

AWS High-Availability Web Architecture with Bastion Host, ALB and EFS

Overview:

Built a secure and highly available AWS architecture where a private Linux EC2 hosts a static website, accessible only through an Application Load Balancer, with administrative access controlled via a bastion host. Shared storage is provided using Amazon EFS.

Objectives:

- Secure access to private EC2 instances
- High availability for web applications
- Network isolation using public and private subnets
- Shared and persistent storage.

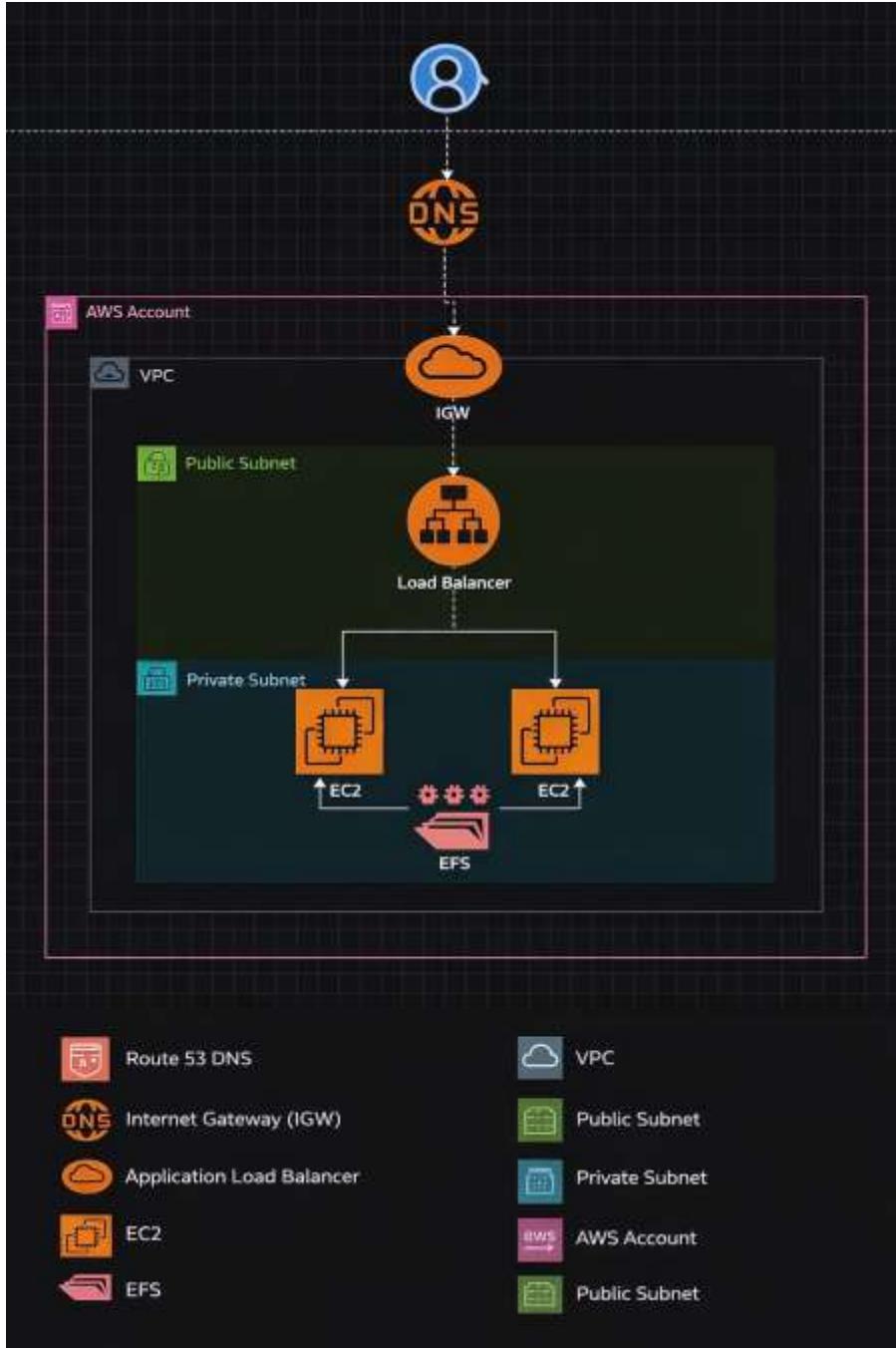
✨ Key Features:

- Bastion host for secure SSH/RDP access
- Private EC2 with no public IP
- ALB for web traffic routing
- Amazon EFS for shared storage
- VPC-based network isolation



Tools & Technologies

- Amazon EC2, Amazon VPC
- Application Load Balancer
- Amazon EFS
- AWS IAM
- Linux, Windows



Architecture Flow:

1. User accesses website via ALB DNS
2. ALB routes traffic to private EC2
3. Admin access via bastion host only
4. Files shared using Amazon EFS

- **Work flow:**
- Create a **VPC**
- Create **Public Subnet** and **Private Subnet**
- Attach **Internet Gateway** to VPC
- Create **Public Route Table → IGW**
- Create **Security Groups** (Bastion, ALB, Private EC2)
- Launch **Bastion EC2** in Public Subnet (with Public IP)
- Launch **Private EC2** in Private Subnet (No Public IP)
- Access Private EC2 **via Bastion only**
- Install **Static Website** on Private EC2
- Create **Target Group** and register Private EC2
- Create **Application Load Balancer** in Public Subnets
- Access website using **ALB DNS name**

 Search

[Alt+S]

Asia Pacific (Mumbai) ▾
mani

mani (3869-9964-4139) ▾

VPC > Your VPCs



VPCs VPC encryption controls

Your VPCs (1/3)

Last updated
7 minutes ago

Actions ▾

Create VPC

Find VPCs by attribute or tag

< 1 >

Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...	⋮
<input checked="" type="checkbox"/> PROJECT-1-VPC-vpc	vpc-037a353fbaae8dec3	Available	-	-	Off	1
<input type="checkbox"/> -	vpc-0ffa188c3854d80a8	Available	-	-	Off	1
<input type="checkbox"/> -	vpc-0b0c256ac465459a0	Available	-	-	Off	1

vpc-037a353fbaae8dec3 / PROJECT-1-VPC-vpc



ap-south-1a

PROJECT-1-VPC-subnet-public1-ap-south-1a

PROJECT-1-VPC-subnet-private1-ap-south-1a

rtb-0b6fe41fcf59bfa9b

PROJECT-1-VPC-rtb-public

PROJECT-1-VPC-rtb-private1-ap-south-1a

PROJECT-1-VPC-igw

PROJECT-1-VPC-nat-public1-ap-south-1a

PROJECT-1-VPC-vpce-s3

 Search

[Alt+S] ⌘



Asia Pacific (Mumbai) ▾

mani (3869-9964-4139) ▾

mani

☰ EC2 > Instances

Instances (2/4) InfoLast updated
less than a minute ago

Connect

Instance state ▾

Actions ▾

Launch instances ▾

 Find Instance by attribute or tag (case-sensitive)

All states ▾

< 1 >



-	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
<input checked="" type="checkbox"/>	Private-Server	i-0b9566561c5c3c261	Running	t3.micro	Initializing	View alarms +	ap-south-1a	-
<input checked="" type="checkbox"/>	Bastion-windo...	i-0039233c208073b50	Running	t3.micro	3/3 checks passed	View alarms +	ap-south-1a	ec2-13-232-

2 instances selected



Monitoring

[Investigate with AI - new](#)

1h

3h

12h

1d

3d

1w

Custom

UTC timezone ▾

[Explore related](#)

CPU Utilization (%)



Network in (bytes)



Network out (bytes)



Network packets in (count)



63c208073b50

0039233c208073b50

1.compute.internal

e

Subnet ID

Auto Scaling Group name

Remote Desktop Connection

Remote Desktop Connection

General Display Local Resources Experience Advanced

Logon settings

Enter the name of the remote computer.

