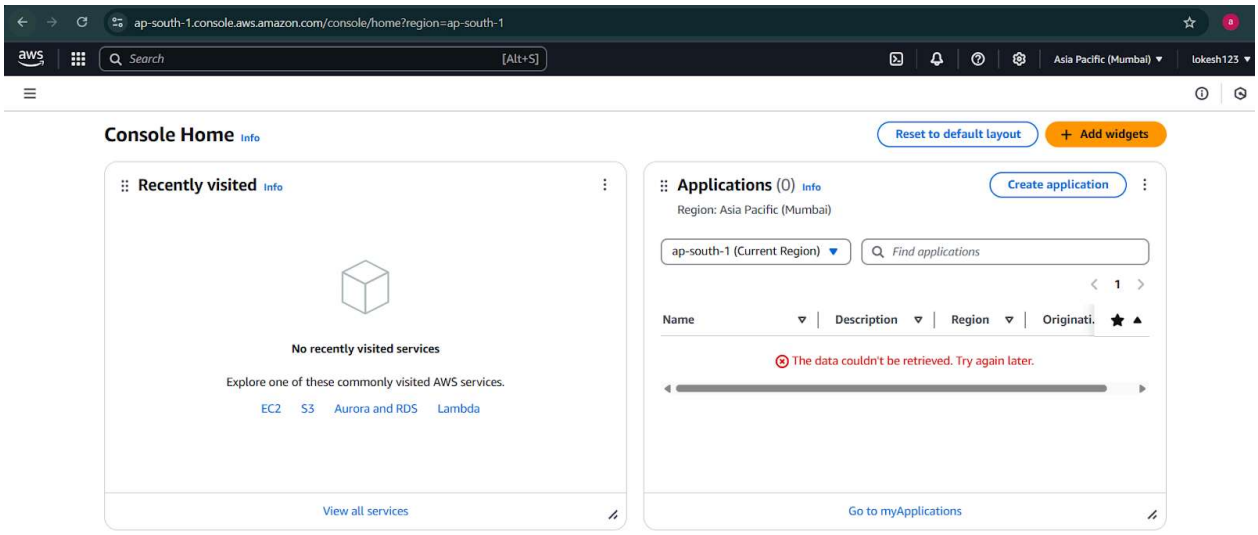
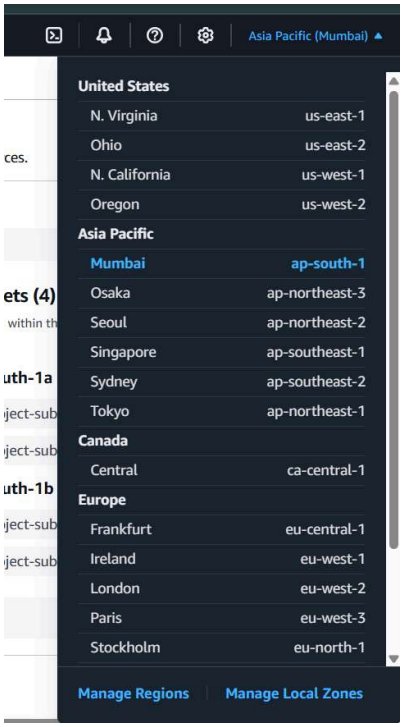
PART1

1. Set up AWS/GCP/Azure VPC with subnets, NAT gateways, and security groups.

AWS Console



Make sure region should be same for entire project you do

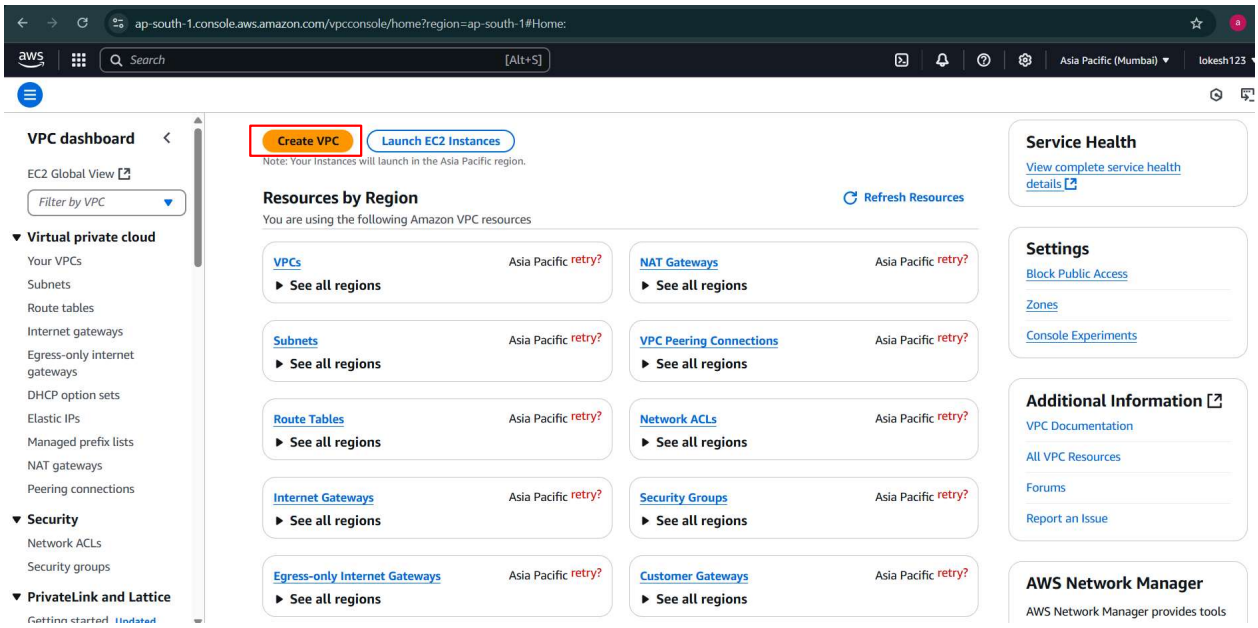


VPC

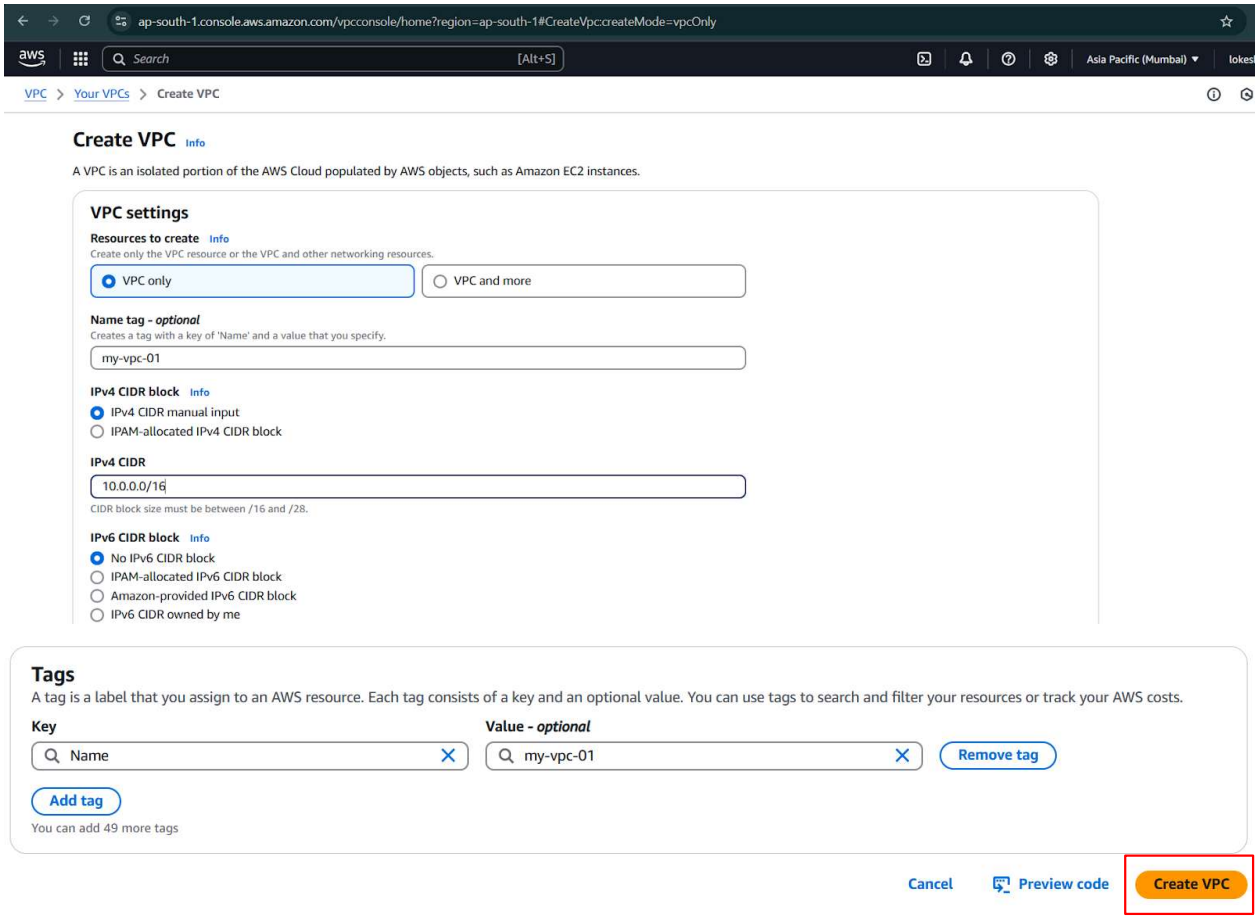
Service that lets you launch your AWS resources in a logically isolated virtual network. By default, you can have a maximum of 5 VPC per region (soft limit) and 5 CIDR per VPC.

Default vpc is created when you create an account in aws for every region , default vpc comes with Subnets , route table , internet gateway.

Creating Custom VPC

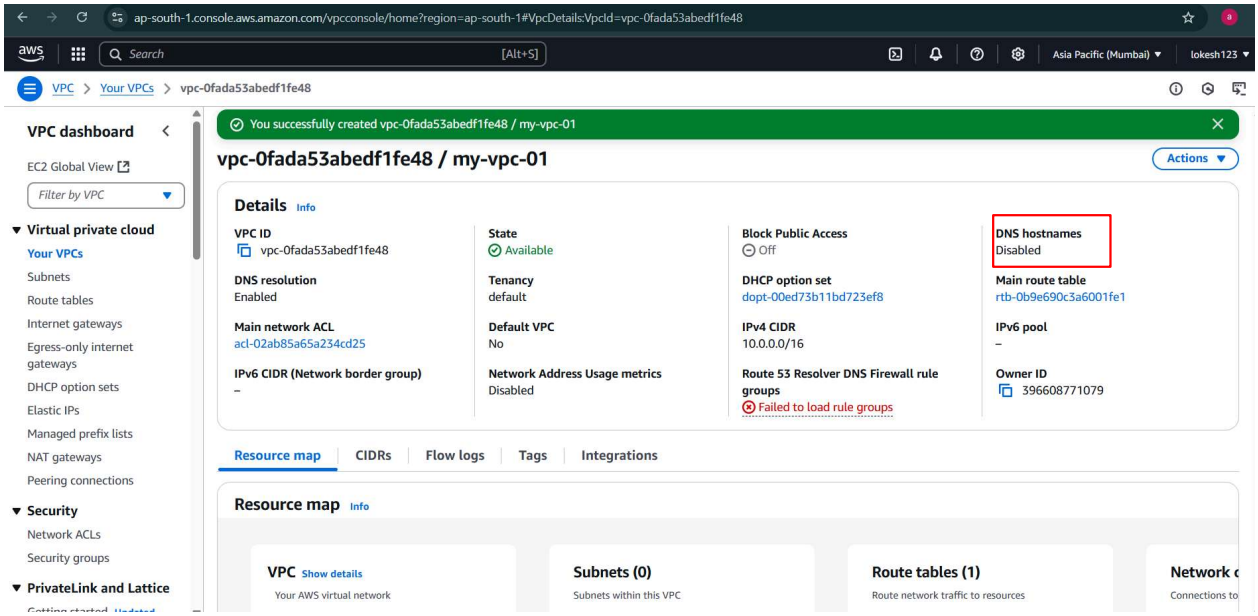


Give custom name for VPC
/16 is maximum CIDR notation for VPC

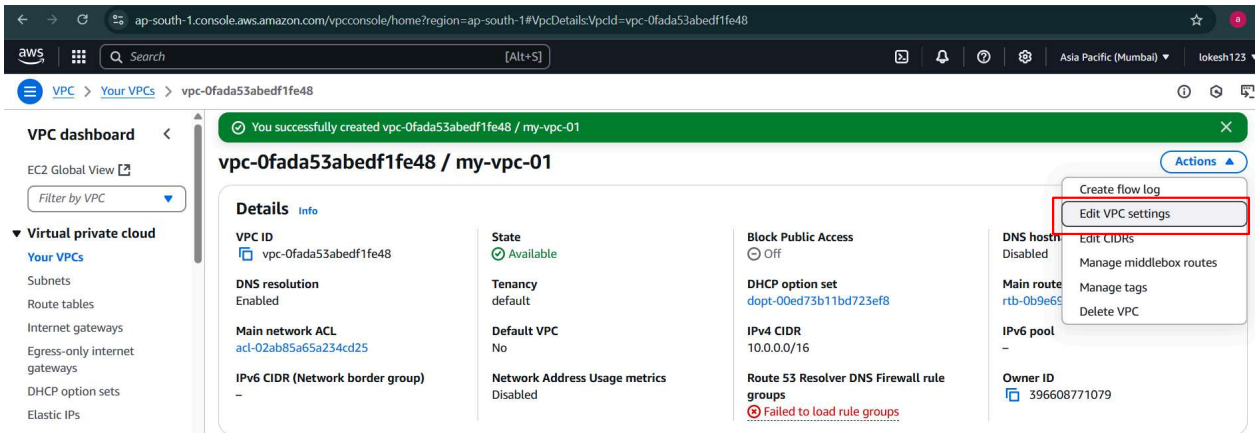


Created custom vpc with no other component (like subnets , Internet GateWay, route table)

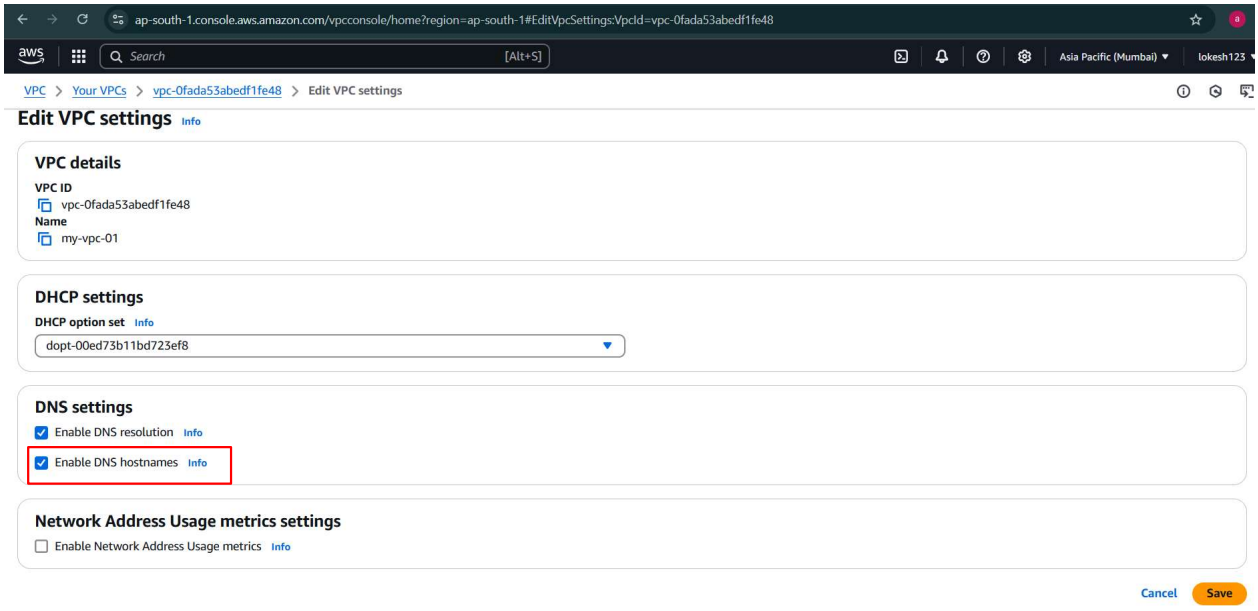
Make sure you to enable DNS hostname & DNS resolution so that any instance that running in VPC can connect to public internet



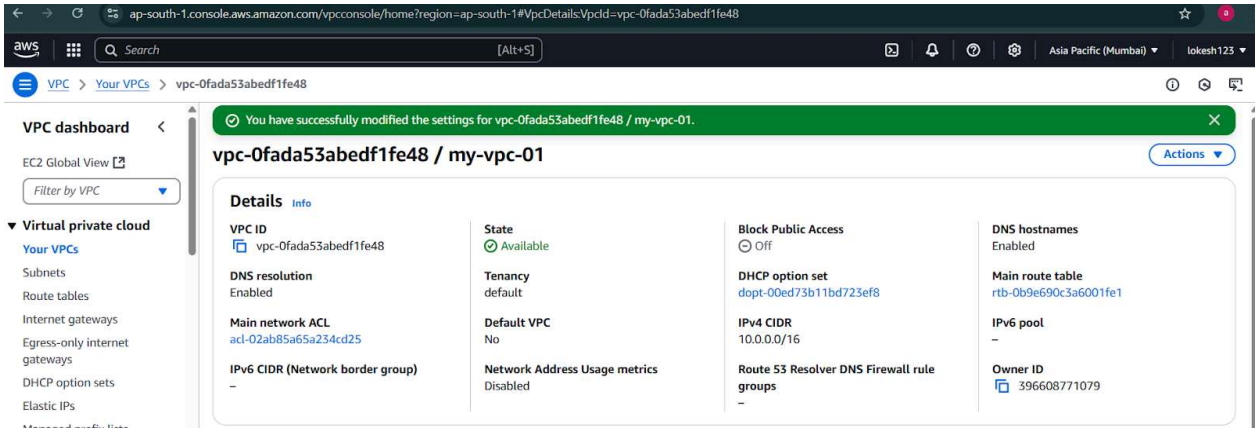
Edit VPC Settings -> Enable DNS hostnames

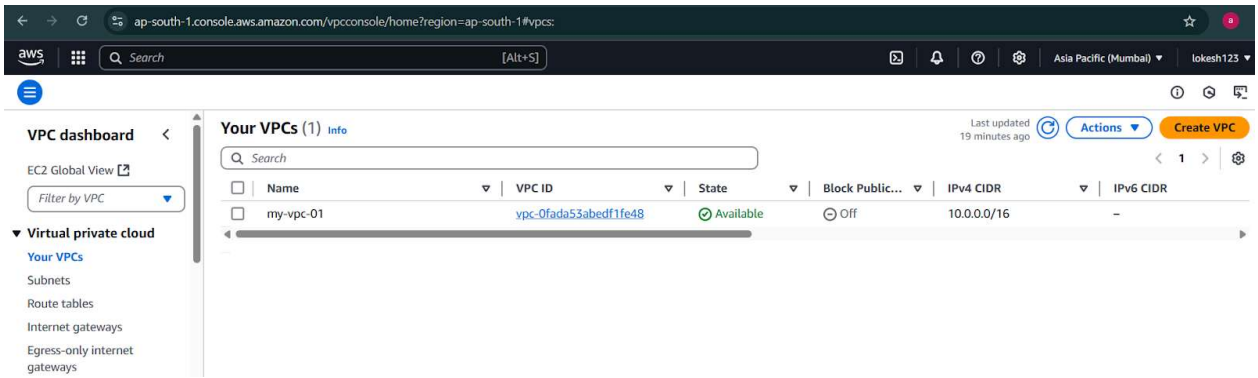


Click on save



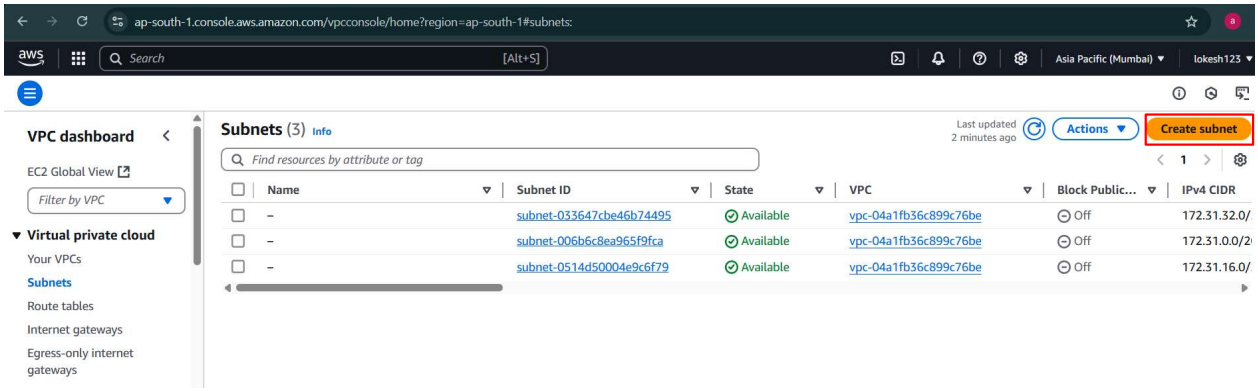
Now you can see



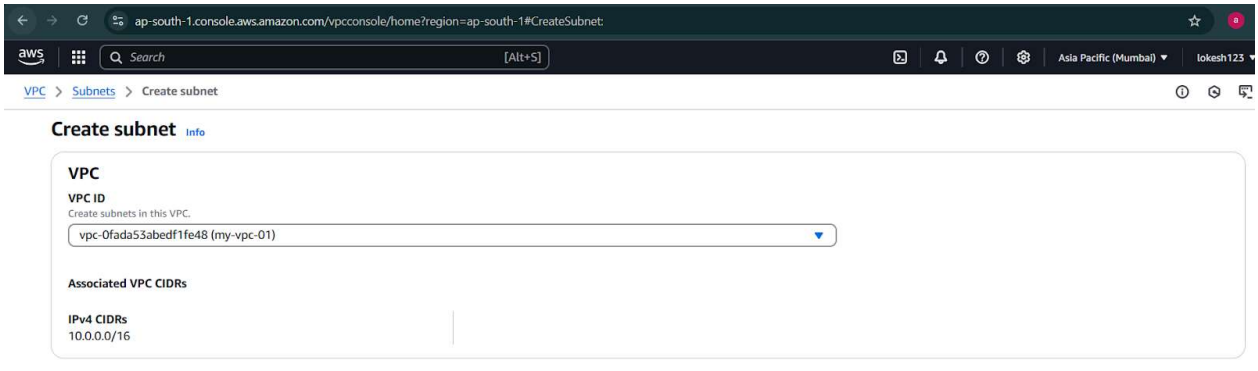


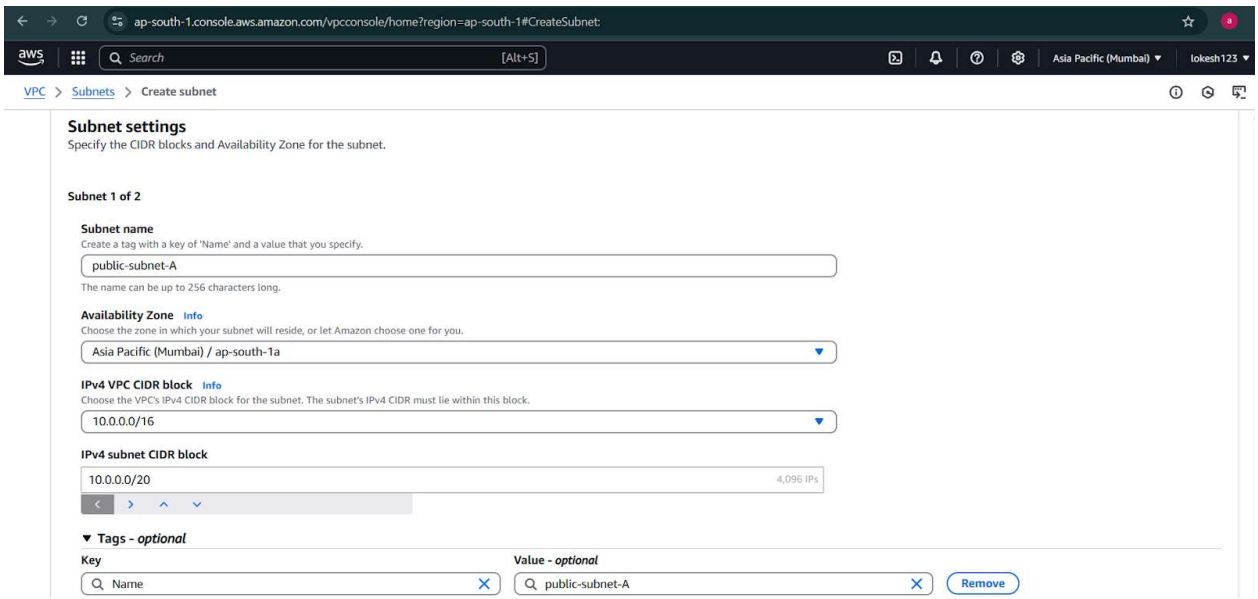
Subnets

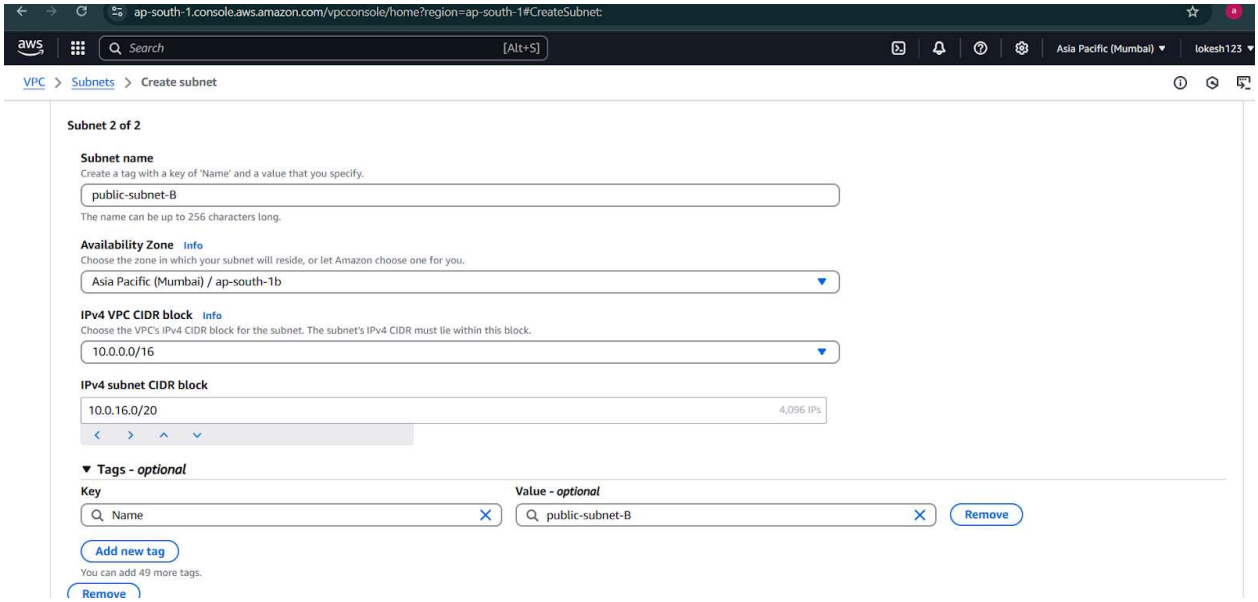
In console these all subnet are default subnet of that particular region
Click on Create Subnet



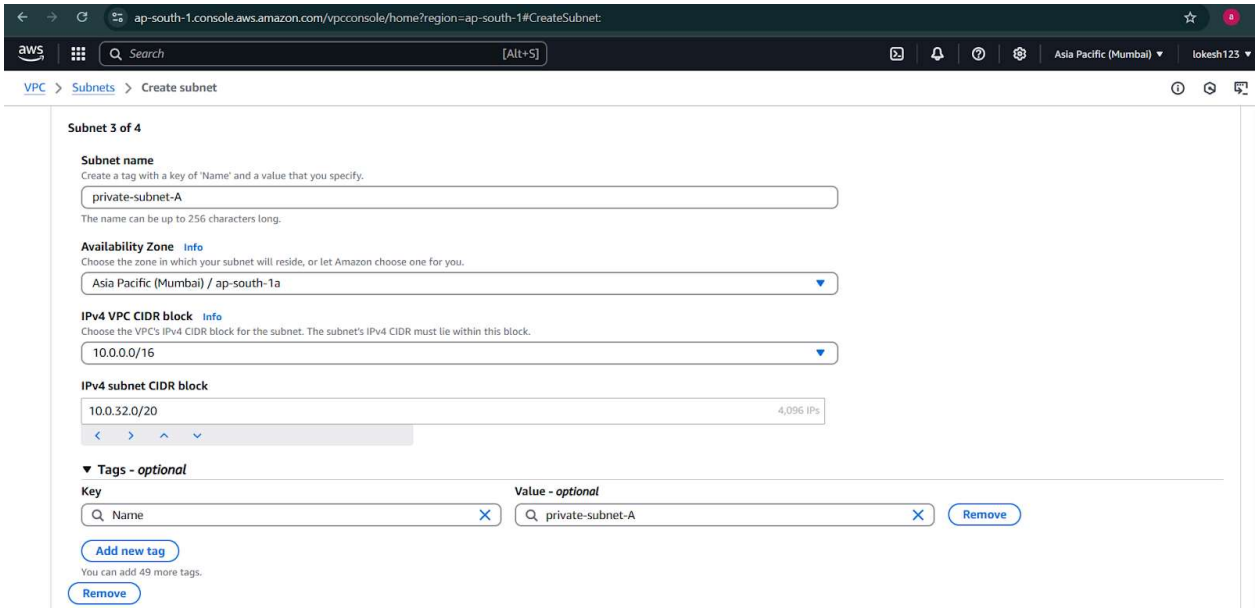
Creating 2 public subnets for zone A and zone B

