run this command : **sudo apt update**

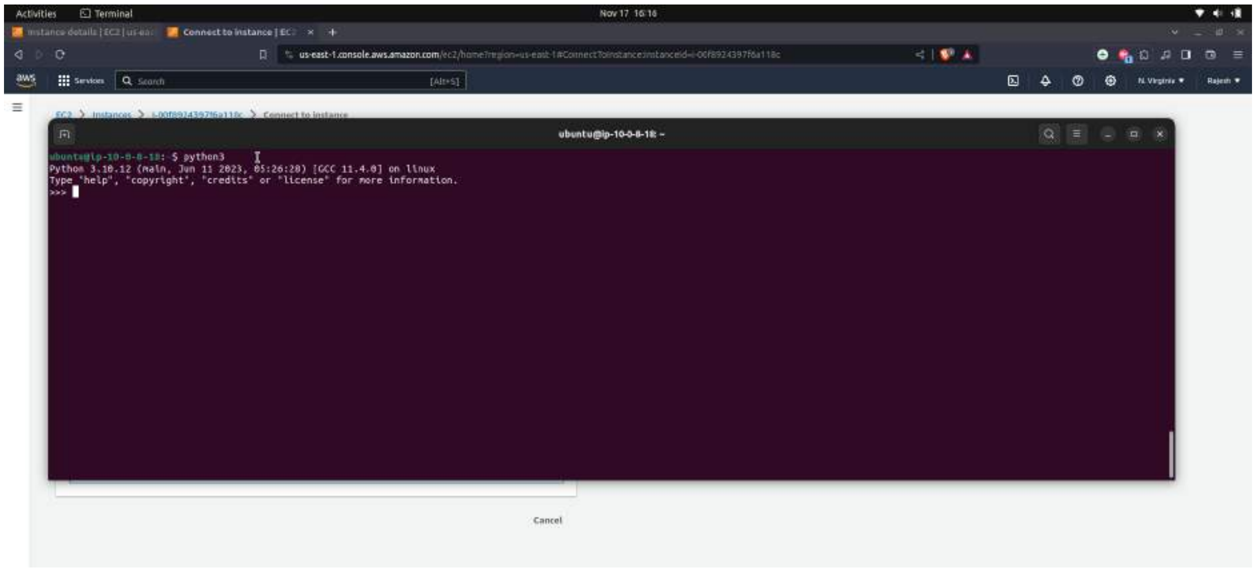


```
ubuntu@ip-10-0-8-18:~$ sudo apt update
```

Step 33: Check python3 is available or not ?

Run this command : **python3**

If you don’t have it ,then install it.

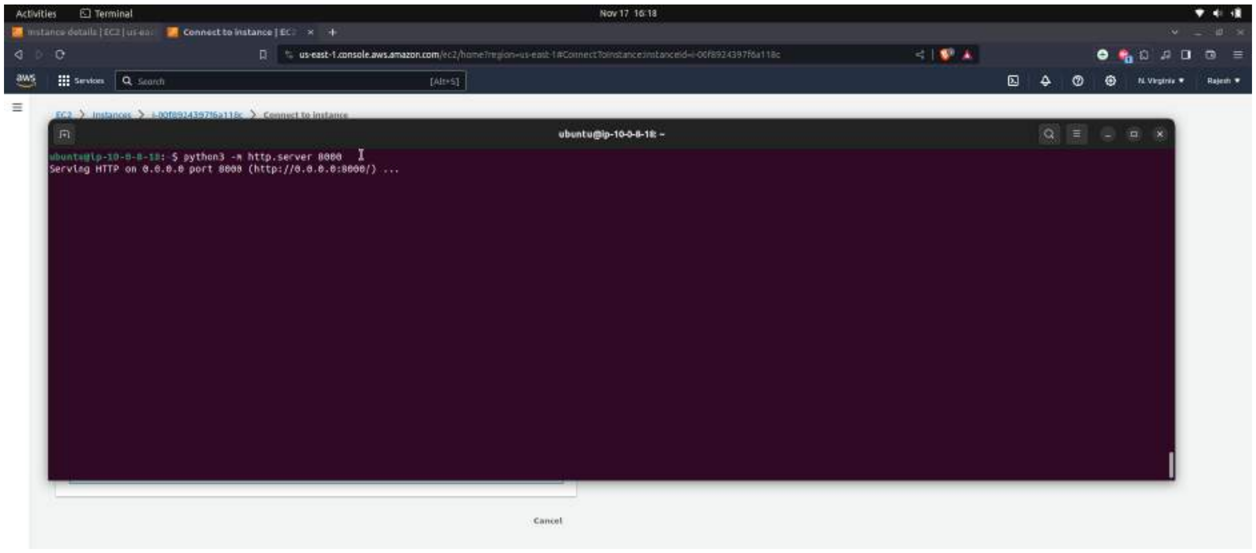


```
ubuntu@ip-10-0-8-18:~$ python3
Python 3.10.12 (main, Jun 11 2023, 05:26:20) [GCC 11.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 
```

Step 34: Now run the basic python server

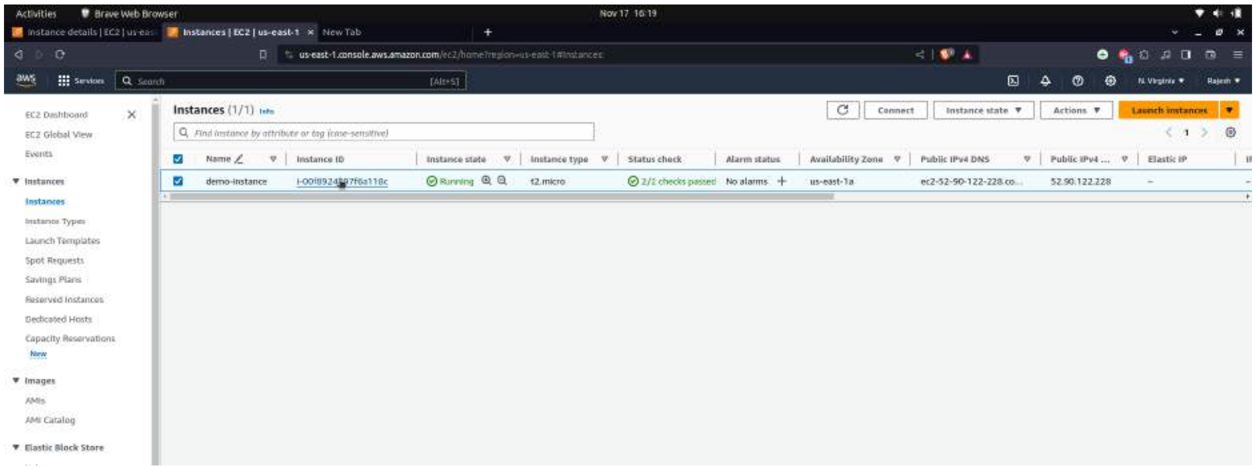
Run this command: **python3 -m http.server 8000**

It Will start a basic http server in our Instance.you can access it from port 8000.



```
ubuntu@ip-10-0-0-18:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

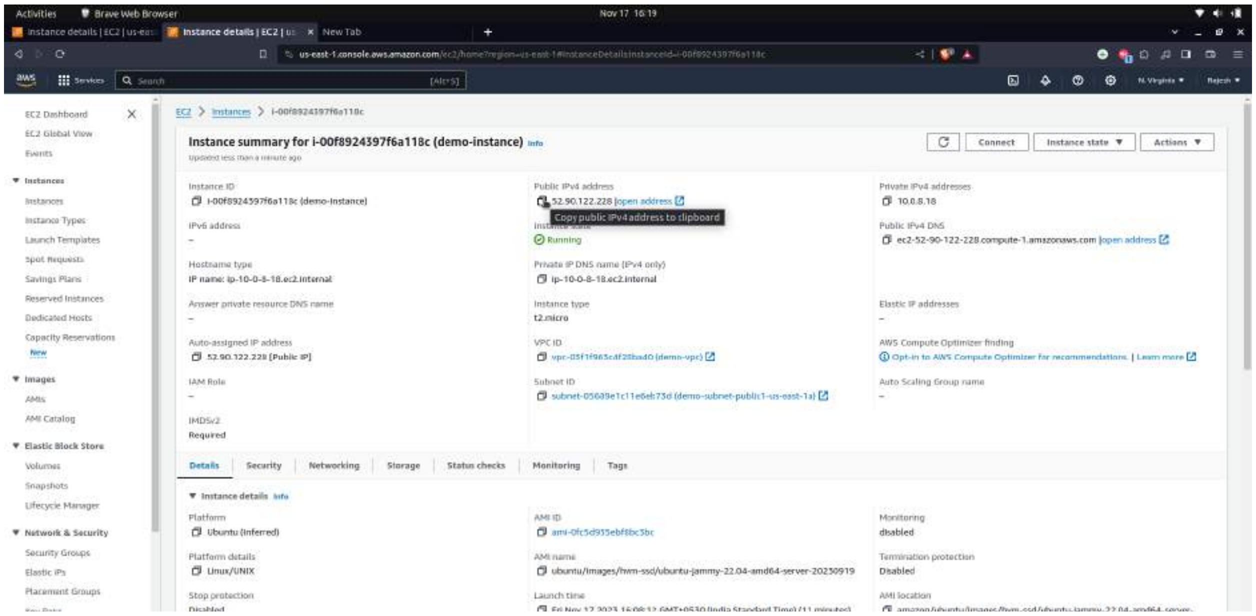
Step 35: Go to your Instance



Instances (1/1)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
demo-instance	i-00f8924397f6a118c	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-52-90-122-228.co...	52.90.122.228	–

Step 36:copy your Instance public IP address



EC2 > Instances > i-00f8924397f6a118c

Instance summary for i-00f8924397f6a118c (demo-instance) Info
Updated less than a minute ago

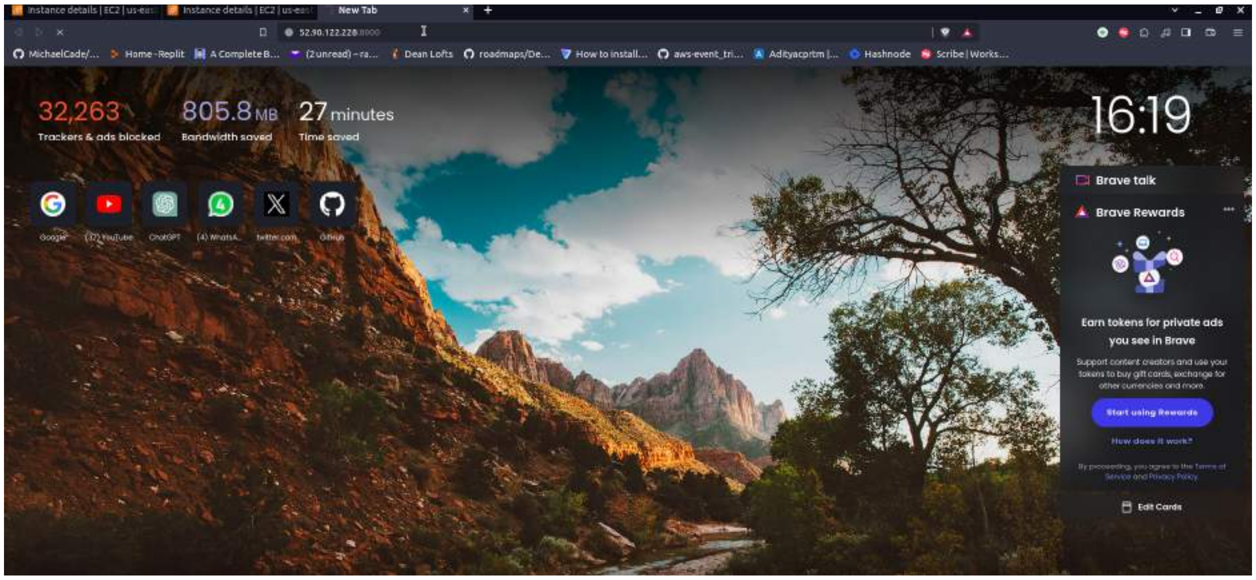
Instance ID: i-00f8924397f6a118c (demo-instance)
Public IPv4 address: 52.90.122.228 | open address
Copy public IPv4 address to clipboard
Private IPv4 addresses: 10.0.8.18
IPv6 address: –
Instance state: Running
Public IPv4 DNS: ec2-52-90-122-228.compute-1.amazonaws.com | open address
Hostname type: IP name: ip-10-0-8-18.ec2.internal
