Virtual Private Cloud (VPC) designed for running production-grade server infrastructure

Project Overview: Highly Available and Secure VPC Architecture

This project demonstrates how to create a Virtual Private Cloud (VPC) designed for running production-grade server infrastructure on AWS.

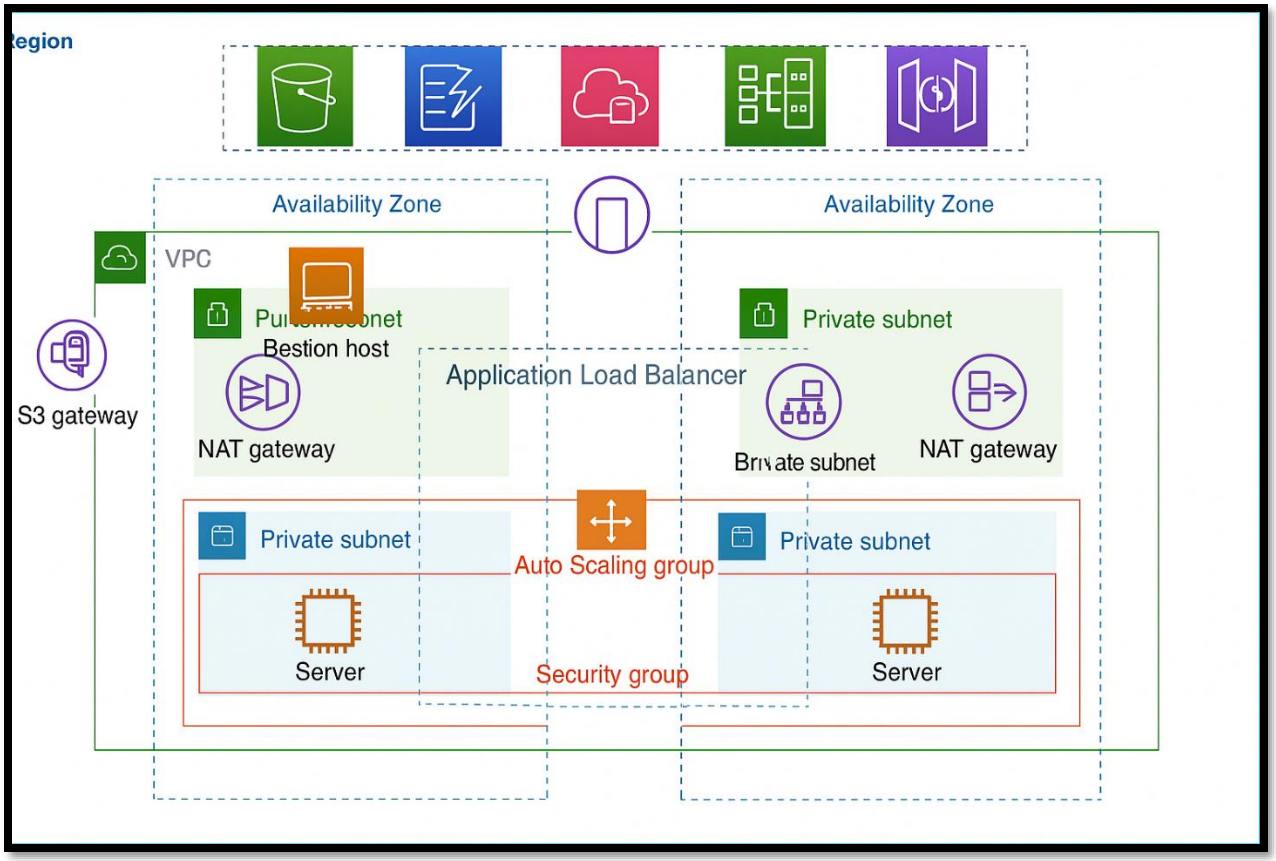
Key Features:

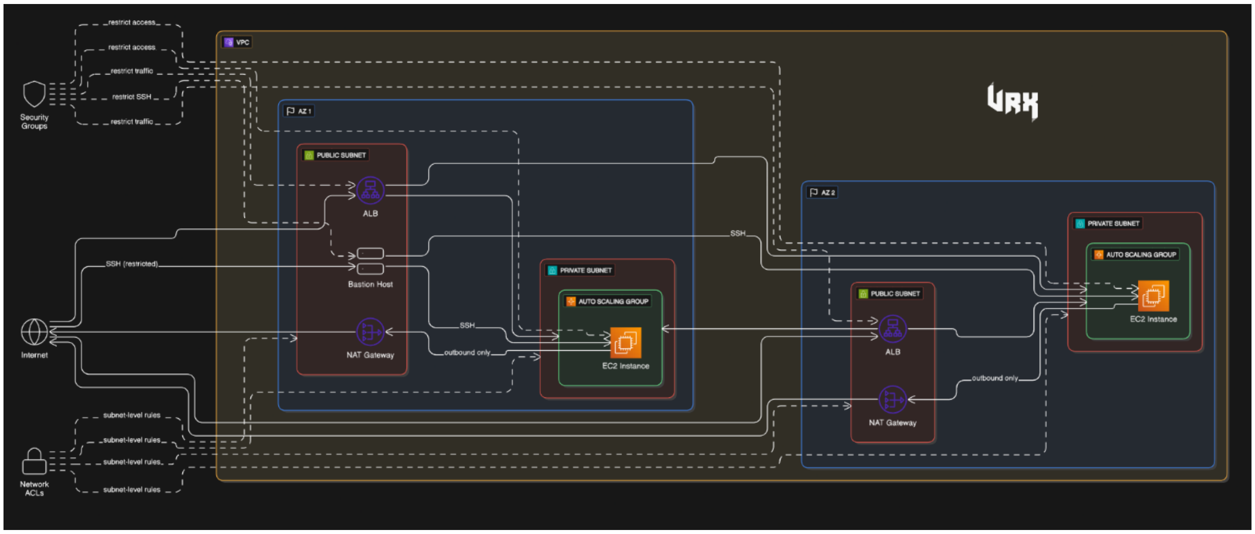
- **High Availability:** The architecture spans **two Availability Zones (AZs)** to ensure fault tolerance and improved uptime.
- **Public and Private Subnets:** Each AZ contains both public and private subnets:
  - **Public Subnets:** Host the **Application Load Balancer (ALB)** and **NAT Gateways**.
  - **Private Subnets:** Host **EC2 instances** launched via an **Auto Scaling Group (ASG)**.
- **Load Balancing:** The **ALB** routes incoming internet traffic to the EC2 instances running in private subnets.
- **Auto Scaling:** The **ASG** manages EC2 instance provisioning and termination based on demand.
- **Internet Access for Private Instances:** Private instances access the internet via **NAT Gateways**, one in each public subnet for improved resilience.
- **Security:** Private subnets isolate backend servers from direct internet exposure, enhancing security.

Architecture Summary:

- A VPC with public and private subnets across two Availability Zones.
- Public subnets contain a load balancer and NAT gateway in each AZ.
- Private subnets host application servers managed by an Auto Scaling Group.
- Servers handle traffic forwarded from the Application Load Balancer.
- NAT gateways enable secure internet access for servers in private subnets

- **Public Subnets:**
  - Application Load Balancer
  - NAT Gateway
  - Bastion Host for SSH access
- **Private Subnets:**
  - EC2 instances (Auto Scaling Group-managed)
  - No direct internet access; NAT Gateway used for outbound traffic
- Load balancer forwards external requests to backend servers in private subnets.
- Bastion Host provides secure jump access to private EC2s using SSH (restricted by IP and key-based authentication)

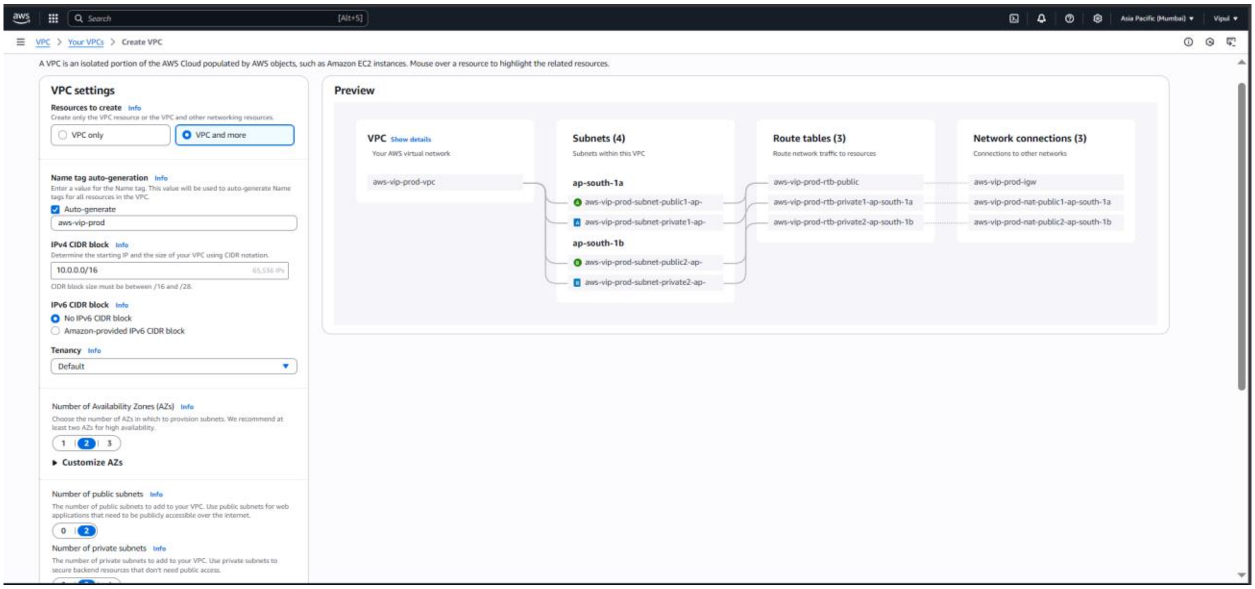




Architecture

Steps:

1. Creating the VPC with 2 public subnet and 2 private subnet in 2 availability zones. With an internet gateway and 2 NAT Gateway.



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

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

○ VPC only ● VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

aws-vip-prod

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

● No IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

Tenancy Info

Default ▾

Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 | [✓ 2] | 3

▶ Customize AZs

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 | [✓ 2]

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

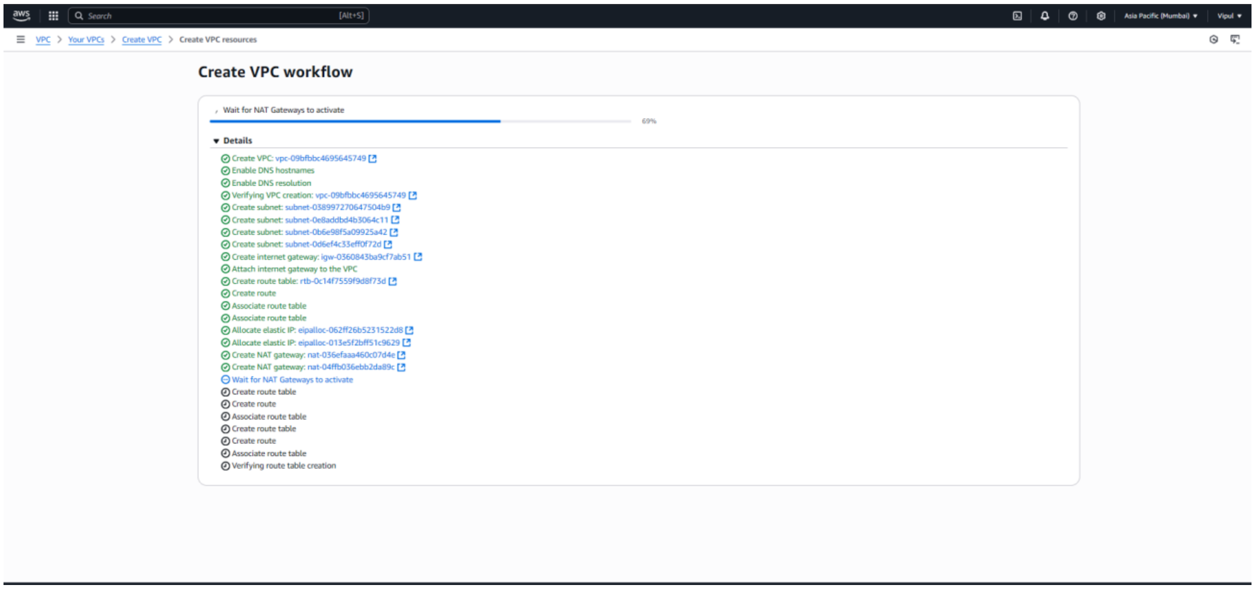
Preview

VPC Show details
Your AWS virtual network
aws-vip-prod-vpc

Subnets (4)
Subnets within this VPC
ap-south-1a
aws-vip-prod-subnet-public1-ap-
aws-vip-prod-subnet-private1-ap-
ap-south-1b
aws-vip-prod-subnet-public2-ap-
aws-vip-prod-subnet-private2-ap-