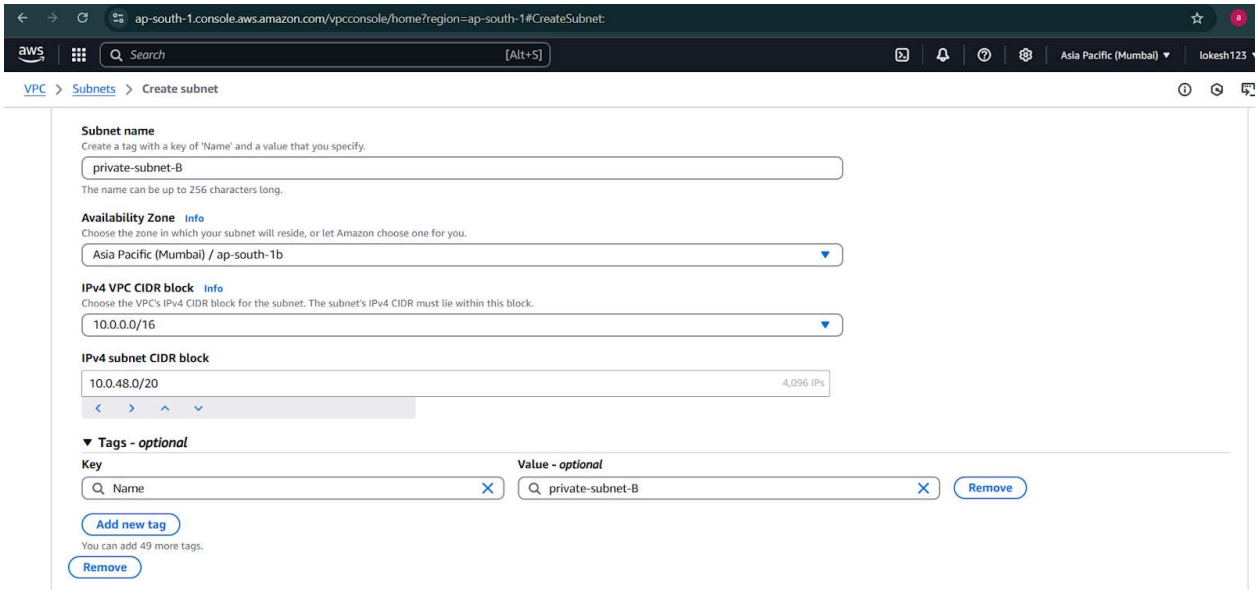






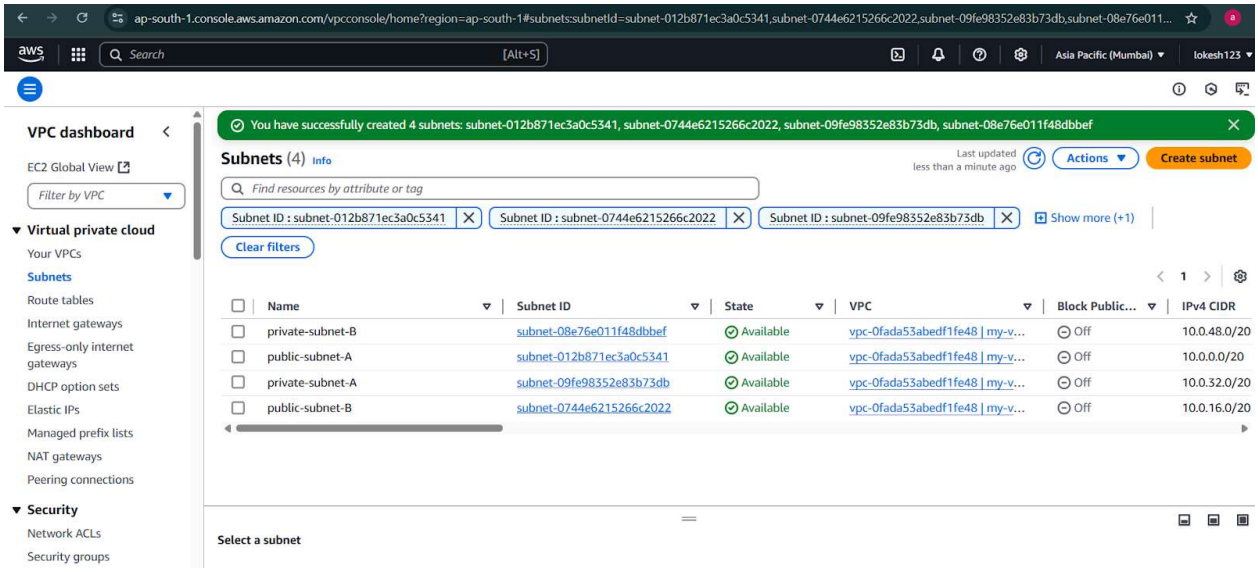
Creating 2 private subnets for zone A and zone B





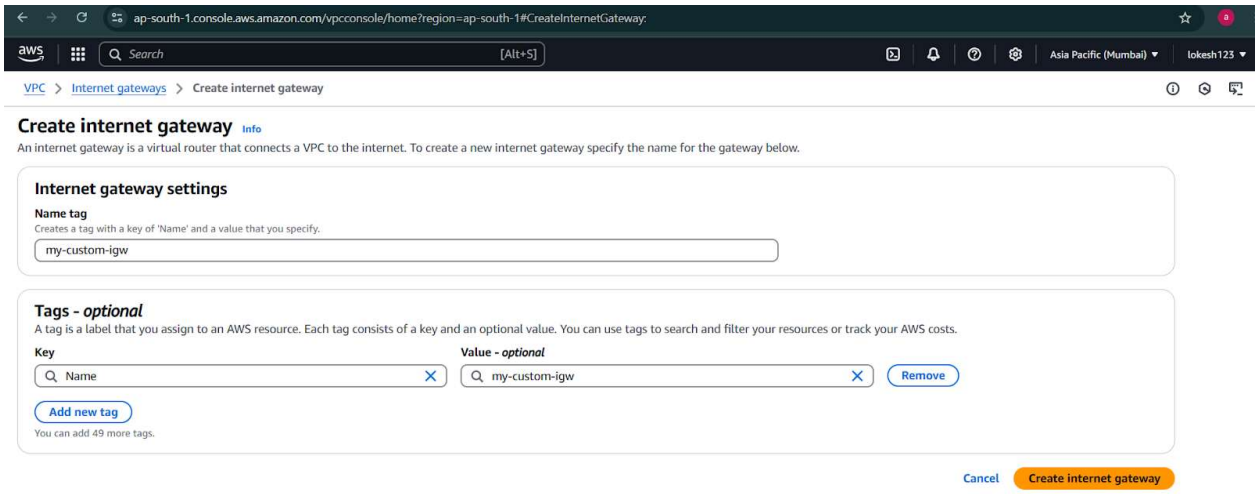
Click on create subnets

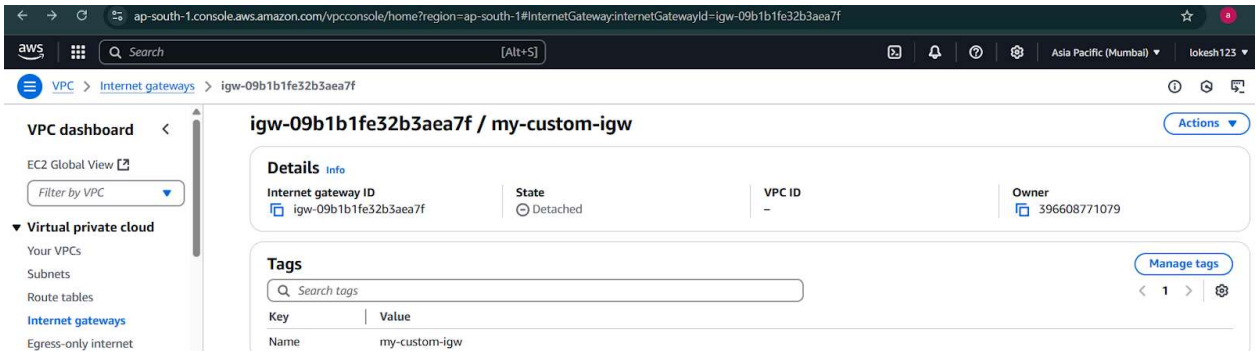
Newly created Subnets



Internet Gateway

Create Internet Gateway
Internet Gate way -> create internet gateway

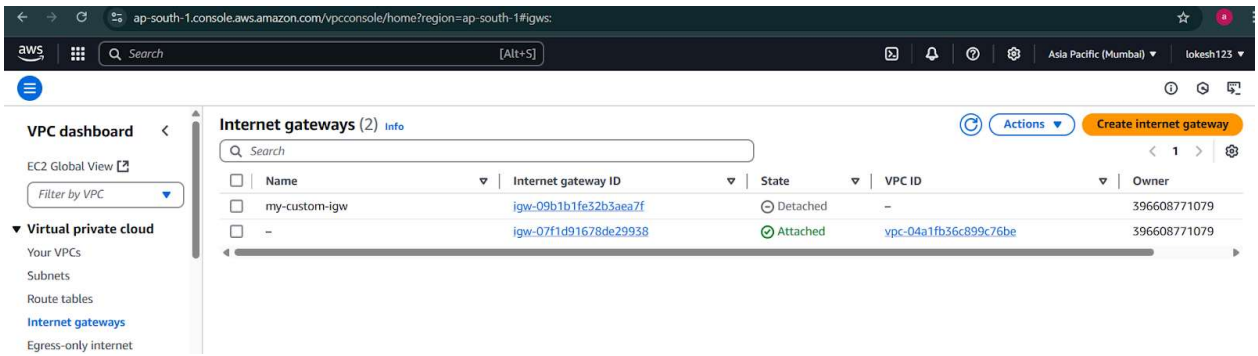


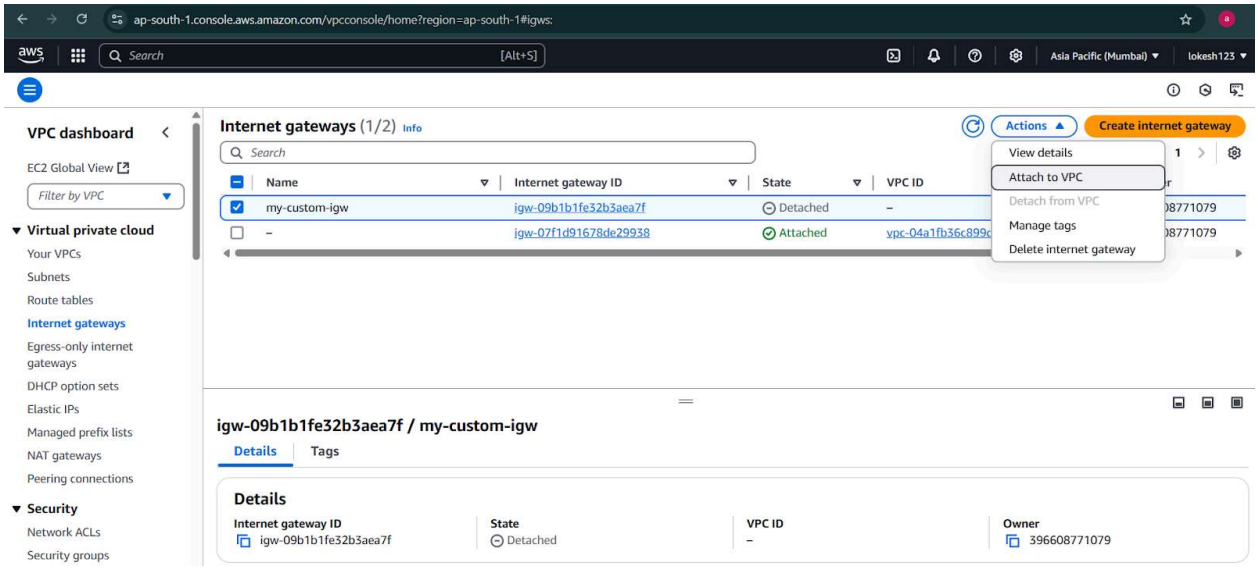


2 internet gateways listed

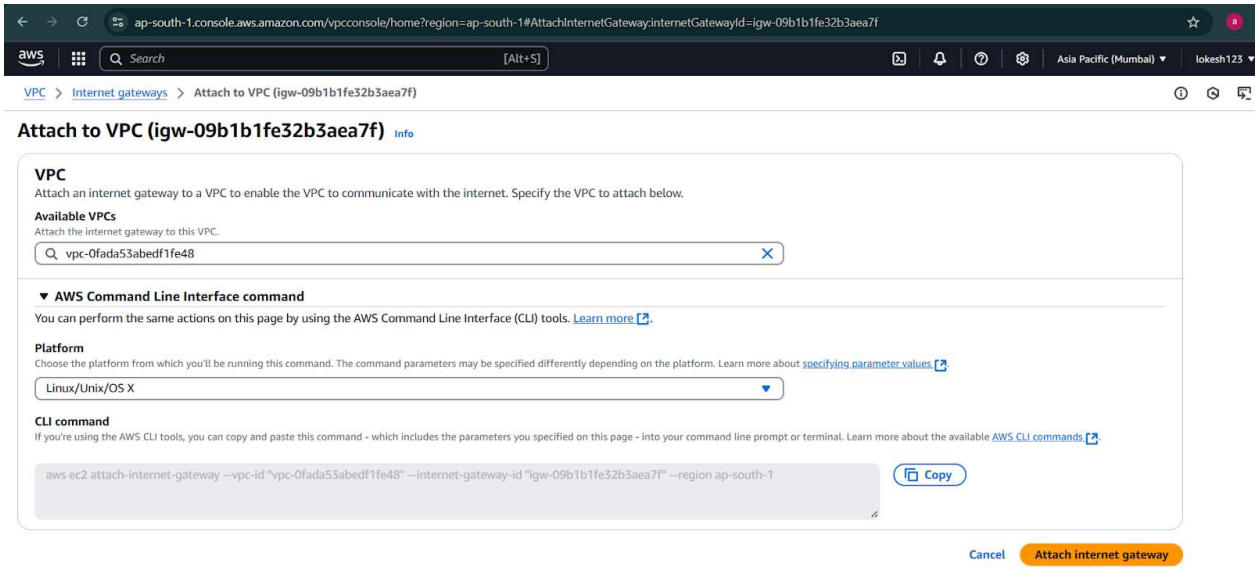
One is default internet gateway

Other is which is custom gateway which I created

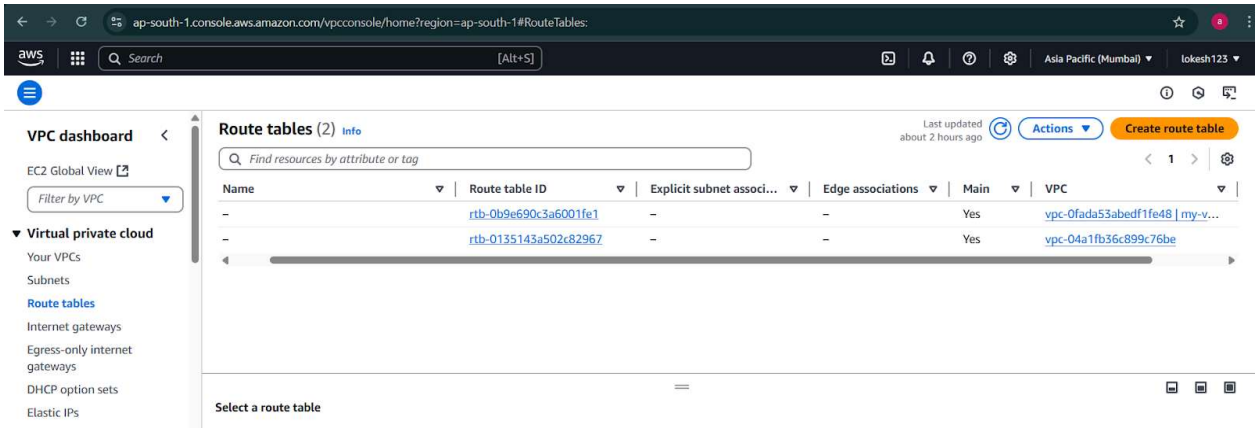




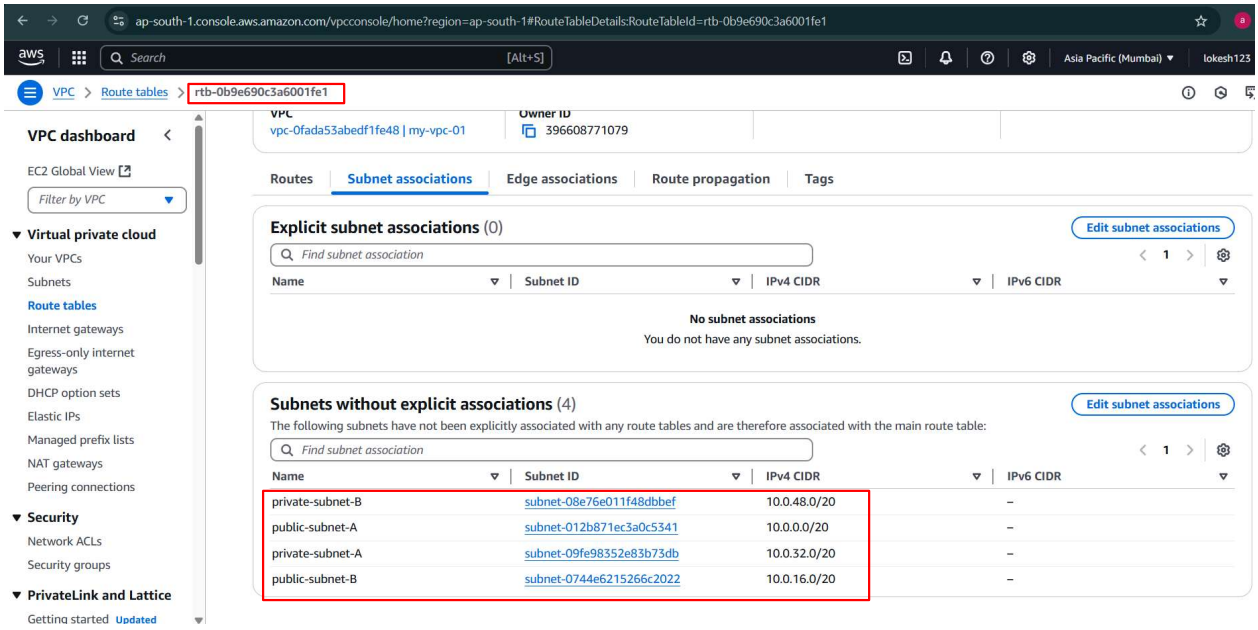
Only 1 internet gateway is attached to 1 VPC



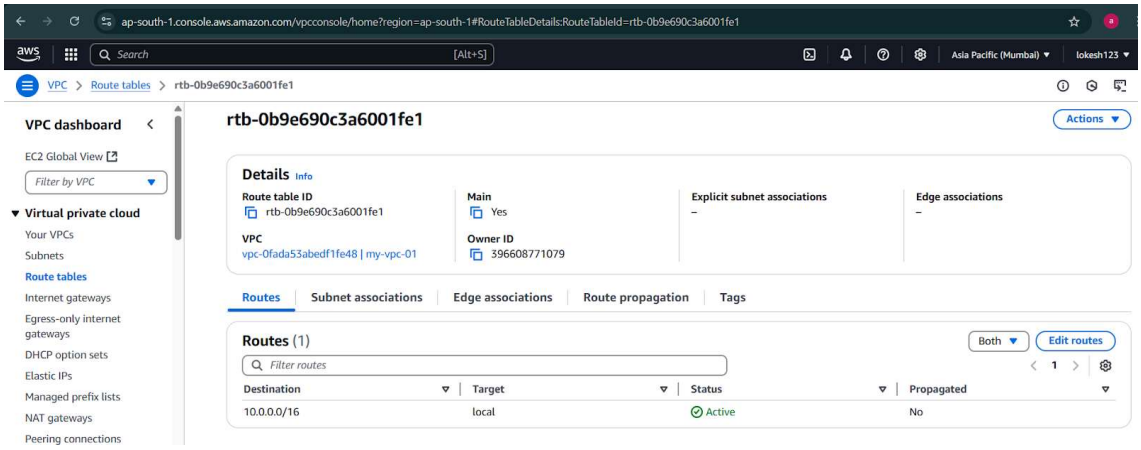
Route Table



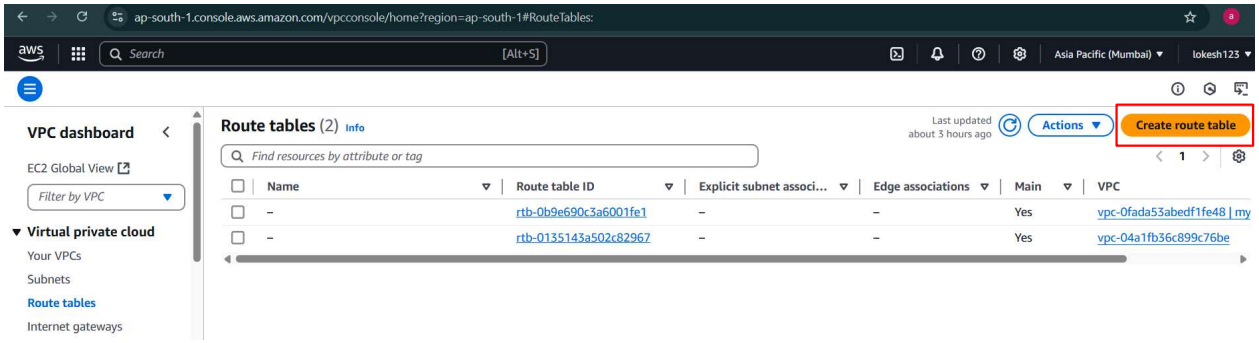
Routable created with vpc, it has all the subnets which we created in vpc



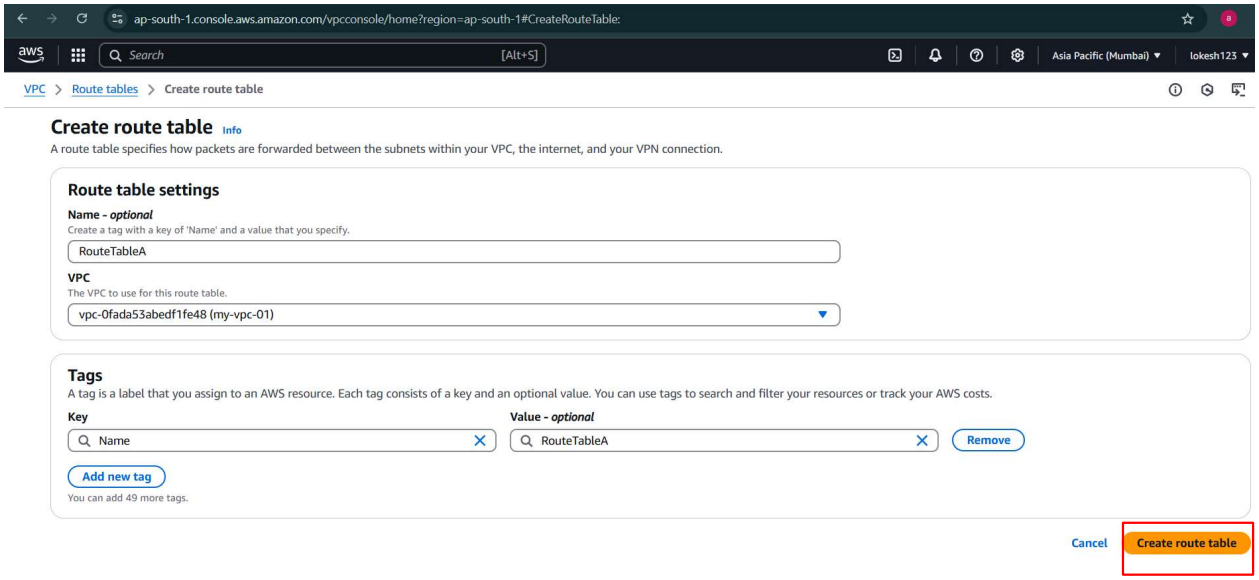
The route table with the custom internet gateway does not have access to internet



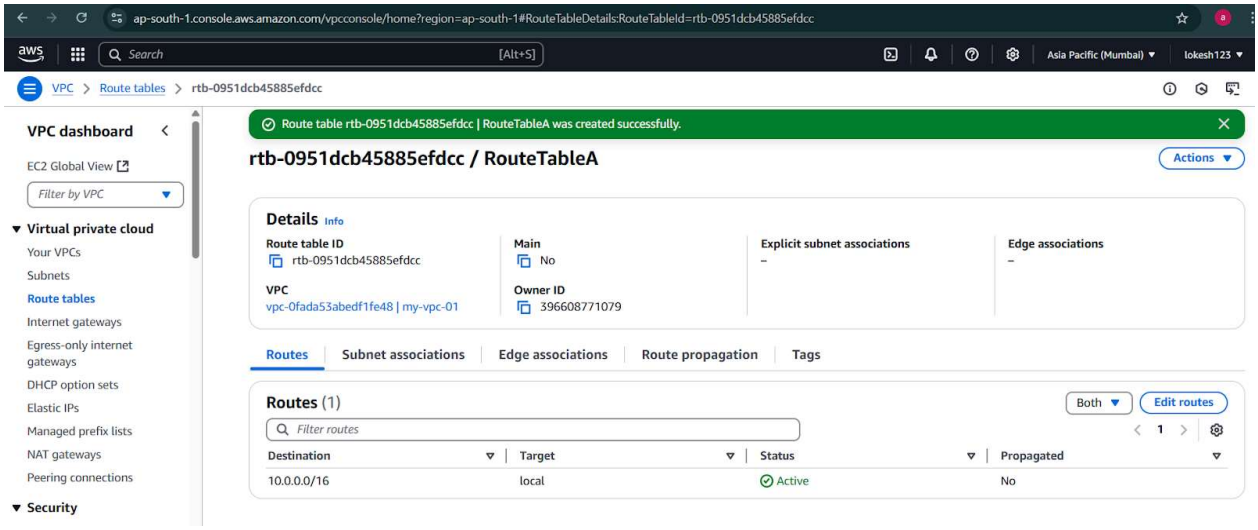
Click on create route table



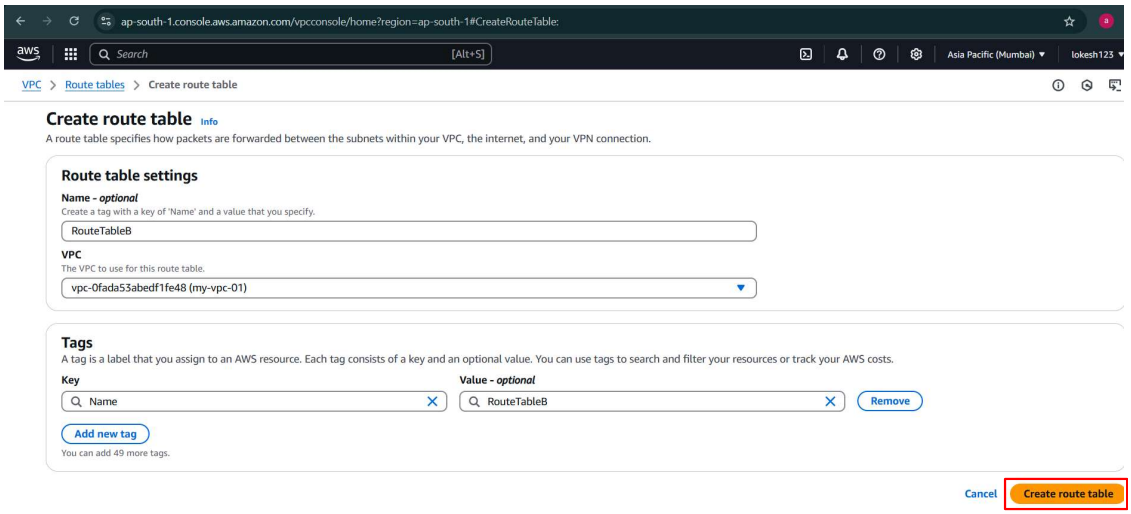
Give name and select VPC that I have created then click on create route table



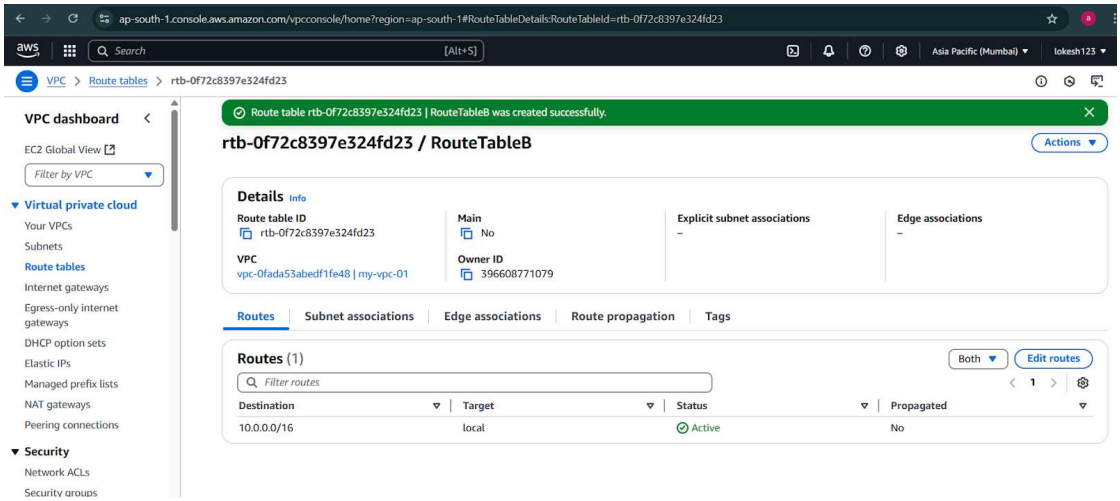
Now its created New Route Tabe named as RouteTableA