Private IP DNS name (IPv4 only): ip-10-0-8-18.ec2.internal
Answer private resource DNS name: –
Instance type: t2.micro
Elastic IP addresses: –
Auto-assigned IP address: 52.90.122.228 [Public IP]
VPC ID: vpc-05f1f963cdf20bad0 (demo-vpc)
AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role: –
Subnet ID: subnet-05609e1c11e6eb73d (demo-subnet-public1-us-east-1a)
Auto Scaling Group name: –
IMDSv2: Required

Instance details Info
Platform: Ubuntu (Inferred)
AMI ID: ami-0fc5d935ebf8bc3bc
Monitoring: disabled
Platform details: Linux/UNIX
AMI name: ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20230919
Termination protection: Disabled
Stop protection: Disabled
Launch time: Fri Nov 17 2023 16:08:12 GMT+0530 (India Standard Time) (11 minutes)
AMI location: amazon/ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-

Step 37:Try to access our server

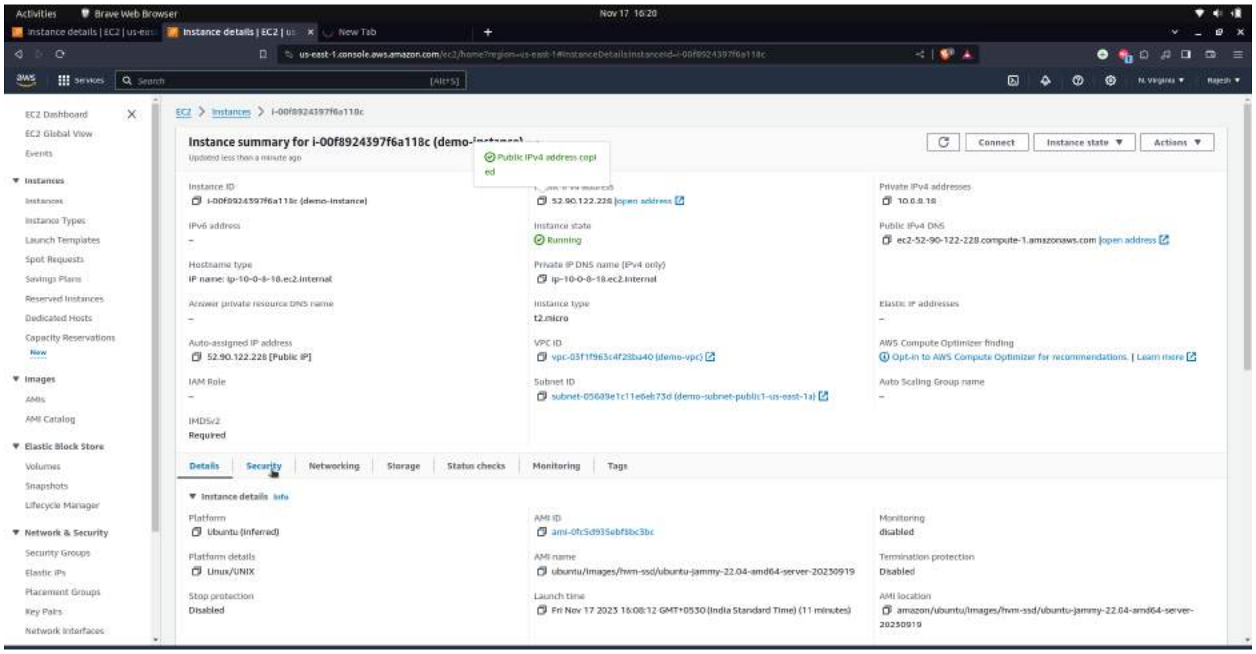
Open a new tab in your browser and type like this in your address bar:
" [http://copiedipaddrees:8000".](http://copiedipaddrees:8000) Replace *copiedipaddress* with your instance public ip address.

You can't open it .By default the security groups won't allow traffic inbound.

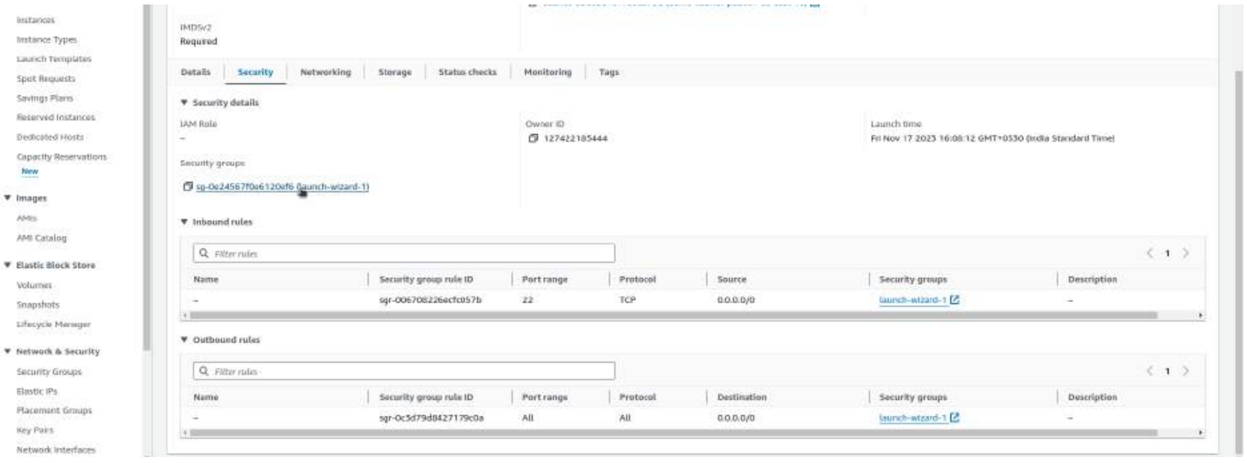


Step 38:Go back to your instance settings (security)

Open your instance tab and click on security tab



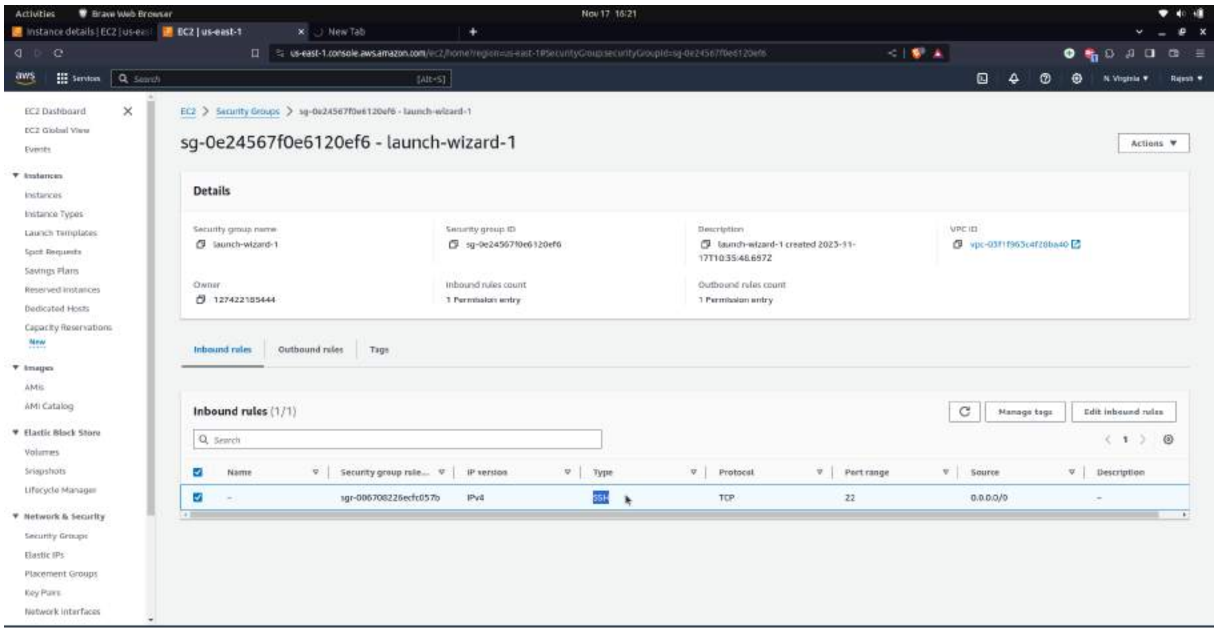
Step 39:Click on security groups



Step 40: Observe a bit

Initially the security groups are allowing port 22 only for ssh .Now we need to add a new rule.