Route tables (3)
Route network traffic to resources
aws-vip-prod-rtb-public
aws-vip-prod-rtb-private1-ap-south-1a
aws-vip-prod-rtb-private2-ap-south-1b

Network connections (3)
Connections to other networks
aws-vip-prod-igw
aws-vip-prod-nat-public1-ap-south-1a
aws-vip-prod-nat-public2-ap-south-1b

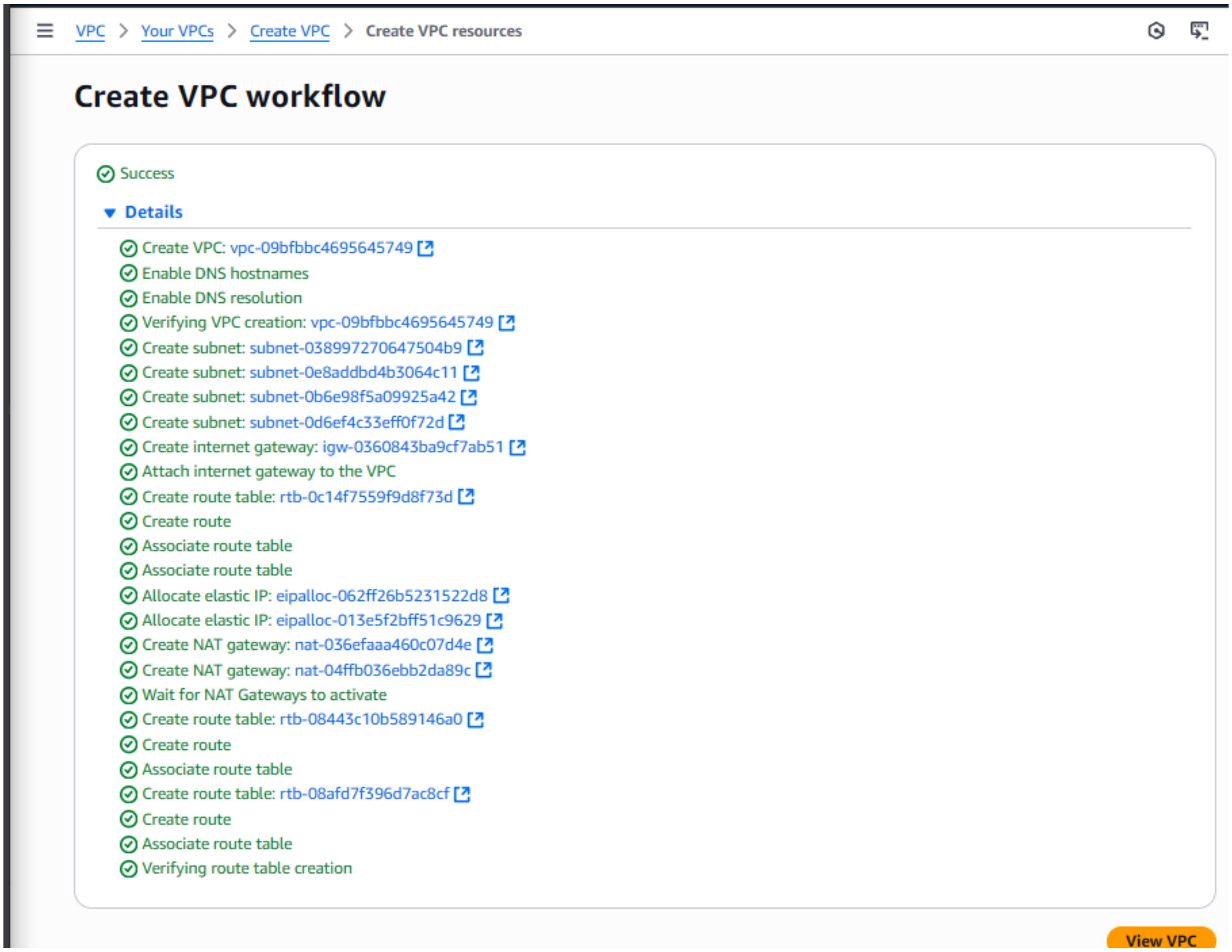


Create VPC workflow

Wait for NAT Gateways to activate 69%

▼ Details

- ✓ Create VPC: vpc-09bfbbc4695645749
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-09bfbbc4695645749
- ✓ Create subnet: subnet-038997270647504b9
- ✓ Create subnet: subnet-0e8addbd4b3064c11
- ✓ Create subnet: subnet-0b6e98f5a09925a42
- ✓ Create subnet: subnet-0d6ef4c33eff0f72d
- ✓ Create internet gateway: igw-0360843ba9cf7ab51
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-0c14f7559f9d8f73d
- ✓ Create route
- ✓ Associate route table
- ✓ Associate route table
- ✓ Allocate elastic IP: eipalloc-062ff26b5231522d8
- ✓ Allocate elastic IP: eipalloc-013e5f2bff51c9629
- ✓ Create NAT gateway: nat-036efaaa460c07d4e
- ✓ Create NAT gateway: nat-04ffb036ebb2da89c
- ⊖ Wait for NAT Gateways to activate
- ◷ Create route table
- ◷ Create route
- ◷ Associate route table
- ◷ Create route table
- ◷ Create route
- ◷ Associate route table
- ◷ Verifying route table creation



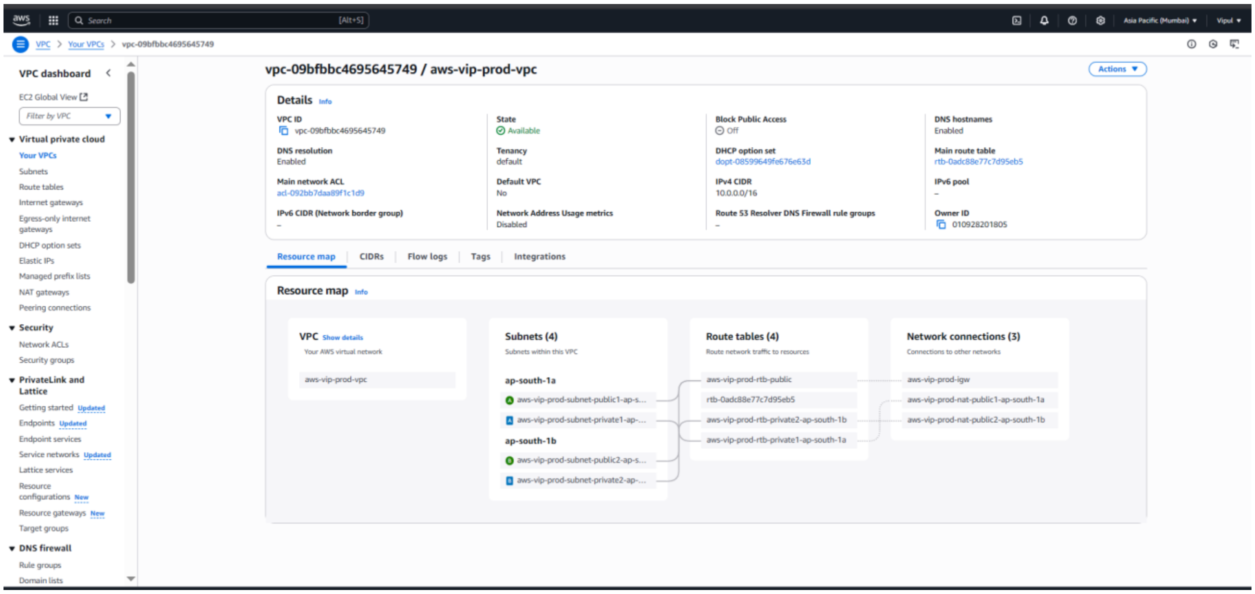
Create VPC workflow

Success

Details

- Create VPC: vpc-09bfbbc4695645749
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: vpc-09bfbbc4695645749
- Create subnet: subnet-038997270647504b9
- Create subnet: subnet-0e8addbd4b3064c11
- Create subnet: subnet-0b6e98f5a09925a42
- Create subnet: subnet-0d6ef4c33eff0f72d
- Create internet gateway: igw-0360843ba9cf7ab51
- Attach internet gateway to the VPC
- Create route table: rtb-0c14f7559f9d8f73d
- Create route
- Associate route table
- Associate route table
- Allocate elastic IP: eipalloc-062ff26b5231522d8
- Allocate elastic IP: eipalloc-013e5f2bff51c9629
- Create NAT gateway: nat-036efaaa460c07d4e
- Create NAT gateway: nat-04ffb036ebb2da89c
- Wait for NAT Gateways to activate
- Create route table: rtb-08443c10b589146a0
- Create route
- Associate route table
- Create route table: rtb-08afd7f396d7ac8cf
- Create route
- Associate route table
- Verifying route table creation

VPC Created Successfully.



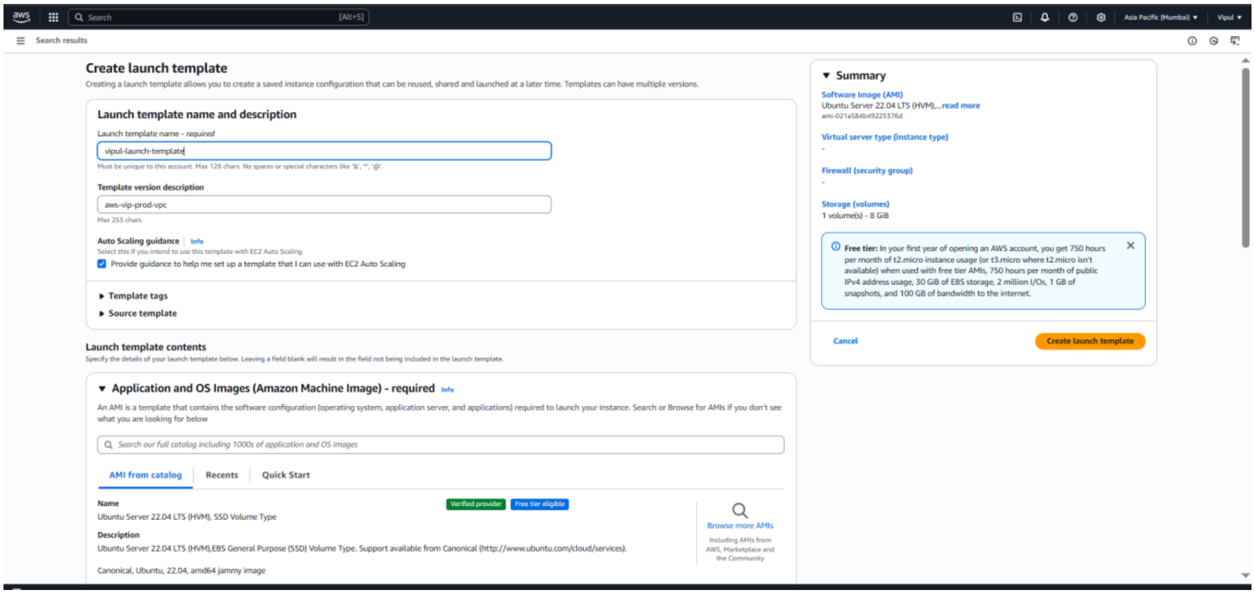
vpc-09bfbbc4695645749 / aws-vip-prod-vpc

Details Info

VPC ID vpc-09bfbbc4695645749	State Available	Block Public Access Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-08599649fe676e63d	Main route table rtb-0adc88e77c7d95eb5
Main network ACL acl-092bb7daa89f1c1d9	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –
IPv6 CIDR (Network border group) –	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 010928201805

Resource map
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Your AWS virtual network
aws-vip-prod-vpc
Subnets (4)
Subnets within this VPC
ap-south-1a
aws-vip-prod-subnet-public1-ap-s...
aws-vip-prod-subnet-private1-ap-...
ap-south-1b
aws-vip-prod-subnet-public2-ap-s...
aws-vip-prod-subnet-private2-ap-...
Route tables (4)
Route network traffic to resources
aws-vip-prod-rtb-public
rtb-0adc88e77c7d95eb5
aws-vip-prod-rtb-private2-ap-south-1b
aws-vip-prod-rtb-private1-ap-south-1a
Network connections (3)
Connections to other networks
aws-vip-prod-igw
aws-vip-prod-nat-public1-ap-south-1a
aws-vip-prod-nat-public2-ap-south-1b

2. Creating Launch templates for Autoscaling groups.



Search [Alt+S]