Computer: 13.232.34.170

User name: Administrator

You will be asked for credentials when you connect.

Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

Save Save As... Open...

Hide Options Connect Help

Private IPv4 addresses

10.0.11.254

Public DNS

ec2-13-232-34-170.ap-south-1.c
open address ↗

Elastic IP addresses

AWS Compute Optimizer finding

Opt-in to AWS Compute Optim
Learn more ↗

Asia Pacific (Mum



13.232.34.170



Settings

Find a setting

 Administrator
Local Account

System

Bluetooth & devices

Network & internet

Personalization

Apps

Accounts

Time & language

Accessibility

Privacy & security

Windows Update

System

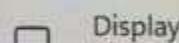


EC2AMAZ-K26PM4C

t3.micro
Rename

Windows Update

Up to date



Display

Monitors, brightness, night light, display profile



Sound

Volume levels, output, input, sound devices



Notifications

Alerts from apps and system, do not disturb



Focus

Reduce distractions



Power

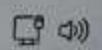
Screen and sleep, power mode, energy-saver



Hostname: EC2AMAZ-K26PM4C
Instance ID: i-0039233c208073b50
Private IPv4 address: 10.0.11.254
Public IPv4 address: 13.232.34.170
Instance size: t3.micro
Availability Zone: ap-south-1a
Architecture: AMD64
Total memory: 1024 MB
Network: Up to 5 Gigabit



Search

ENG
IN5:25 AM
12/23/2025

Add SG of bastion host in the inbound rule of private server

Searched for "Search" [Alt+S]

aws | Search Asia Pacific (Mumbai) mani (3869-9964-4139) mani

EC2 > Security Groups > sg-09bbebdf768ad8400 - SG-for-Private-host > Edit inbound rules

Edit inbound rules

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

Inbound rules	Security group rule ID	Type	Protocol	Port range	Source	Description - optional
	sgr-0364a33a68e5452e4	SSH	TCP	22	Cus...	SG-bastion

SG for ALB



Search

[Alt+S] ⌘



Asia Pacific (Mumbai) ▾

mani (3869-9964-4139) ▾

mani

☰ EC2 > Security Groups > Create security group



Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

SG-For-ALB

Name cannot be edited after creation.

Description Info

for ALB

VPC Info

vpc-037a353fbaae8dec3 (PROJECT-1-VPC-vpc)



Inbound rules Info

Type Info

Protocol

Port range Info

Info

Source Info

Description - optional Info

 Search

[Alt+S]



Asia Pacific (Mumbai)

mani (3869-9964-4139)

mani

EC2 > Security Groups > Create security group

Inbound rules

Type **Protocol** **Port range** **Source** **Description - optional** **HTTP** **TCP****80****An...** **to access the website****Delete****0.0.0.0/0** **Add rule**

Outbound rules

Type **Protocol** **Port range** **Destination** **Description - optional** **All traffic** **All****All****Cus...** **Delete****0.0.0.0/0** **Add rule**

CloudShell

Feedback

Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Add SG of ALB in private host

aws | Search [Alt+S] Ask Amazon Q | Asia Pacific (Mumbai) mani (3869-9964-4139) mani

EC2 > Security Groups > sg-09bbebdf768ad8400 - SG-for-Private-host > Edit inbound rules

Edit inbound rules Info

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

Security group rule ID	Type	Info	Protocol	Port range	Source	Info	Description - optional	Info
				Info	Info			
sgr-0364a33a68e5452e4	SSH	▼	TCP	22	Cus... ▼	<input type="text"/> Q	SG-bastion	Delete
-	HTTP	▼	TCP	80	Cus... ▼	<input type="text"/> Q sg-0dae3d92edf1d48f9 X	SG-ALB	Delete