Before that we will check NACLs


sg-0e24567f0e6120ef6 - launch-wizard-1

Details

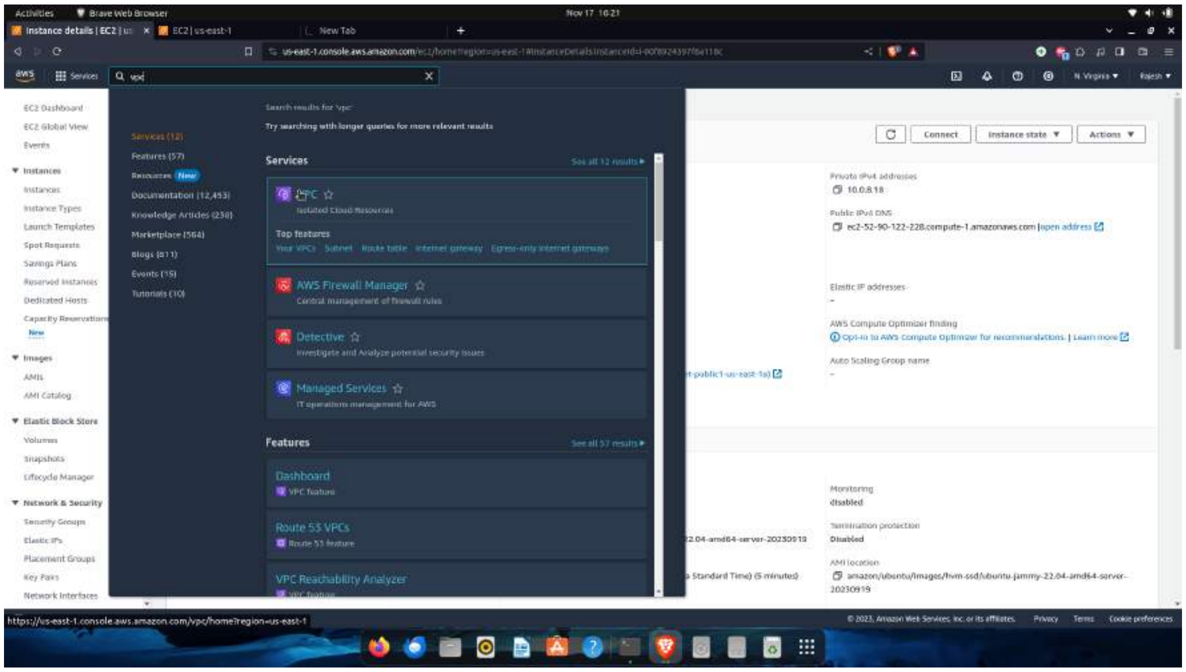
Security group name	Security group ID	Description	VPC ID
launch-wizard-1	sg-0e24567f0e6120ef6	launch-wizard-1 created 2023-11-17T10:35:48.697Z	vpc-03f1f963c4f28ba40

Owner	Inbound rules count	Outbound rules count
127422185444	1 Permission entry	1 Permission entry

Inbound rules (1/1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
–	sgr-006708226ecfc057b	IPv4	SSH	TCP	22	0.0.0.0/0	–

Step 41: Open VPC


Search results for 'vpc'

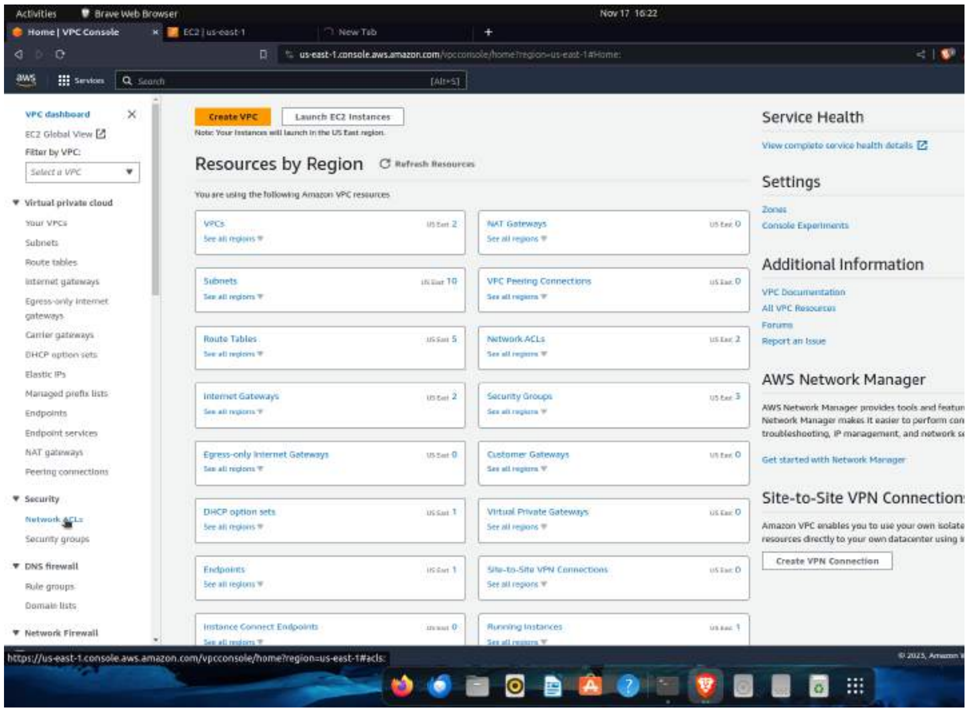
Try searching with longer queries for more relevant results

Services (12), Features (57), Resources, Documentation (12,453), Knowledge Articles (238), Marketplace (564), Blogs (811), Events (15), Tutorials (10)

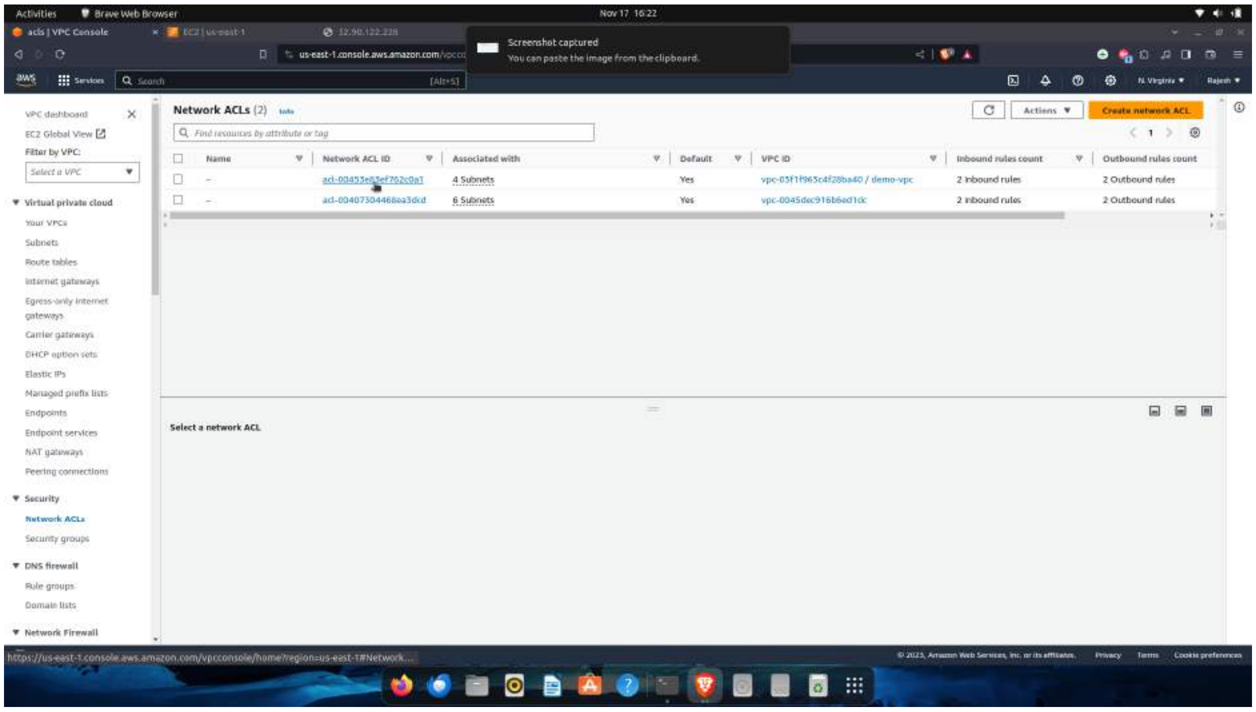
Services:
- VPC – Isolated Cloud Resources. Top features: Your VPCs, Subnet, Route table, Internet gateway, Egress-only internet gateways
- AWS Firewall Manager – Central management of firewall rules
- Detective – Investigate and Analyze potential security issues
- Managed Services – IT operations management for AWS

Features:
- Dashboard – VPC feature
- Route 53 VPCs – Route 53 feature
- VPC Reachability Analyzer – VPC feature

Step 42: Click “network NACLs” in under “security”



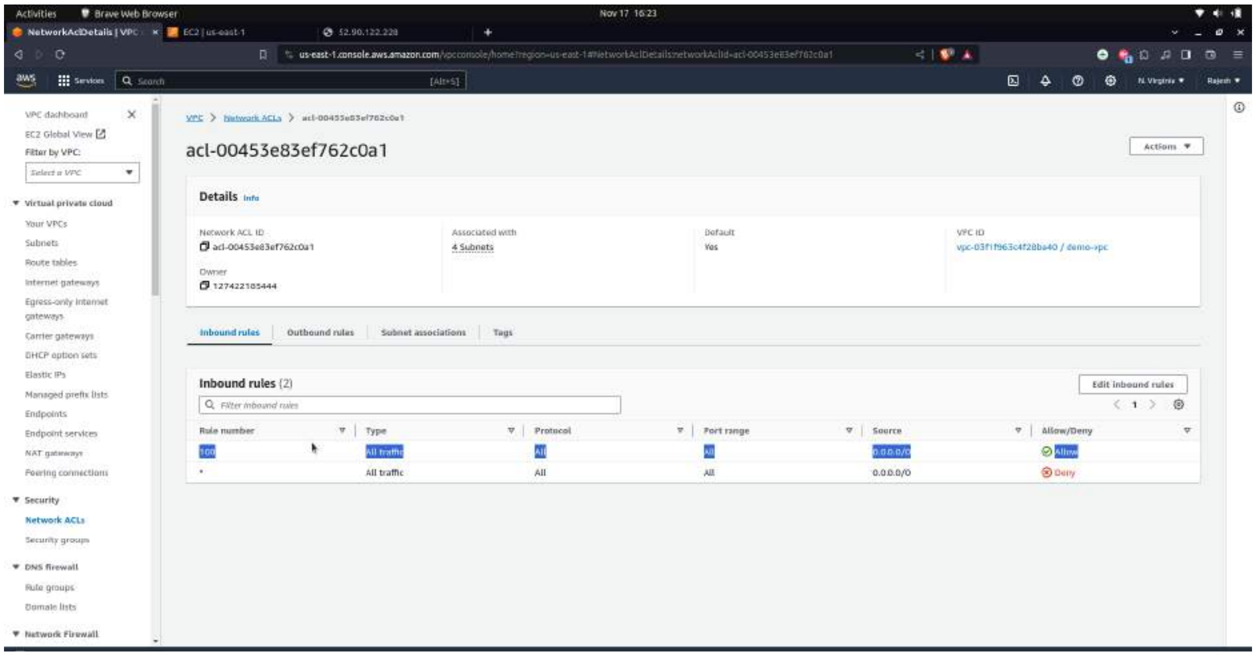
Step 43:Click on your demo vpc



Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
–	acl-00453e83ef762c0a1	4 Subnets	Yes	vpc-03f1f963c4f28ba40 / demo-vpc	2 Inbound rules	2 Outbound rules