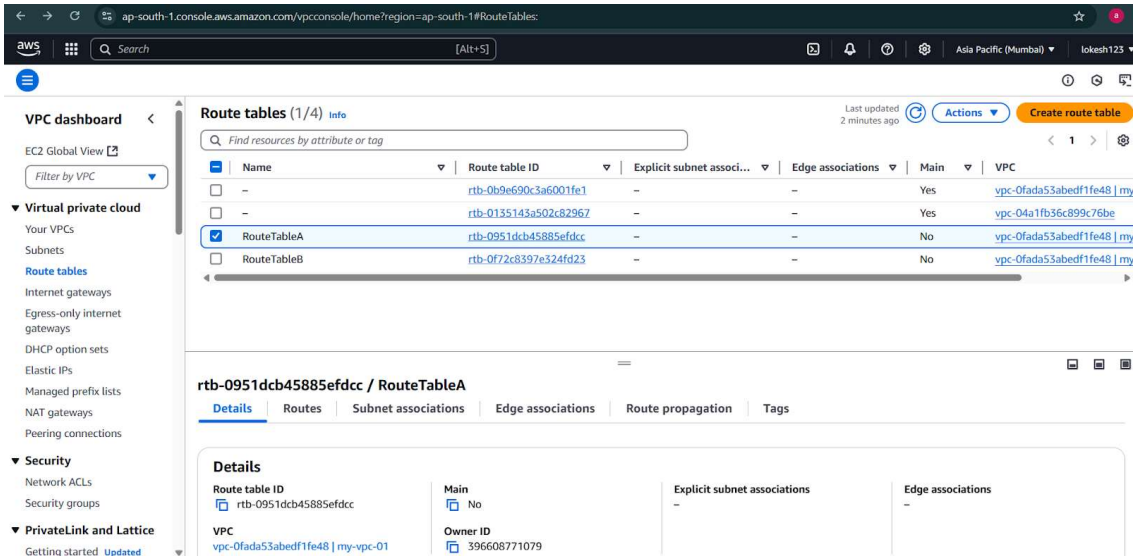
Create another routetable for private subnet



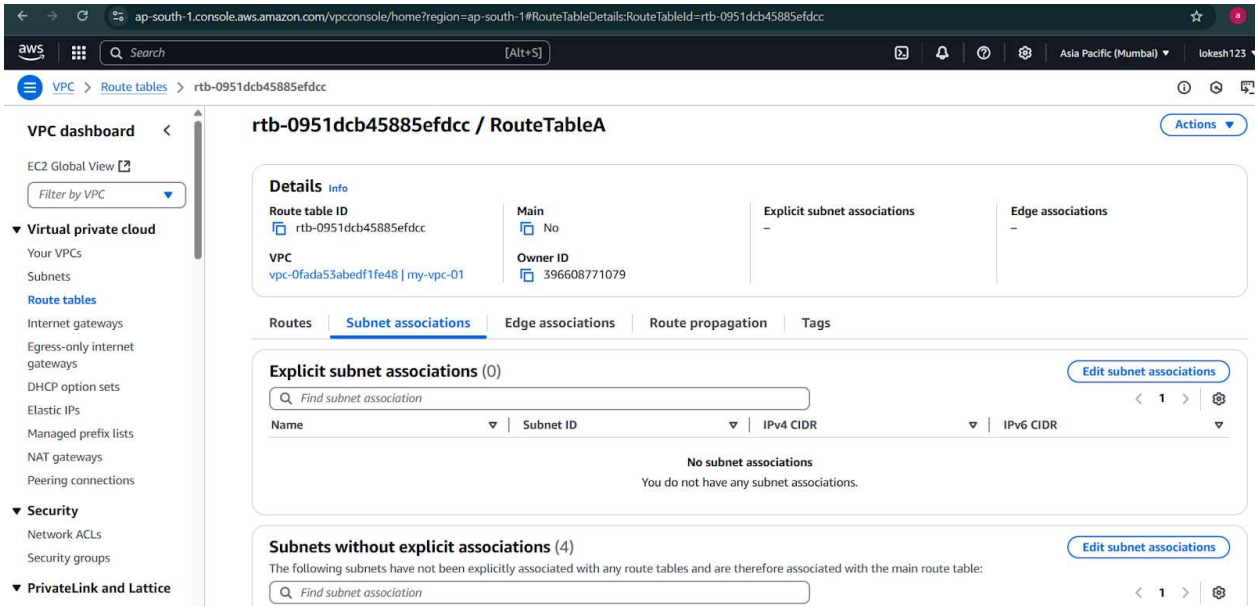
Now its created New Route Tabe named as RouteTableB



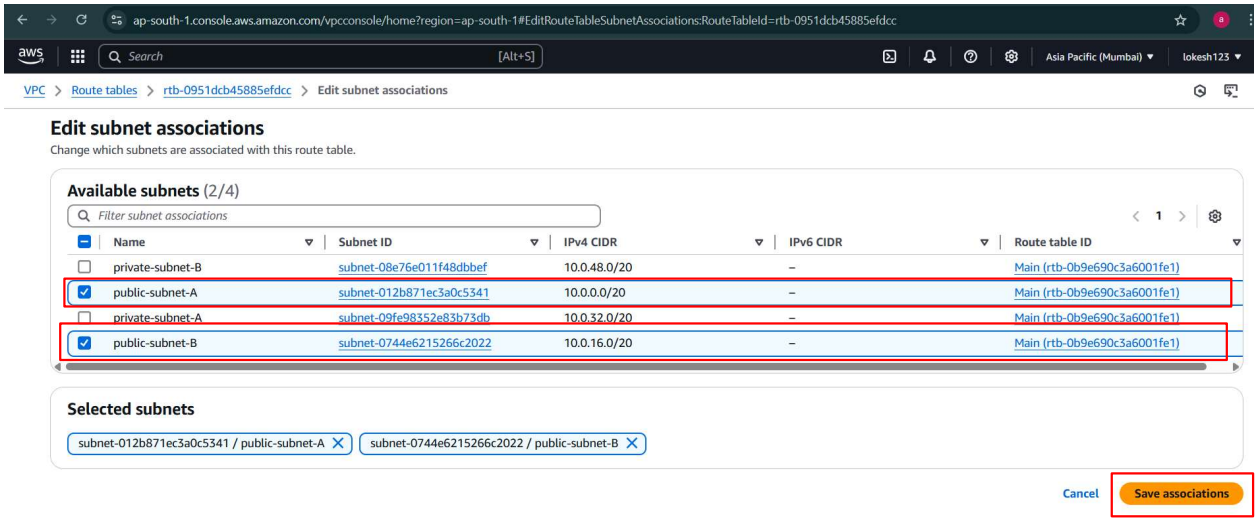
Click on RouteTable1



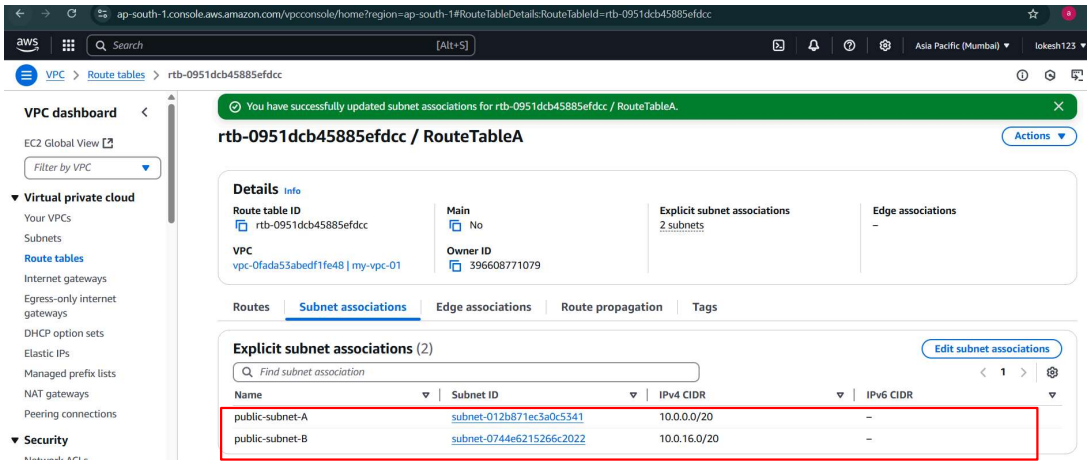
There are no Subnets in RouteTableA as of newly created



Add public subnet A and public subnet B to the RouteTableA

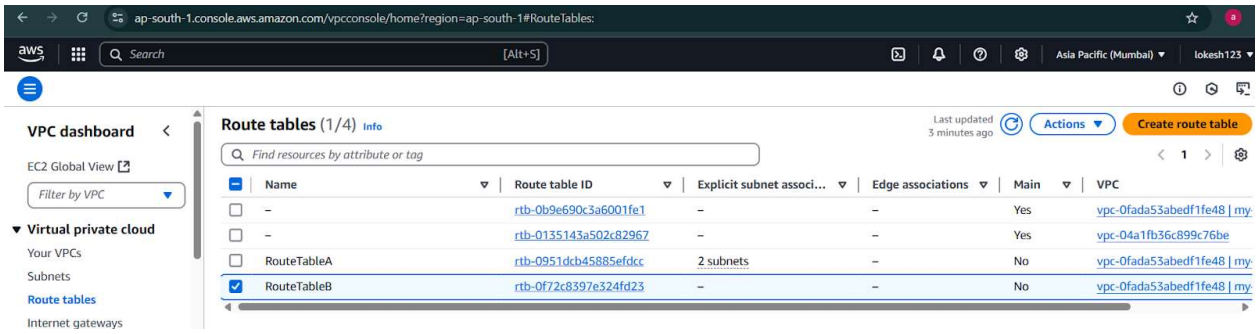


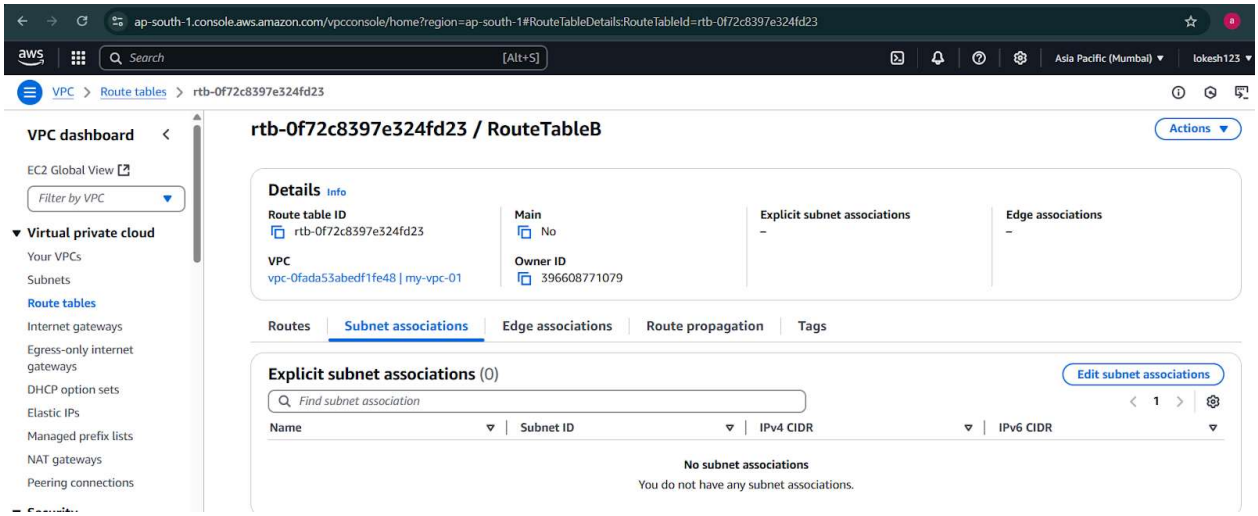
Now public-subnet-A and public-subnet-B will detach with main route and attach with RouteTableA



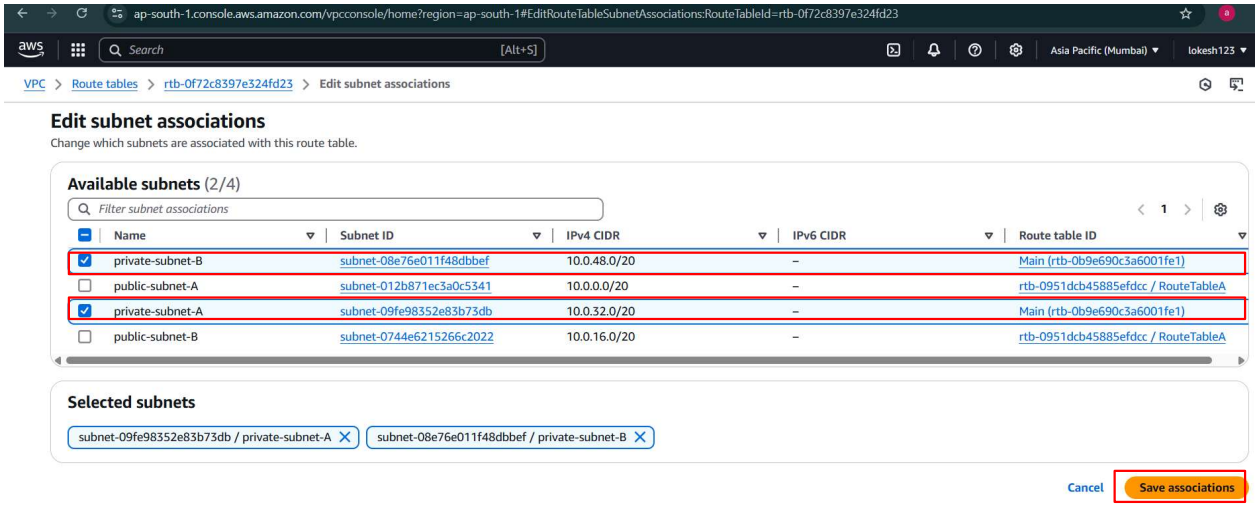
Similarly RouteTableB

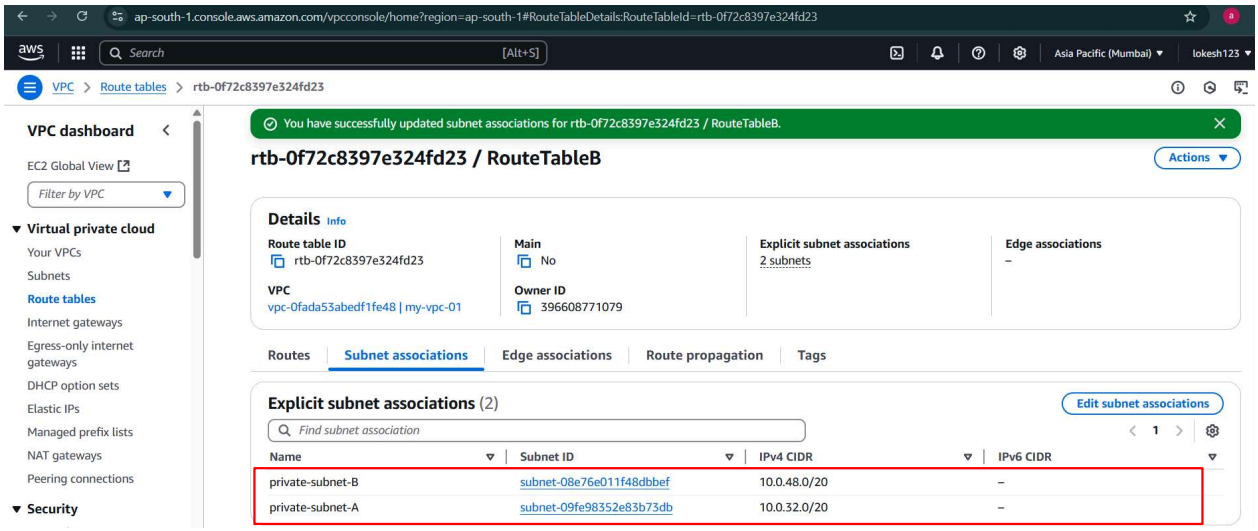
Now priavte-subnet-A and private-subnet-B will detach with main route and attach with RouteTableB





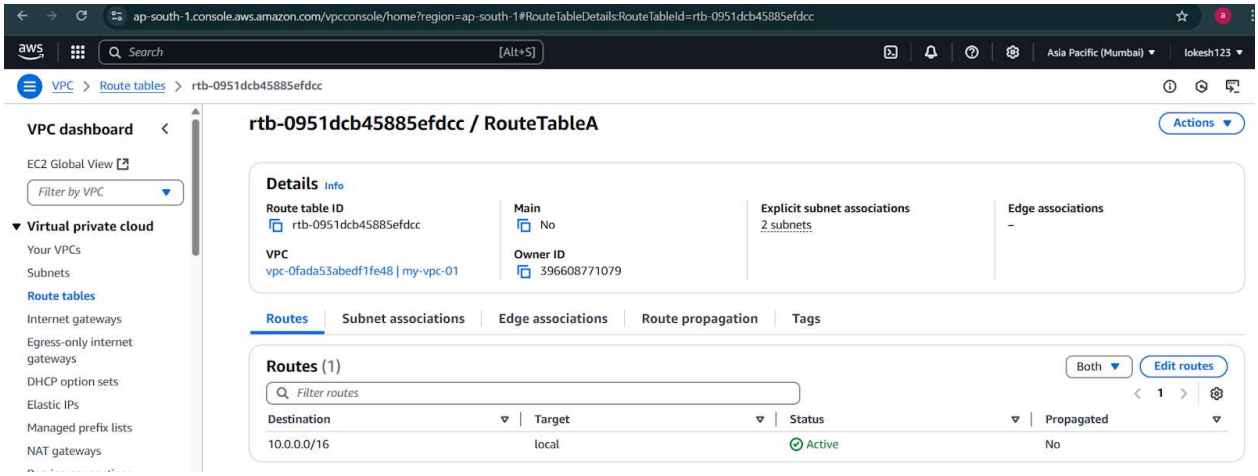
Now add private-subnet-B, private-subnet-A to the RouteTableB



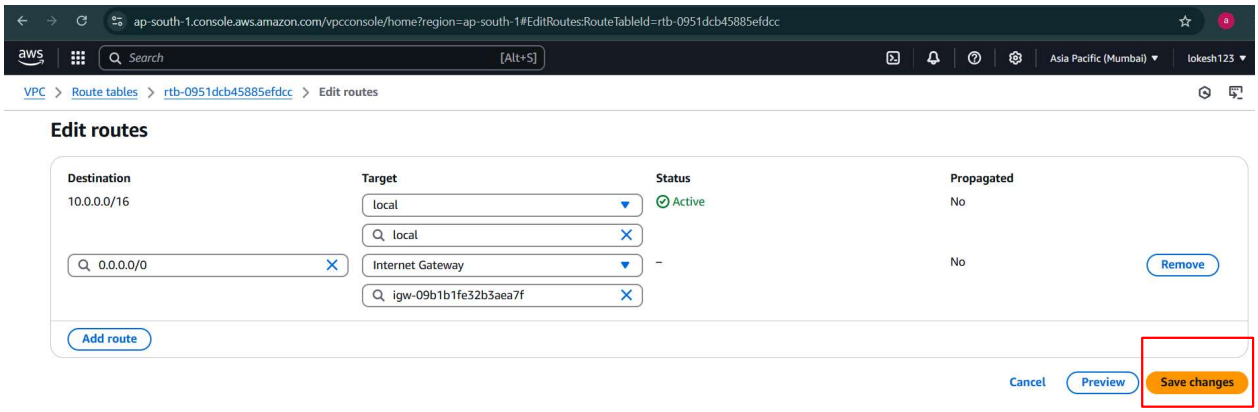


When we create route table and associate with the custom vpc bu default it doesn't have access to the internet unless we add route to the internet gateway

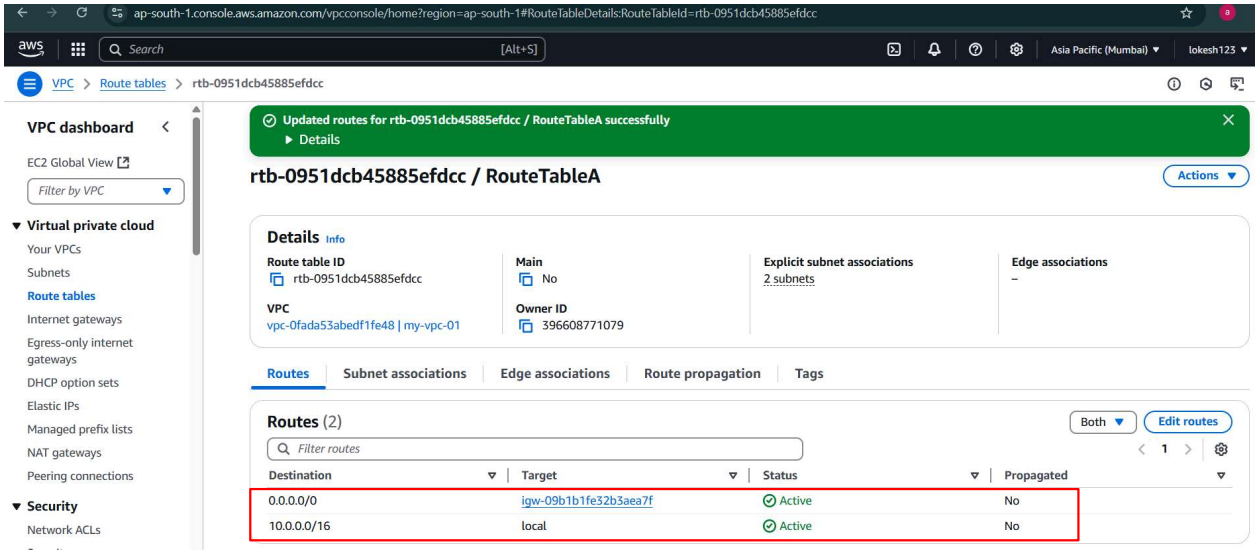
Go to RouteTableA



Choose 0.0.0.0/0 means all the ips applicable at destination and choose target as Internet Gateway and then click on save changes



Now RouteTableA has internet gateway has route to internet via internet gateway



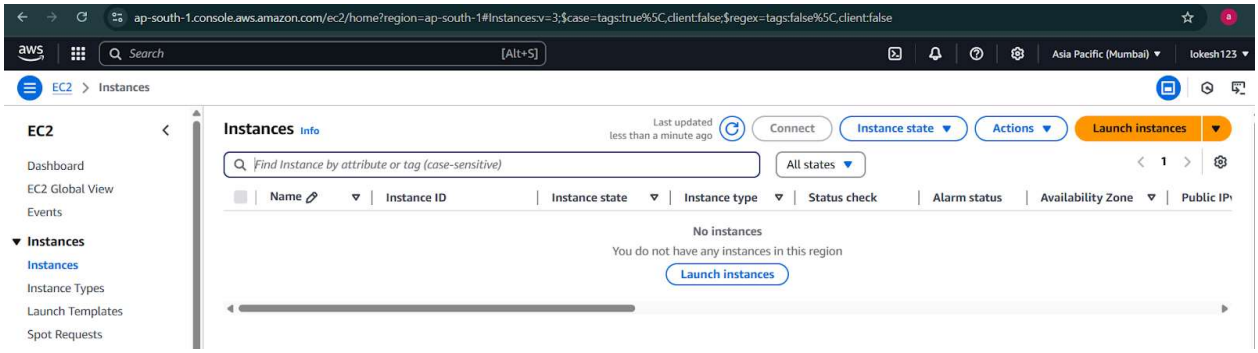
Security Groups

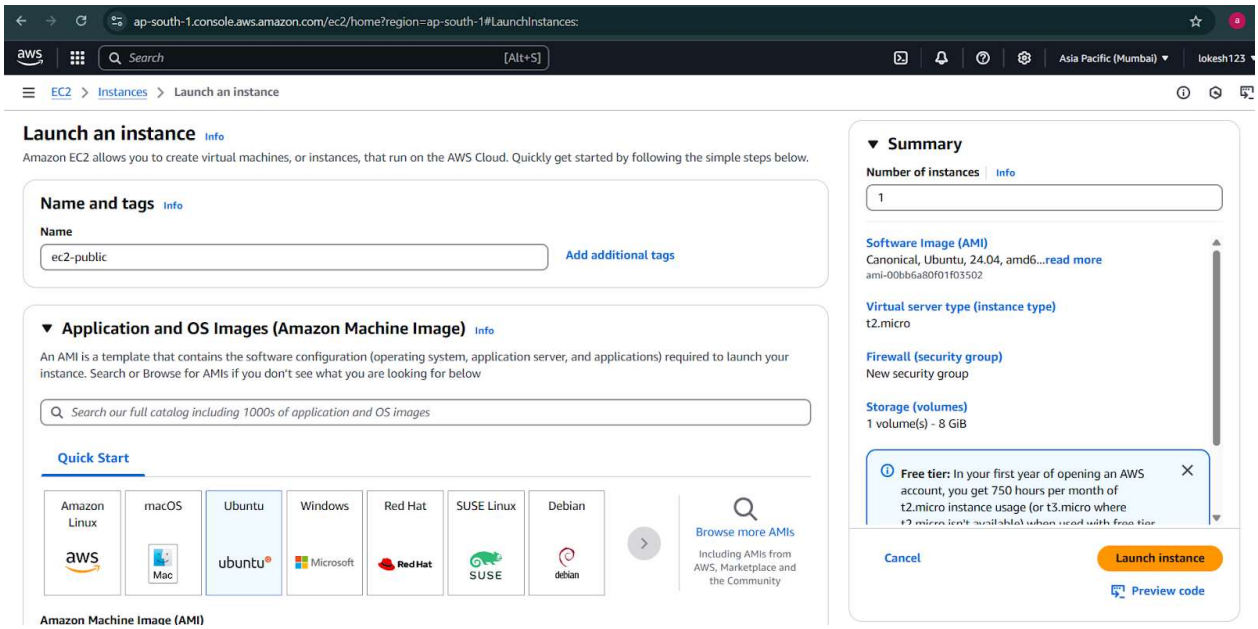
- A security group acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic.
- Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance.
- If you don't specify a security group, Amazon EC2 uses the default security group.
- By default, security groups allow all outbound traffic.
- Security groups are stateful-if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules.
- You can associate more than one security group with an instance.