Asia Pacific (Mumbai) ▾ | Vipul ▾

Search results

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Launch template name - *required*

vipul-launch-template

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

aws-vip-prod-vpc

Max 255 chars

Auto Scaling guidance | Info

Select this if you intend to use this template with EC2 Auto Scaling

☑ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

▸ Template tags

▸ Source template

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▾ **Application and OS Images (Amazon Machine Image) - required** 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

AMI from catalog | Recents | Quick Start

Name

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

Verified provider | Free tier eligible

Description

Ubuntu Server 22.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Canonical, Ubuntu, 22.04, amd64 jammy image

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

▾ **Summary**

Software Image (AMI)

Ubuntu Server 22.04 LTS (HVM),...read more

ami-021a584b49225376d

Virtual server type (instance type)

-

Firewall (security group)

-

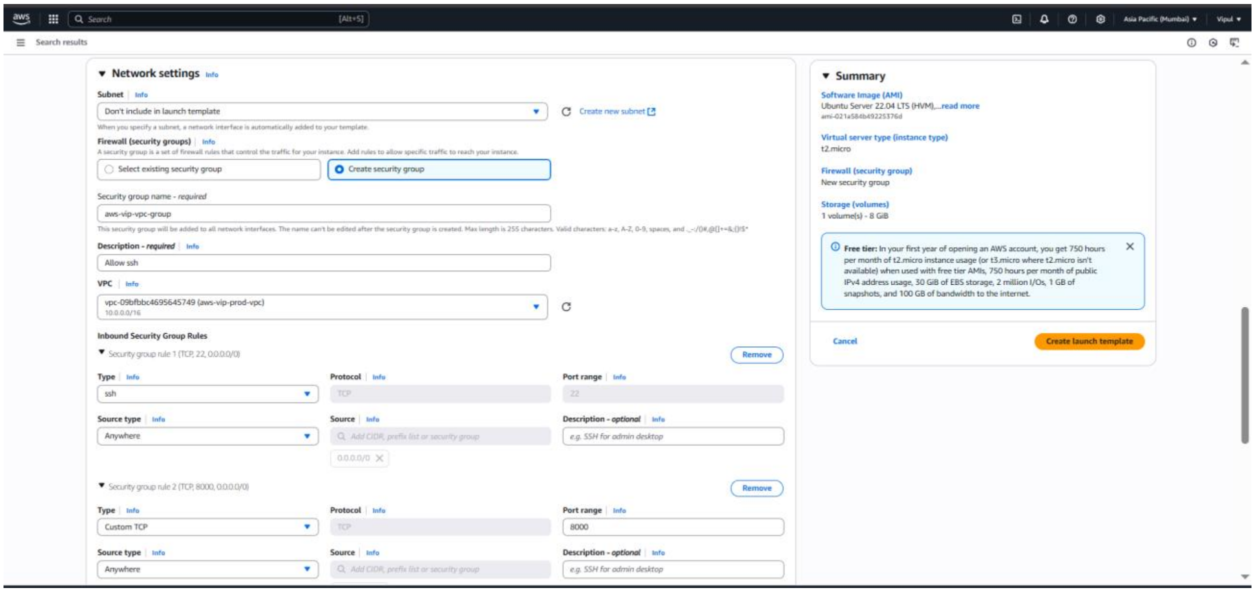
Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel | Create launch template

Select the Created VPC



Search [Alt+S]

Asia Pacific (Mumbai) ▾ | Vipul ▾

Search results

▾ **Network settings** Info

Subnet | Info

Don't include in launch template

Create new subnet

When you specify a subnet, a network interface is automatically added to your template.

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.

○ Select existing security group ● Create security group

Security group name - *required*

aws-vip-vpc-group

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

Allow ssh

VPC | Info

vpc-09bfbbc4695645749 (aws-vip-prod-vpc)
10.0.0.0/16

Inbound Security Group Rules

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

Type | Info	**Protocol** | Info	**Port range** | Info
ssh	TCP	22
Source type | Info	**Source** | Info	**Description - *optional*** | Info
Anywhere	Add CIDR, prefix list or security group 0.0.0.0/0 ✕	e.g. SSH for admin desktop

▾ Security group rule 2 (TCP, 8000, 0.0.0.0/0) Remove

Type | Info	**Protocol** | Info	**Port range** | Info
Custom TCP	TCP	8000
Source type | Info	**Source** | Info	**Description - *optional*** | Info
Anywhere	Add CIDR, prefix list or security group	e.g. SSH for admin desktop

▾ **Summary**

Software Image (AMI)

Ubuntu Server 22.04 LTS (HVM),...read more

ami-021a584b49225376d

Virtual server type (instance type)

t2.micro

Firewall (security group)

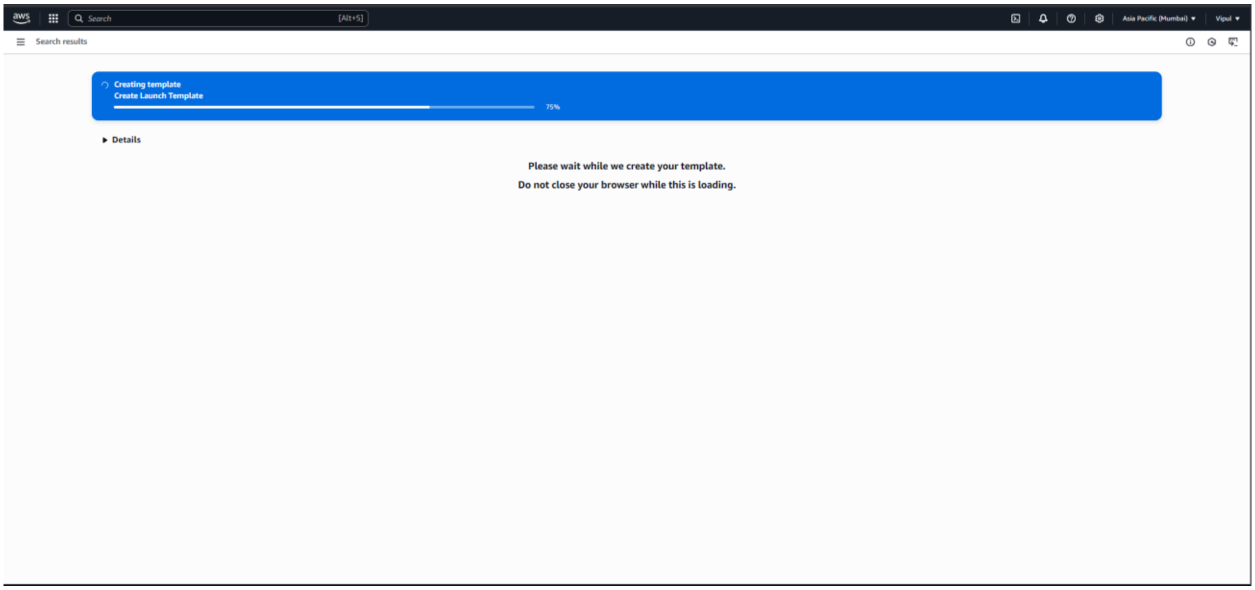
New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel | Create launch template

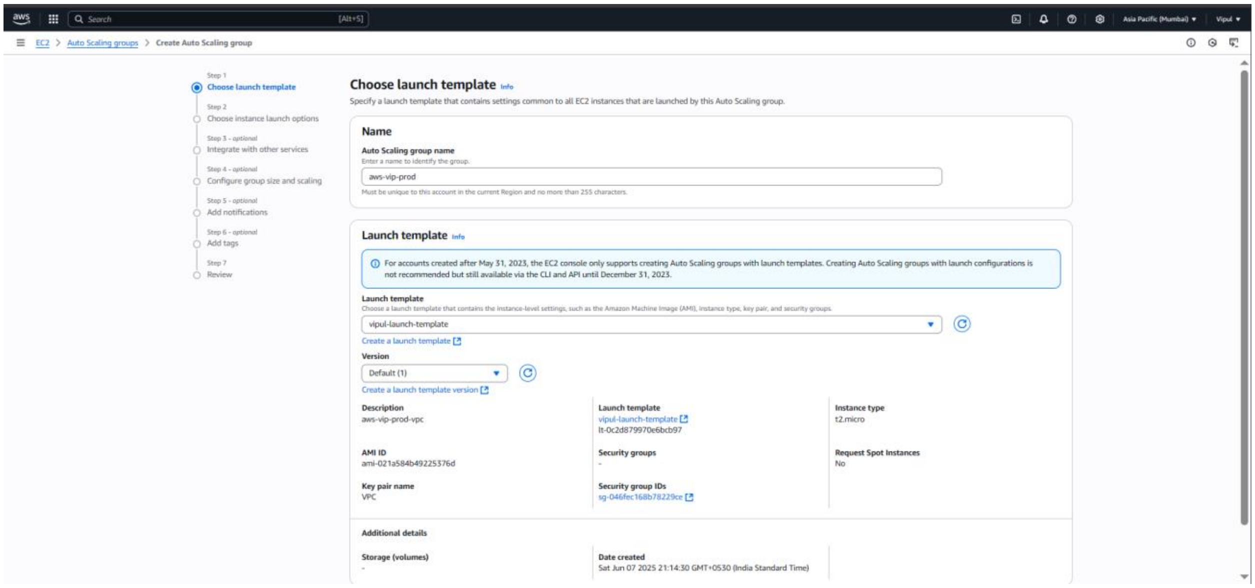


Creating template
Create Launch Template
75%

▸ Details

Please wait while we create your template.
Do not close your browser while this is loading.

After Creating of launch templates use the template in the Auto scaling groups.



Choose launch template

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name
Enter a name to identify the group.
aws-vip-prod
Must be unique to this account in the current Region and no more than 255 characters.

Launch template

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

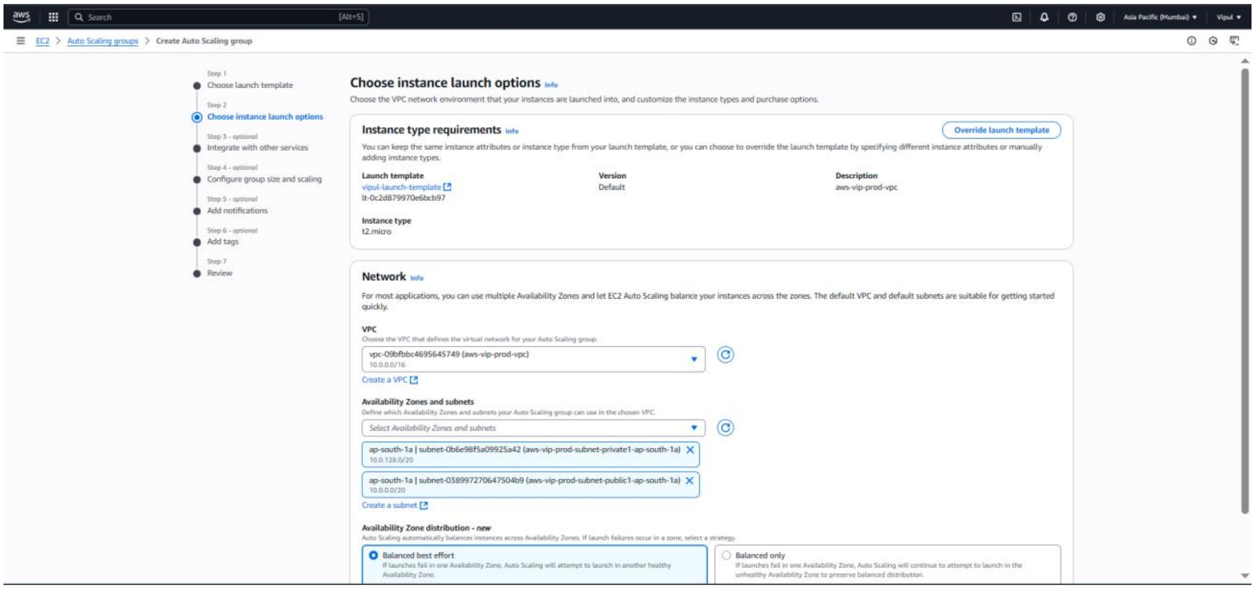
Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.
vipul-launch-template ▾
Create a launch template

Version
Default (1) ▾
Create a launch template version

Description aws-vip-prod-vpc	Launch template vipul-launch-template lt-0c2d879970e6bcb97	Instance type t2.micro
AMI ID ami-021a584b49225376d	Security groups -	Request Spot Instances No
Key pair name VPC	Security group IDs sg-046fec168b78229ce	

Additional details

Storage (volumes) -	Date created Sat Jun 07 2025 21:14:30 GMT+0530 (India Standard Time)



Choose instance launch options

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

Instance type requirements

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Launch template	Version	Description
vipul-launch-template lt-0c2d879970e6bcb97	Default	aws-vip-prod-vpc