–	acl-00407304468ea3dcd	6 Subnets	Yes	vpc-0045dec916b6ed1dc	2 Inbound rules	2 Outbound rules

Step 44:Observe the inbound rules

NACLs allowing all traffic .Here we got an idea that there is no problem in VPC NACLs



VPC > Network ACLs > acl-00453e83ef762c0a1

acl-00453e83ef762c0a1

Details

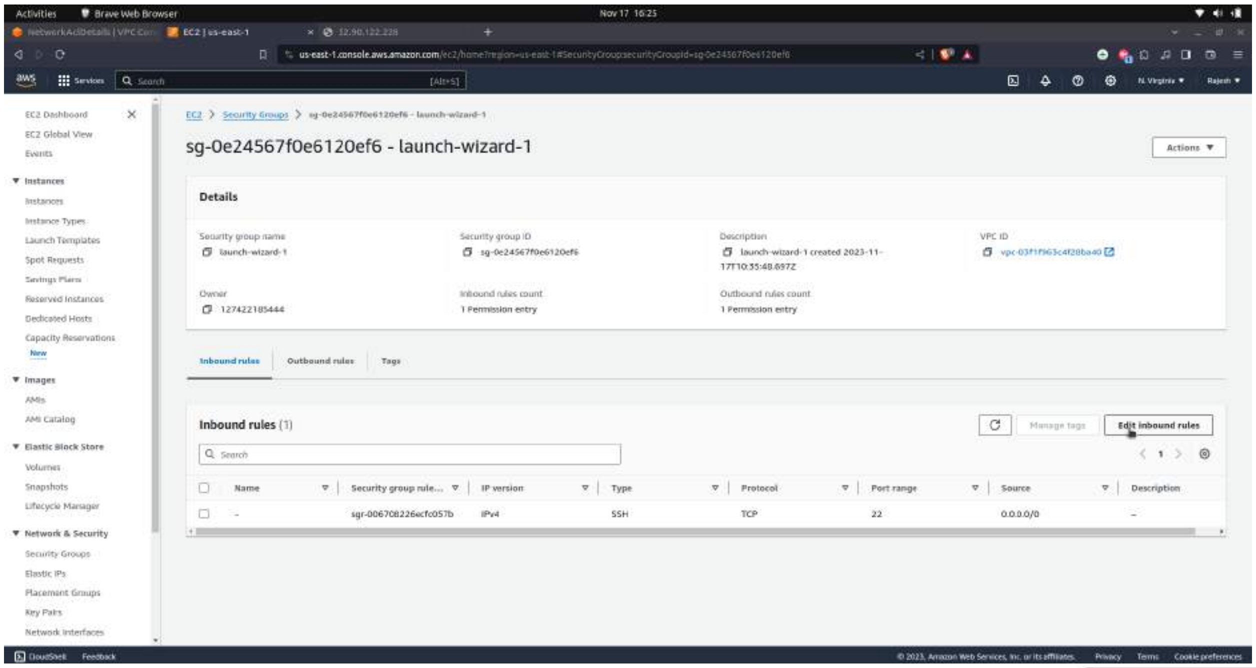
Network ACL ID: acl-00453e83ef762c0a1
Associated with: 4 Subnets
Default: Yes
VPC ID: vpc-03f1f963c4f28ba40 / demo-vpc
Owner: 127422185444

Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Step 45:Come back to ec2 instance security groups

Click on **Edit Inbound Rules**



EC2 > Security Groups > sg-0e24567f0e6120ef6 - launch-wizard-1

sg-0e24567f0e6120ef6 - launch-wizard-1

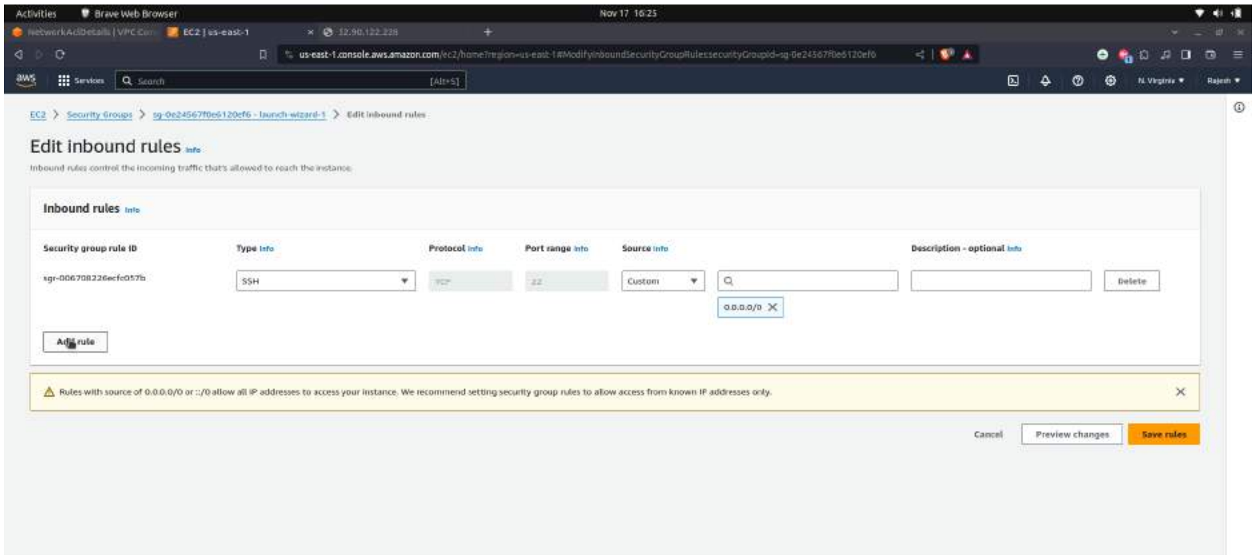
Details

Security group name: launch-wizard-1
Security group ID: sg-0e24567f0e6120ef6
Description: launch-wizard-1 created 2023-11-17T10:35:48.697Z
VPC ID: vpc-03f1f963c4f28ba40
Owner: 127422185444
Inbound rules count: 1 Permission entry
Outbound rules count: 1 Permission entry

Inbound rules (1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-006708226ecfc057b	IPv4	SSH	TCP	22	0.0.0.0/0	–

Step 46: Click on Add Rule



EC2 > Security Groups > sg-0e24567f0e6120ef6 - 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	Protocol	Port range	Source		Description - optional
sgr-006708226ecfc057b	SSH	TCP	22	Custom	0.0.0.0/0	

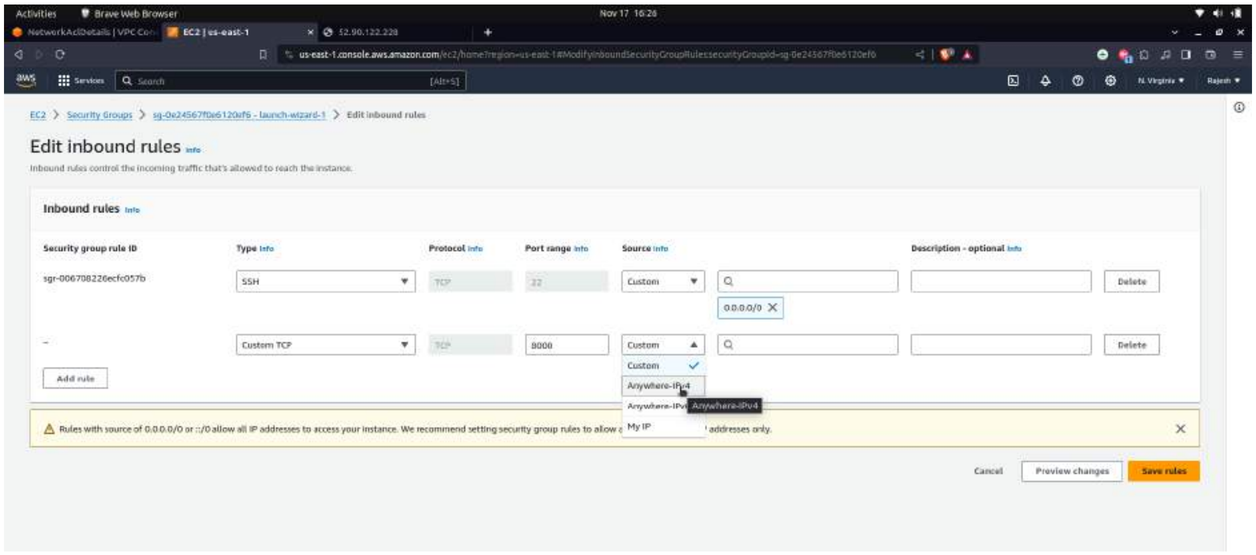
Add rule

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