Security group - Rules
Amazon EC2 blocks traffic on port 25 by default.
Security group rules are always permissive; you can't create rules that deny access.
You can add and remove rules at any time. Your changes are automatically applied to the instances that are associated with the security group.
Specify below at the time of rule creation:
Name
Protocol
Port Range
Type
Source: Custom/AnyWhere/MyIP
Source Value: CIDR Block, Security Group

EC2 one for public subnet -> for webserver
EC2 one for private subnet -> for database server

Go to EC2 instance
Launch Instance





Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture	AMI ID	Publish Date	Username	
64-bit (x86)	ami-00bb6a80f01f03502	2025-01-15	ubuntu	Verified provider

Instance type Info | Get advice

Instance type

t2.micro — Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

ec2-public

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

- (•) RSA — RSA encrypted private and public key pair
- ( ) ED25519 — ED25519 encrypted private and public key pair

Private key file format

- (•) .pem — For use with OpenSSH
- ( ) .ppk — For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Cancel | Create key pair

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-public

Create new key pair

Network settings Info

VPC - *required* | Info

vpc-0fada53abedf1fe48 (my-vpc-01)
10.0.0.0/16

Subnet | Info

subnet-012b871ec3a0c5341 public-subnet-A
VPC: vpc-0fada53abedf1fe48 Owner: 396608771079 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 4091 CIDR: 10.0.0.0/20)

Create new subnet

Auto-assign public IP | Info

Enable

Additional charges apply when outside of free tier allowance

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*

pub-ssh-http

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 2025-03-14T13:28:55.152Z

Inbound Security Group Rules

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

Type	Protocol	Port range
ssh	TCP	22

Source type	Source	Description - *optional*
Custom	Add CIDR, prefix list or security group	e.g. SSH for admin desktop

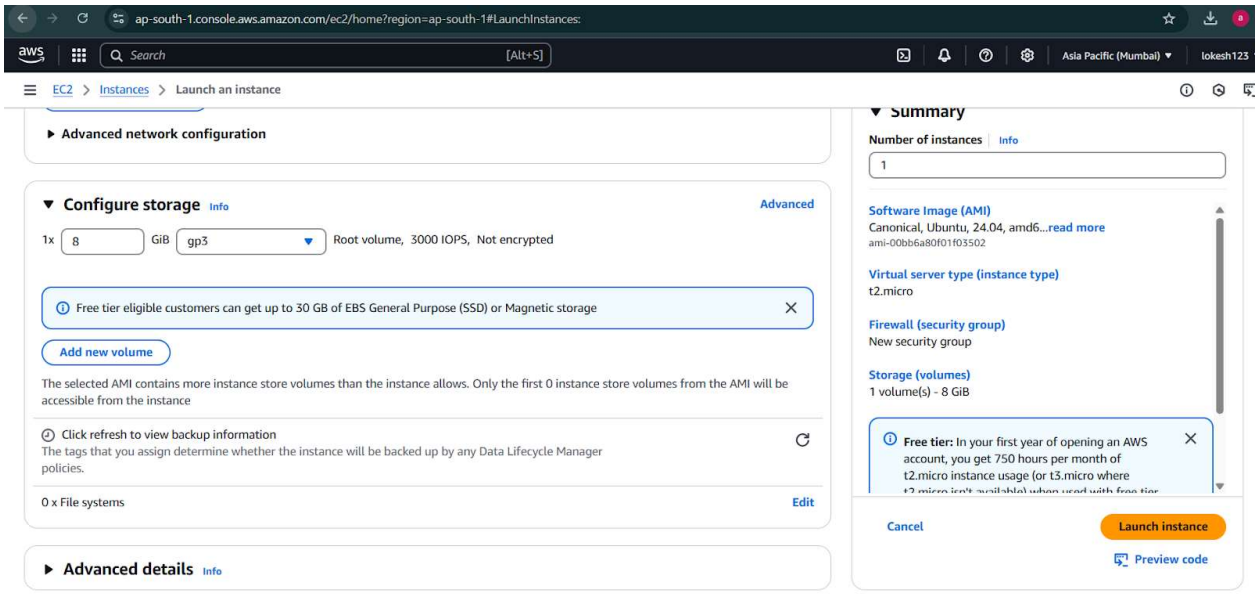
0.0.0.0/0

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0) — Remove

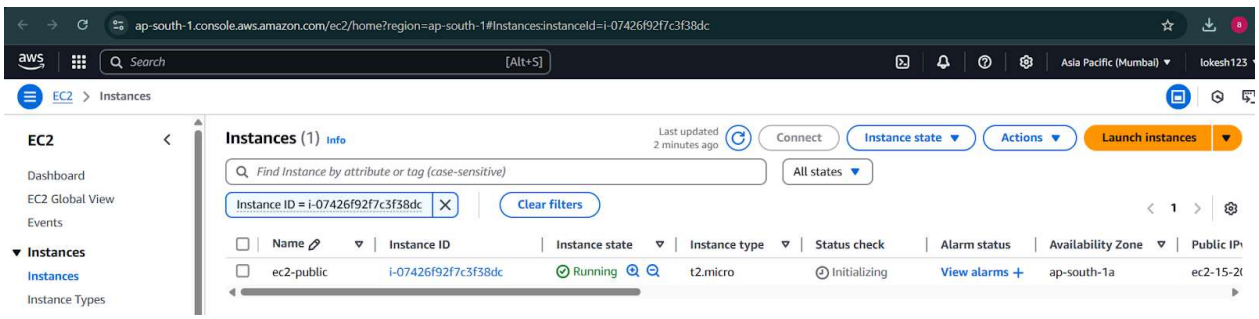
Type	Protocol	Port range
HTTP	TCP	80

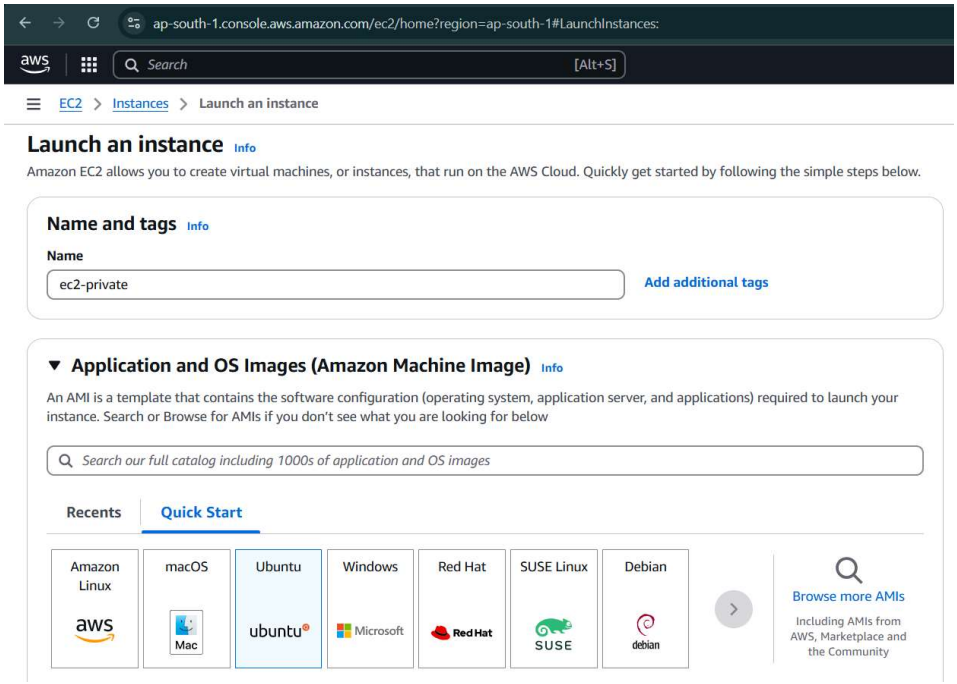
Source type	Source	Description - *optional*
Custom	Add CIDR, prefix list or security group	e.g. SSH for admin desktop

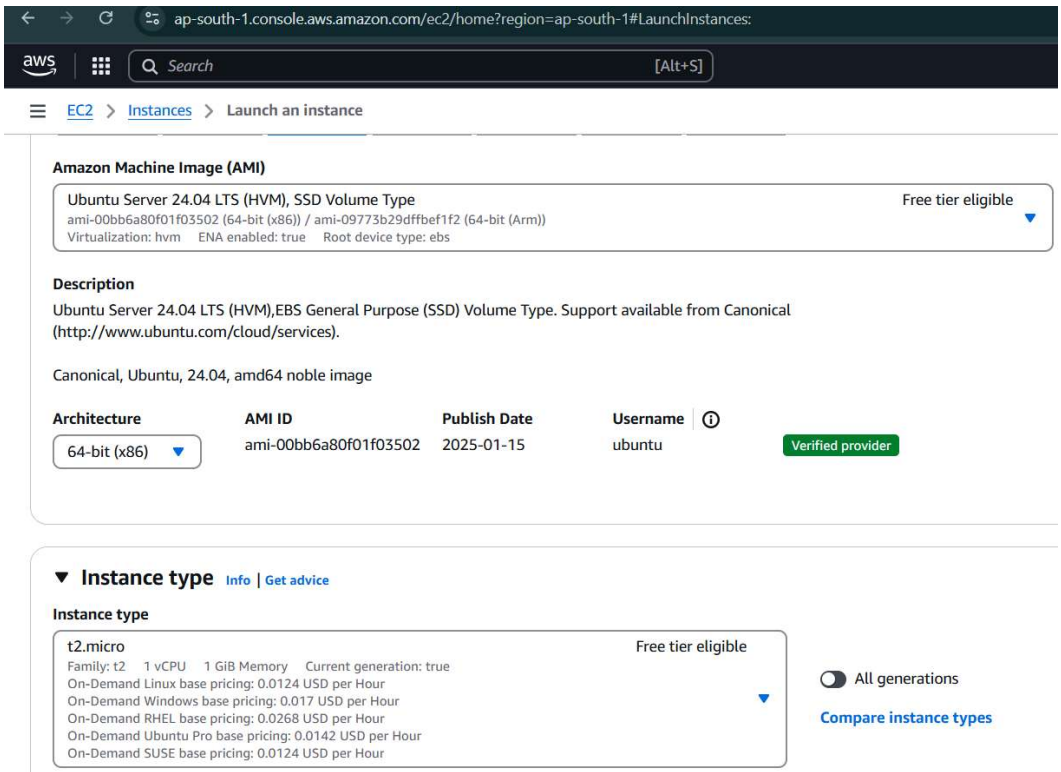
0.0.0.0/0



Launch 2nd ec2 instance as database server




ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
aws
Search
[Alt+S]
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
ec2-private
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
aws
Search
[Alt+S]
EC2 > Instances > Launch an instance
Amazon Machine Image (AMI)
Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
Free tier eligible
ami-00bb6a80f01f03502 (64-bit (x86)) / ami-09773b29dffbef1f2 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs
Description
Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Canonical, Ubuntu, 24.04, amd64 noble image
Architecture
64-bit (x86)
AMI ID
ami-00bb6a80f01f03502
Publish Date
2025-01-15
Username
ubuntu
Verified provider
Instance type Info | Get advice
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour
All generations
Compare instance types

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

private-ec2

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

- (•) RSA — RSA encrypted private and public key pair
- ( ) ED25519 — ED25519 encrypted private and public key pair

Private key file format

- (•) .pem — For use with OpenSSH
- ( ) .ppk — For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Cancel | Create key pair

▼ 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*

private-ec2 ▼ | Create new key pair

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

aws | Search [Alt+S]

EC2 > Instances > Launch an instance

▼ Network settings Info

VPC - *required* Info

vpc-0fada53abedf1fe48 (my-vpc-01)
10.0.0.0/16

Subnet Info

subnet-09fe98352e83b73db private-subnet-A
VPC: vpc-0fada53abedf1fe48 Owner: 396608771079 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 4091 CIDR: 10.0.32.0/20)

Create new subnet

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

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*

private-sg-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 2025-03-14T13:36:55.877Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, sg-0757e55565b9f6ca4) Remove

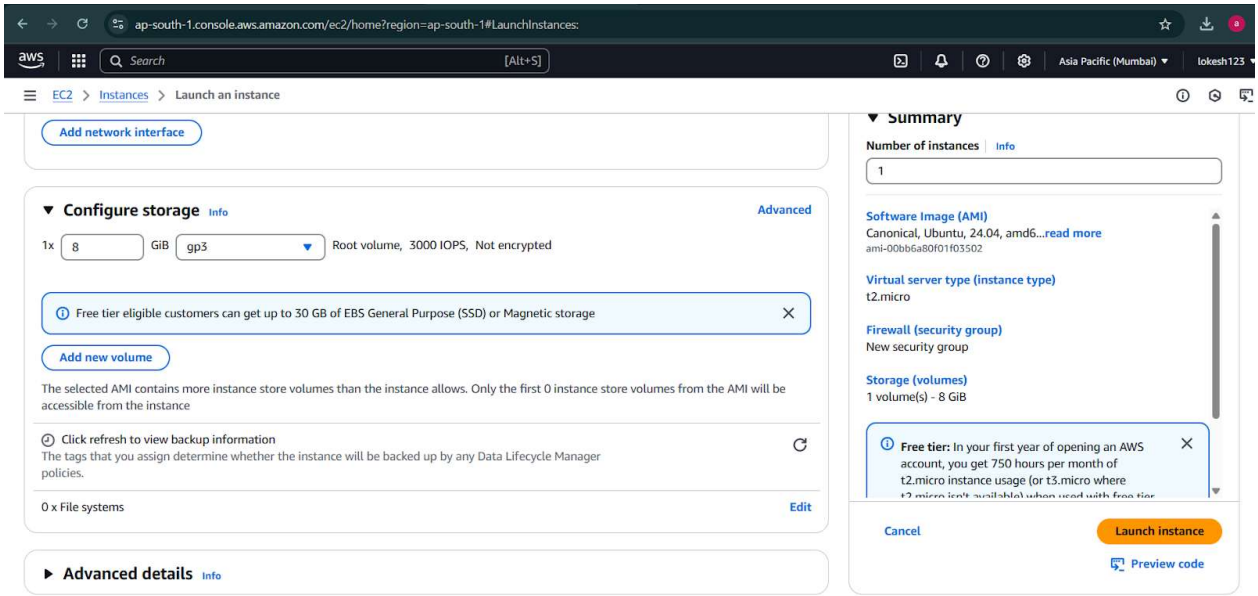
Type	Protocol	Port range
ssh	TCP	22

Source type	Source	Description - *optional*
Custom	Add CIDR, prefix list or security group: sg-0757e55565b9f6ca4	e.g. SSH for admin desktop

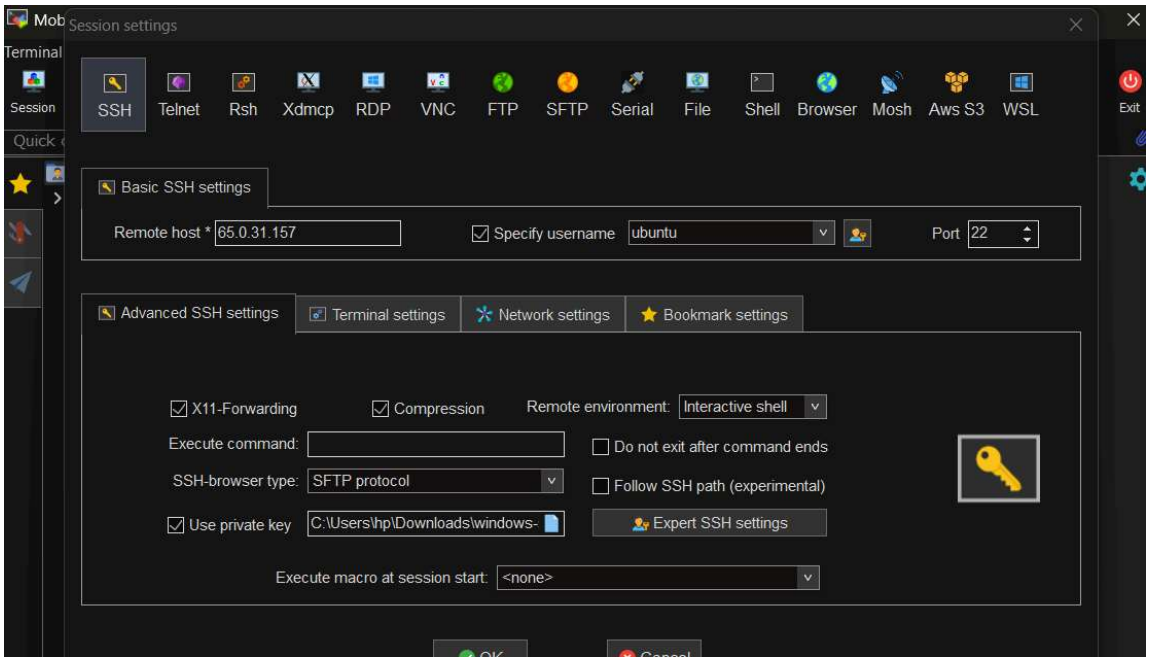
▼ Security group rule 2 (TCP, 3306, sg-0757e55565b9f6ca4) Remove

Type	Protocol	Port range
MYSQL/Aurora	TCP	3306

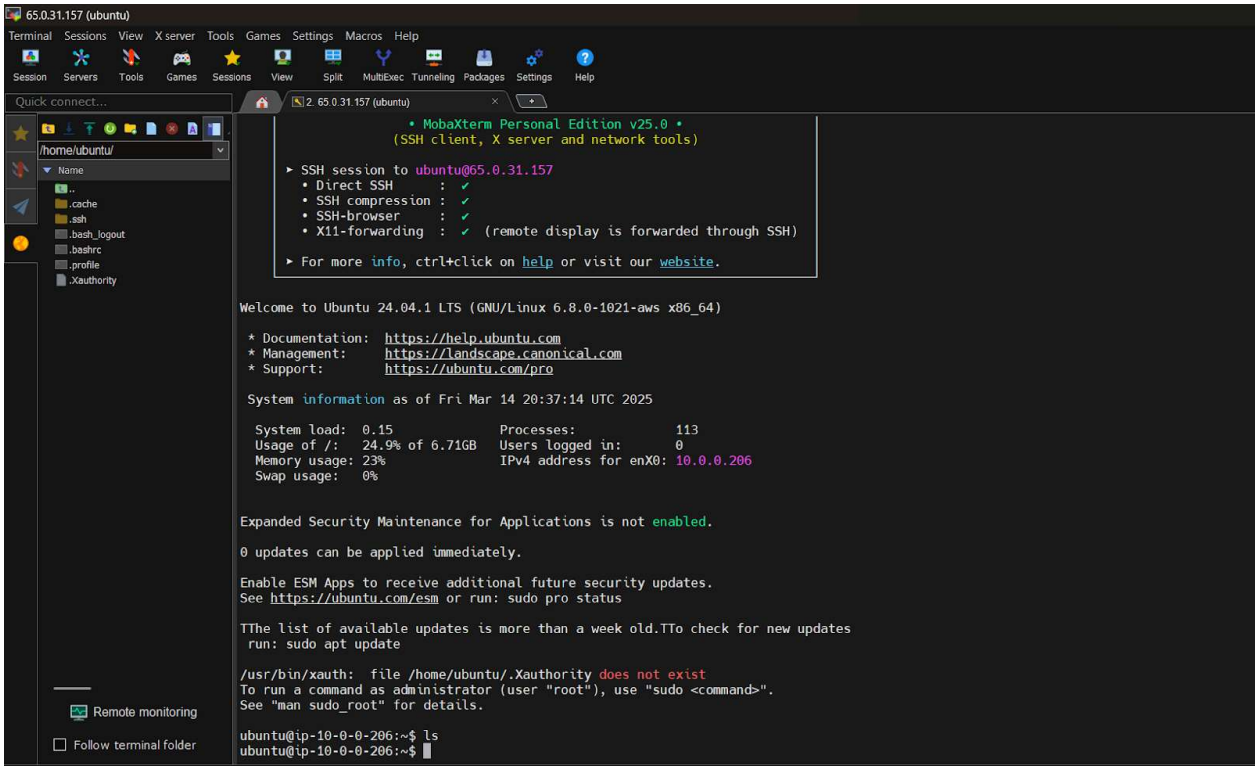
Source type	Source	Description - *optional*
Custom	Add CIDR, prefix list or security group: sg-0757e55565b9f6ca4	e.g. SSH for admin desktop



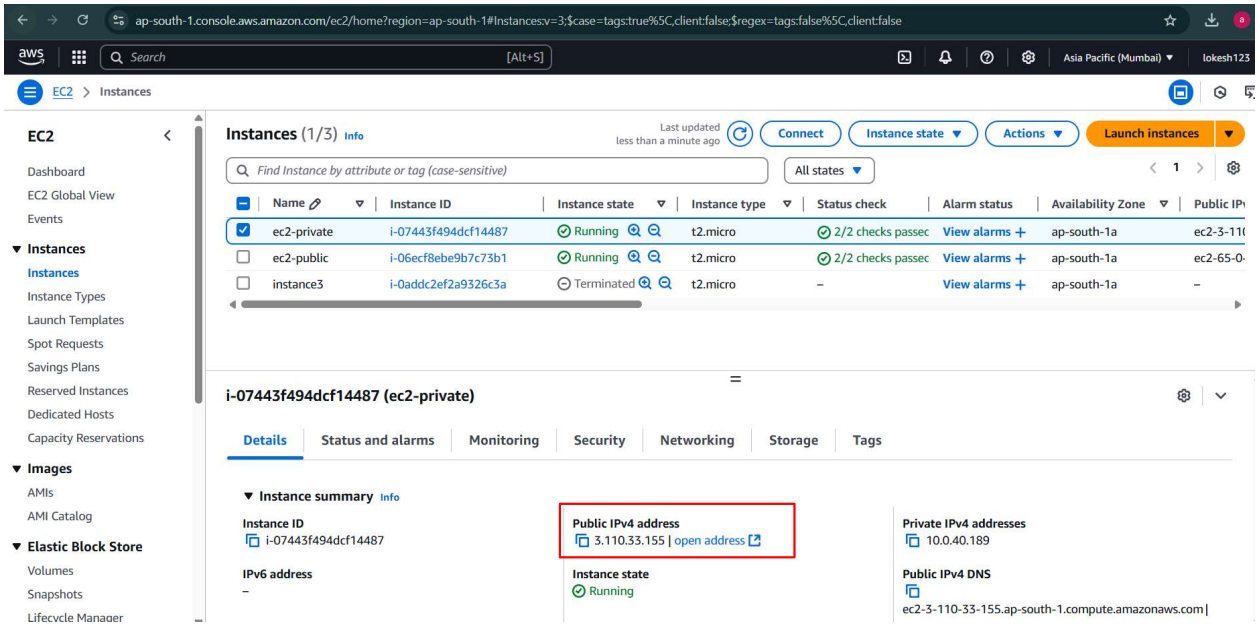
Go to ec2-public and copy Public IPv4 take it as host , give user name as ubuntu and also take key pair past in path give it inthe MobaXtrem

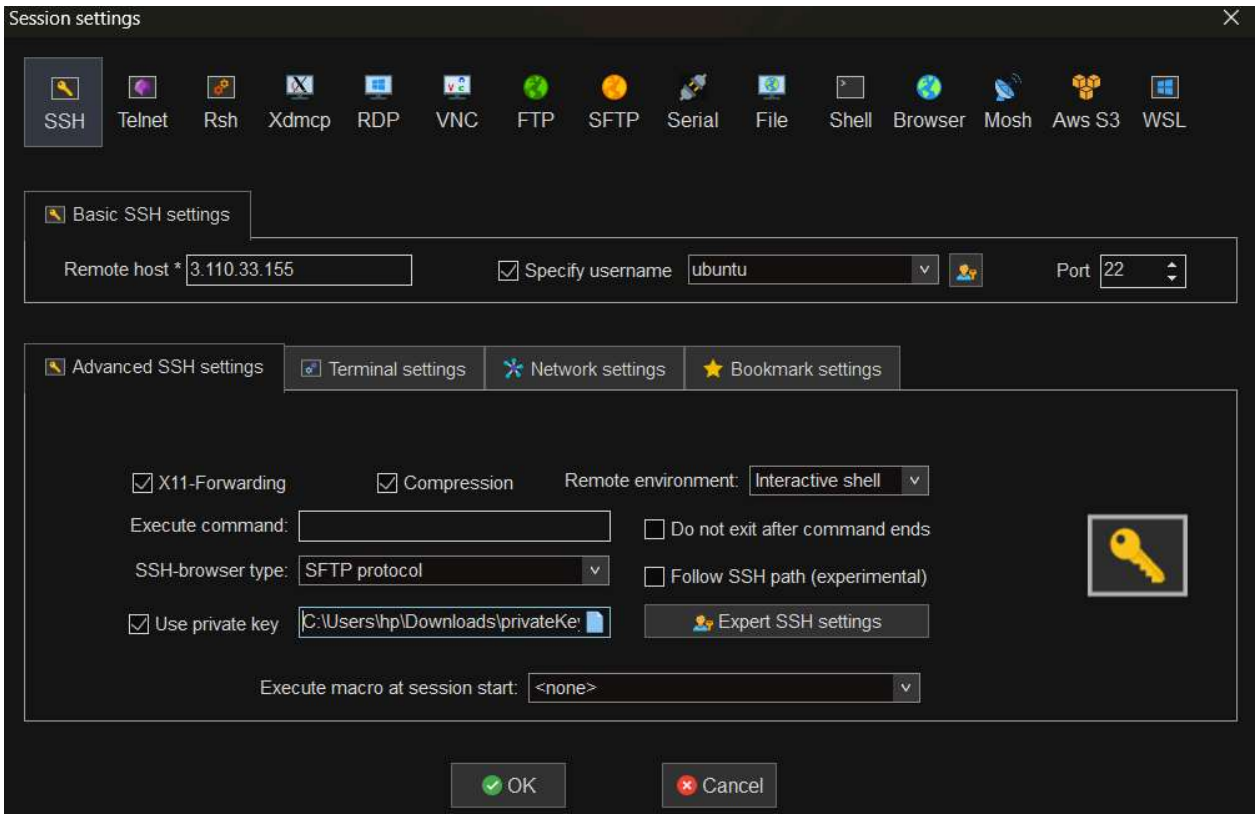


Now you can access the ec2 instance of webserver in MobaXtrem

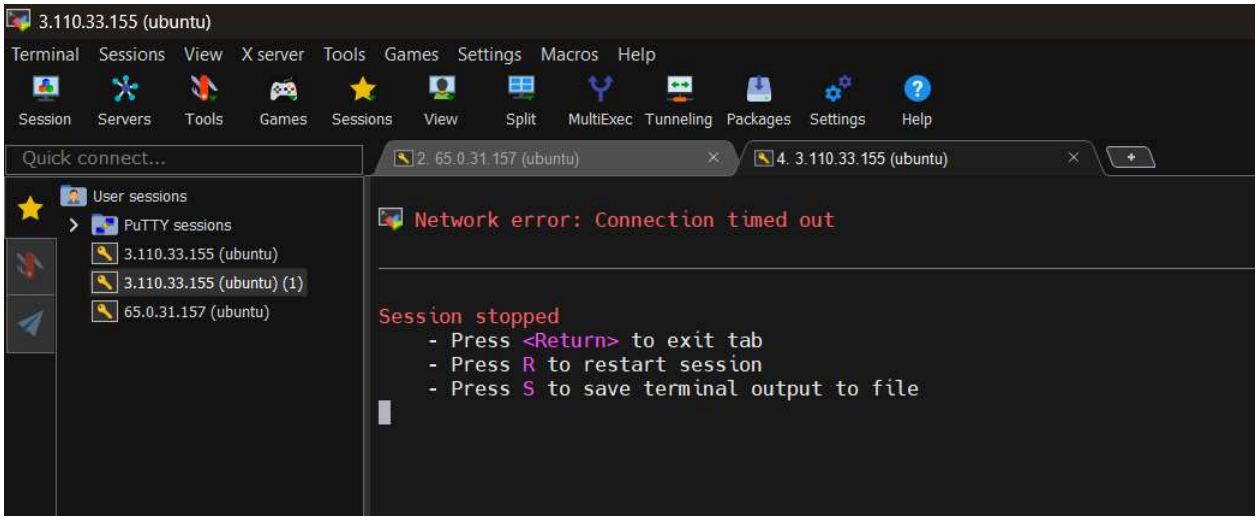


Go to ec2-private and copy Public IPv4 take it as host , give user name as ubuntu and also take key pair past in path give it in MobaXtrem





It cant connect as its private network and didnt initiate ssh access to this server

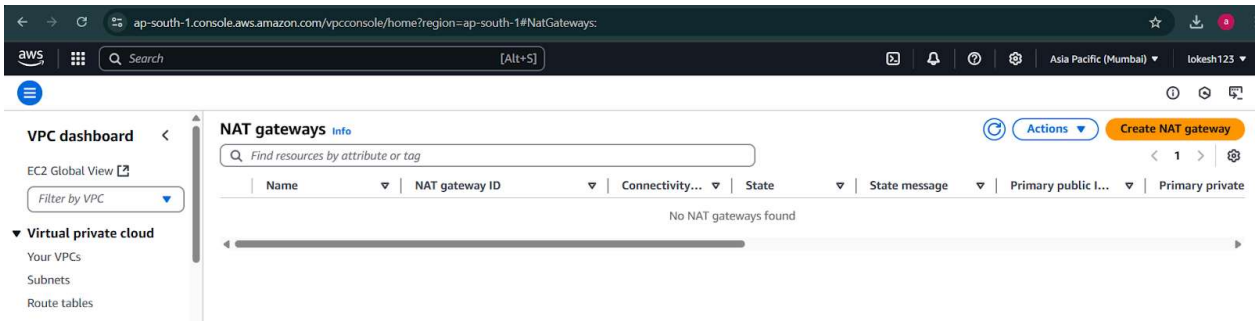


Note :
In Security Groups we can have inbound and outbound rules for the allowed traffic and we dont have have any inbound and outbound rule that denies traffic ,whereas NACL have inbound and outbound rules for the allowed and denies traffic