Instance type
t2.micro

Network

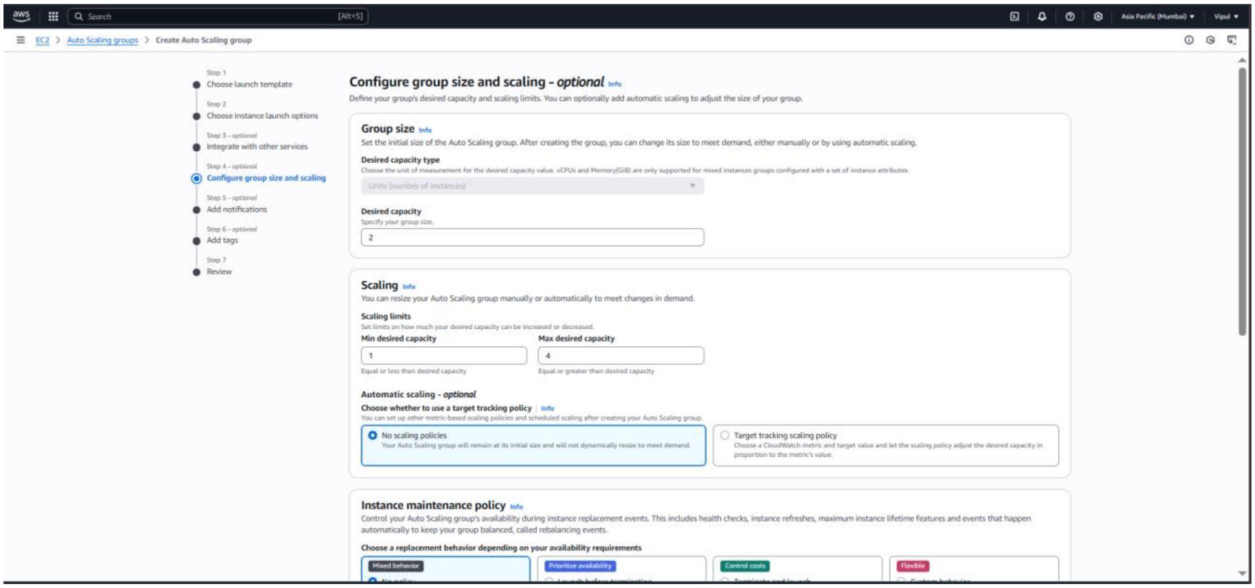
For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.
vpc-09bfbbc4695645749 (aws-vip-prod-vpc) ▾
10.0.0.0/16

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.
Select Availability Zones and subnets ▾
ap-south-1a | subnet-0b6e98f5a09925a42 (aws-vip-prod-subnet-private1-ap-south-1a) ✕
10.0.128.0/20
ap-south-1a | subnet-038997270647504b9 (aws-vip-prod-subnet-public1-ap-south-1a) ✕
10.0.0.0/20

Availability Zone distribution - *new*
Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.
● Balanced best effort
If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.
○ Balanced only
If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

Here select the two zones and private subnets of both the zones as we will be creating the EC2 inside the Private subnets.



Configure group size and scaling - *optional*

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

Group size

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type
Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.
Units (number of instances) ▾

Desired capacity
Specify your group size.
2

Scaling

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits
Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity	Max desired capacity
1	4
Equal or less than desired capacity	Equal or greater than desired capacity

Automatic scaling - *optional*
Choose whether to use a target tracking policy | Info
You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.
● No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.
○ Target tracking scaling policy
Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

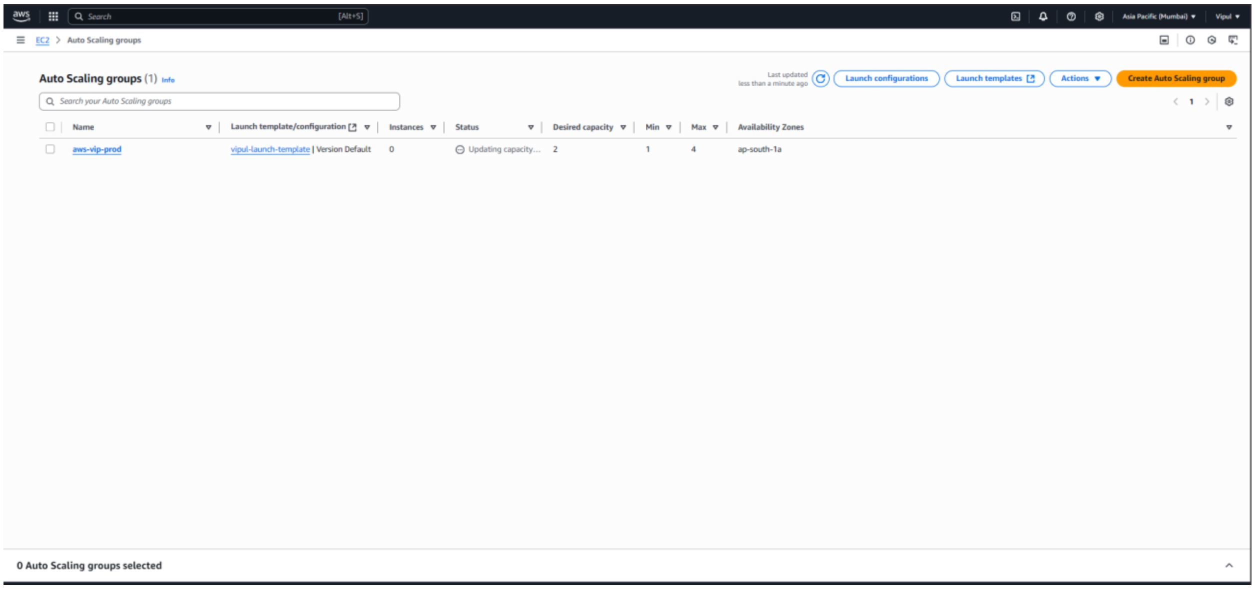
Instance maintenance policy

Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.

Choose a replacement behavior depending on your availability requirements

Mixed behavior | Prioritize availability | Control costs | Flexible

Choose the number upto which it should create the instances.



EC2 > Auto Scaling groups

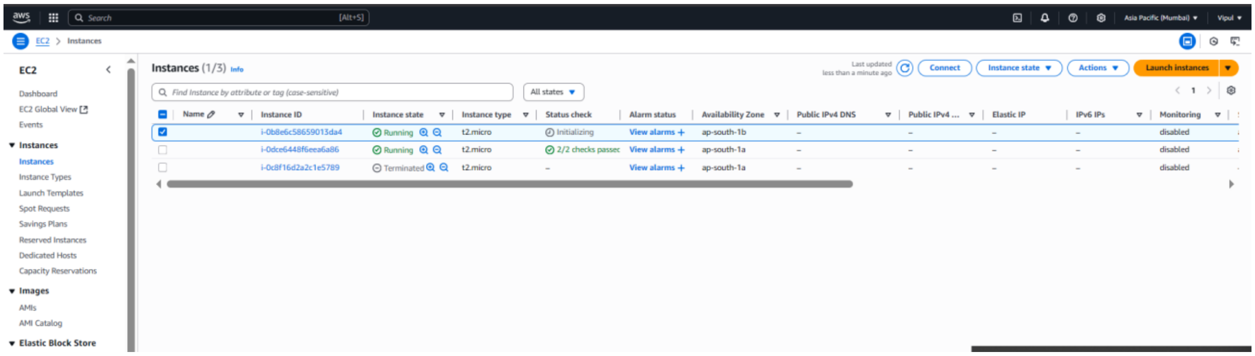
Auto Scaling groups (1) Info

Last updated less than a minute ago

Search your Auto Scaling groups

□	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
□	aws-vip-prod	vipul-launch-template | Version Default	0	Updating capacity...	2	1	4	ap-south-1a

0 Auto Scaling groups selected



EC2 > Instances

Instances (1/3) Info

Last updated less than a minute ago

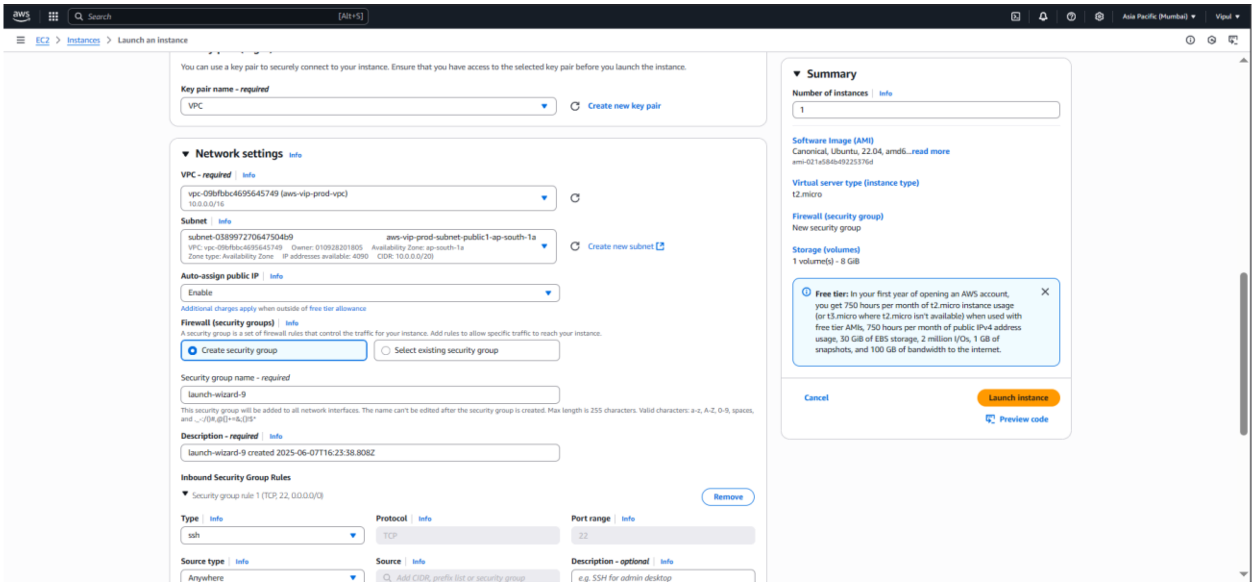
Find Instance by attribute or tag (case-sensitive)

All states

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring
☑		i-0b8e6c58659013da4	Running	t2.micro	Initializing	View alarms +	ap-south-1b	–	–	–	–	disabled
□		i-0dce6448f6eea6a86	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1a	–	–	–	–	disabled
□		i-0c8f16d2a2c1e5789	Terminated	t2.micro	–	View alarms +	ap-south-1a	–	–	–	–	disabled

Here We can see two instances got created without public Ips.

Now creating the bastion host in order to access the Private EC2 instances.



EC2 > Instances > Launch an instance

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*: VPC

▼ Network settings Info

VPC - *required*: vpc-09bfbbc4695645749 (aws-vip-prod-vpc) 10.0.0.0/16

Subnet: subnet-038997270647504b9 aws-vip-prod-subnet-public1-ap-south-1a
VPC: vpc-09bfbbc4695645749 Owner: 010928201805 Availability Zone: ap-south-1a
Zone type: Availability Zone IP addresses available: 4090 CIDR: 10.0.0.0/20)

Auto-assign public IP: Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*: launch-wizard-9

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

Description - *required*: launch-wizard-9 created 2025-06-07T16:23:38.808Z

Inbound Security Group Rules

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

Type: ssh

Protocol: TCP

Port range: 22

Source type: Anywhere

Source: Add CIDR, prefix list or security group

Description - *optional*: e.g. SSH for admin desktop

▼ Summary

Number of instances: 1

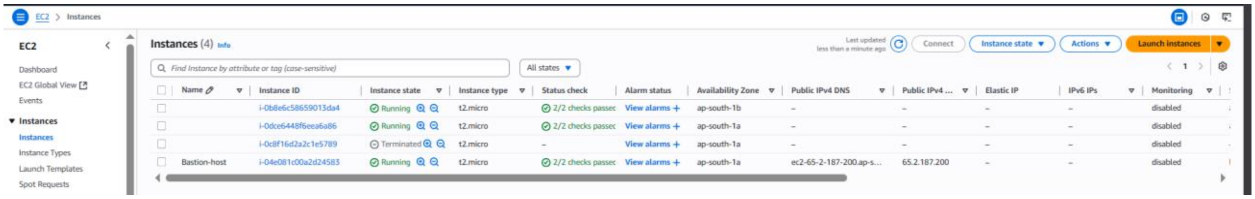
Software Image (AMI)
Canonical, Ubuntu, 22.04, amd6...read more
ami-021a584b49225376d