Step 47: Apply this changes

Choose **CustomTcp** as type mention **8000** in port range .In source select **anywhere ipv4**



EC2 > Security Groups > sg-0e24567f0e6120ef6 - 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

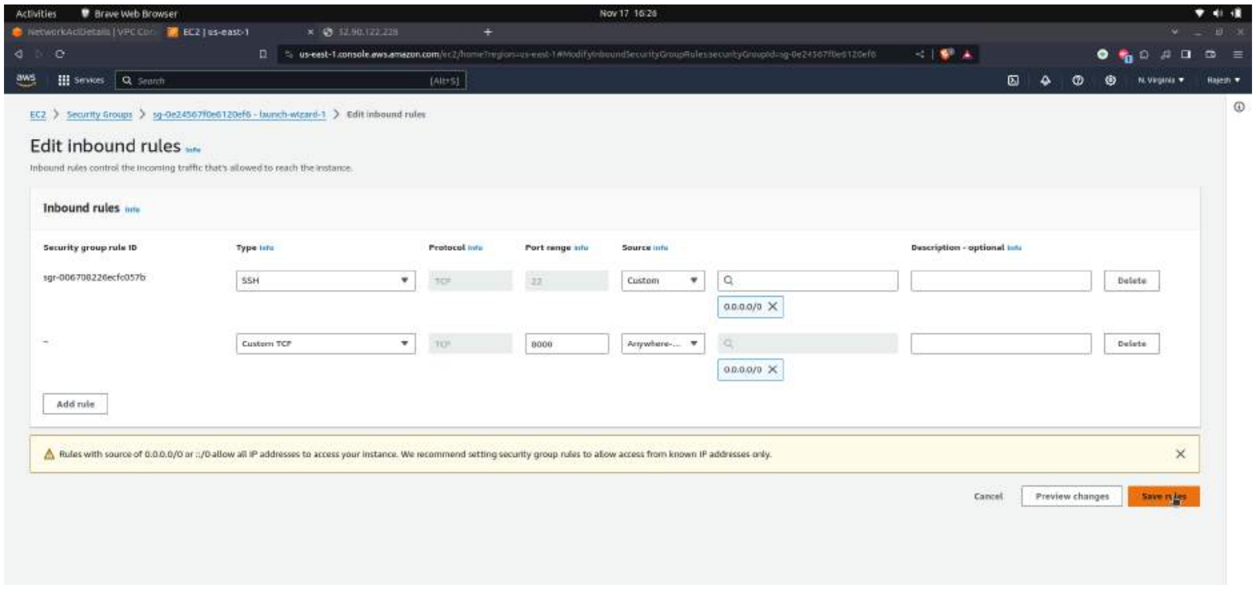
Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-006708226ecfc057b	SSH	TCP	22	Custom	0.0.0.0/0	
-	Custom TCP	TCP	8000	Custom		

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

Step 48: Click on save



Edit inbound rules

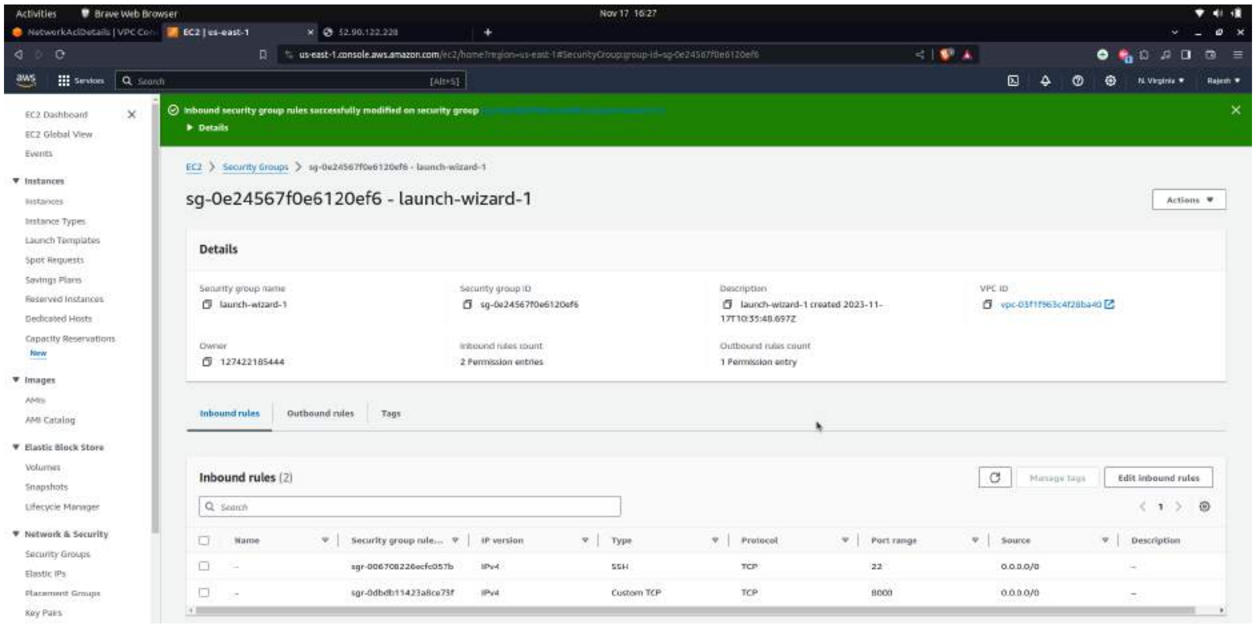
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-006708226ecfc057b	SSH	TCP	22	Custom	0.0.0.0/0	
-	Custom TCP	TCP	8000	Anywhere-...	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.

Step 49: successfully edited the inbound rules



Inbound security group rules successfully modified on security group

sg-0e24567f0e6120ef6 - launch-wizard-1

Details

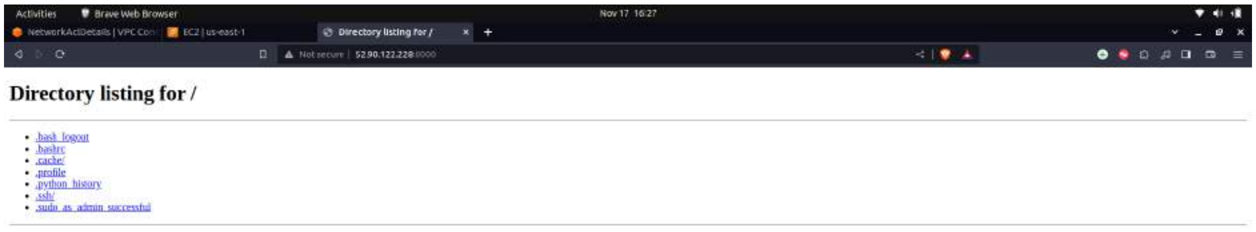
Security group name: launch-wizard-1	Security group ID: sg-0e24567f0e6120ef6	Description: launch-wizard-1 created 2023-11-17T10:35:48.697Z	VPC ID: vpc-03f1f963c4f28ba40
Owner: 127422185444	Inbound rules count: 2 Permission entries	Outbound rules count: 1 Permission entry	

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
–	sgr-006708226ecfc057b	IPv4	SSH	TCP	22	0.0.0.0/0	–
–	sgr-0dbdb11423a8ce73f	IPv4	Custom TCP	TCP	8000	0.0.0.0/0	–

Step 50:Open your previous tab and refresh it

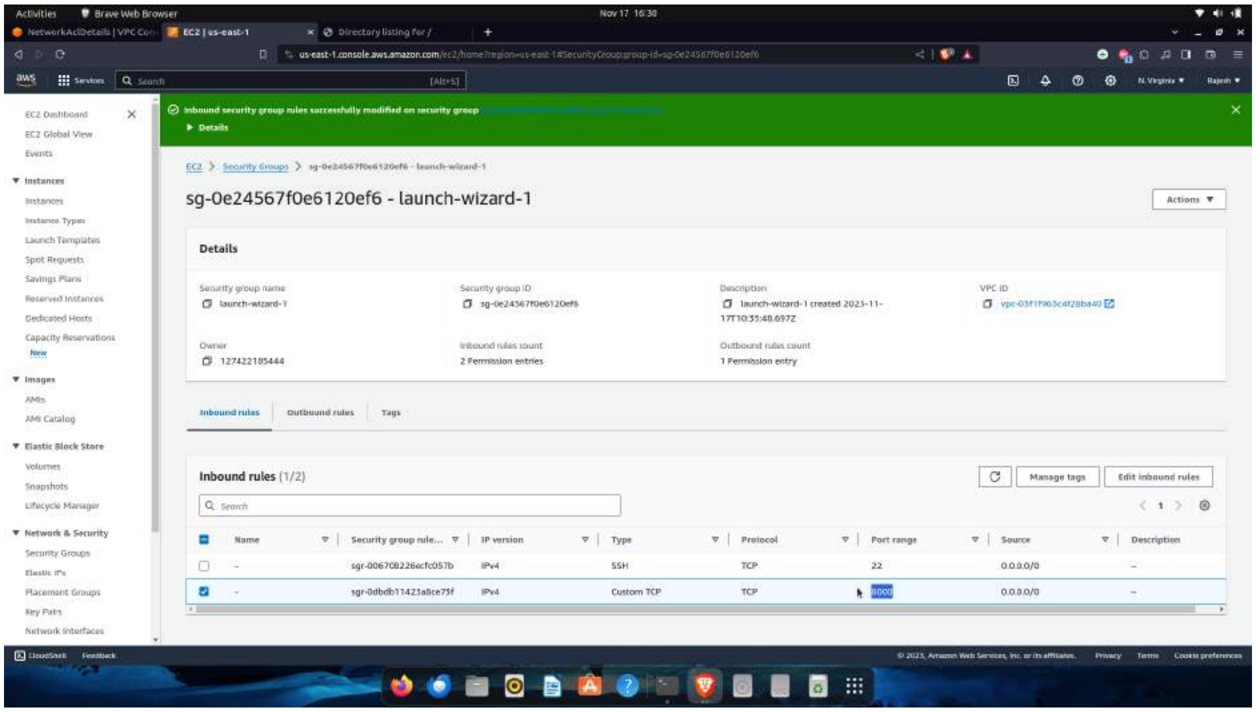
Now you may accessing your instance 🌐



Directory listing for /