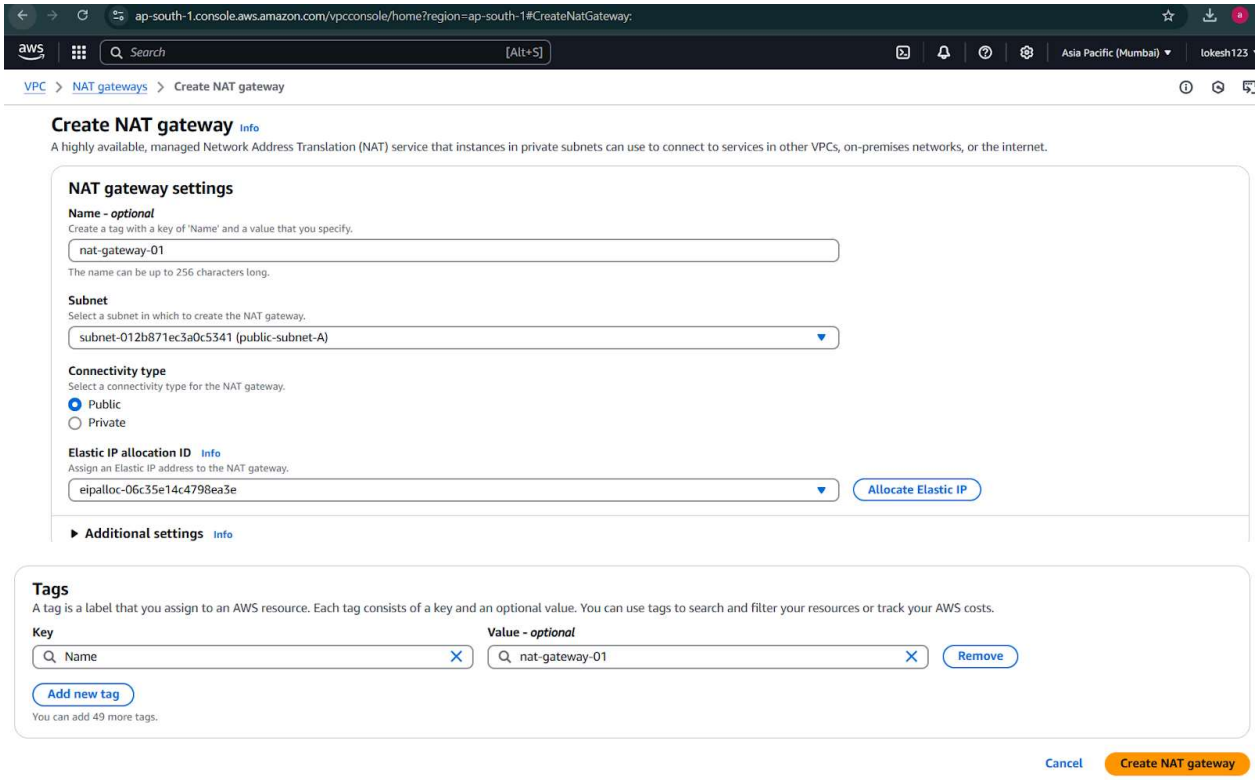
NAT GATEWAY

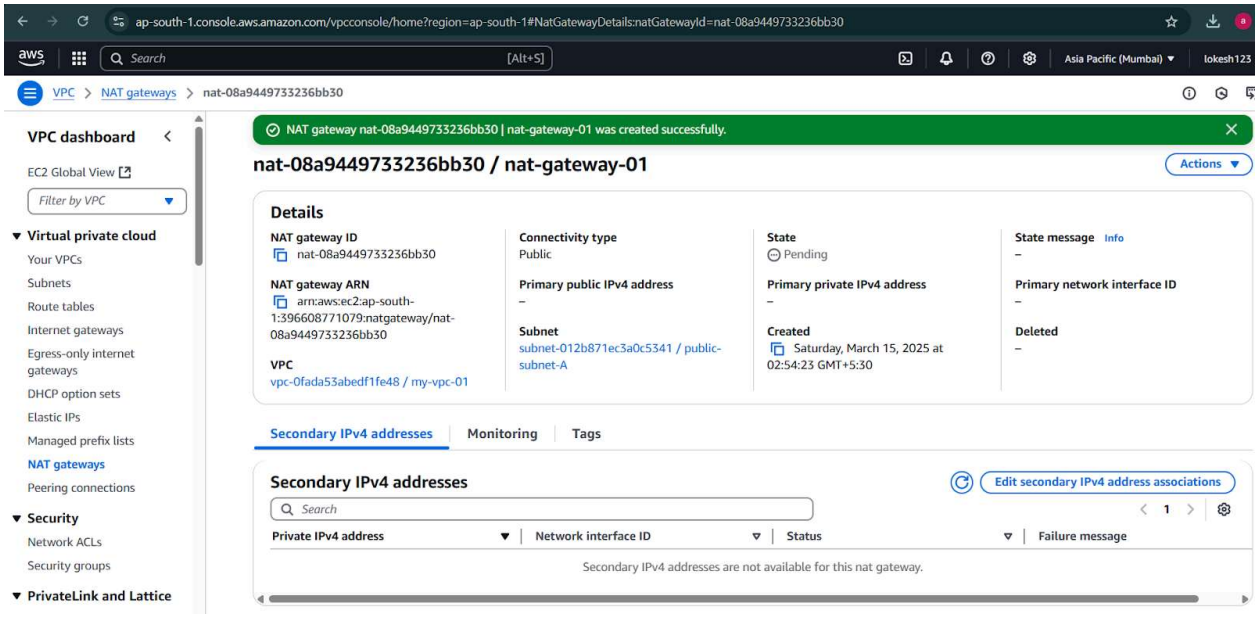
Gateway is a better alternative of Nat instance
Managed service by AWS, high availability, higher bandwidth, auto-scaling
No security groups to manage
No infra management/server patching is required
1 NAT Gateway can span over 1 AZ for auto-failover

Click on create Nat Gatway



Give name, choose public subnet, Allocate Elastic IP and then click on create NAT gateway


ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateNatGateway:
Search
[Alt+S]
Asia Pacific (Mumbai)
lokesh123
VPC > NAT gateways > Create NAT gateway
Create NAT gateway Info
A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.
NAT gateway settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
nat-gateway-01
The name can be up to 256 characters long.
Subnet
Select a subnet in which to create the NAT gateway.
subnet-012b871ec3a0c5341 (public-subnet-A)
Connectivity type
Select a connectivity type for the NAT gateway.
Public
Private
Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-06c35e14c4798ea3e
Allocate Elastic IP
Additional settings Info
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Name
Value - optional
nat-gateway-01
Remove
Add new tag
You can add 49 more tags.
Cancel
Create NAT gateway


ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#NatGatewayDetails:natGatewayId=nat-08a9449733236bb30
Search
[Alt+S]
Asia Pacific (Mumbai)
lokesh123
VPC > NAT gateways > nat-08a9449733236bb30
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
PrivateLink and Lattice
NAT gateway nat-08a9449733236bb30 | nat-gateway-01 was created successfully.
nat-08a9449733236bb30 / nat-gateway-01
Actions
Details
NAT gateway ID
nat-08a9449733236bb30
NAT gateway ARN
arn:aws:ec2:ap-south-1:396608771079:natgateway/nat-08a9449733236bb30
VPC
vpc-0fada53abedf1fe48 / my-vpc-01
Connectivity type
Public
Primary public IPv4 address
–
Subnet
subnet-012b871ec3a0c5341 / public-subnet-A
State
Pending
Primary private IPv4 address
–
Created
Saturday, March 15, 2025 at 02:54:23 GMT+5:30
State message Info
–
Primary network interface ID
–
Deleted
–
Secondary IPv4 addresses
Monitoring
Tags
Secondary IPv4 addresses
Edit secondary IPv4 address associations
Search
1
Private IPv4 address
Network interface ID
Status
Failure message
Secondary IPv4 addresses are not available for this nat gateway.

PART 3

Automated Intrusion Detection & Response (IDR):

1. Deploy **Suricata or Snort for network traffic anomaly detection**.

Snort Installation and setup

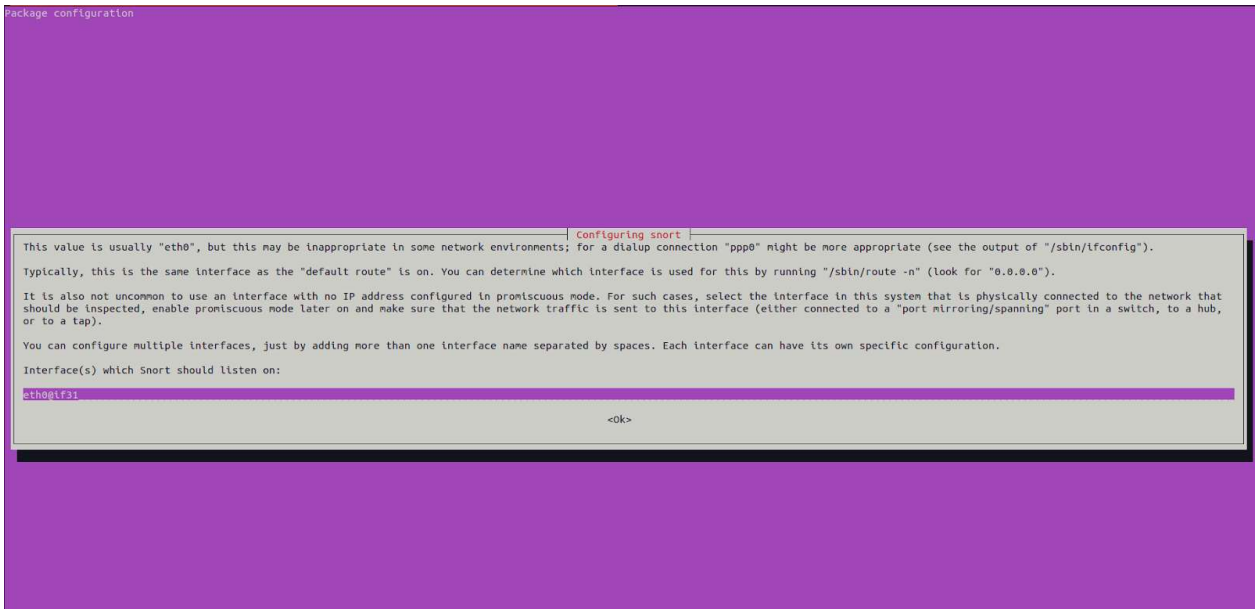
Update all the apt packages

```
lokesh@agent1:~$ sudo apt-get update
[sudo] password for lokesh:
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
```

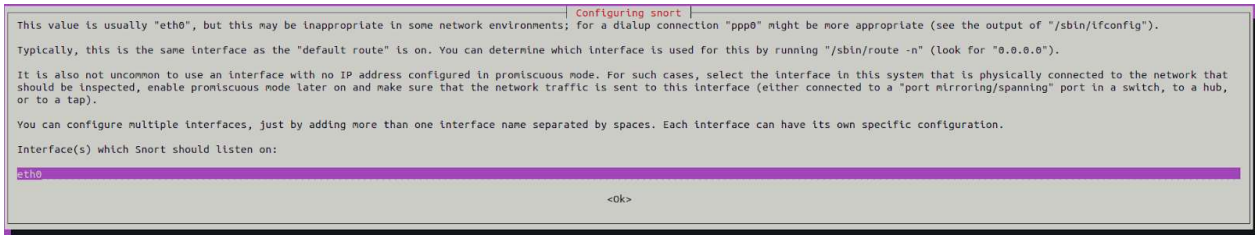
Install Snort

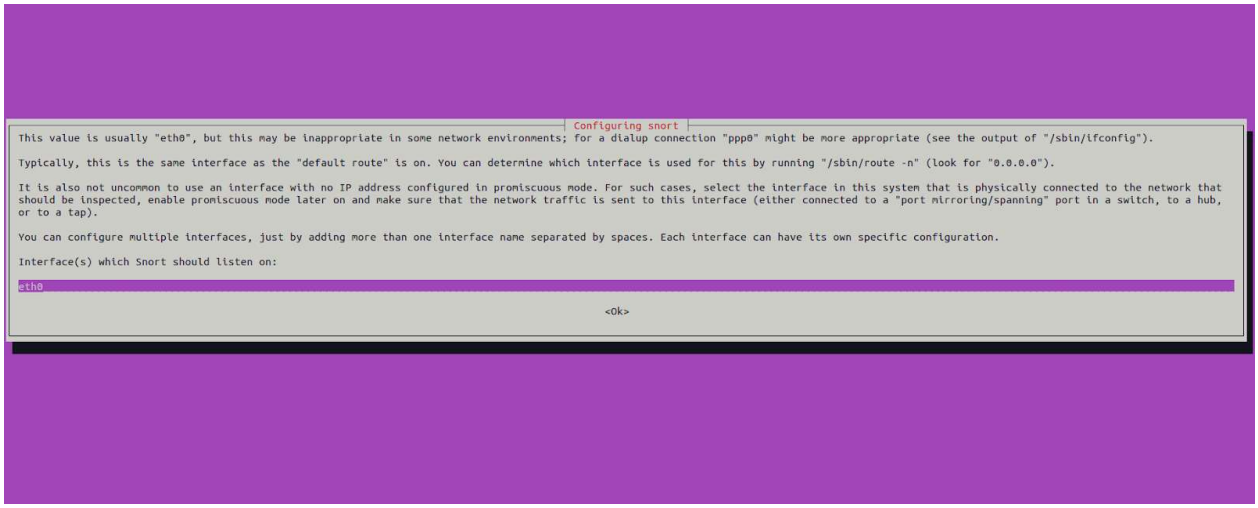
```
lokesh@agent1:~$ sudo apt-get install snort -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauthen-sasl-perl libclone-perl libdaq2 libdata-dump-perl libdumbnet1
  libencode-locale-perl libfile-listing-perl libfont-afm-perl
.
'

.
.
```

Choose Interface as eth0 for LXD



Give eth0 as interface





To determine which version of the Snort is installed, type the following command:

```
lokesh@agent1:~$ snort -V

  ,,_     -*> Snort! <*-
 o"  )~   Version 2.9.15.1 GRE (Build 15125)
  ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
          Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using libpcap version 1.10.1 (with TPACKET_V3)
          Using PCRE version: 8.39 2016-06-14
          Using ZLIB version: 1.2.11
```

List /etc/snort

```
lokesh@agent1:~$ ls -la /etc/snort/
total 368
drwxr-xr-x  3 root root    4096 Nov 15 19:36 .
drwxr-xr-x 90 root root    4096 Nov 15 06:48 ..
-rw-r--r--  1 root root    1281 Dec  3  2019 attribute_table.dtd
-rw-r--r--  1 root root    3757 Dec  3  2019 classification.config
-rw-r--r--  1 root root   82469 Dec  3  2021 community-sid-msg.map
-rw-r--r--  1 root root   23657 Dec  3  2019 file_magic.conf
-rw-r--r--  1 root root   32789 Dec  3  2019 gen-msg.map
-rw-r--r--  1 root root     687 Dec  3  2019 reference.config
drwxr-xr-x  2 root root    4096 Nov 15 06:46 rules
-rw-r-----  1 root snort  29775 Dec  3  2021 snort.conf
-rw-------  1 root root     806 Nov 15 19:36 snort.debian.conf
-rw-r--r--  1 root root    2335 Dec  3  2019 threshold.conf
-rw-r--r--  1 root root  160606 Dec  3  2019 unicode.map
```

Edit /etc/snort/snort.conf

```
lokesh@agent1:~$ sudo nano /etc/snort/snort.conf
ipvar HOME_NET 192.168.122.141/32
//ipvar HOME_NET [10.189.151.13,10.189.151.97,10.189.151.161]
var RULE_PATH /etc/snort/rules
include $RULE_PATH/local.rules
#pcap
output log_tcpdump: /var/log/snort/tcpdump.log
#csv
output alert_csv: /var/log/snort/alert.csv default
# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
#include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
#include $RULE_PATH/ddos.rules
#include $RULE_PATH/dns.rules
#include $RULE_PATH/dos.rules
#include $RULE_PATH/experimental.rules
```

Test all the configuration changes right or wrong

```
lokesh@agent1:~$ sudo snort -T -i eth0 -c /etc/snort/snort.conf
Running in Test mode

      --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!

.
.
        Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
        Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
        Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>

Snort successfully validated the configuration!
Snort exiting
```

Create custome rules for snort

```
lokesh@agent1:~$ sudo nano /etc/snort/rules/local.rules
alert icmp any any -> $HOME_NET any (msg:"ICMP Detection Rule"; sid:100001;)
alert tcp any any -> $HOME_NET 22 (msg: "SSH Connection Attempts"; sid:100002; )
alert tcp any any -> $HOME_NET 80 (msg:"Command Execution Attempt"; content:"GET";
content:"/etc/passwd"; sid:100003; )
```

Testing Snort Rules

Firstly; we will send ICMP Ping packets from the Attacker Machine which has IP address 192.168.189.128 to the Ubuntu Machine.
Secondly; we will make an SSH connection attempt from the Attacker Machine to the Ubuntu Machine.
Thirdly; we will send a command execution request with the curl from the Attacker Machine to the Ubuntu Machine.

Snort will also write alerts to the CSV file and PCAP file because we configured We can use these files to investigate attacks later. We can reach this file in the /var/log/snort directory.

lokesh@cybercub:~$ ping 10.189.151.53
PING 10.189.151.53 (10.189.151.53) 56(84) bytes of data.
64 bytes from 10.189.151.53: icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from 10.189.151.53: icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from 10.189.151.53: icmp_seq=3 ttl=64 time=0.050 ms
64 bytes from 10.189.151.53: icmp_seq=4 ttl=64 time=0.072 ms

Check logs in Agent1

root@agent1:~# sudo snort -q -l /var/log/snort -i eth0 -A console -c /etc/snort/snort.conf
11/18-19:10:58.251654 [**] [1:100001:0] "ICMP Detection Rule" [**] [Priority: 0] {ICMP}
10.189.151.1 -> 10.189.151.53
11/18-19:10:59.276037 [**] [1:100001:0] "ICMP Detection Rule" [**] [Priority: 0] {ICMP}
10.189.151.1 -> 10.189.151.53
11/18-19:11:00.300047 [**] [1:100001:0] "ICMP Detection Rule" [**] [Priority: 0] {ICMP}

2. Configure **fail2ban to block repeated SSH & web attacks automatically**.

WHAT IS FAIL2BAN?
01 Helps prevent brute-force attacks
02 Watches logs for authentication failure
03 Creates firewall rules to block IP addresses
04 Able to protect multiple services
05 Completely customizable

root@fail2ban:~# apt update
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [3433 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
.
.
.

```
root@fail2ban:~# apt install fail2ban -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify whois
0 upgraded, 3 newly installed, 0 to remove and 52 not upgraded.
Need to get 444 kB of archives.
After this operation, 2400 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 fail2ban all 0.11.1-1 [375 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal/main amd64 python3-pyinotify all 0.9.6-1.2ubuntu1
[24.8 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/main amd64 whois amd64 5.5.6 [44.7 kB]
.
.
.


root@fail2ban:~# systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban

root@fail2ban:~# ls -al /etc/fail2ban/
total 72
drwxr-xr-x  6 root root  4096 Mar 14 22:53 .
drwxr-xr-x 96 root root  4096 Mar 14 22:53 ..
drwxr-xr-x  2 root root  4096 Mar 14 22:53 action.d
-rw-r--r--  1 root root  2817 Jan 11  2020 fail2ban.conf
drwxr-xr-x  2 root root  4096 Mar  2  2020 fail2ban.d
drwxr-xr-x  3 root root  4096 Mar 14 22:53 filter.d
-rw-r--r--  1 root root 25740 Jan 11  2020 jail.conf
drwxr-xr-x  2 root root  4096 Mar 14 22:53 jail.d
-rw-r--r--  1 root root   645 Jan 11  2020 paths-arch.conf
-rw-r--r--  1 root root  2827 Jan 11  2020 paths-common.conf
-rw-r--r--  1 root root   573 Jan 11  2020 paths-debian.conf
-rw-r--r--  1 root root   738 Jan 11  2020 paths-opensuse.conf
```

Jail is a configuration file that contains filters and arguments that protect system or a particular service

```
root@fail2ban:~# less /etc/fail2ban/jail.conf
.
.

root@fail2ban:~# nano /etc/fail2ban/jail.local
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 3600
ignoreip = 127.0.0.1 //this is for whitelisting ip

root@fail2ban:~# systemctl restart fail2ban
root@fail2ban:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor pres>
     Active: active (running) since Sat 2025-03-15 00:10:01 UTC; 8s ago
       Docs: man:fail2ban(1)
    Process: 1455 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status>
   Main PID: 1456 (f2b/server)
      Tasks: 5 (limit: 18795)
     Memory: 11.0M
        CPU: 97ms
     CGroup: /system.slice/fail2ban.service
             └─1456 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Mar 15 00:10:01 fail2ban systemd[1]: Starting Fail2Ban Service...
Mar 15 00:10:01 fail2ban systemd[1]: Started Fail2Ban Service.
Mar 15 00:10:01 fail2ban fail2ban-server[1456]: Server ready
```

SSH jail got activated
root@fail2ban:~# fail2ban-client status
Status
|- Number of jail:	1
`- Jail list:	sshd

From another machine trying brute ssh
root@sensor1:~# hydra -l root -P /wordlists/rockyou.txt ssh://10.189.151.97 -l -v
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-15 02:48:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: /wordlists/rockyou.txt

On the machine where fail2ban hosted it worked as ssh login failed over brute force
root@fail2ban:~# cat /var/log/auth.log
Mar 14 22:47:38 sensor4 sshd[219]: Server listening on 0.0.0.0 port 22.
Mar 14 22:47:38 sensor4 sshd[219]: Server listening on :: port 22.
Mar 14 22:47:38 sensor4 systemd-logind[173]: New seat seat0.
Mar 14 22:49:53 fail2ban sshd[218]: Server listening on 0.0.0.0 port 22.
Mar 14 22:49:53 fail2ban sshd[218]: Server listening on :: port 22.
Mar 14 22:49:53 fail2ban systemd-logind[201]: New seat seat0.
Mar 14 22:50:26 fail2ban sshd[221]: Server listening on 0.0.0.0 port 22.
Mar 14 22:50:26 fail2ban sshd[221]: Server listening on :: port 22.
Mar 14 22:50:26 fail2ban systemd-logind[202]: New seat seat0.
Mar 14 23:06:01 fail2ban CRON[1315]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 14 23:06:01 fail2ban CRON[1315]: pam_unix(cron:session): session closed for user root
Mar 14 23:17:01 fail2ban CRON[1320]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 14 23:17:01 fail2ban CRON[1320]: pam_unix(cron:session): session closed for user root
Mar 15 00:12:33 fail2ban sshd[1468]: Connection closed by authenticating user root 10.189.151.79 port 54714 [preauth]
Mar 15 00:12:59 fail2ban sshd[1470]: Connection closed by authenticating user root 10.189.151.79 port 36770 [preauth]
Mar 15 00:13:29 fail2ban sshd[1472]: Connection closed by authenticating user root 10.189.151.79 port 50430 [preauth]
Mar 15 00:16:42 fail2ban sshd[1478]: Connection closed by authenticating user root 10.189.151.1 port 55416 [preauth]
Mar 15 00:17:01 fail2ban CRON[1480]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 15 00:17:01 fail2ban CRON[1480]: pam_unix(cron:session): session closed for user root

Mar 15 02:30:41 fail2ban sshd[221]: Received signal 15; terminating.
Mar 15 02:30:41 fail2ban sshd[1535]: Server listening on 0.0.0.0 port 22.
Mar 15 02:30:41 fail2ban sshd[1535]: Server listening on :: port 22.
Mar 15 02:30:48 fail2ban sshd[1535]: Received signal 15; terminating.
Mar 15 02:30:48 fail2ban sshd[1539]: Server listening on 0.0.0.0 port 22.
Mar 15 02:30:48 fail2ban sshd[1539]: Server listening on :: port 22.
Mar 15 02:31:06 fail2ban sshd[1540]: Connection closed by authenticating user root 10.189.151.79 port 44738 [preauth]
Mar 15 02:31:14 fail2ban sshd[1542]: Connection closed by authenticating user root 10.189.151.79 port 32808 [preauth]
Mar 15 02:32:13 fail2ban sshd[1546]: Connection closed by authenticating user root 10.189.151.79 port 46542 [preauth]
Mar 15 02:56:51 fail2ban sshd[1568]: Connection closed by authenticating user root 10.189.151.1 port 38304 [preauth]
Mar 15 02:56:55 fail2ban sshd[1570]: Connection closed by authenticating user root 10.189.151.1 port 38308 [preauth]

SIEM & Log Aggregation

1. Centralize logs with **ELK Stack (Elasticsearch, Logstash, Kibana)**

Before installation of ELK do set up for dependencies required :
Check ubuntu version you are using

```
root@elk:~# lsb_release -a
No LSB modules are available.
Distributor ID:  Ubuntu
Description:     Ubuntu 20.04.6 LTS
Release:         20.04
Codename:        focal
```

Install java dependencies

```
root@elk:~# apt install default-jdk default-jre -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  at-spi2-core ca-certificates-java default-jdk-headless default-jre-headless
.
.
.
```

Check java version

```
root@elk:~# javac -version
javac 11.0.26
```

Make sure that curl installed if not then install curl

```
root@elk:~# sudo apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
curl is already the newest version (7.68.0-1ubuntu2.25).
curl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 29 not upgraded.
```

Add the elasticsearch APT repository key by using the below command (run these commands Root

```
root@elk:~# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
OK
```

Add the Elastic Search to the APT source List by using the below command

```
root@elk:~# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" >
 /etc/apt/sources.list.d/elastic-7.x.list
```

Installation of Elastic search:

```
root@elk:~# apt update
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]
Get:2 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [143 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Hit:4 http://archive.ubuntu.com/ubuntu focal InRelease
Get:5 http://archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
Fetched 540 kB in 2s (320 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
29 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Install elastic search

```
root@elk:~# apt install elasticsearch -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 29 not upgraded.
Need to get 325 MB of archives.
After this operation, 542 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elasticsearch amd64 7.17
```

Configuration of elasticsearch

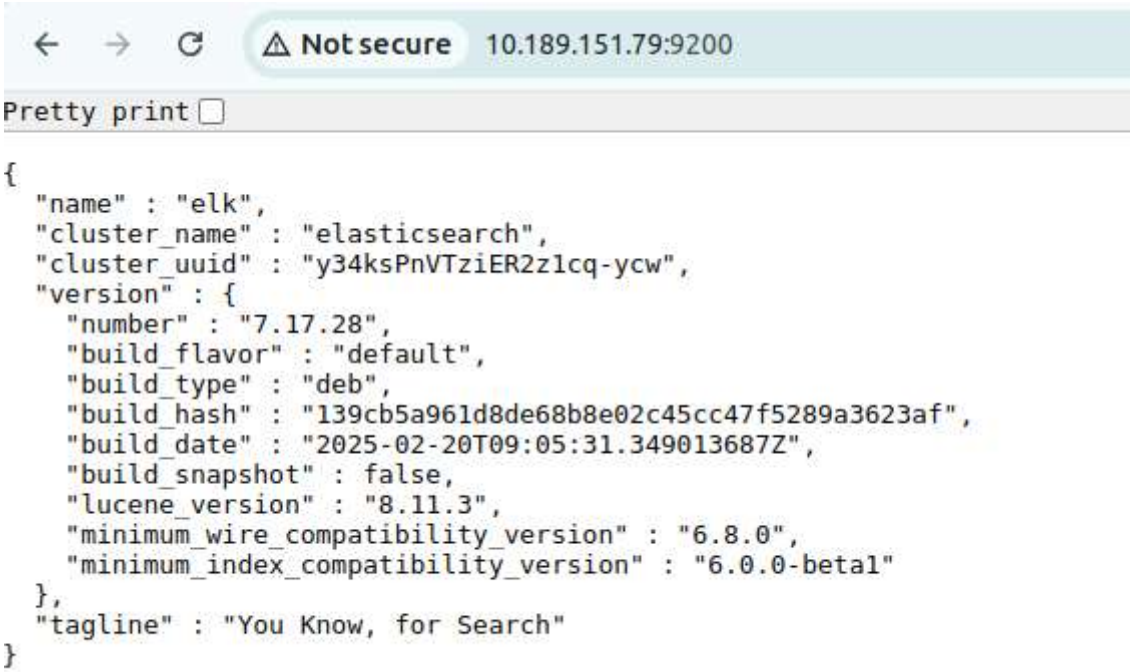
```
root@elk:~# nano /etc/elasticsearch/elasticsearch.yml
network.host: '10.189.151.79'
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
discovery.type: single-node

root@elk:~# nano /etc/elasticsearch/jvm.options
-Xms512m
-Xmx512m
```

Enable Elasticsearch

```
root@elk:~# systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service →
/lib/systemd/system/elasticsearch.service.
```

Start Elasticsearch

```
root@elk:~# systemctl start elasticsearch

root@elk:~# curl -X GET "10.189.151.79:9200"
{
  "name" : "elk",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "y34ksPnVTziER2z1cq-ycw",
  "version" : {
    "number" : "7.17.28",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "139cb5a961d8de68b8e02c45cc47f5289a3623af",
    "build_date" : "2025-02-20T09:05:31.349013687Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.3",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```



Logstash setup
Install logstash
root@elk:~# apt install logstash -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 29 not upgraded.
Need to get 375 MB of archives.
After this operation, 632 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash amd64 1:7.17.28-1 [375 MB]
Fetched 375 MB in 1min 40s (3738 kB/s)
Selecting previously unselected package logstash.
.
.
.
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in versio
n 9.0 and will likely be removed in a future release.
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaserun/pl
atform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash

```
root@elk:~# systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service →
/etc/systemd/system/logstash.service.
root@elk:~# systemctl start logstash
root@elk:~# systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2025-03-15 04:44:44 UTC; 7s ago
   Main PID: 5130 (java)
      Tasks: 25 (limit: 18795)
     Memory: 535.3M
        CPU: 31.473s
     CGroup: /system.slice/logstash.service
             └─5130 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSIn
.
.
Kibana Set up
root@elk:~# apt update
Hit:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
29 packages can be upgraded. Run 'apt list --upgradable' to see them.

root@elk:~# apt install kibana -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 29 not upgraded.
Need to get 293 MB of archives.
After this operation, 744 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.17.28 [293 MB]
.
.
```

Creating kibana group... OK
root@elk:~# systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service →
/etc/systemd/system/kibana.service.

root@elk:~# systemctl start kibana
root@elk:~# systemctl status kibana
● kibana.service - Kibana
Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
Active: active (running) since Sat 2025-03-15 04:53:07 UTC; 8s ago
Docs: https://www.elastic.co
Main PID: 7519 (node)
Tasks: 11 (limit: 18795)
Memory: 246.8M
CPU: 8.224s
CGroup: /system.slice/kibana.service
.
.
Before Configuration set up make sure that you stop all services
Stop Kibana service
root@elk:~# sudo systemctl stop kibana
Stop Elasticsearch service
root@elk:~# sudo systemctl stop elasticsearch
root@elk:~# sudo nano /etc/elasticsearch/elasticsearch.yml
.
.
xpack.security.enabled: true
xpack.security.authc.api_key.enabled:true

root@elk:~# sudo systemctl restart elasticsearch

Generate Passwords
Go to /usr/share/elasticsearch/bin/
root@elk:~# cd /usr/share/elasticsearch/bin/
root@elk:/usr/share/elasticsearch/bin# sudo ./elasticsearch-setup-passwords auto
Initiating the setup of passwords for reserved users elastic_system,beats_system,remote_monitoring_user.
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y
Changed password for user apm_system

PASSWORD apm_system = 5JYIfFJZ7LE71X6sLMTh

Changed password for user kibana_system
PASSWORD kibana_system = sMIBnZ4xK9Od1yLbvyRH