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

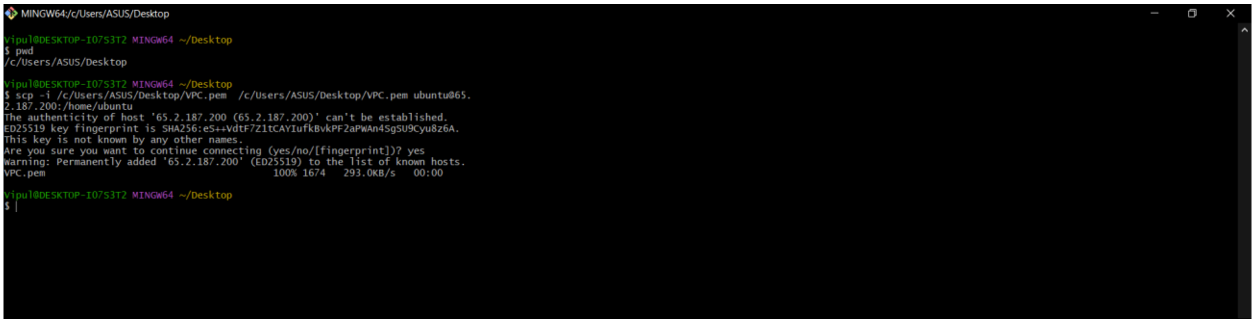
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring
□		i-0b8e6c58659013da4	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1b	–	–	–	–	disabled
□		i-0dce6448f6eea6a86	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1a	–	–	–	–	disabled
□		i-0c8f16d2a2c1e5789	Terminated	t2.micro	–	View alarms +	ap-south-1a	–	–	–	–	disabled
□	Bastion-host	i-04e081c00a2d24583	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1a	ec2-65-2-187-200.ap-s...	65.2.187.200	–	–	disabled

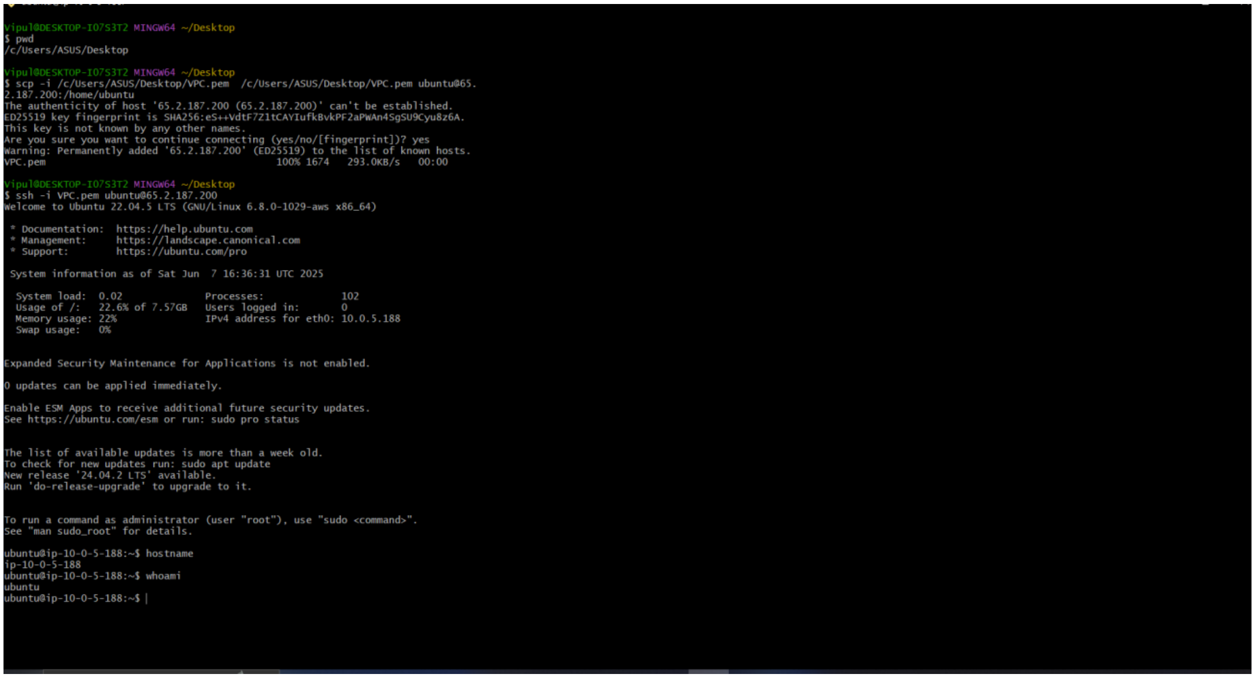
bastion host got created make sure all 3 of them has the same keypair in order to ssh.

Moving pem file to the other 2 hosts

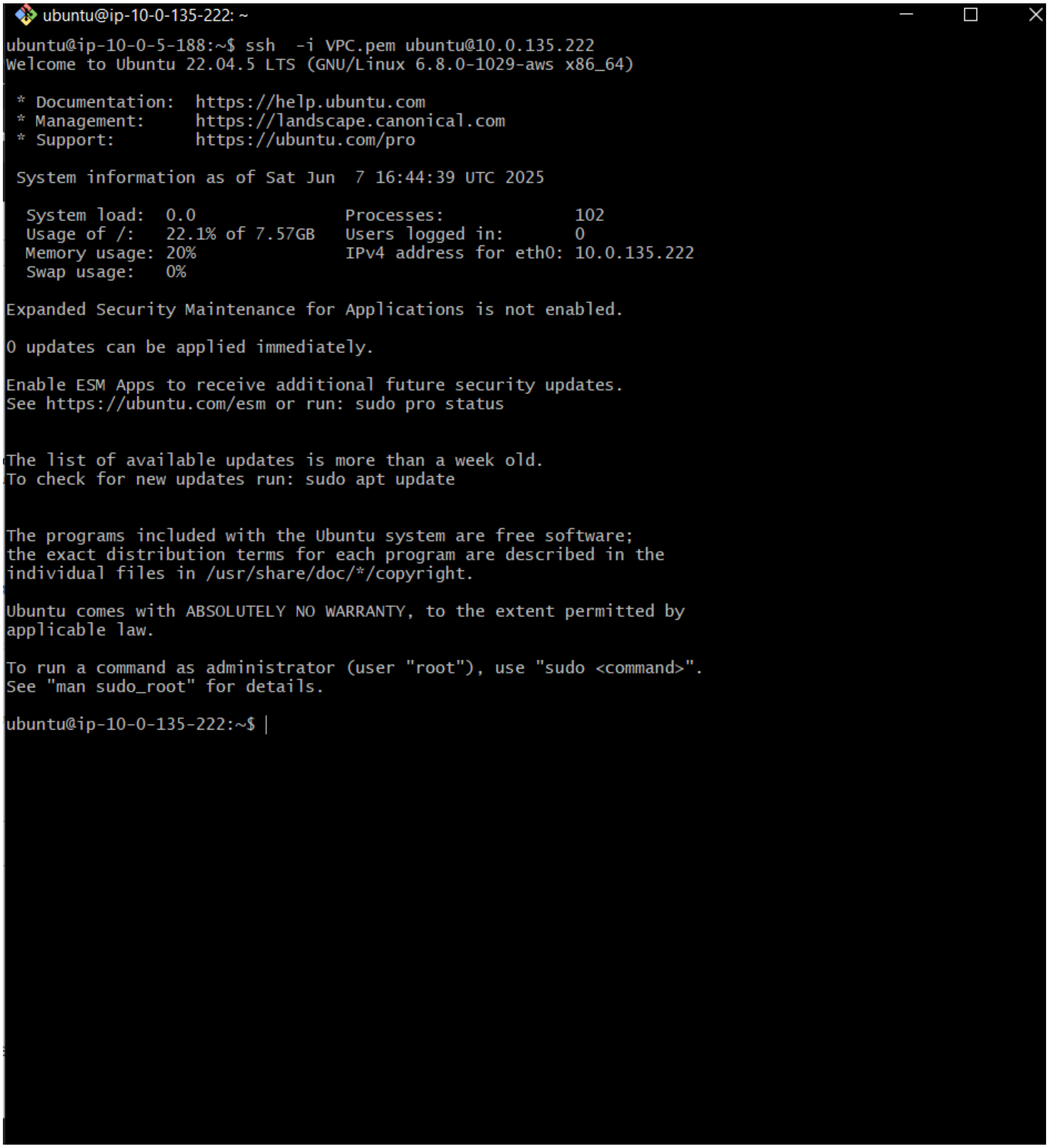


MINGW64:/c/Users/ASUS/Desktop

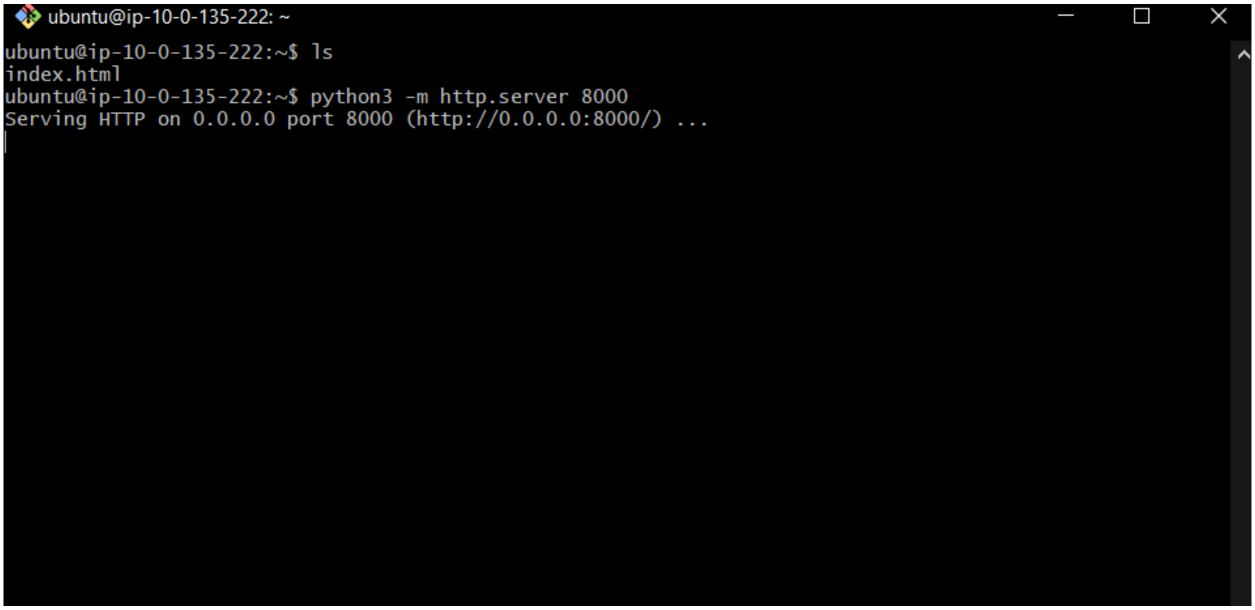
```
Vipul@DESKTOP-I07S3T2 MINGW64 ~/Desktop
$ pwd
/c/Users/ASUS/Desktop

Vipul@DESKTOP-I07S3T2 MINGW64 ~/Desktop
$ scp -i /c/Users/ASUS/Desktop/VPC.pem  /c/Users/ASUS/Desktop/VPC.pem ubuntu@65.
2.187.200:/home/ubuntu
The authenticity of host '65.2.187.200 (65.2.187.200)' can't be established.
ED25519 key fingerprint is SHA256:eS++VdtF7Z1tCAYIufkBvkPF2aPWAn4SgSU9Cyu8z6A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '65.2.187.200' (ED25519) to the list of known hosts.
VPC.pem                                       100% 1674   293.0KB/s   00:00

Vipul@DESKTOP-I07S3T2 MINGW64 ~/Desktop
$ |
```



```
Vipul@DESKTOP-I07S3T2 MINGW64 ~/Desktop
$ pwd
/c/Users/ASUS/Desktop

Vipul@DESKTOP-I07S3T2 MINGW64 ~/Desktop
$ scp -i /c/Users/ASUS/Desktop/VPC.pem  /c/Users/ASUS/Desktop/VPC.pem ubuntu@65.
2.187.200:/home/ubuntu
The authenticity of host '65.2.187.200 (65.2.187.200)' can't be established.
ED25519 key fingerprint is SHA256:eS++VdtF7Z1tCAYIufkBvkPF2aPWAn4SgSU9Cyu8z6A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '65.2.187.200' (ED25519) to the list of known hosts.
VPC.pem                                       100% 1674   293.0KB/s   00:00

Vipul@DESKTOP-I07S3T2 MINGW64 ~/Desktop
$ ssh -i VPC.pem ubuntu@65.2.187.200
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sat Jun  7 16:36:31 UTC 2025

  System load:  0.02              Processes:             102
  Usage of /:   22.6% of 7.57GB   Users logged in:       0
  Memory usage: 22%               IPv4 address for eth0: 10.0.5.188
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


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

ubuntu@ip-10-0-5-188:~$ hostname
ip-10-0-5-188
ubuntu@ip-10-0-5-188:~$ whoami
ubuntu
ubuntu@ip-10-0-5-188:~$ |
```