- .bash_logout
- .bashrc
- .cache/
- .profile
- .python_history
- .ssh/
- .sudo_as_admin_successful

Step 51:Security group allowing port 8000



Inbound security group rules successfully modified on security group

sg-0e24567f0e6120ef6 - launch-wizard-1

Details

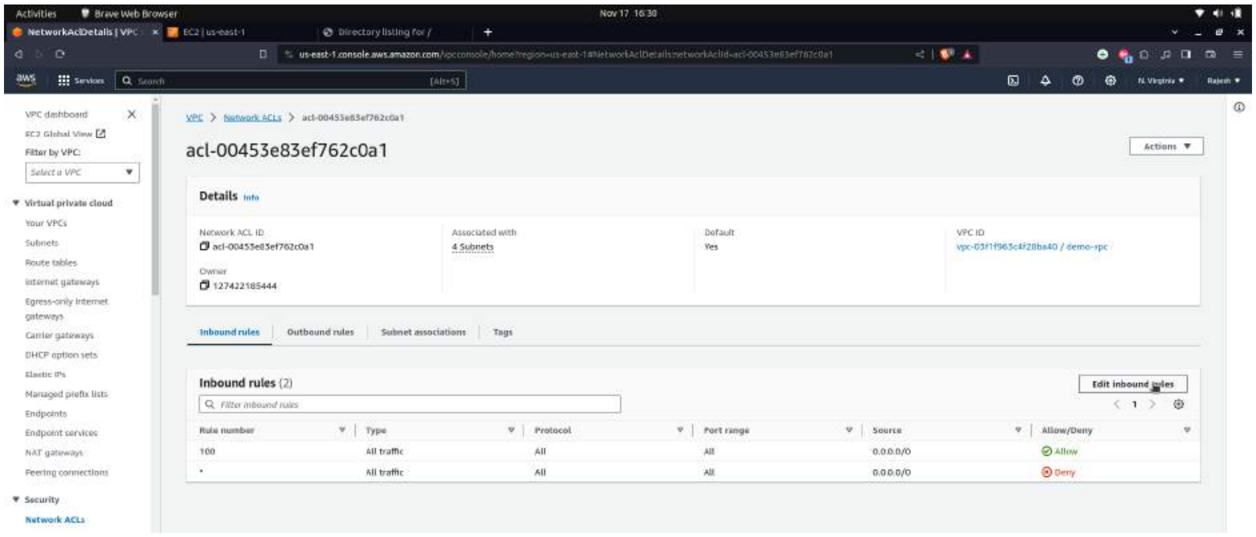
Security group name	Security group ID	Description	VPC ID
launch-wizard-1	sg-0e24567f0e6120ef6	launch-wizard-1 created 2023-11-17T10:35:48.697Z	vpc-03f1f963c4f28ba40
Owner	**Inbound rules count**	**Outbound rules count**	
127422185444	2 Permission entries	1 Permission entry	

Inbound rules (1/2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
–	sgr-006708226ecfc057b	IPv4	SSH	TCP	22	0.0.0.0/0	–
–	sgr-0dbdb11423a8ce75f	IPv4	Custom TCP	TCP	8000	0.0.0.0/0	–

Step 52: Go to NACLs setting of your vpc

Click on **Edit inbound rules**



acl-00453e83ef762c0a1

Details

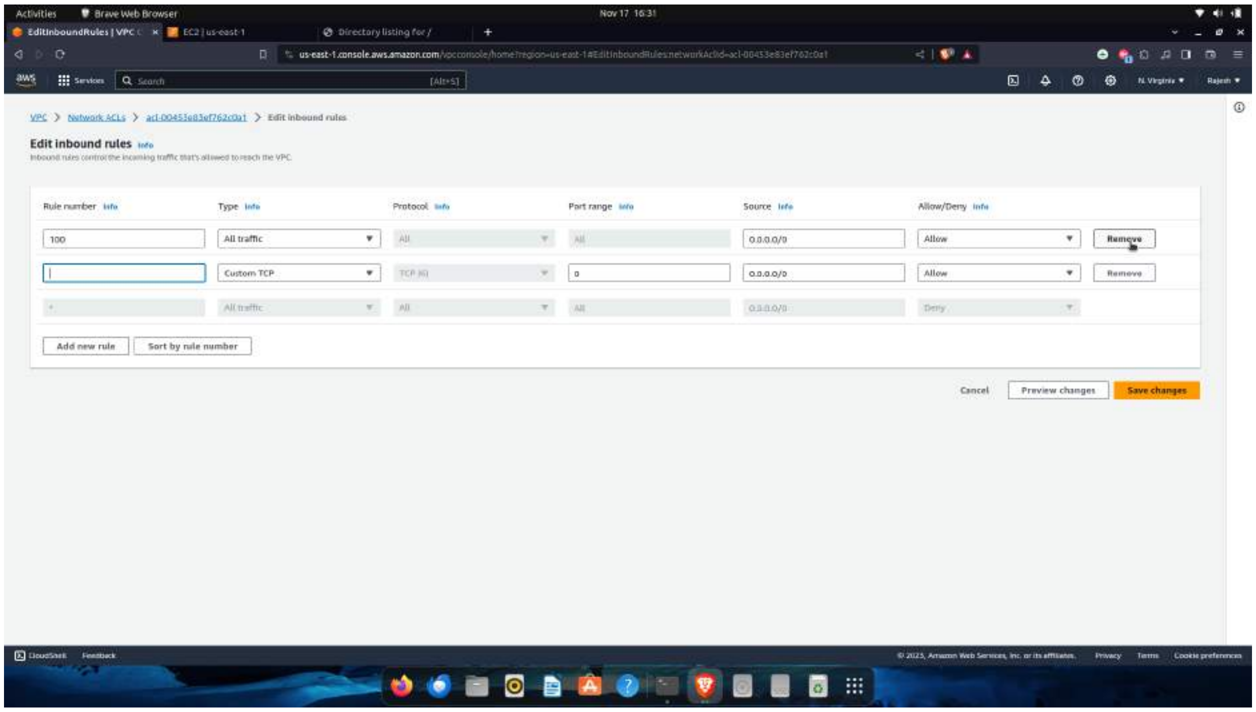
Network ACL ID	Associated with	Default	VPC ID
acl-00453e83ef762c0a1	4 Subnets	Yes	vpc-03f1f963c4f28ba40 / demo-vpc

Owner: 127422185444

Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Step 53: Remove the 100 rule



Edit inbound rules

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

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
	Custom TCP	TCP (6)	0	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

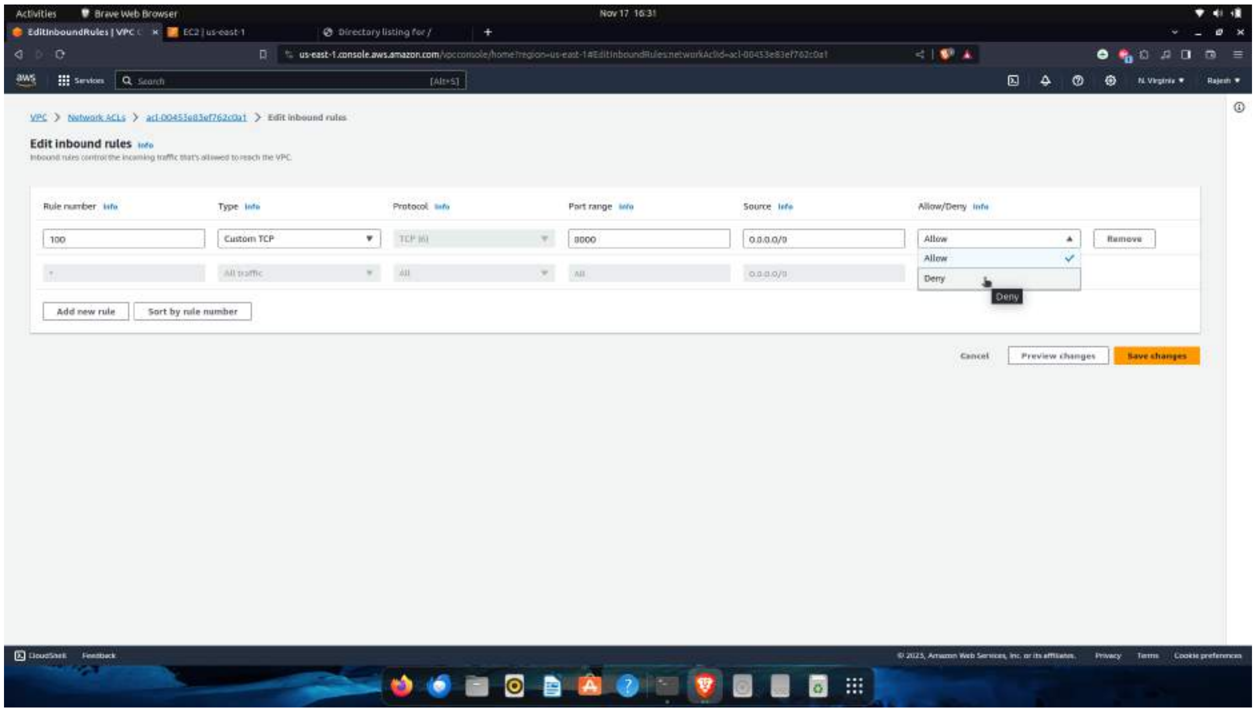
Step 54:Add new 100 rule

Rule number: 100,

Type: Custom TCP

Port range:8000

Choose : Deny



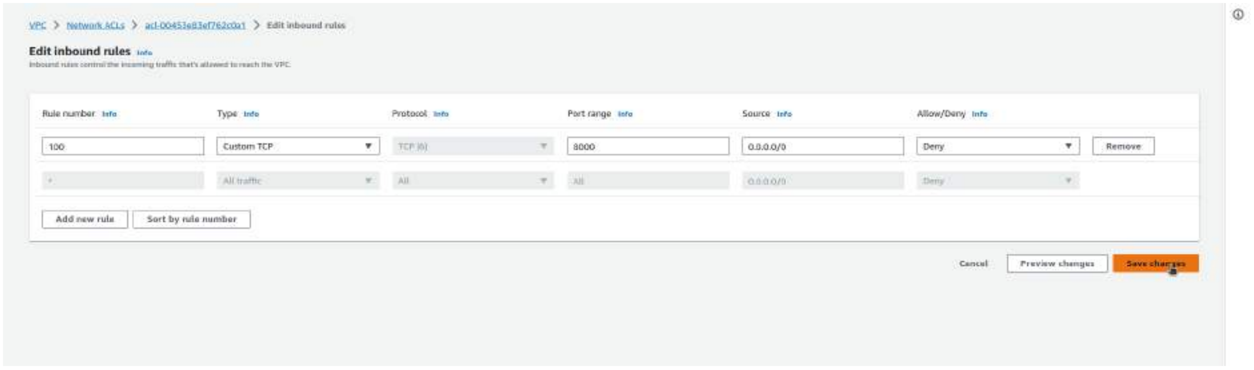