Changed password for user kibana
PASSWORD kibana = sMIBnZ4xK9Od1yLbvyRH

Changed password for user logstash_system
PASSWORD logstash_system = 5XRU2T99usCKWFs0VQO3

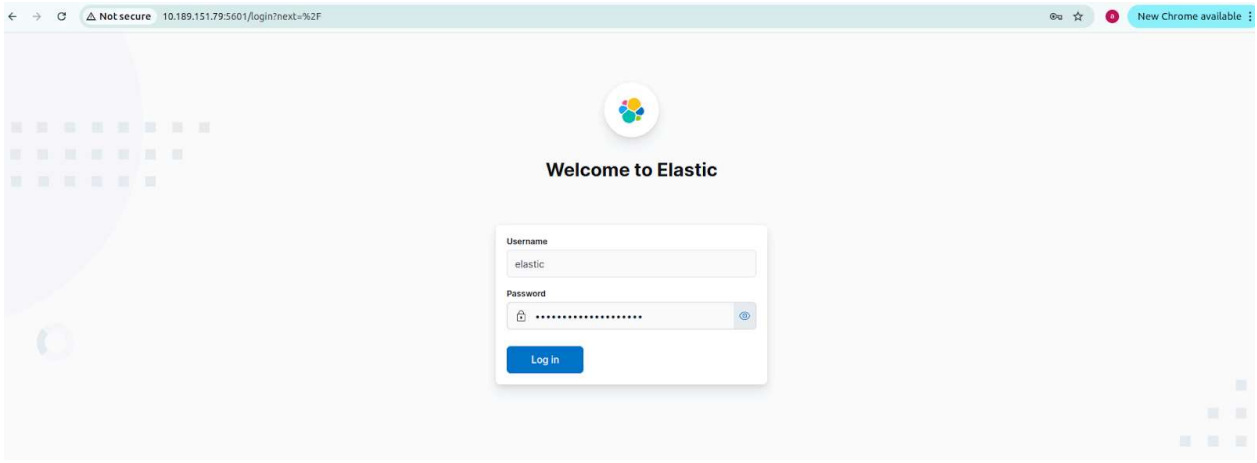
Changed password for user beats_system
PASSWORD beats_system = uSUOq3YDzKYkVvYuiTmh

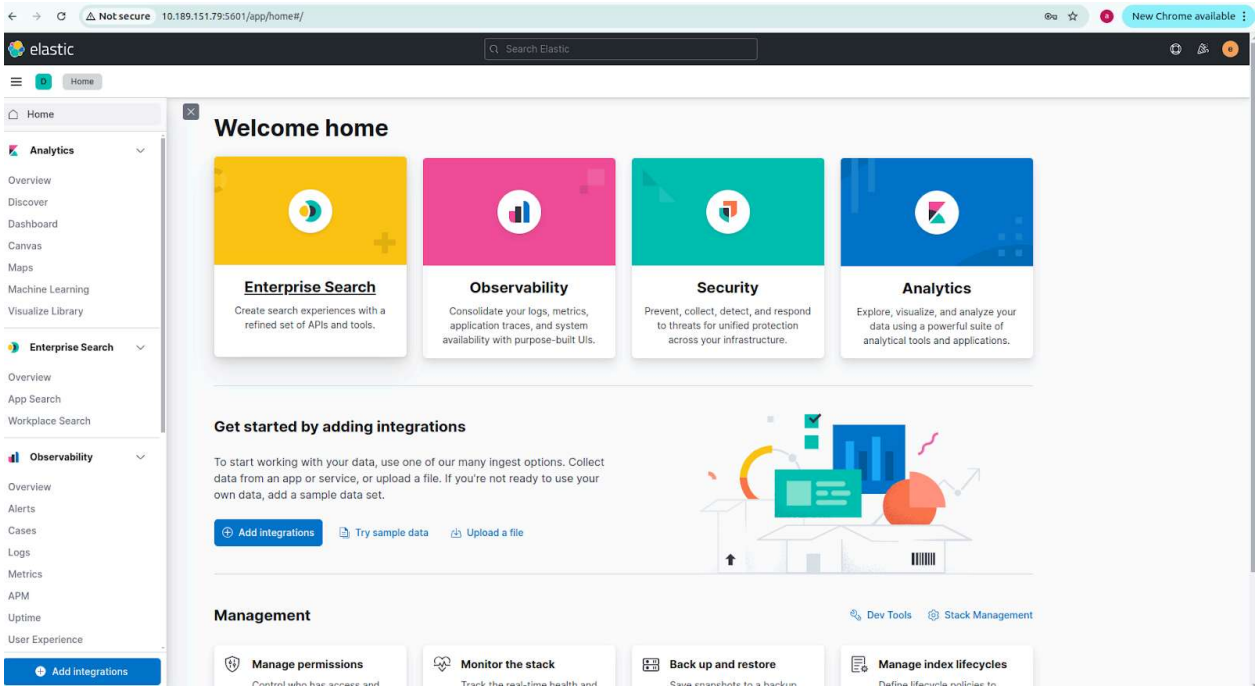
Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = wK8wB4NsTmuZFy5PBhRF

Changed password for user elastic
PASSWORD elastic = 50X1xcn80az1w5HrJjK9

Open kibana.yml
root@elk:/usr/share/elasticsearch/bin# nano /etc/kibana/kibana.yml
server.port: 5601
server.host: "10.189.151.79"
elasticsearch.hosts: ["http://10.189.151.79:9200"]
elasticsearch.username: "elastic"
elasticsearch.password: "50X1xcn80az1w5HrJjK9"

Restart kibana
root@elk:~# systemctl restart kibana





Implement real-time threat detection & alerting for anomalies.

Note : I have already worked on this to save time I am attaching entire procedure of my previous project !

Download filebeat in windows machine
https://www.elastic.co/downloads/past-releases/filebeat-7-17-12

Go to filebeat.yml
In filebeat inputs à type enabed ,path ,tags are configured

```
# ============================== Filebeat inputs ===============================

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

# filestream is an input for collecting log messages from files.
- type: log

  # Unique ID among all inputs, an ID is required.
  #id: my-filestream-id

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx
  tags: ["sysmon"]

    #- /var/log/*.log
    #- c:\programdata\elasticsearch\logs\*
```

In logstash output ip and port of .conf file con.d folder of logstash

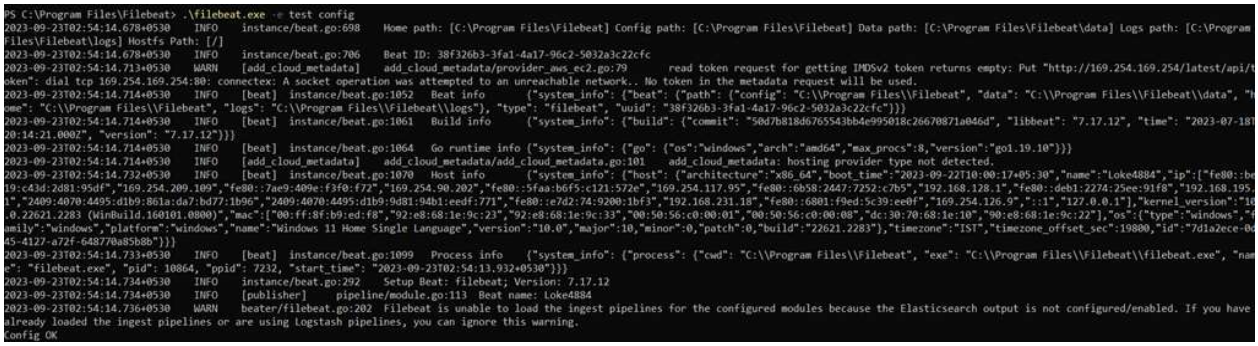
```
# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.195.148:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

Navigate to filbeat path :

```
PS C:\WINDOWS\system32> cd "C:\Program Files\Filebeat"
```

Apply changes

Check configuration of filebeat
.\filebeat.exe -e test config



Install filebeat

PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1

```
PS C:\Program Files\Filebeat> PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Program Files\Filebeat\install-service-filebeat.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R

Status   Name               DisplayName
------   ----               -----------
Stopped  filebeat           filebeat
```

Start the service of filebeat

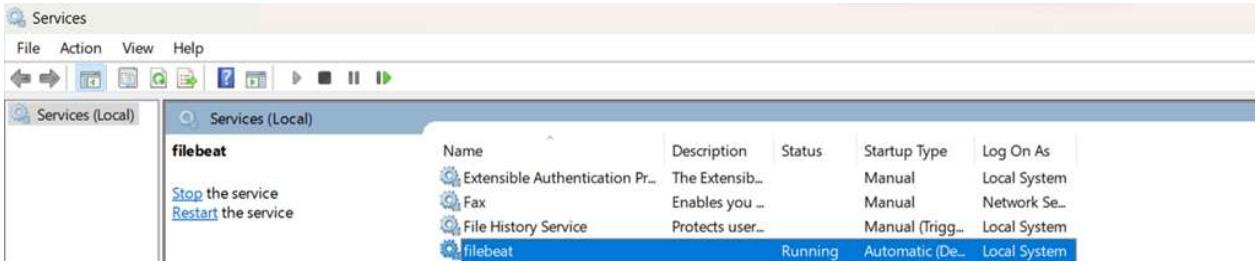
```
PS C:\Program Files\Filebeat> Start-Service filebeat
```

To check configuration of filebeat

```
PS C:\Program Files\Filebeat> .\filebeat.exe test config
Config OK
```

Search services in windows

There you can see status of filebeat



Get-Process -Name "filebeat"

```
PS C:\Program Files\Filebeat> Get-Process -Name "filebeat"

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    213      17    40360      48244       0.80  22700   0 filebeat
```

To check Filebeat logs

.\filebeat.exe -e

Go to conf.d folder

In this folder you write configuration code for logstash to port to elk

```
root@lokesh-manikanta:/# cd /etc/logstash/conf.d/
```

Create a file with extention .conf

```
root@lokesh-manikanta:/etc/logstash/conf.d# touch sysmon.conf
```

To known any other conf file

```
root@lokesh-manikanta:/etc/logstash/conf.d# ls
sysmon.conf
```

Write a code inside sysmon.conf

```
root@lokesh-manikanta:/etc/logstash/conf.d# nano sysmon.conf
```

Save and close Sysmon.conf

Sysmon.conf code :

```
input {
  beats {
        port => 5044
  }
}

filter {
  if "sysmon" in [tags] {
        grok {

match=>{"message"=>["%{DATESTAMP:Date} %{LOGLEVEL:LOGLEVEL} %{IP:ip}
%{GREEDYDATA:data}","%{DATESTAMP:Date1} %{LOGLEVEL:LOGLEVEL1} %{GREEDYDATA:data1}"
,"%{DATESTAMP:Date2} %{GREEDYDATA:data2}"]
    }
   }
        # Add additional filter plugins for further processing as needed
  }
}

output {
  elasticsearch {
        hosts => ["192.168.195.148:9200"]
        user => "elastic"
        password => "u7gin9UoF4vSh1c5n44l"
        index => "sysmon-%{+YYYY.MM.dd}"
  }
}
```

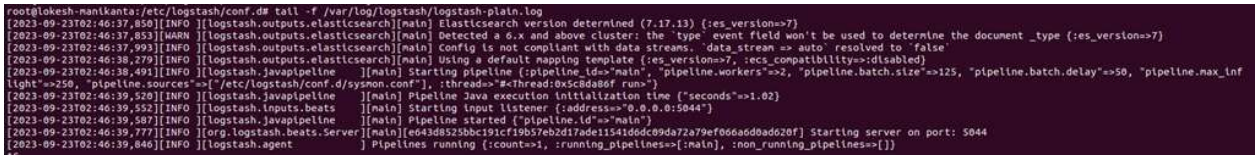
Restart logstash

```
root@lokesh-manikanta:/etc/logstash/conf.d# systemctl restart logstash
```

Start the services of the logstash

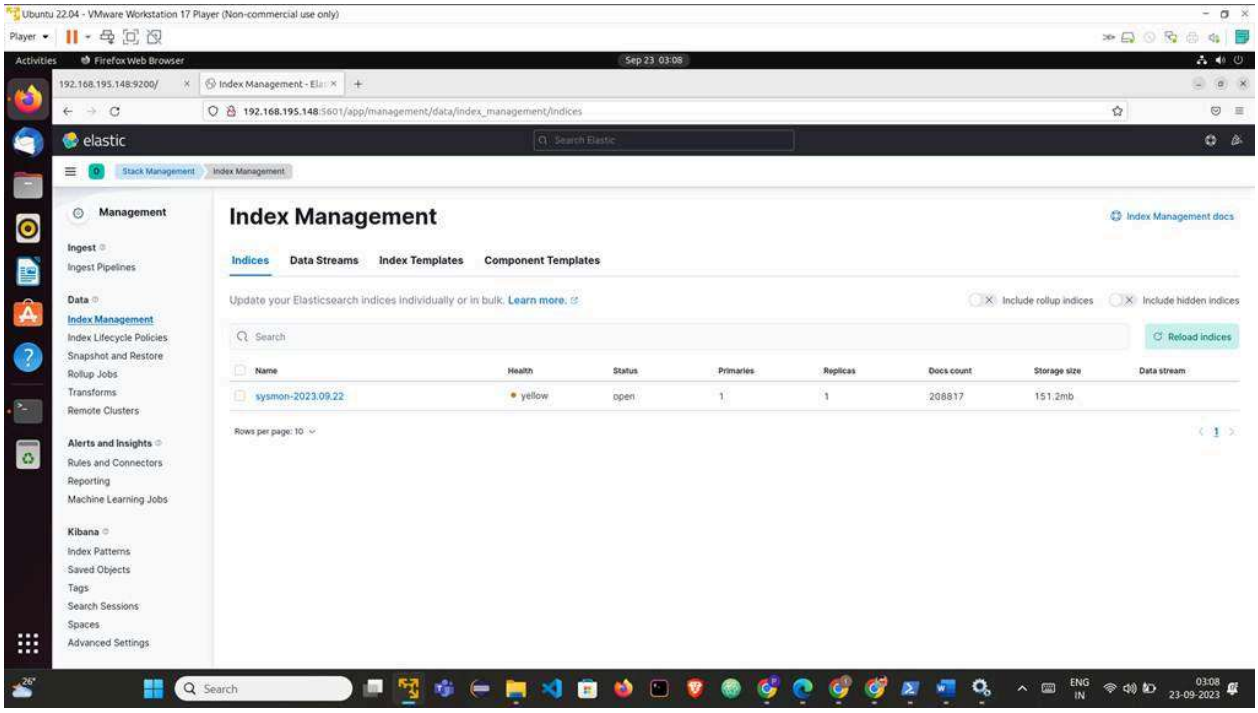
```
root@lokesh-manikanta:/etc/logstash/conf.d# sudo service logstash start
```

To see logs of logstash (logs will be stored in logstash-plain.log)

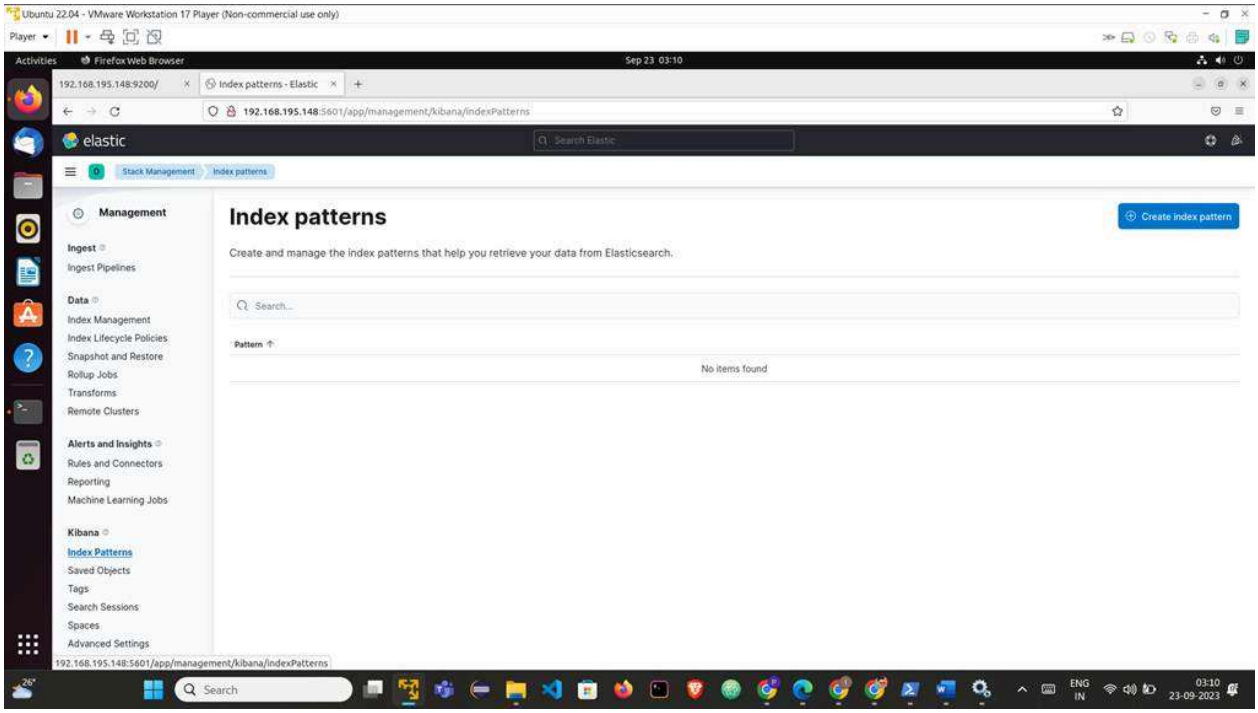


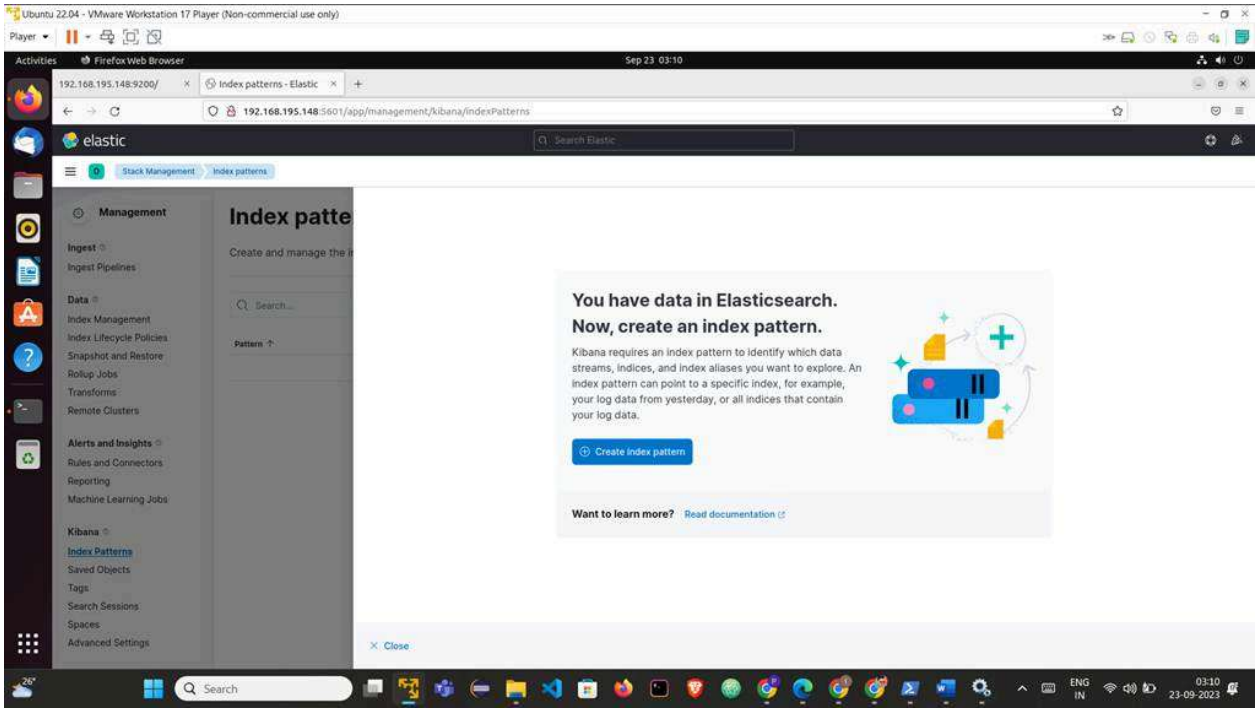
Go to Date à Index Mangement

You will get index you created in logstash configuration file(ex : sysmon.conf)

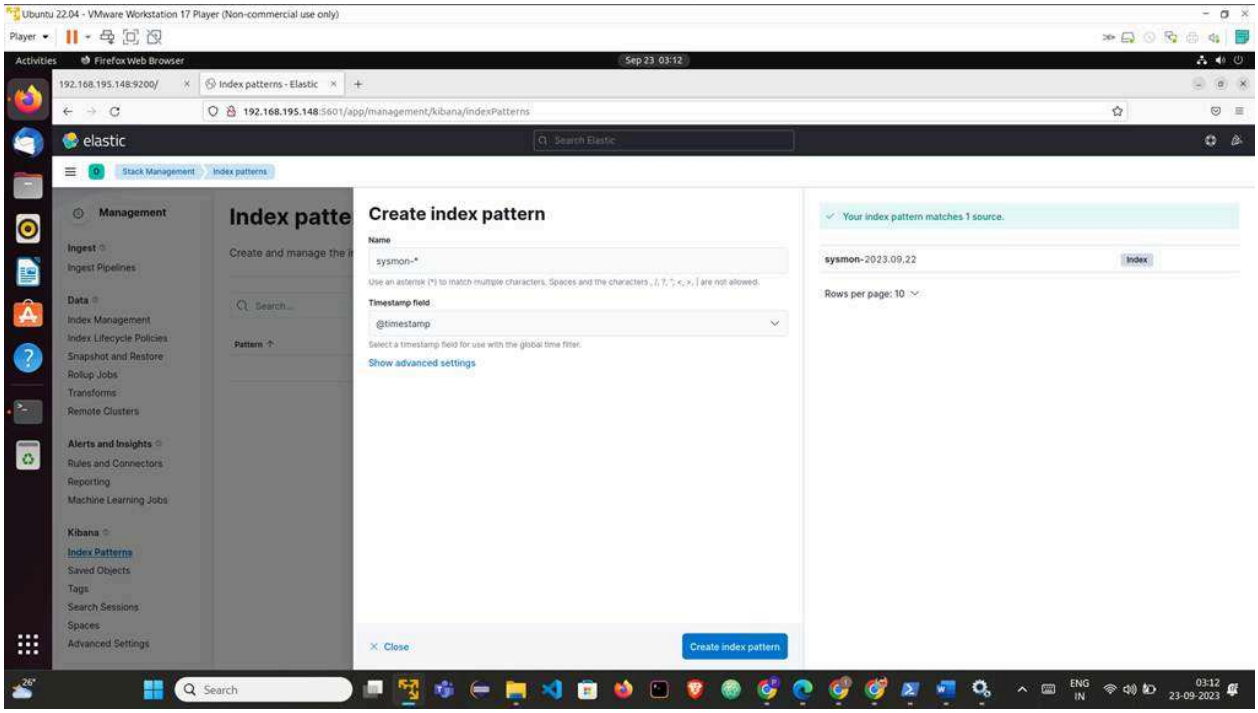


Go to kibana à Index Pattern à Create Index Pattern

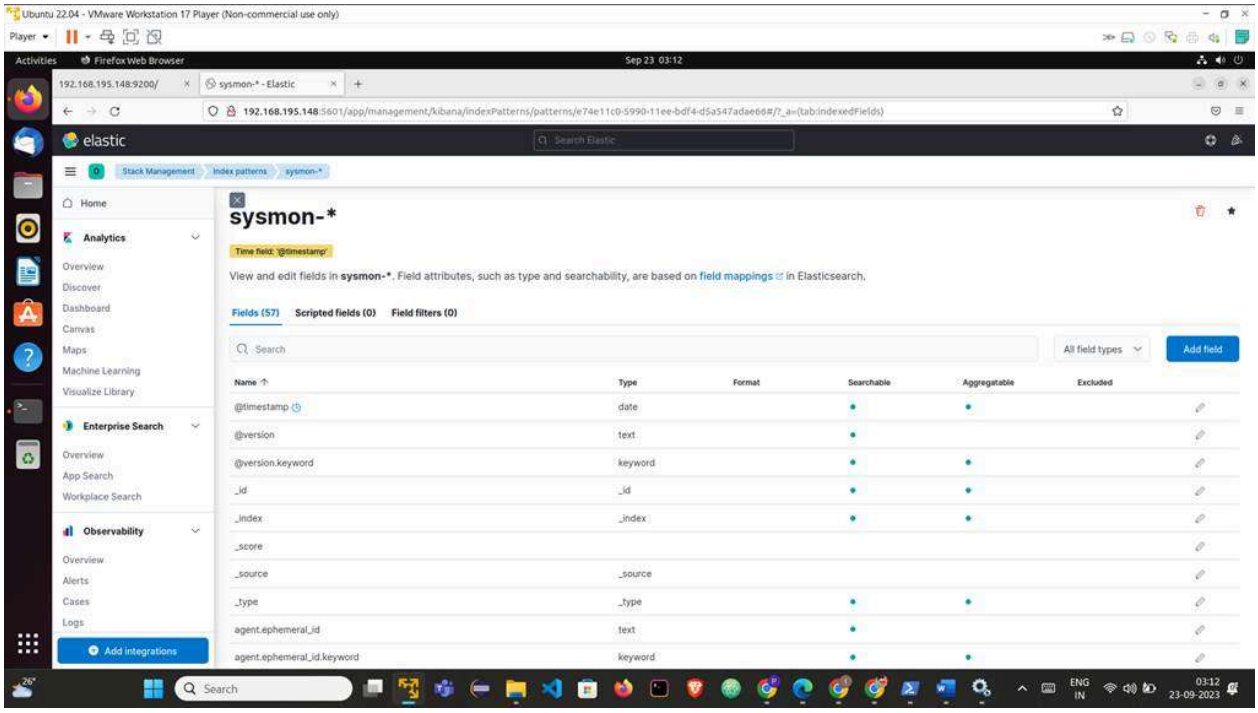


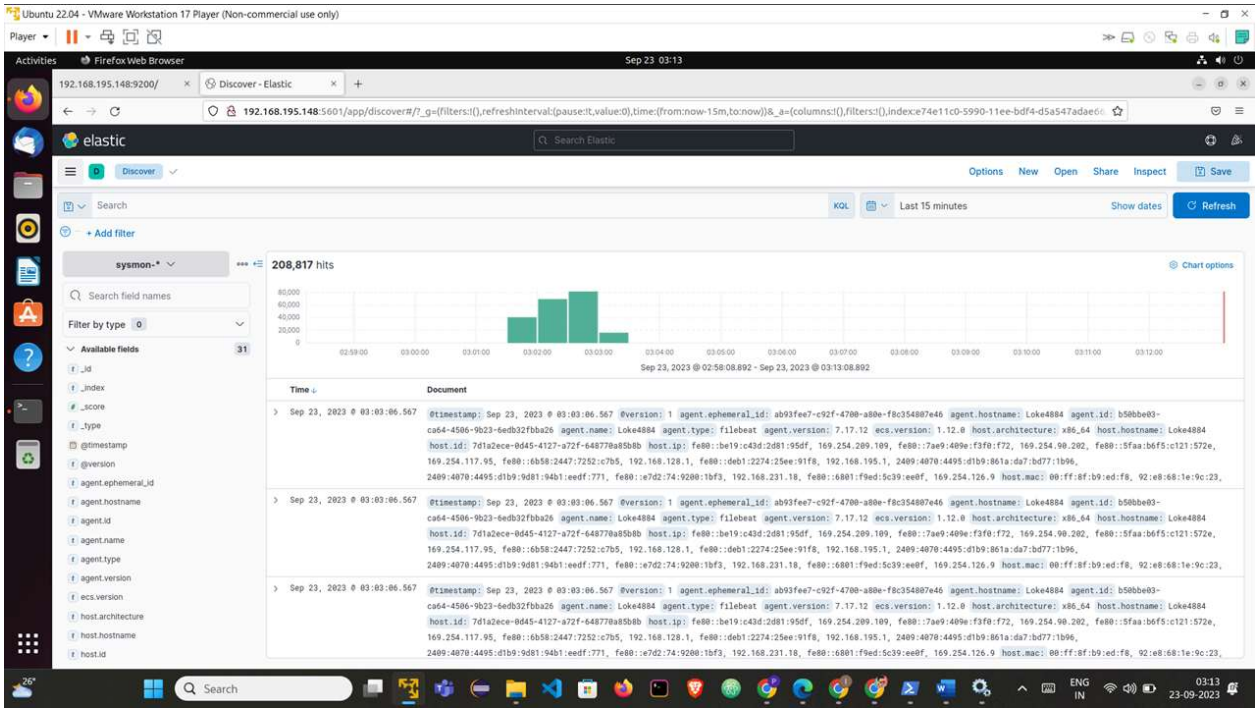


Give name and time stamp and click on create index pattern



Go to discover choose what Index you created


Ubuntu 22.04 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Firefox Web Browser
Sep 23 03:12
192.168.195.148:9200/
sysmon-* - Elastic
192.168.195.148:5601/app/management/kibana/indexPatterns/patterns/e74e11c0-5990-11ee-bdf4-d5a547adae66#/?_a=(tab:indexedFields)
elastic
Search Elastic
Stack Management
Index patterns
sysmon-*
Home
Analytics
Overview
Discover
Dashboard
Canvas
Maps
Machine Learning
Visualize Library
Enterprise Search
Overview
App Search
Workplace Search
Observability
Overview
Alerts
Cases
Logs
Add integrations
sysmon-*
Time field: '@timestamp'
View and edit fields in sysmon-*. Field attributes, such as type and searchability, are based on field mappings in Elasticsearch.
Fields (57)
Scripted fields (0)
Field filters (0)
Search
All field types
Add field
Name
Type
Format
Searchable
Aggregatable
Excluded
@timestamp
date
@version
text
@version.keyword
keyword
_id
_id
_index
_index
_score
_source
_source
_type
_type
agent.ephemeral_id
text
agent.ephemeral_id.keyword
keyword
Search
ENG
IN
03:12
23-09-2023


Ubuntu 22.04 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Firefox Web Browser
Sep 23 03:13
192.168.195.148:9200/
Discover - Elastic
192.168.195.148:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(columns:!(),filters:!(),index:e74e11c0-5990-11ee-bdf4-d5a547adae66
elastic
Search Elastic
Discover
Options
New
Open
Share
Inspect
Save
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
sysmon-*
Search field names
Filter by type
0
Available fields
31
_id
_index
_score
_type
@timestamp
@version
agent.ephemeral_id
agent.hostname
agent.id
agent.name
agent.type
agent.version
ecs.version
host.architecture
host.hostname
host.id
208,817 hits
Chart options
Sep 23, 2023 @ 02:58:08.892 - Sep 23, 2023 @ 03:13:08.892
Time
Document
Search
ENG
IN
03:13
23-09-2023

PART 4: NETWORK AUTOMATION & CI/CD FOR INFRASTRUCTURE

Continuous Compliance & Auditing:

Implement OpenSCAP or CIS Benchmark scans for security compliance.

Download the compressed XML