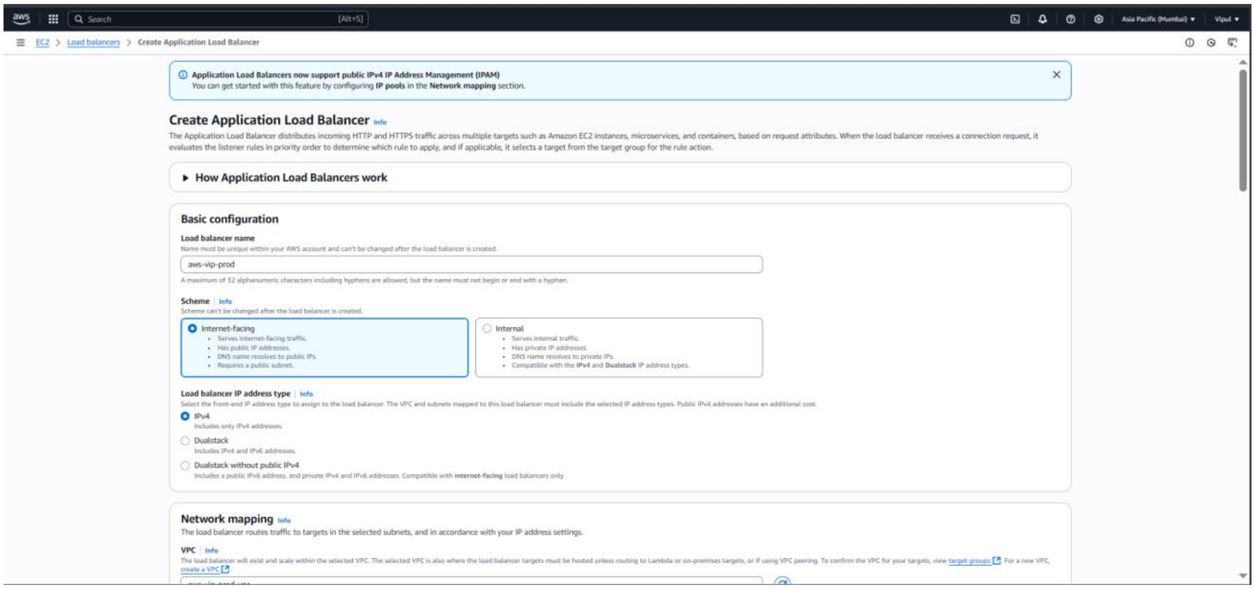
```
ubuntu@ip-10-0-5-188:~$ ssh  -i VPC.pem ubuntu@10.0.135.222
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sat Jun  7 16:44:39 UTC 2025

  System load:  0.0               Processes:             102
  Usage of /:   22.1% of 7.57GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 10.0.135.222
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

ubuntu@ip-10-0-135-222:~$ |
```



```
ubuntu@ip-10-0-135-222:~$ ls
index.html
ubuntu@ip-10-0-135-222:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

so we are able to access the both the Private Ec2 instances

Creating load balancer



Application Load Balancers now support public IPv4 IP Address Management (IPAM)
You can get started with this feature by configuring **IP pools** in the **Network mapping** section.

Create Application Load Balancer Info

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

▶ How Application Load Balancers work

Basic configuration

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

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

● Internet-facing
- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

○ Internal
- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the **IPv4** and **Dualstack** IP address types.

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

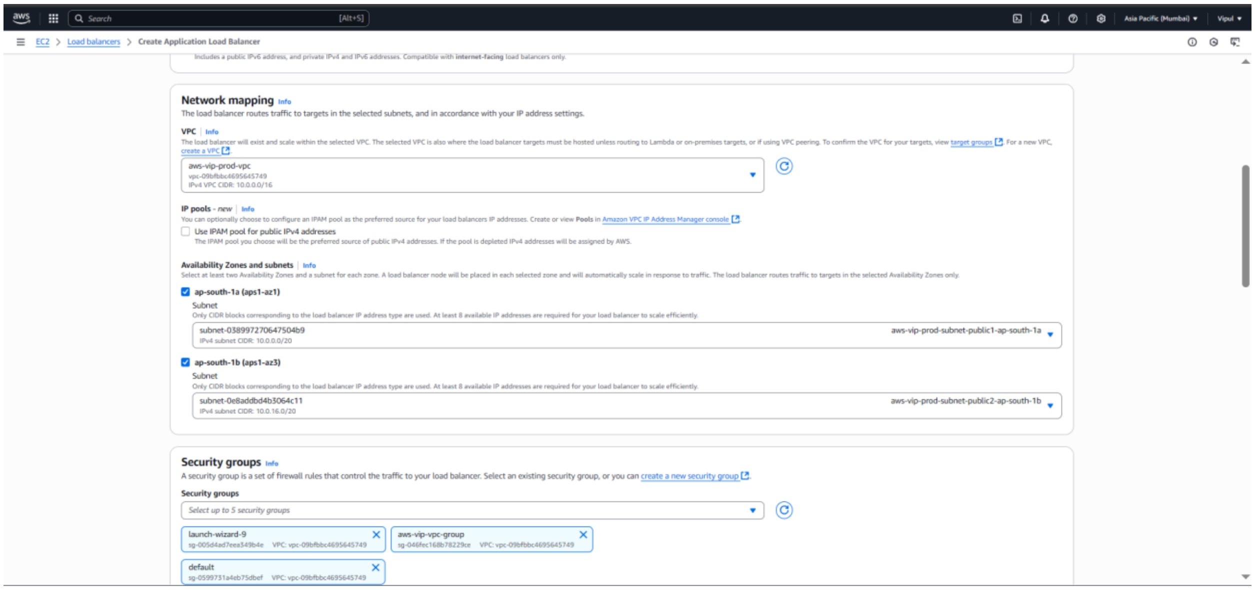
● IPv4
Includes only IPv4 addresses.

○ Dualstack
Includes IPv4 and IPv6 addresses.

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

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

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



Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

Network mapping Info

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

VPC | Info

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

aws-vip-prod-vpc
vpc-09bfbbc4695645749
IPv4 VPC CIDR: 10.0.0.0/16

IP pools - *new* | Info

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view **Pools** in Amazon VPC IP Address Manager console.

□ Use IPAM pool for public IPv4 addresses
The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets | Info

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

☑ **ap-south-1a (aps1-az1)**

Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-038997270647504b9 aws-vip-prod-subnet-public1-ap-south-1a
IPv4 subnet CIDR: 10.0.0.0/20

☑ **ap-south-1b (aps1-az3)**

Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0e8addbd4b3064c11 aws-vip-prod-subnet-public2-ap-south-1b
IPv4 subnet CIDR: 10.0.16.0/20

Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

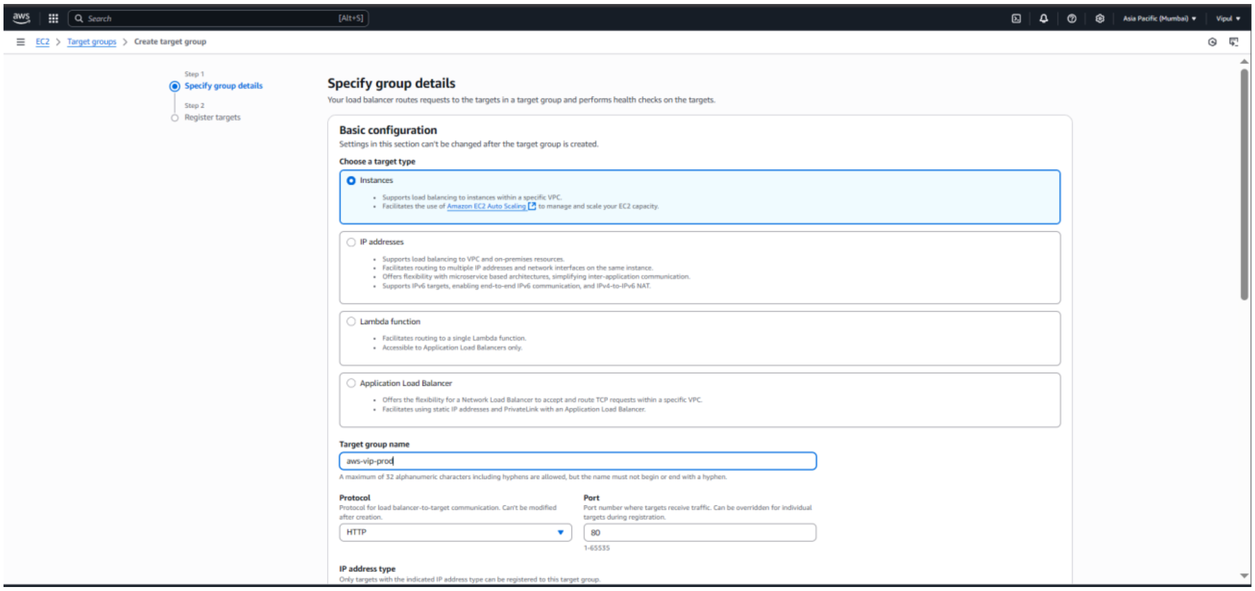
Select up to 5 security groups

launch-wizard-9
sg-005d4ad7eea349b4e VPC: vpc-09bfbbc4695645749

aws-vip-vpc-group
sg-046fec168b78229ce VPC: vpc-09bfbbc4695645749

default
sg-0599731a4eb75dbef VPC: vpc-09bfbbc4695645749

Creating the target groups



Step 1
● Specify group details

Step 2
○ Register targets

Specify group details

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

Basic configuration

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

Choose a target type

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

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

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

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

Target group name

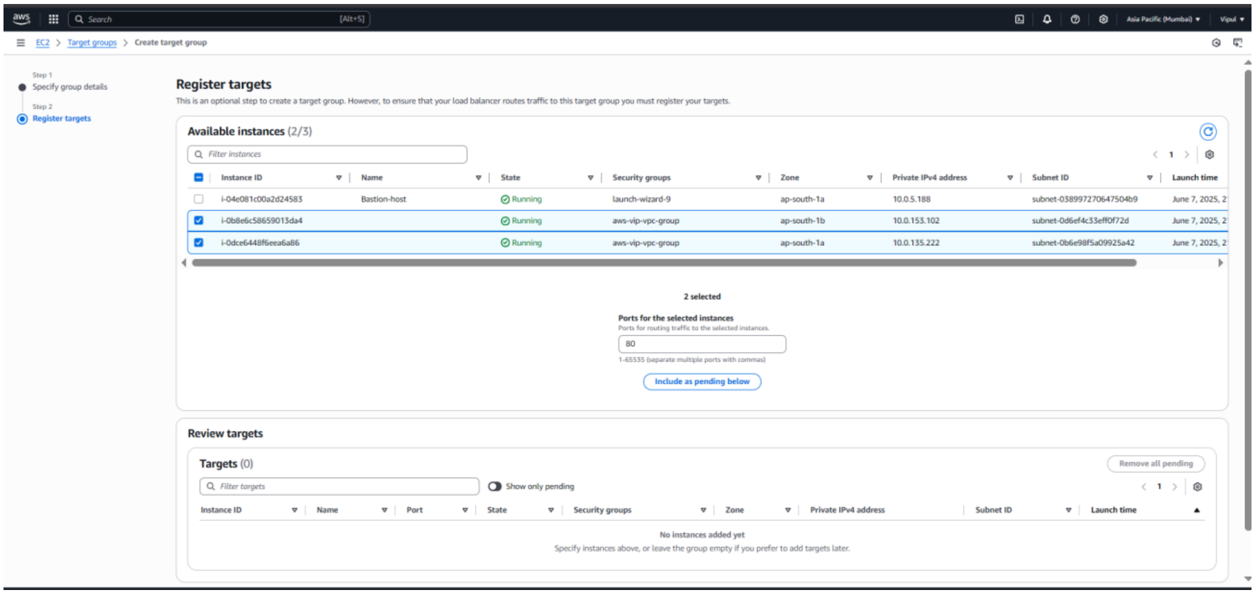
aws-vip-prod

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol
Protocol for load balancer-to-target communication. Can't be modified after creation.
HTTP

Port
Port number where targets receive traffic. Can be overridden for individual targets during registration.
80
1-65535

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



EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

Register targets

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

Available instances (2/3)

Filter instances

	Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
□	i-04e081c00a2d24583	Bastion-host	✓ Running	launch-wizard-9	ap-south-1a	10.0.5.188	subnet-038997270647504b9	June 7, 2025, 2
☑	i-0b8e6c58659013da4		✓ Running	aws-vip-vpc-group	ap-south-1b	10.0.153.102	subnet-0d6ef4c33eff0f72d	June 7, 2025, 2