VPC > Network ACLs > acl-00453e83ef762c0a1 > Edit inbound rules

Edit inbound rules

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

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	Custom TCP	TCP (6)	8000	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	

Step 55:Save Changes



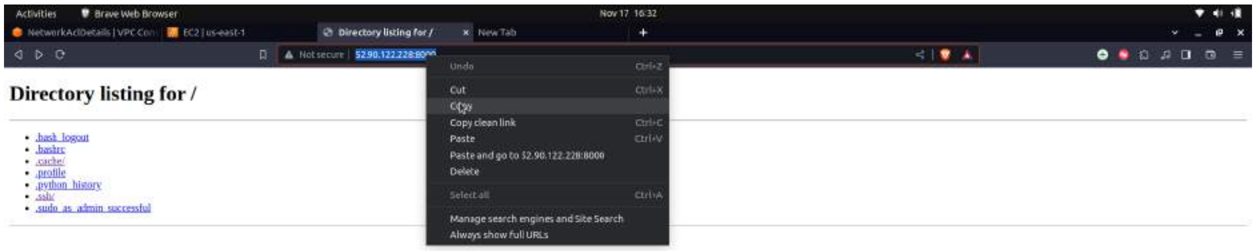
VPC > Network ACLs > acl-00453e83ef762c0a1 > Edit inbound rules

Edit inbound rules

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

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	Custom TCP	TCP (6)	8000	0.0.0.0/0	Deny
*	All traffic	All	All	0.0.0.0/0	Deny

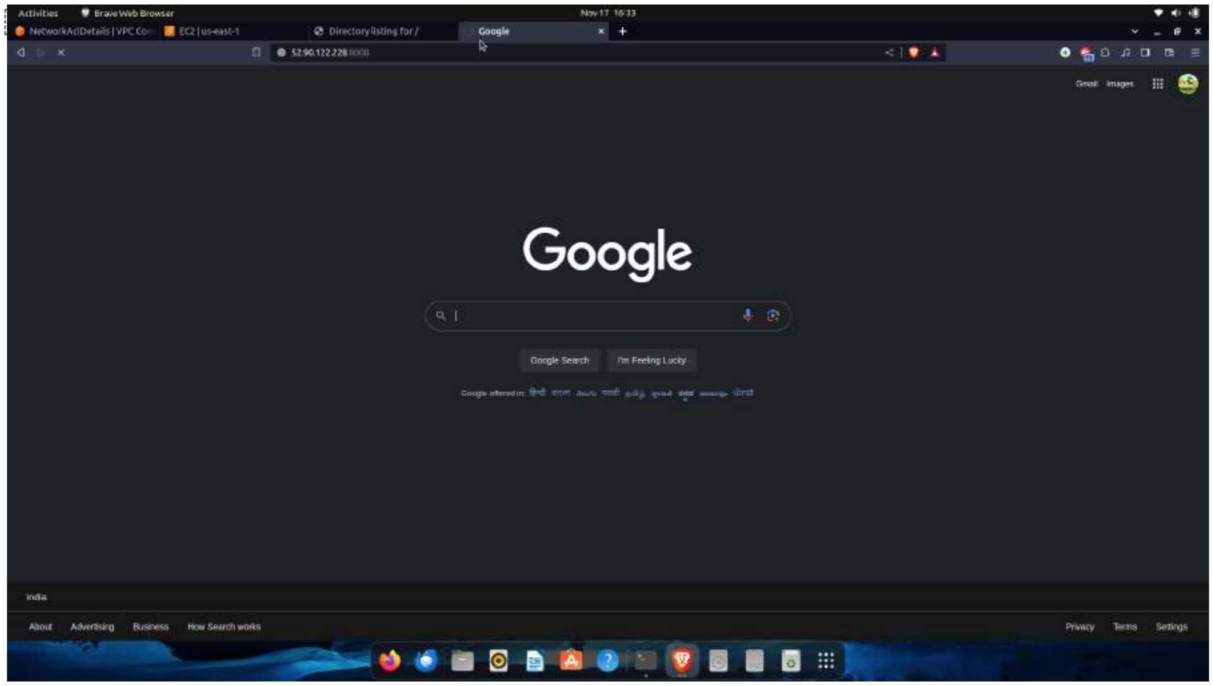
Step 56:Now copy the url of our instance


Directory listing for /

- .bash_logout
- .bashrc
- .cache/
- .profile
- .python_history
- .ssh/
- .sudo_as_admin_successful

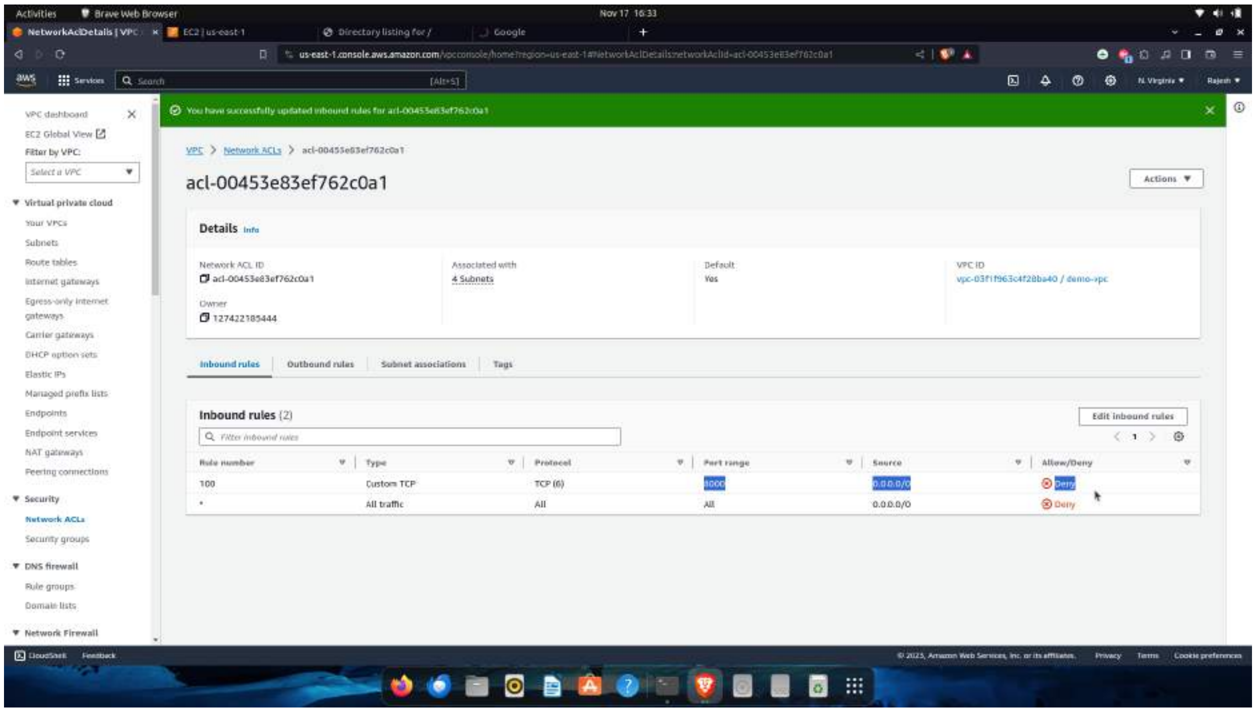
Step 57:paste it a new tab or browser

You don't get any response from our instance.



Step 58:Reason

because ,we deny the traffic from port 8000 at NACLs level.



You have successfully updated inbound rules for acl-00453e83ef762c0a1

VPC > Network ACLs > acl-00453e83ef762c0a1

acl-00453e83ef762c0a1

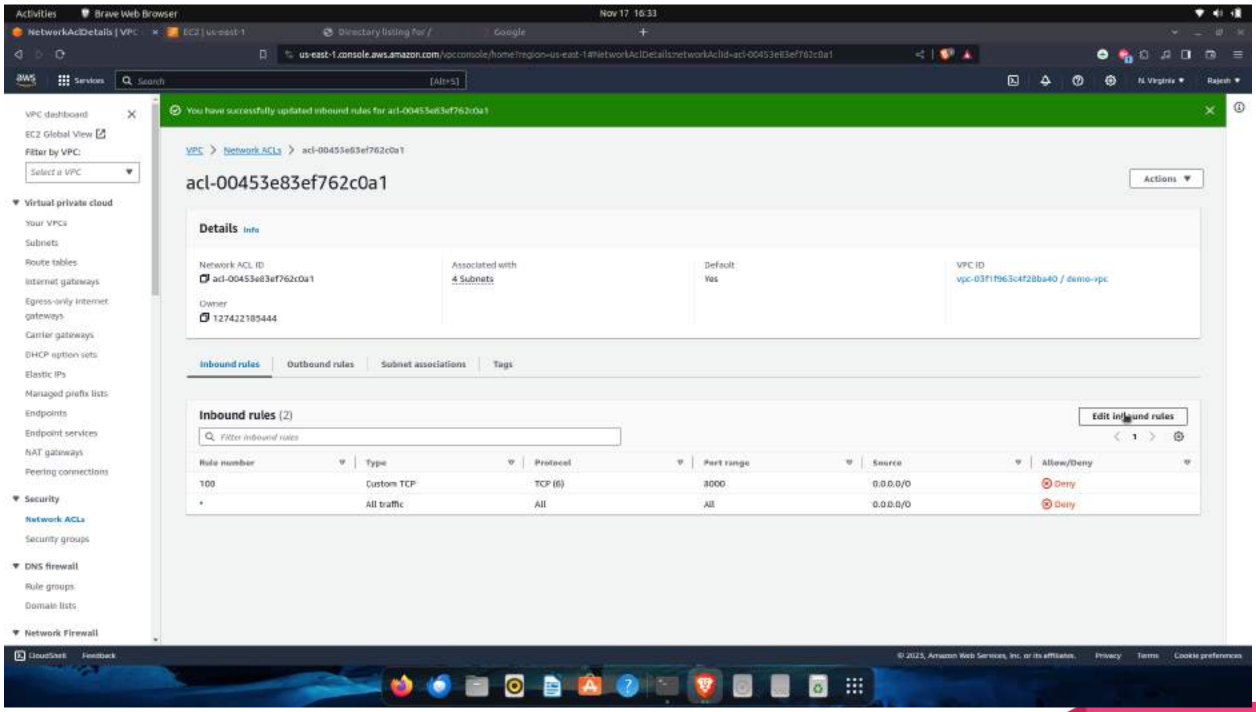
Details

Network ACL ID: acl-00453e83ef762c0a1
Owner: 127422185444
Associated with: 4 Subnets
Default: Yes
VPC ID: vpc-03f1f963c4f28ba40 / demo-vpc

Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	Custom TCP	TCP (6)	8000	0.0.0.0/0	Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Step 59:click on edit inbound rules