```
lokesh@cybercub:~$ wget
https://security-metadata.canonical.com/oval/com.ubuntu.$(lsb_release -cs).usn.oval.xml.bz2
--2025-03-15 15:55:54--
https://security-metadata.canonical.com/oval/com.ubuntu.jammy.usn.oval.xml.bz2
Resolving security-metadata.canonical.com (security-metadata.canonical.com)...
2620:2d:4000:1::28, 2620:2d:4000:1::27, 2620:2d:4000:1::26, ...
Connecting to security-metadata.canonical.com
(security-metadata.canonical.com)|2620:2d:4000:1::28|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 653195 (638K) [application/x-bzip2]
Saving to: ‘com.ubuntu.jammy.usn.oval.xml.bz2’

com.ubuntu.jammy.us 100%[===================>] 637.89K   435KB/s    in 1.5s

2025-03-15 15:56:33 (435 KB/s) - ‘com.ubuntu.jammy.usn.oval.xml.bz2’ saved [653195/653195]
```

Uncompress the data

```
lokesh@cybercub:~$ bunzip2 com.ubuntu.$(lsb_release -cs).usn.oval.xml.bz2
```

To evaluate the OVAL , Install Dependencies

```
lokesh@cybercub:~$ sudo apt install libopenscap8
[sudo] password for lokesh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  libopenscap8
0 upgraded, 1 newly installed, 0 to remove and 54 not upgraded.
Need to get 2,189 kB of archives.
```

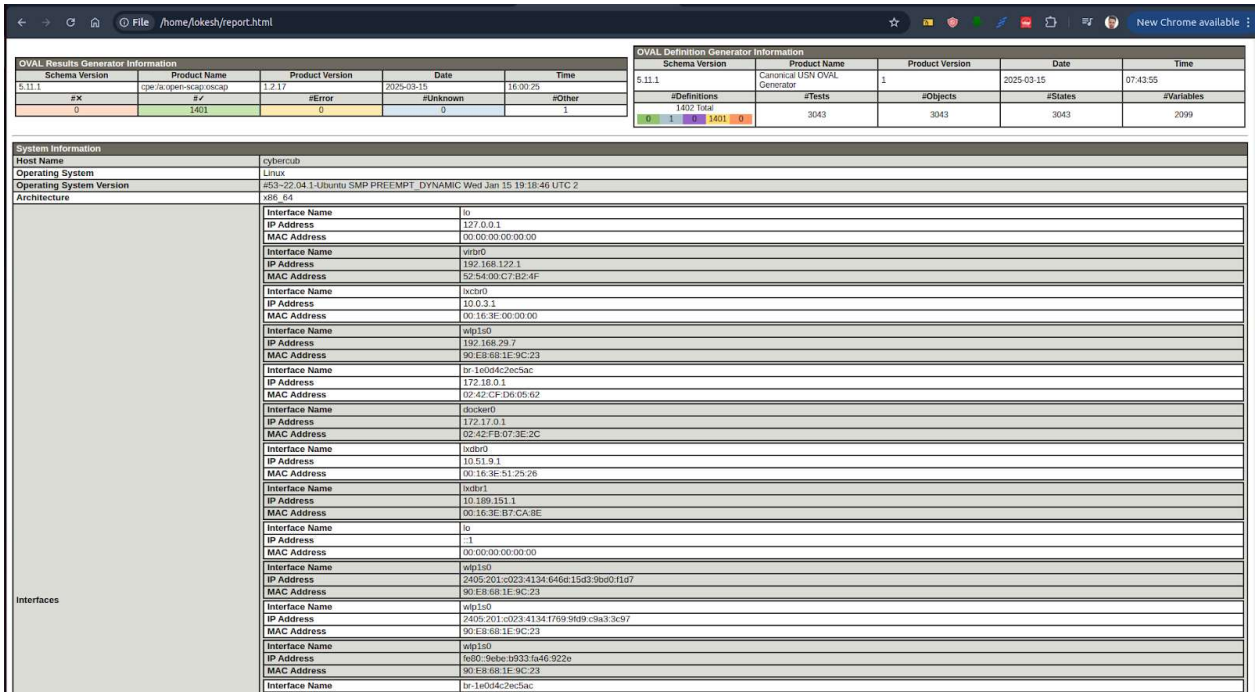
After this operation, 66.0 MB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libopenscap8 amd64 1.2.17-0.1ubuntu7.22.04.2 [2,189 kB]
Fetched 2,189 kB in 6s (379 kB/s)
Selecting previously unselected package libopenscap8.
(Reading database ... 245543 files and directories currently installed.)
Preparing to unpack .../libopenscap8_1.2.17-0.1ubuntu7.22.04.2_amd64.deb ...
Unpacking libopenscap8 (1.2.17-0.1ubuntu7.22.04.2) ...
Setting up libopenscap8 (1.2.17-0.1ubuntu7.22.04.2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.9) ...

Use OpenSCAP to evaluate the OVAL and generate an html report:

lokesh@cybercub:~$ oscap oval eval --report report.html com.ubuntu.$(lsb_release -cs).usn.oval.xml
Definition oval:com.ubuntu.jammy:def:991000000: false
Definition oval:com.ubuntu.jammy:def:981000000: false
Definition oval:com.ubuntu.jammy:def:971000000: false
Definition oval:com.ubuntu.jammy:def:961000000: false
Definition oval:com.ubuntu.jammy:def:951000000: false
Definition oval:com.ubuntu.jammy:def:941000000: false
Definition oval:com.ubuntu.jammy:def:931000000: false
Definition oval:com.ubuntu.jammy:def:921000000: false
Definition oval:com.ubuntu.jammy:def:911000000: false
Definition oval:com.ubuntu.jammy:def:901000000: false
Definition oval:com.ubuntu.jammy:def:891000000: false
.
.
.
.
Definition oval:com.ubuntu.jammy:def:100: true
Evaluation done.

```
lokesh@cybercub:~$ ll
total 18856
drwxr-x---+ 23 lokesh lokesh     4096 Mar 15 16:00  ./
drwxr-xr-x.  3 root   root       4096 Jul 27  2024  ../
-rw-------   1 lokesh lokesh    34550 Mar 15 15:02  .bash_history
-rw-r--r--.  1 lokesh lokesh      220 Jul 27  2024  .bash_logout
-rw-r--r--.  1 lokesh lokesh     3881 Nov 11 00:39  .bashrc
drwx------. 21 lokesh lokesh     4096 Feb 12 01:51  .cache/
.
.
.
-rw-rw-r--   1 lokesh lokesh  2480339 Mar 15 16:00  report.html

.
```

OpenScap result of scans for security compliance for my local machine



OVAL Results Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.11.1	cpe:/a:open-scap:oscap	1.2.17	2025-03-15	16:00:25

#x	#✓	#Error	#Unknown	#Other
0	1401	0	0	1

OVAL Definition Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.11.1	Canonical USN OVAL Generator	1	2025-03-15	07:43:55

#Definitions	#Tests	#Objects	#States	#Variables
1402 Total: 0 / 1 / 0 / 1401 / 0	3043	3043	3043	2099

System Information

Host Name	cybercub
Operating System	Linux
Operating System Version	#53~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Wed Jan 15 19:18:46 UTC 2
Architecture	x86_64

Interfaces

Interface Name	lo
IP Address	127.0.0.1
MAC Address	00:00:00:00:00:00
Interface Name	virbr0
IP Address	192.168.122.1
MAC Address	52:54:00:C7:B2:4F
Interface Name	lxcbr0
IP Address	10.0.3.1
MAC Address	00:16:3E:00:00:00
Interface Name	wlp1s0
IP Address	192.168.29.7
MAC Address	90:E8:68:1E:9C:23
Interface Name	br-1e0d4c2ec5ac
IP Address	172.18.0.1
MAC Address	02:42:CF:D6:05:62
Interface Name	docker0
IP Address	172.17.0.1
MAC Address	02:42:FB:07:3E:2C
Interface Name	lxdbr0
IP Address	10.51.9.1
MAC Address	00:16:3E:51:25:26
Interface Name	lxdbr1
IP Address	10.189.151.1
MAC Address	00:16:3E:B7:CA:8E
Interface Name	lo
IP Address	::1
MAC Address	00:00:00:00:00:00
Interface Name	wlp1s0
IP Address	2405:201:c023:4134:646d:15d3:9bd0:f1d7
MAC Address	90:E8:68:1E:9C:23
Interface Name	wlp1s0
IP Address	2405:201:c023:4134:f769:9fd9:c9a3:3c97
MAC Address	90:E8:68:1E:9C:23
Interface Name	wlp1s0
IP Address	fe80::9ebe:b933:fa46:922e
MAC Address	90:E8:68:1E:9C:23
Interface Name	br-1e0d4c2ec5ac

OVAL Definition Results

Error | Unknown | Other

ID	Result	Class	Reference ID	Title
oval:com.ubuntu.jammy:def:100	true	inventory		Check that Ubuntu 22.04 LTS (jammy) is installed.
oval:com.ubuntu.jammy:def:991000000	false	patch	[LSN-0099-1], [CVE-2023-42752], [CVE-2023-3777], [CVE-2023-3609], [CVE-2023-42753], [CVE-2023-4623], [CVE-2023-3567], [CVE-2023-40283], [CVE-2023-5197], [CVE-2023-3776], [CVE-2023-4622], [CVE-2023-4004], [CVE-2023-34319], [CVE-2022-3643], [CVE-2023-31436]	LSN-0099-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:981000000	false	patch	[LSN-0098-1], [CVE-2023-3776], [CVE-2023-3609], [CVE-2023-21400], [CVE-2023-4004], [CVE-2023-3777], [CVE-2023-40283], [CVE-2023-3090], [CVE-2023-3567]	LSN-0098-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:971000000	false	patch	[LSN-0097-1], [CVE-2023-31248], [CVE-2023-32629], [CVE-2023-3090], [CVE-2023-3390], [CVE-2023-35788], [CVE-2023-35001], [CVE-2023-3389]	LSN-0097-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:961000000	false	patch	[LSN-0096-1], [CVE-2023-31436], [CVE-2023-35001], [CVE-2023-30456], [CVE-2023-31248], [CVE-2023-1380]	LSN-0096-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:951000000	false	patch	[LSN-0095-1], [CVE-2023-32233], [CVE-2023-2612], [CVE-2023-0386], [CVE-2023-1872], [CVE-2023-1380], [CVE-2023-31436]	LSN-0095-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:941000000	false	patch	[LSN-0094-1], [CVE-2023-1281], [CVE-2023-0468]	LSN-0094-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:931000000	false	patch	[LSN-0093-1], [CVE-2023-0461], [CVE-2023-0179]	LSN-0093-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:921000000	false	patch	[LSN-0092-1], [CVE-2022-42896], [CVE-2022-4378], [CVE-2022-43945]	LSN-0092-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:911000000	false	patch	[LSN-0091-1], [CVE-2022-42719], [CVE-2022-41222]	LSN-0091-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:901000000	false	patch	[LSN-0090-1], [CVE-2022-42720], [CVE-2022-1015], [CVE-2022-41674], [CVE-2022-42722], [CVE-2022-2602], [CVE-2022-42721]	LSN-0090-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:891000000	false	patch	[LSN-0089-1], [CVE-2022-2588], [CVE-2022-2585], [CVE-2022-29581], [CVE-2022-2588], [CVE-2022-34918], [CVE-2022-21499]	LSN-0089-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:871000000	false	patch	[LSN-0087-1]	LSN-0087-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:861000000	false	patch	[LSN-0086-1], [CVE-2022-1055], [CVE-2022-0492], [CVE-2022-30594], [CVE-2022-1116], [CVE-2022-21499], [CVE-2021-39713], [CVE-2022-29581]	LSN-0086-1 -- Kernel Live Patch Security Notice
oval:com.ubuntu.jammy:def:73511000000	false	patch	[USN-7351-1], [CVE-2020-10688], [CVE-2020-1695], [CVE-2020-25633], [CVE-2021-20289], [CVE-2023-0482], [CVE-2024-9622]	USN-7351-1 -- RESTEasy vulnerabilities
oval:com.ubuntu.jammy:def:73501000000	false	patch	[USN-7350-1], [CVE-2022-30333], [CVE-2022-48579], [CVE-2023-40477], [CVE-2024-33899]	USN-7350-1 -- UnRAR vulnerabilities
oval:com.ubuntu.jammy:def:73491000000	false	patch	[USN-7349-1], [CVE-2022-30333], [CVE-2023-40477]	USN-7349-1 -- RAR vulnerabilities
oval:com.ubuntu.jammy:def:73471000000	false	patch	[USN-7347-1], [CVE-2024-38439], [CVE-2024-38440], [CVE-2024-38441]	USN-7347-1 -- Netatalk vulnerabilities
oval:com.ubuntu.jammy:def:73461000000	false	patch	[USN-7346-1], [CVE-2021-42780], [CVE-2021-42782], [CVE-2023-2977], [CVE-2023-40660], [CVE-2023-40661], [CVE-2023-5992], [CVE-2024-45615], [CVE-2024-45616], [CVE-2024-45617], [CVE-2024-45618], [CVE-2024-45619], [CVE-2024-45620], [CVE-2024-8443]	USN-7346-1 -- OpenSC vulnerabilities
oval:com.ubuntu.jammy:def:73451000000	false	patch	[USN-7345-1], [CVE-2025-24070]	USN-7345-1 -- .NET vulnerability
oval:com.ubuntu.jammy:def:73431000000	false	patch	[USN-7343-1], [CVE-2024-56201], [CVE-2024-56326], [CVE-2025-27516]	USN-7343-1 -- Jinja2 vulnerabilities
oval:com.ubuntu.jammy:def:73371000000	false	patch	[USN-7337-1], [CVE-2025-1080]	USN-7337-1 -- LibreOffice vulnerability
oval:com.ubuntu.jammy:def:73361000000	false	patch	[USN-7336-1], [CVE-2021-30184]	USN-7336-1 -- GNU Chess vulnerability
oval:com.ubuntu.jammy:def:73351000000	false	patch	[USN-7335-1], [CVE-2025-26699]	USN-7335-1 -- Django vulnerability
oval:com.ubuntu.jammy:def:73291000000	false	patch	[USN-7329-1], [CVE-2024-50274], [CVE-2024-53064], [CVE-2024-56672], [CVE-2025-0927]	USN-7329-1 -- Linux kernel vulnerabilities
oval:com.ubuntu.jammy:def:73283000000	false	patch	[USN-7328-3], [CVE-2024-56672], [CVE-2025-0927]	USN-7328-3 -- Linux kernel vulnerabilities
oval:com.ubuntu.jammy:def:73282000000	false	patch	[USN-7328-2], [CVE-2024-56672], [CVE-2025-0927]	USN-7328-2 -- Linux kernel vulnerabilities

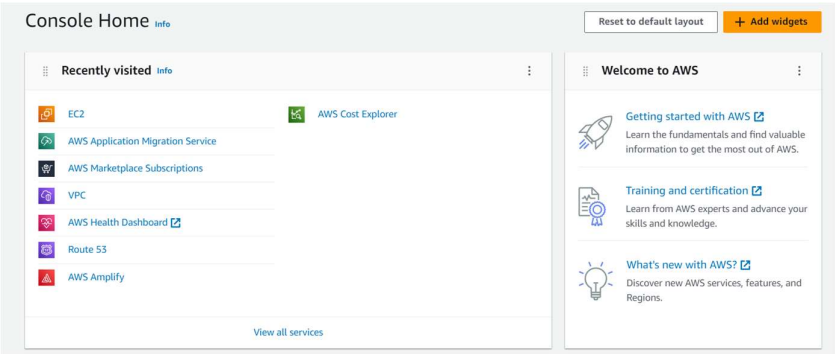
PART 5: ENTERPRISE-GRADE BACKUP & DATA PROTECTION

Data Encryption & Access Control:

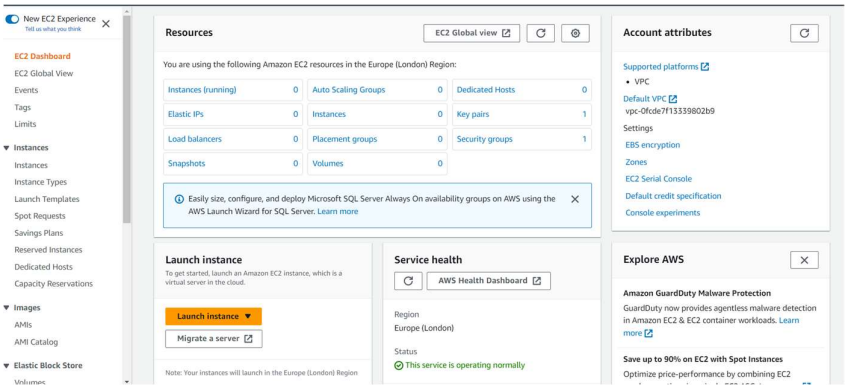
Implement **Zero Trust Security Model (ZTNA) for remote access**.

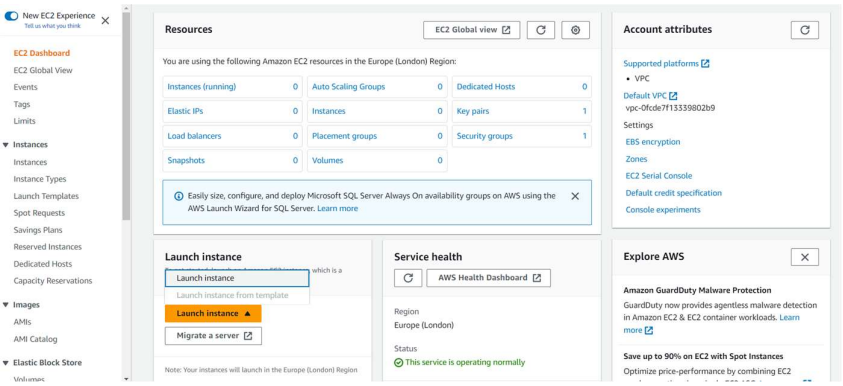
Implemented a **Zero Trust Security Model (ZTNA)** for remote access using **OpenVPN** deployed on an **Amazon EC2 instance**. The setup enforces a "**Never Trust, Always Verify**" policy, ensuring strict authentication and authorization for every access request. Additionally, for enhanced security, **key pairs** are enabled to establish secure and verified remote connections.

Click on EC2

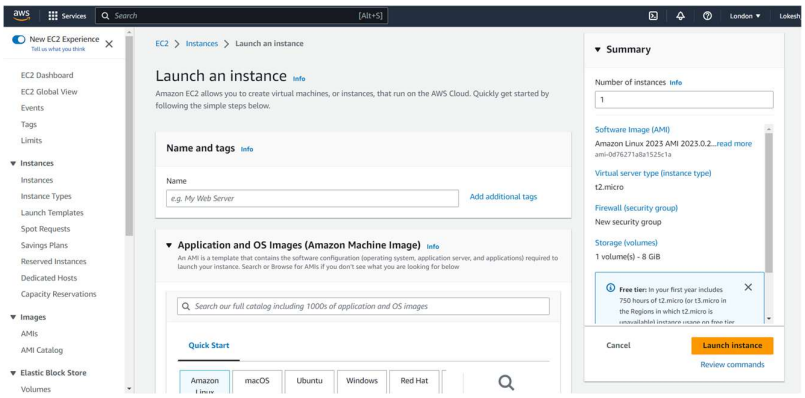


Go to EC2 -> Lauch Instance

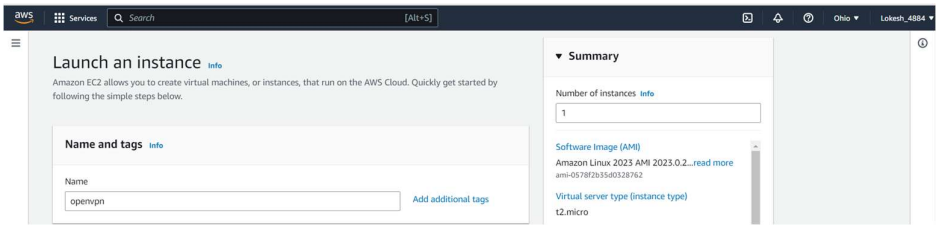




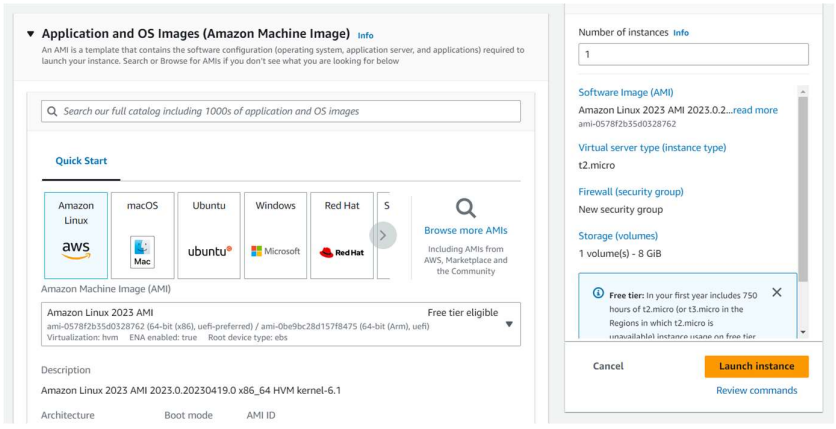
Launch the instance



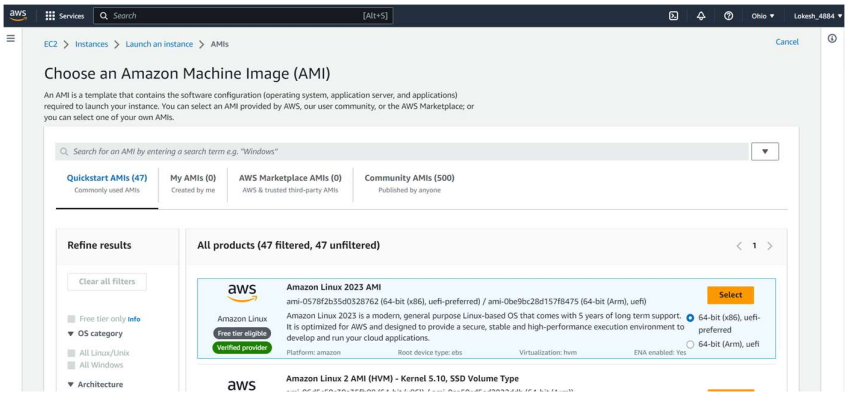
Set name for launch instance :



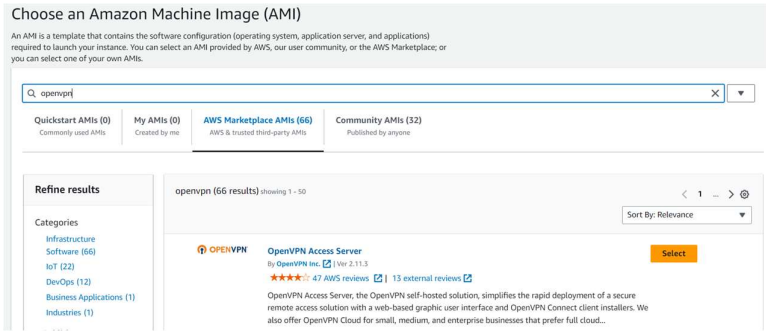
Click on Browse more AMIs



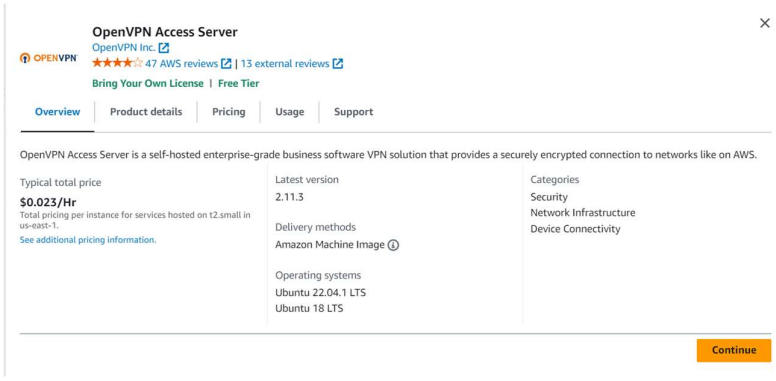
After clicking AMIs

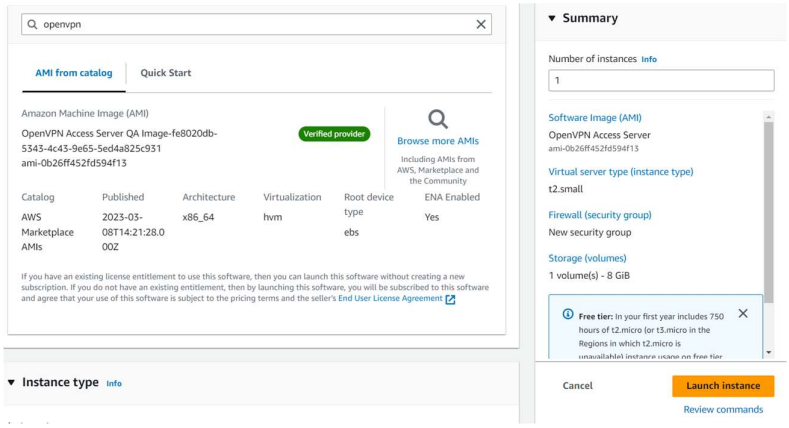


Go to AMIS Marketplace and search for openvpn

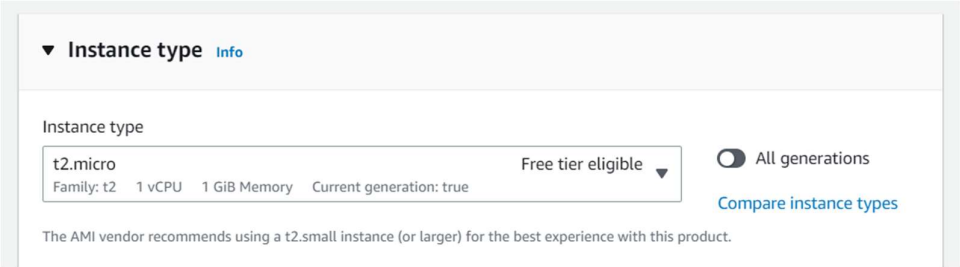


Click on continue

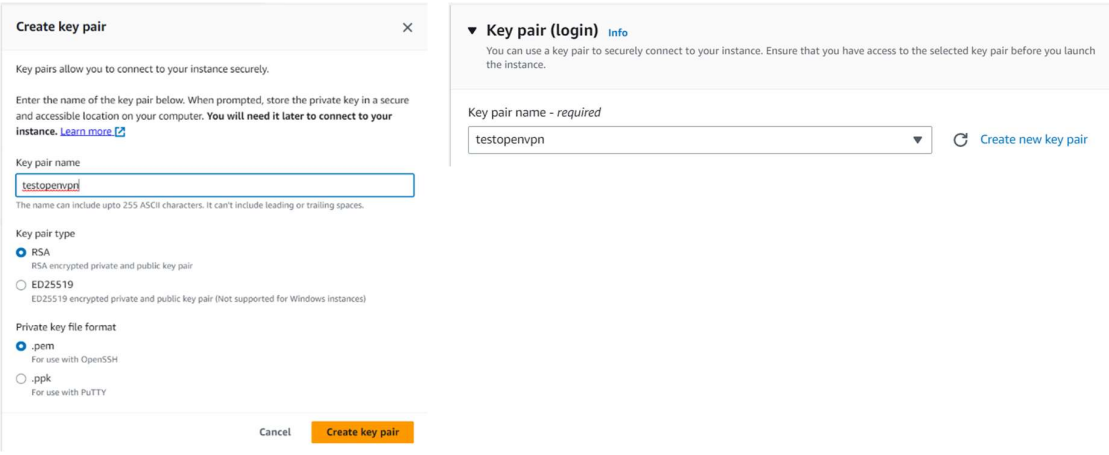




Select free tier Instance type as t2.micro

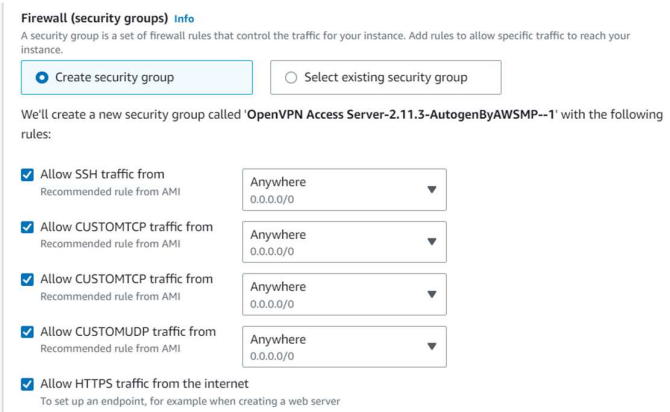


Create a new Key pair using RSA for OpenSSH then choose .pem file and click on create key pair

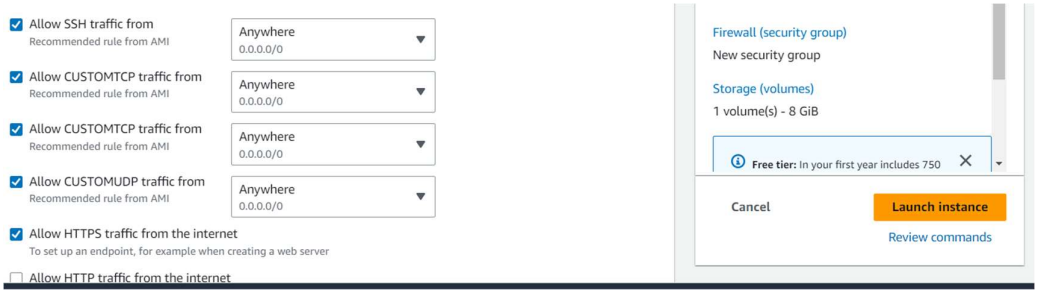


Allow SSH traffic , CUSTOMTCP traffic, CUSTOMUDP, HTTPS traffic from the internet

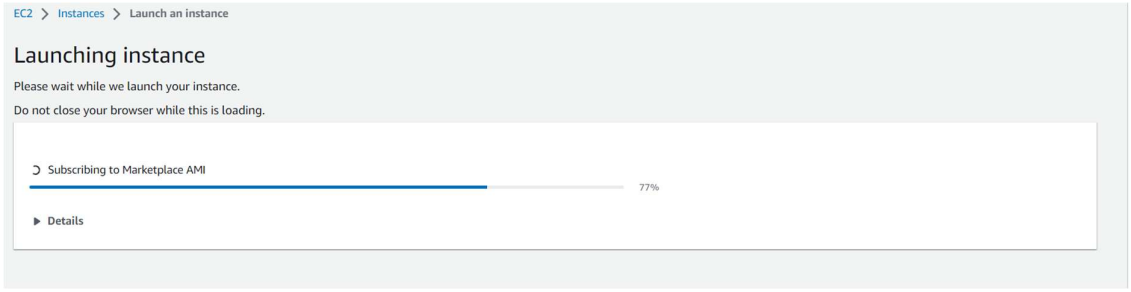
0.0.0.0/0 **means "anywhere on the internet."**



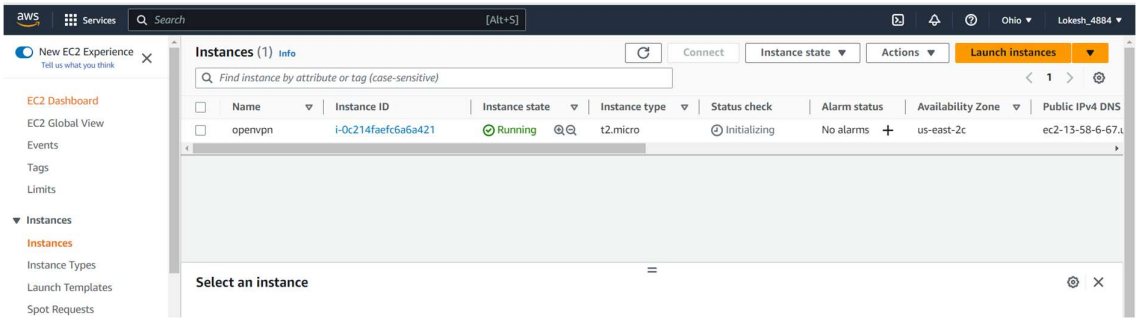
Click on Launch Instance :



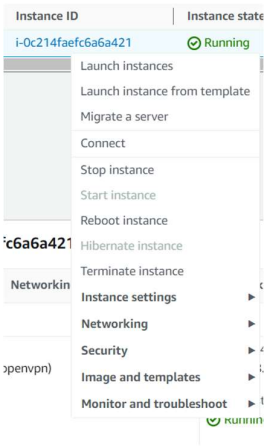
It takes some time



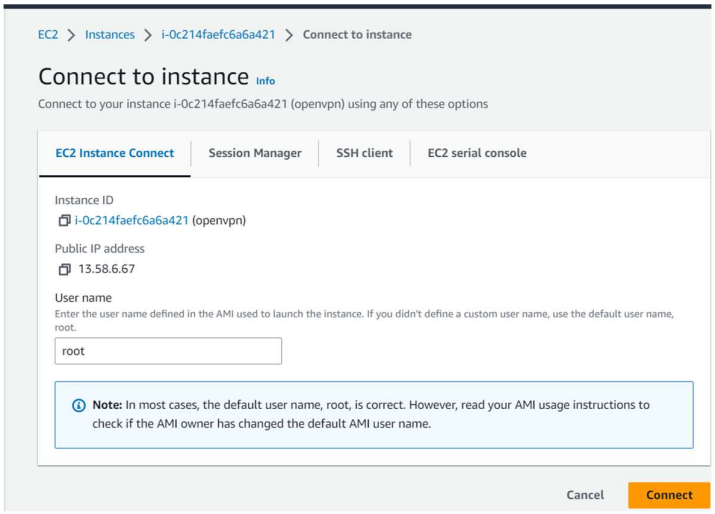
Go to Instances -> Instances



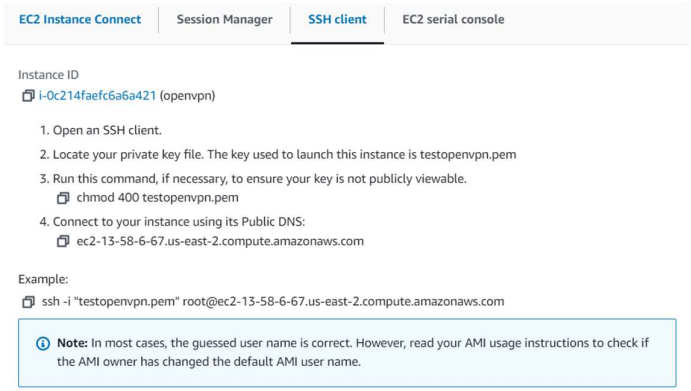
Right Click on Instance ID



Click on Connect



Go to SSH client

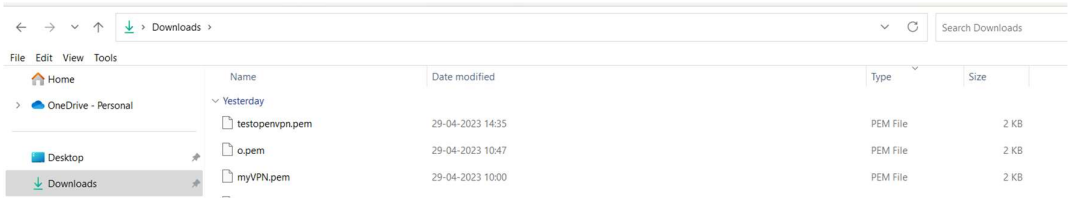


Copy example

Example:

ssh -i "testopenvpn.pem" root@ec2-13-58-6-67.us-east-2.compute.amazonaws.com

Copy that Command and paste it on Command Prompt (only where testopenvpn file is existed) :



Open Command prompt in download location and Execute that command :