☑	i-0dce6448f6eea6a86		✓ Running	aws-vip-vpc-group	ap-south-1a	10.0.135.222	subnet-0b6e98f5a09925a42	June 7, 2025, 2

2 selected

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

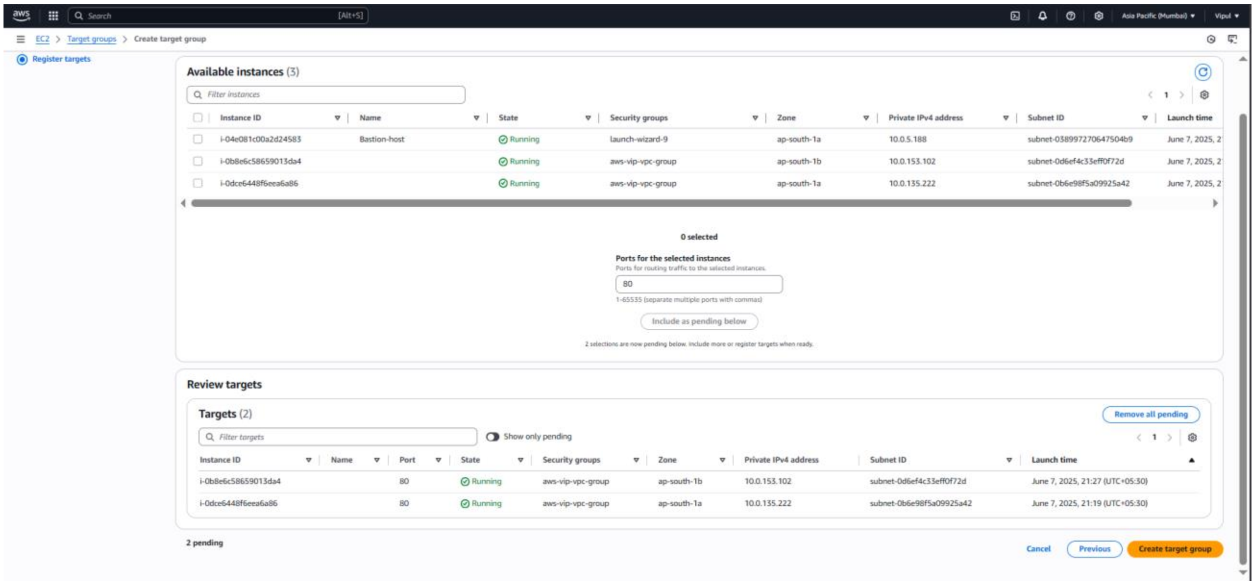
Review targets

Targets (0)

Filter targets

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time

No instances added yet
Specify instances above, or leave the group empty if you prefer to add targets later.



EC2 > Target groups > Create target group

Register targets

Available instances (3)

Filter instances

	Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
□	i-04e081c00a2d24583	Bastion-host	✓ Running	launch-wizard-9	ap-south-1a	10.0.5.188	subnet-038997270647504b9	June 7, 2025, 2
□	i-0b8e6c58659013da4		✓ Running	aws-vip-vpc-group	ap-south-1b	10.0.153.102	subnet-0d6ef4c33eff0f72d	June 7, 2025, 2
□	i-0dce6448f6eea6a86		✓ Running	aws-vip-vpc-group	ap-south-1a	10.0.135.222	subnet-0b6e98f5a09925a42	June 7, 2025, 2

0 selected

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

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

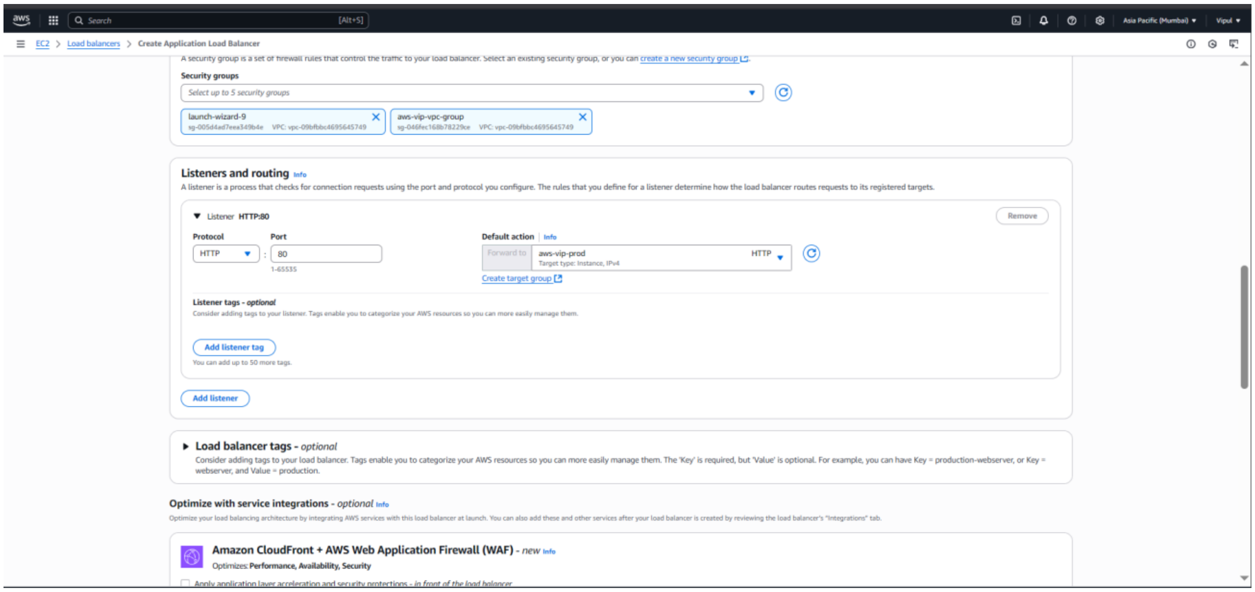
Review targets

Targets (2)

Filter targets

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-0b8e6c58659013da4		80	✓ Running	aws-vip-vpc-group	ap-south-1b	10.0.153.102	subnet-0d6ef4c33eff0f72d	June 7, 2025, 21:27 (UTC+05:30)
i-0dce6448f6eea6a86		80	✓ Running	aws-vip-vpc-group	ap-south-1a	10.0.135.222	subnet-0b6e98f5a09925a42	June 7, 2025, 21:19 (UTC+05:30)

2 pending



A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups

launch-wizard-9 sg-005d4ad7eea349b4e VPC: vpc-09bfbbc4695645749

aws-vip-vpc-group sg-046fec168b78229ce VPC: vpc-09bfbbc4695645749

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Protocol: HTTP
Port: 80 (1-65535)
Default action: Forward to aws-vip-prod HTTP
Target type: Instance, IPv4

Listener tags - *optional*

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

You can add up to 50 more tags.

▶ Load balancer tags - *optional*

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

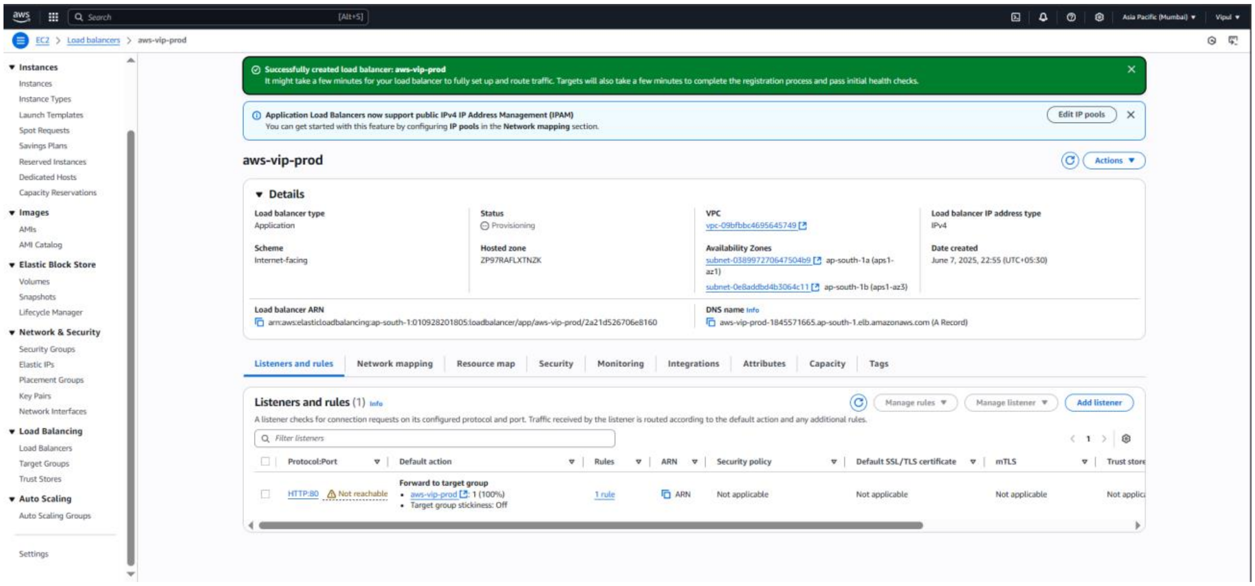
Optimize with service integrations - *optional* Info

Optimize your load balancing architecture by integrating AWS services with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the load balancer's "Integrations" tab.

Amazon CloudFront + AWS Web Application Firewall (WAF) - *new* Info

Optimizes: Performance, Availability, Security

□ Apply application layer acceleration and security protections - *in front of the load balancer*



Successfully created load balancer: aws-vip-prod

It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.

Application Load Balancers now support public IPv4 IP Address Management (IPAM)

You can get started with this feature by configuring **IP pools** in the **Network mapping** section.

aws-vip-prod

▼ Details

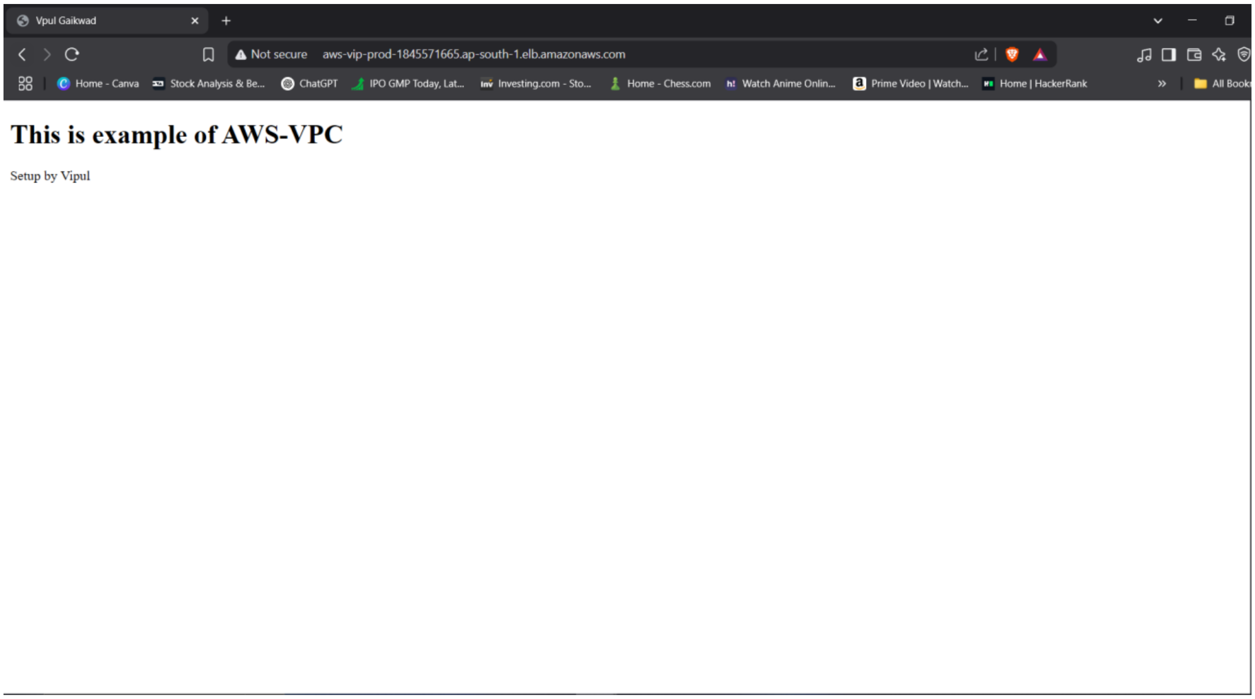
Load balancer type: Application
Status: Provisioning
VPC: vpc-09bfbbc4695645749
Load balancer IP address type: IPv4
Scheme: Internet-facing
Hosted zone: ZP97RAFLXTNZK
Availability Zones: subnet-038997270647504b9 ap-south-1a (aps1-az1); subnet-0e8addbd4b3064c11 ap-south-1b (aps1-az3)
Date created: June 7, 2025, 22:55 (UTC+05:30)
Load balancer ARN: arn:aws:elasticloadbalancing:ap-south-1:010928201805:loadbalancer/app/aws-vip-prod/2a21d526706e8160
DNS name: aws-vip-prod-1845571665.ap-south-1.elb.amazonaws.com (A Record)

Listeners and rules (1) Info

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

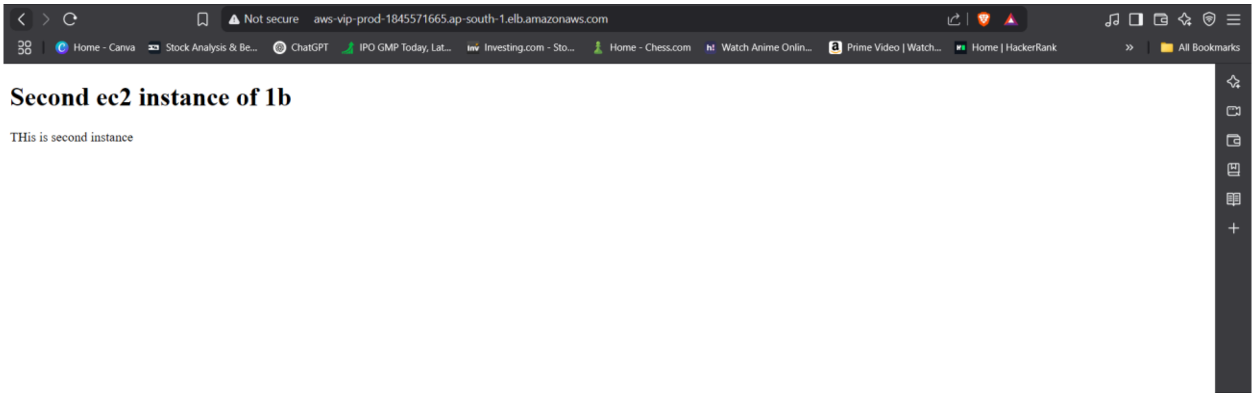
□	Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS	Trust store
□	HTTP:80 ⚠ Not reachable	Forward to target group • aws-vip-prod: 1 (100%) • Target group stickiness: Off	1 rule	ARN	Not applicable	Not applicable	Not applicable	Not applic

Created index.html on both the servers and ran python application and below is the output as it directs traffic on both the nodes



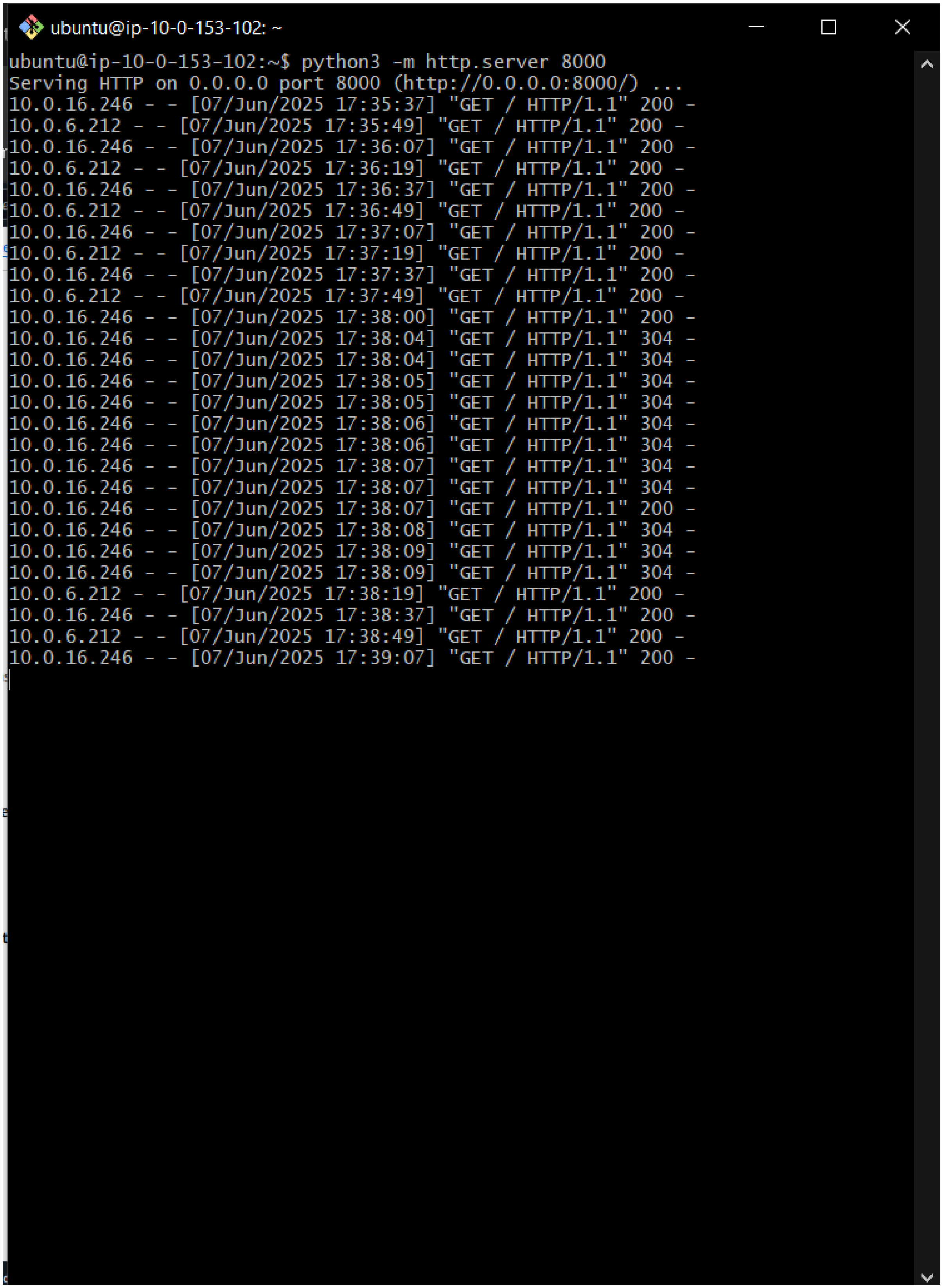
This is example of AWS-VPC

Setup by Vipul

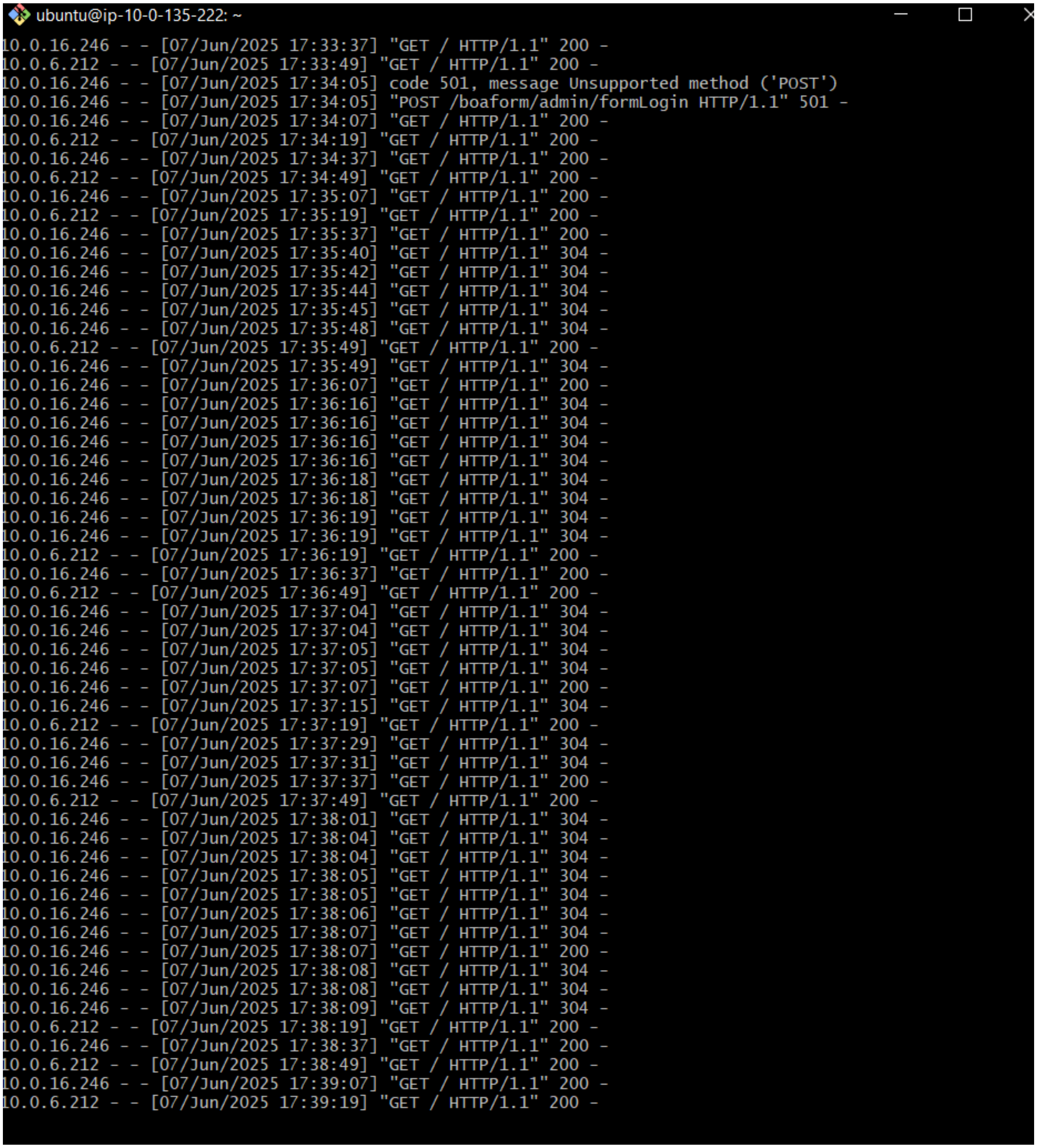


Second ec2 instance of 1b

THis is second instance