You have successfully updated inbound rules for acl-00453e83ef762c0a1

VPC > Network ACLs > acl-00453e83ef762c0a1

acl-00453e83ef762c0a1

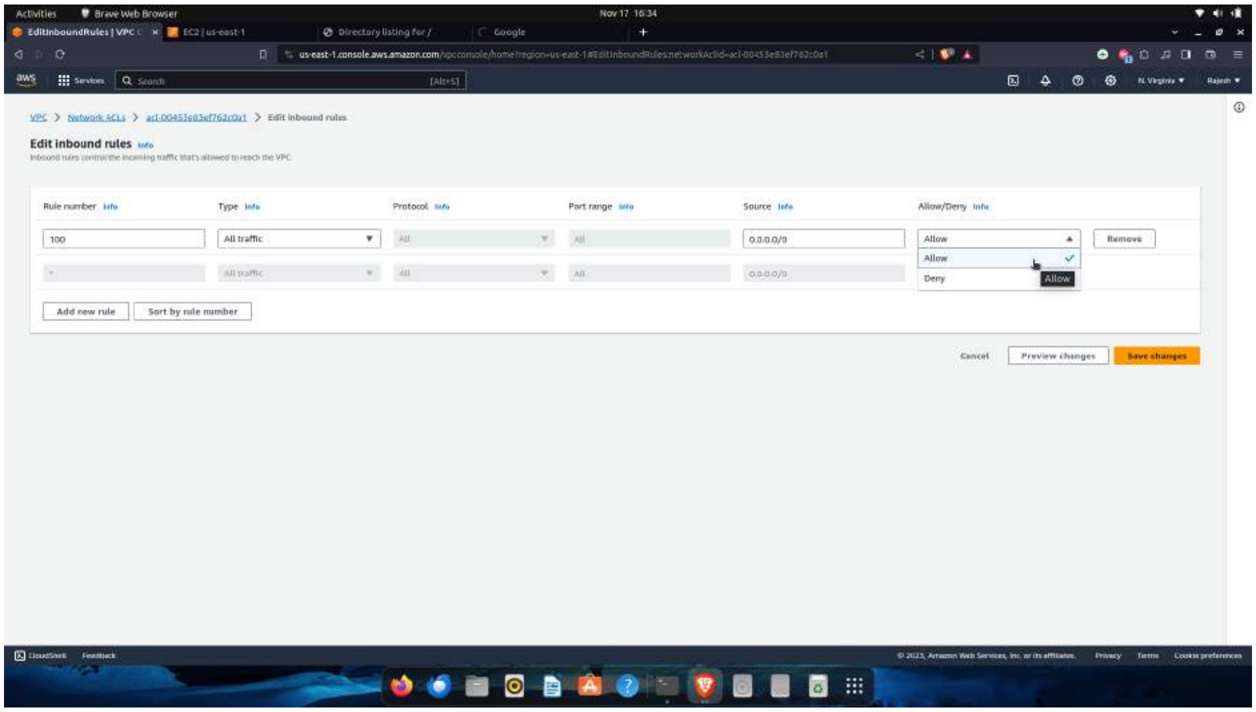
Details

Network ACL ID: acl-00453e83ef762c0a1
Owner: 127422185444
Associated with: 4 Subnets
Default: Yes
VPC ID: vpc-03f1f963c4f28ba40 / demo-vpc

Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	Custom TCP	TCP (6)	8000	0.0.0.0/0	Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Step 60:Now allow all traffic



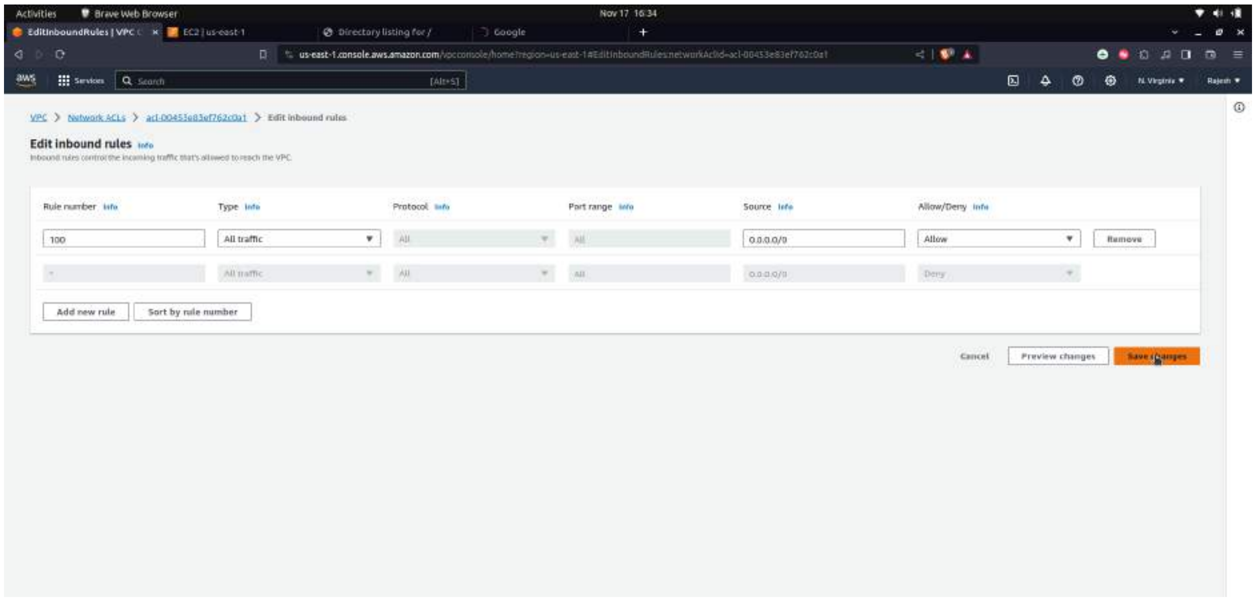
VPC > Network ACLs > acl-00453e83ef762c0a1 > Edit inbound rules

Edit inbound rules Info

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

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	

Step 61:Save changes



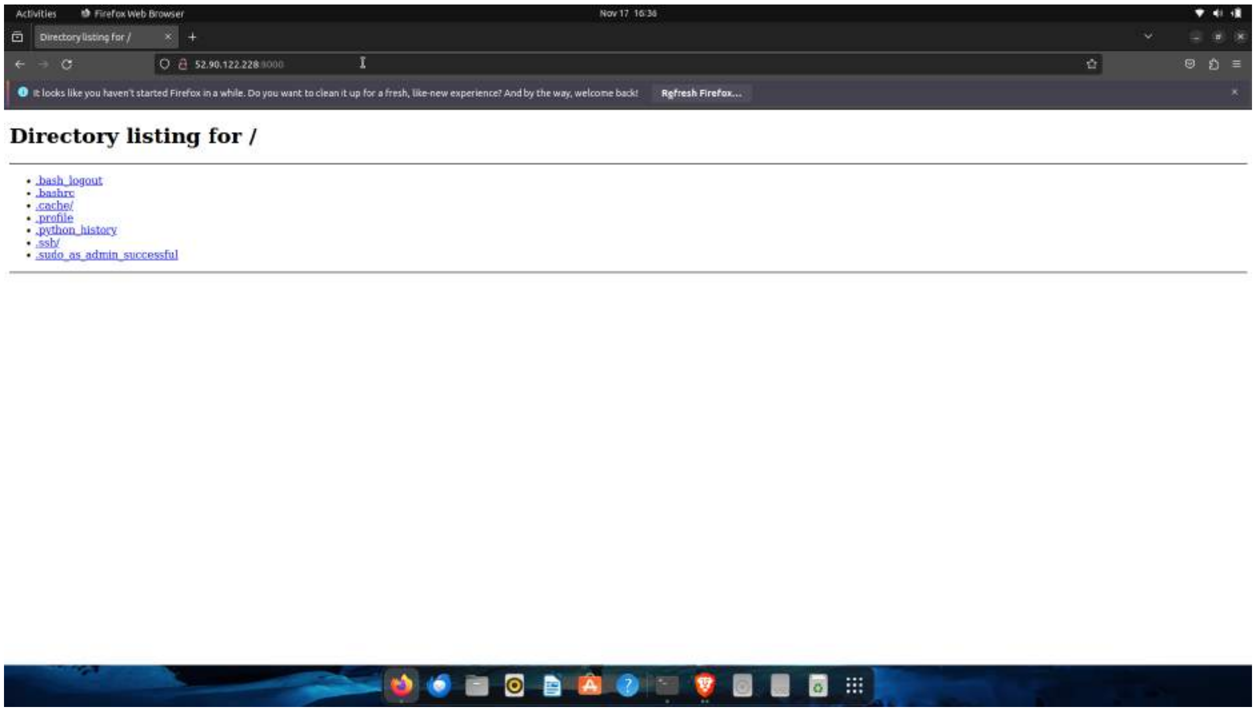
VPC > Network ACLs > acl-00453e83ef762c0a1 > Edit inbound rules

Edit inbound rules Info

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

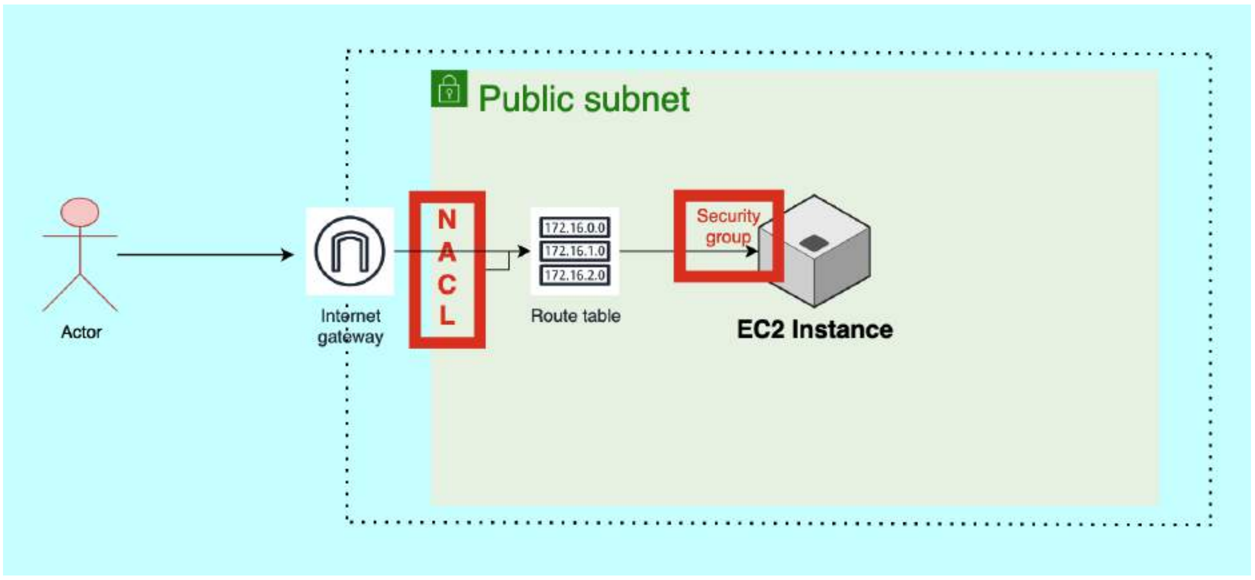
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Step 62:Now server is getting response to port 8000


Activities
Firefox Web Browser
Nov 17 16:36
Directory listing for /
52.90.122.228:8000
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...

Directory listing for /

- .bash_logout
- .bashrc
- .cache/
- .profile
- .python_history
- .ssh/
- .sudo_as_admin_successful



The above is the Architecture of our entire project.

This is all about a small practice project on Security Groups and NACLs .I hope you like this project 🙋.Thank you

by

[Rajesh's blog]