```
Microsoft Windows [Version 10.0.22621.1555]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP\Downloads>ssh -i "testopenvpn.pem" root@ec2-13-58-6-67.us-east-2.compute.amazonaws.com
The authenticity of host 'ec2-13-58-6-67.us-east-2.compute.amazonaws.com (13.58.6.67)' can't be established.
ED25519 key fingerprint is SHA256:nSjMdM2e3VNsU0AL+r87ITw72U4FIwtNSi12Ll7YHMA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-58-6-67.us-east-2.compute.amazonaws.com' (ED25519) to the list of known hosts.
Please login as the user "openvpnas" rather than the user "root".

Connection to ec2-13-58-6-67.us-east-2.compute.amazonaws.com closed.
```

It asks to use as openvpnas as User than root so it refuses

Use Same Command replace root as openvpnas :

Example:

ssh -i "testopenvpn.pem" root@ec2-13-58-6-67.us-east-2.compute.amazonaws.com

Instead root we use openvpnas(from the command)

```
C:\Users\HP\Downloads>ssh -i "testopenvpn.pem" openvpnas@ec2-13-58-6-67.us-east-2.compute.amazonaws.com
Welcome to OpenVPN Access Server Appliance 2.11.3

  System information as of Sun Apr 30 12:34:50 UTC 2023

  System load:  0.0               Processes:             98
  Usage of /:   38.6% of 7.57GB   Users logged in:       0
  Memory usage: 27%               IPv4 address for eth0: 172.31.40.195
  Swap usage:   0%

53 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable


*** System restart required ***
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.


         OpenVPN Access Server
         Initial Configuration Tool
------------------------------------------------------
```

```
OpenVPN Access Server End User License Agreement (OpenVPN-AS EULA)

    1. Copyright Notice: OpenVPN Access Server License;
       Copyright (c) 2009-2022 OpenVPN Inc. All rights reserved.
       "OpenVPN" is a trademark of OpenVPN Inc.
    2. Redistribution of OpenVPN Access Server binary forms and related documents,
       are permitted provided that redistributions of OpenVPN Access Server binary
       forms and related documents reproduce the above copyright notice as well as
       a complete copy of this EULA.
    3. You agree not to reverse engineer, decompile, disassemble, modify,
       translate, make any attempt to discover the source code of this software,
       or create derivative works from this software.
    4. The OpenVPN Access Server is bundled with other open source software
       components, some of which fall under different licenses. By using OpenVPN
       or any of the bundled components, you agree to be bound by the conditions
       of the license for each respective component. For more information, you can
       find our complete EULA (End-User License Agreement) on our website
       (http://openvpn.net), and a copy of the EULA is also distributed with the
       Access Server in the file /usr/local/openvpn_as/license.txt.
```

Like that it shows all User License Agreement

Just go with all default option

```
Please enter 'yes' to indicate your agreement [no]: yes

Once you provide a few initial configuration settings,
OpenVPN Access Server can be configured by accessing
its Admin Web UI using your Web browser.

Will this be the primary Access Server node?
(enter 'no' to configure as a backup or standby node)
> Press ENTER for default [yes]: yes

Please specify the network interface and IP address to be
used by the Admin Web UI:
(1) all interfaces: 0.0.0.0
(2) eth0: 172.31.40.195
Please enter the option number from the list above (1- 2).
> Press Enter for default [1]:
```

```
What public/private type/algorithms do you want to use for the OpenVPN CA?

Recommended choices:

rsa       - maximum compatibility
secp384r1 - elliptic curve, higher security than rsa, allows faster connection setup and smaller user profile files
showall   - shows all options including non-recommended algorithms.
> Press ENTER for default [rsa]:

What key size do you want to use for the certificates?
Key size should be between 2048 and 4096

> Press ENTER for default [ 2048 ]:

What public/private type/algorithms do you want to use for the self-signed web certificate?

Recommended choices:

rsa       - maximum compatibility
secp384r1 - elliptic curve, higher security than rsa, allows faster connection setup and smaller user profile files
showall   - shows all options including non-recommended algorithms.
> Press ENTER for default [rsa]:

What key size do you want to use for the certificates?
Key size should be between 2048 and 4096
```

```
> Press ENTER for default [ 2048 ]:

Please specify the port number for the Admin Web UI.
> Press ENTER for default [943]:

Please specify the TCP port number for the OpenVPN Daemon
> Press ENTER for default [443]:

Should client traffic be routed by default through the VPN?
> Press ENTER for default [no]:

Should client DNS traffic be routed by default through the VPN?
> Press ENTER for default [no]:
Admin user authentication will be  local

Private subnets detected: ['172.31.0.0/16']

Should private subnets be accessible to clients by default?
> Press ENTER for EC2 default [yes]:
```

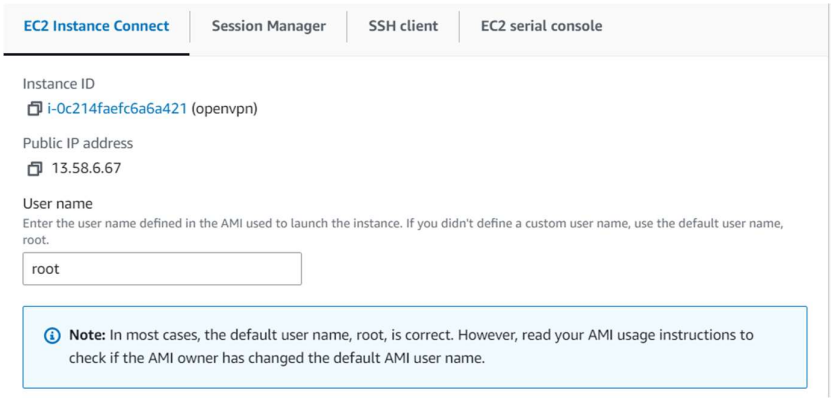
You can give password manually or otherwise just give enter it assigns a default password

```
To initially login to the Admin Web UI, you must use a
username and password that successfully authenticates you
with the host UNIX system (you can later modify the settings
so that RADIUS or LDAP is used for authentication instead).

You can login to the Admin Web UI as "openvpn" or specify
a different user account to use for this purpose.

Do you wish to login to the Admin UI as "openvpn"?
> Press ENTER for default [yes]:
Type a password for the 'openvpn' account (if left blank, a random password will be generated):
Please, remember this password Scq4qRvFYlgM

> Please specify your Activation key (or leave blank to specify later):
```

```
Initializing OpenVPN...
Removing Cluster Admin user login...
userdel "admin_c"
Writing as configuration file...
Perform sa init...
Wiping any previous userdb...
Creating default profile...
Modifying default profile...
Adding new user to userdb...
Modifying new user as superuser in userdb...
Auto-generated pass = "Scq4qRvFYlgM". Setting in db...
Getting hostname...
Hostname: 13.58.6.67
Preparing web certificates...
Getting web user account...
Adding web group account...
Adding web group...
Adjusting license directory ownership...
Initializing confdb...
Initial version is not set. Setting it to 2.11.3...
Generating PAM config for openvpnas ...
Enabling service
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service → /lib/systemd/system/openvpnas.service.
Starting openvpnas...

NOTE: Your system clock must be correct for OpenVPN Access Server
to perform correctly.  Please ensure that your time and date
are correct on this system.
```

```
Initial Configuration Complete!

You can now continue configuring OpenVPN Access Server by
directing your Web browser to this URL:

https://13.58.6.67:943/admin

During normal operation, OpenVPN AS can be accessed via these URLs:
Admin  UI: https://13.58.6.67:943/admin
Client UI: https://13.58.6.67:943/
To login please use the "openvpn" account with "Scq4qRvFYlgM" password.

See the Release Notes for this release at:
   https://openvpn.net/vpn-server-resources/release-notes/
```

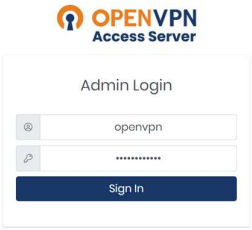
Go to EC2 Instance Connect Copy Public IP address :



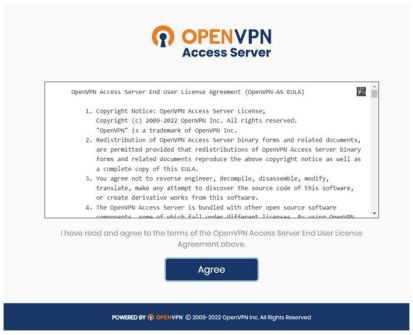
Search : https://13.58.6.67:943/admin/

Just proceed for action and you will get a login page :

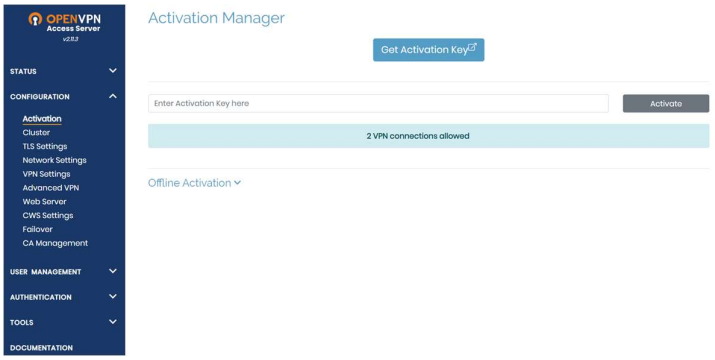
Enter user name as openvpn which you have given in making a instance in AWS and next give password which was created in command prompt



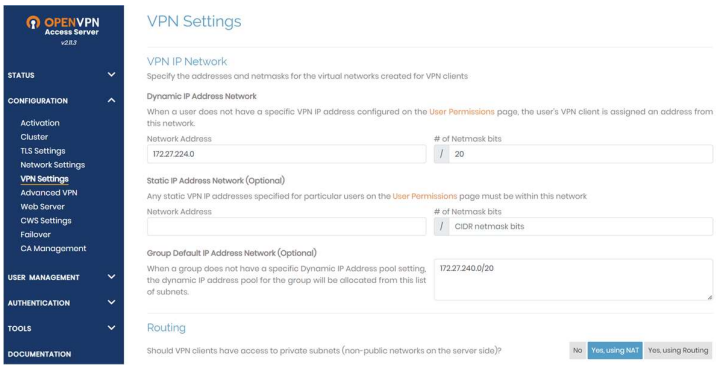
Next you will get this page press on Agree



You will get this page



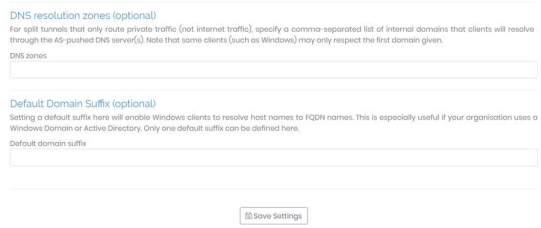
Go to VPN settings



By default in VPN settings

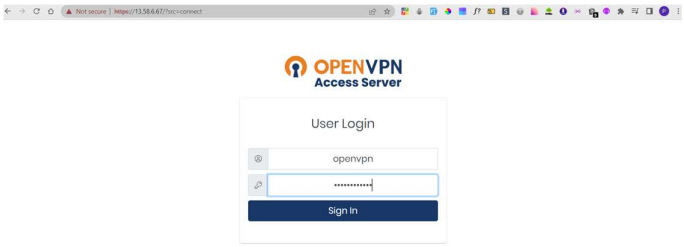
Enable client Internet traffic be routed through VPN?

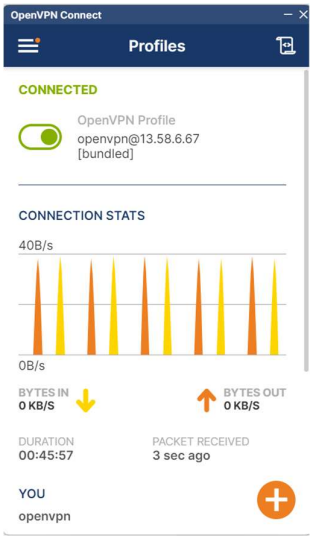
Click on Save Settings



Search in chrome: https://13.58.6.67/

Implement **Zero Trust Security Model (ZTNA) for remote access**, credentials which you gave in creating Instance in AWS as openvpn and enter password (which you gave in command prompt) this OpenVPN always follow ZTNA – Never Trust Always Verify poilicy





PART 6

Zeek (formerly Bro) - Network Security Monitoring Tool

- **Network Traffic Analysis –** Zeek monitors and logs network activity for security analysis.
- **Deep Packet Inspection –** Extracts detailed metadata from network packets.
- **Flexible Scripting –** Uses Zeek scripting language for custom security policies.
- **Protocol Detection –** Supports HTTP, DNS, SSL/TLS, and many more.
- **Security Event Detection** – Identifies anomalies, intrusions, and threats.
- **Log Generation –** Creates structured logs for further analysis in SIEMs.
- **Open Source & Scalable –** Used in large-scale network monitoring setups.

The `apt-get update` command updates the local package index by fetching the latest package lists from the repositories. This ensures the system is aware of available updates but does not install them.

```
root@agent:/home/lokesh# apt-get update
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
.
.
```

The apt-get upgrade command installs the latest versions of all installed packages without removing any existing ones. It updates only those packages that do not require dependency changes.

```
root@agent:/home/lokesh# apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
.
.
```

Downloading zeek-7.0.5.tar.gz zip file from zeek official website

```
root@agent:/home/lokesh# wget https://download.zeek.org/zeek-7.0.5.tar.gz
```

```
--2025-02-28 07:44:33--  https://download.zeek.org/zeek-7.0.5.tar.gz
Resolving download.zeek.org (download.zeek.org)... 52.84.45.124, 52.84.45.34, 52.84.45.68, ...
Connecting to download.zeek.org (download.zeek.org)|52.84.45.124|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 95847393 (91M) [application/x-gzip]
Saving to: ‘zeek-7.0.5.tar.gz’

zeek-7.0.5.tar.gz
100%[=============================================================================
==========================================>]  91.41M  3.79MB/s    in 25s


root@agent:/home/lokesh# ls
wazuh-agent_4.9.2-1_amd64.deb  zeek-7.0.5.tar.gz
```

use the following commands to add zeek repository into binary packages.

```
root@agent:/home/lokesh# apt-get install cmake make gcc g++ flex bison libpcap-dev libssl-dev
python3-dev swig zlib1g-dev -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done

Extract zeek-7.0.5.tar.gz
root@agent:/home/lokesh# tar -xzf zeek-7.0.5.tar.gz
root@agent:/home/lokesh# ls
wazuh-agent_4.9.2-1_amd64.deb  zeek-7.0.5  zeek-7.0.5.tar.gz

Go to zeek-7.0.5
root@agent:/home/lokesh# cd zeek-7.0.5
root@agent:/home/lokesh/zeek-7.0.5# ls
CHANGES           Makefile   auxil          doc            src
CMakeLists.txt    NEWS       ci             docker         testing
COPYING           README     cmake          man            vcpkg.json
COPYING-3rdparty  README.md  cmake_templates  repo-info.json  zeek-path-dev.in
INSTALL           VERSION    configure      scripts
```

The `./configure` command checks system dependencies and prepares the build environment for compiling Zeek 7.0.5.

```
root@agent:/home/lokesh/zeek-7.0.5# ./configure
```

.
.
-- Configuring done
-- Generating done
-- Build files have been written to: /home/lokesh/zeek-7.0.5/build

The command make install compiles and installs Zeek 7.0.5 from source in the /home/lokesh/zeek-7.0.5 directory on the agent system.

root@agent:/home/lokesh/zeek-7.0.5# make install
.
.
-- Installing: /usr/local/zeek/share/zeek/cmake/ZeekConfigVersion.cmake
-- Installing: /usr/local/zeek/share/zeek/cmake/ZeekTargets.cmake
make[1]: Leaving directory '/home/lokesh/zeek-7.0.5/build'

The command `make` compiles the Zeek 7.0.5 source code in the `/home/lokesh/zeek-7.0.5` directory on the `agent` system.

root@agent:/home/lokesh/zeek-7.0.5# make
.
.

[100%] Built target rst
make[2]: Leaving directory '/home/lokesh/zeek-7.0.5/build'
make[1]: Leaving directory '/home/lokesh/zeek-7.0.5/build'
root@agent:/home/lokesh/zeek-7.0.5#

Go to /usr/local/zeek/

root@agent:/home/lokesh/zeek-7.0.5# cd /usr/local/zeek/
root@agent:/usr/local/zeek# ls
bin etc include lib logs share spool var
root@agent:/usr/local/zeek# cd bin

root@agent:/usr/local/zeek/bin#

Edit the Bash configuration file for the current user.

root@agent:/usr/local/zeek/bin# nano ~/.bashrc
.
.
export PATH=/usr/local/zeek/bin:$PATH #Add this line at last

The command source ~/.bashrc reloads the .bashrc file without needing to restart the shell. This applies any changes made, such as new aliases, environment variables, or custom configurations, immediately.

root@agent:/usr/local/zeek/bin# source ~/.bashrc

Check whether zeek is deployed

root@agent:/usr/local/zeek/bin# zeek --version
zeek version 7.0.5

Check where zeek installed

root@agent:/usr/local/zeek/bin# which zeek
/usr/local/zeek/bin/zeek
root@agent:/usr/local/zeek/bin# cd ..
root@agent:/usr/local/zeek# cd etc
root@agent:/usr/local/zeek/etc#

root@agent:/usr/local/zeek/etc# ls
networks.cfg node.cfg zeekctl.cfg zkg

Edit node.cfg make sure to use standalone , localhost , ethernet of local machine where zeek is hosting

root@agent:/usr/local/zeek/etc# nano node.cfg
[zeek]
type=standalone
host=localhost
interface=eth0

```
root@agent:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
17: eth0@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:09:fc:b3 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.189.151.4/24 metric 100 brd 10.189.151.255 scope global dynamic eth0
       valid_lft 3147sec preferred_lft 3147sec
    inet6 fd42:71c6:d70c:1045:216:3eff:fe09:fcb3/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::216:3eff:fe09:fcb3/64 scope link
       valid_lft forever preferred_lft forever
```

root@agent:/usr/local/zeek/etc# zeekctl check
Hint: Run the zeekctl "deploy" command to get started.
zeek scripts are ok.

root@agent:/usr/local/zeek/spool# apt-get install mailutils -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done

Deploy zeek

root@agent:/usr/local/zeek/etc# zeekctl deploy
checking configurations ...
installing ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /usr/local/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...

```
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
starting ...
starting zeek ...
root@agent:/usr/local/zeek/etc# zeekctl status
Name         Type       Host          Status    Pid    Started
zeek         standalone localhost     running   29477  28 Feb 11:17:04
```

Go to logs that captured by zeek

```
root@agent:/usr/local/zeek/etc# cd ..
root@agent:/usr/local/zeek# ls
bin  etc  include  lib  logs  share  spool  var
root@agent:/usr/local/zeek# cd logs/
root@agent:/usr/local/zeek/logs# ls
2025-02-28  current

root@agent:/usr/local/zeek/logs# cd current
```

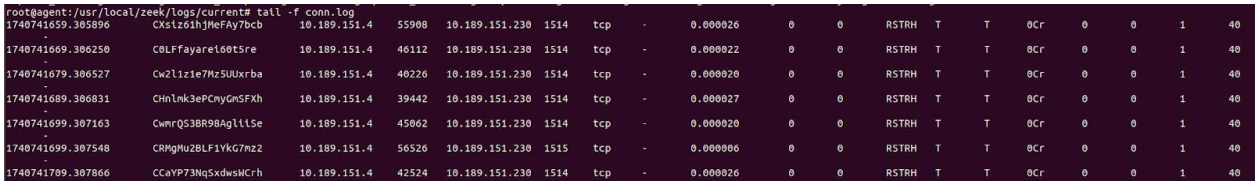
These all are different logs that generated by zeek

```
root@agent:/usr/local/zeek/logs/current# ls
capture_loss.log  conn.log  loaded_scripts.log  notice.log  packet_filter.log  reporter.log  stats.log
stderr.log  stdout.log  telemetry.log  weird.log
```

Printing to the screen conn.log

In Zeek, conn.log is a foundational log file that tracks network connections, providing information about the source and destination hosts, ports, protocols, and connection state, allowing for analysis of network traffic and detection of unusual activity.

```
root@agent:/usr/local/zeek/logs/current# tail -f conn.log
```



I have changed logs format to json

root@agent:/usr/local/zeek/logs/current# tail -f conn.log
{"ts":1740954863.250134,"uid":"CyCGXM2n791ANkwBSl","id_orig_h":"fd42:71c6:d70c:1045::1","id_orig_p":5353,"id_resp_h":"ff02::fb","id_resp_p":5353,"proto":"udp","conn_state":"OTH","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"C","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1740954863.250256,"uid":"CUMjeL2eDwRrHbKBa","id_orig_h":"10.189.151.1","id_orig_p":5353,"id_resp_h":"224.0.0.251","id_resp_p":5353,"proto":"udp","conn_state":"OTH","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"C","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1740954872.461894,"uid":"CdVgF23kGRzguGp0v8","id_orig_h":"10.189.151.4","id_orig_p":68,"id_resp_h":"10.189.151.1","id_resp_p":67,"proto":"udp","conn_state":"OTH","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"C","orig_pkts":0,"orig_ip_bytes":0,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}
{"ts":1740954863.254029,"uid":"CskYGd2bMnUrvMrQ4l","id_orig_h":"fe80::216:3eff:feb7:ca8e","id_orig_p":143,"id_resp_h":"ff02::16","id_resp_p":0,"proto":"icmp","duration":0.27585291862487793,"orig_bytes":40,"resp_bytes":0,"conn_state":"OTH","local_orig":true,"local_resp":false,"missed_bytes":0,"orig_pkts":2,"orig_ip_bytes":152,"resp_pkts":0,"resp_ip_bytes":0,"ids_malicious":"zeek_conn"}