```
ubuntu@ip-10-0-153-102:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.16.246 - - [07/Jun/2025 17:35:37] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:35:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:36:07] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:36:19] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:36:37] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:36:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:37:07] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:37:19] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:37:37] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:37:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:38:00] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:38:04] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:04] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:05] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:05] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:06] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:06] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:07] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:07] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:07] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:38:08] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:09] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:09] "GET / HTTP/1.1" 304 -
10.0.6.212 - - [07/Jun/2025 17:38:19] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:38:37] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:38:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:39:07] "GET / HTTP/1.1" 200 -
```



ubuntu@ip-10-0-135-222: ~

```
10.0.16.246 - - [07/Jun/2025 17:33:37] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:33:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:34:05] code 501, message Unsupported method ('POST')
10.0.16.246 - - [07/Jun/2025 17:34:05] "POST /boaform/admin/formLogin HTTP/1.1" 501 -
10.0.16.246 - - [07/Jun/2025 17:34:07] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:34:19] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:34:37] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:34:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:35:07] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:35:19] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:35:37] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:35:40] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:35:42] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:35:44] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:35:45] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:35:48] "GET / HTTP/1.1" 304 -
10.0.6.212 - - [07/Jun/2025 17:35:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:35:49] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:36:07] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:36:16] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:36:16] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:36:16] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:36:16] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:36:18] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:36:18] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:36:19] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:36:19] "GET / HTTP/1.1" 304 -
10.0.6.212 - - [07/Jun/2025 17:36:19] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:36:37] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:36:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:37:04] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:37:04] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:37:05] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:37:05] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:37:07] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:37:15] "GET / HTTP/1.1" 304 -
10.0.6.212 - - [07/Jun/2025 17:37:19] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:37:29] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:37:31] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:37:37] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:37:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:38:01] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:04] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:04] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:05] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:05] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:06] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:07] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:07] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:38:08] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:08] "GET / HTTP/1.1" 304 -
10.0.16.246 - - [07/Jun/2025 17:38:09] "GET / HTTP/1.1" 304 -
10.0.6.212 - - [07/Jun/2025 17:38:19] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:38:37] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:38:49] "GET / HTTP/1.1" 200 -
10.0.16.246 - - [07/Jun/2025 17:39:07] "GET / HTTP/1.1" 200 -
10.0.6.212 - - [07/Jun/2025 17:39:19] "GET / HTTP/1.1" 200 -
```

Hence, Completed the project.