Add rule

Connect to private-Linux Server

The screenshot shows a Windows terminal window titled "ec2-user@ip-10-0-132-218:~". The IP address 13.127.126.141 is displayed in the title bar. The terminal content is as follows:

```
PS C:\Windows\system32> C: \Users\Administrator\bastion-key.pem
PS C:\Windows\system32> ssh -i C:\Users\Administrator\Downloads\bastion-key.pem ec2-user@10.0.132.218
#_
###_
Amazon Linux 2023
####
###|#
#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
V~' '-->
/ \
/ \
/m'/ [ec2-user@ip-10-0-132-218 ~]$ |
```

The terminal shows a command-line interface for connecting to an Amazon Linux 2023 instance via SSH. The connection is established successfully, and the user is at the prompt [ec2-user@ip-10-0-132-218 ~]\$.

Install nginx

```
root@ip-10-0-132-218:/home/ 13.127.126.141
Transaction test succeeded.
Running transaction
Preparing : 1/1
Running scriptlet: nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch 1/7
Installing : nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch 1/7
Installing : nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch 1/7
Installing : libunwind-1.4.0-5.amzn2023.0.3.x86_64 2/7
Installing : gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64 3/7
Installing : nginx-core-1:1.28.0-1.amzn2023.0.2.x86_64 4/7
Installing : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch 5/7
Installing : nginx-1:1.28.0-1.amzn2023.0.2.x86_64 6/7
Installing : nginx-1:1.28.0-1.amzn2023.0.2.x86_64 7/7
Running scriptlet: nginx-1:1.28.0-1.amzn2023.0.2.x86_64 7/7
Verifying : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch 1/7
Verifying : gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64 2/7
Verifying : libunwind-1.4.0-5.amzn2023.0.3.x86_64 3/7
Verifying : nginx-1:1.28.0-1.amzn2023.0.2.x86_64 4/7
Verifying : nginx-core-1:1.28.0-1.amzn2023.0.2.x86_64 5/7
Verifying : nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch 6/7
Verifying : nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch 7/7

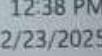
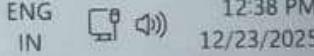
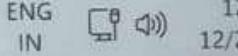
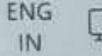
Installed:
generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
libunwind-1.4.0-5.amzn2023.0.3.x86_64
nginx-core-1:1.28.0-1.amzn2023.0.2.x86_64
nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch
gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64
nginx-1:1.28.0-1.amzn2023.0.2.x86_64
nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch

Complete!
[root@ip-10-0-132-218 ec2-user]#
[root@ip-10-0-132-218 ec2-user]#
[root@ip-10-0-132-218 ec2-user]#
```

```
root@ip-10-0-132-218:/home/ + ~ - X 4C  
Installing : nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch 1/7  
Installing : nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch 2/7  
Installing : libunwind-1.4.0-5.amzn2023.0.3.x86_64 254  
Installing : gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64 26.141  
Installing : nginx-core-1:1.28.0-1.amzn2023.0.2.x86_64 3/7  
Installing : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch 4/7  
Installing : nginx-1:1.28.0-1.amzn2023.0.2.x86_64 5/7  
Installing : nginx-1:1.28.0-1.amzn2023.0.2.x86_64 6/7  
Running scriptlet: nginx-1:1.28.0-1.amzn2023.0.2.x86_64 7/7  
Verifying : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch 7/7  
Verifying : gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64 1/7  
Verifying : libunwind-1.4.0-5.amzn2023.0.3.x86_64 2/7  
Verifying : nginx-1:1.28.0-1.amzn2023.0.2.x86_64 3/7  
Verifying : nginx-core-1:1.28.0-1.amzn2023.0.2.x86_64 4/7  
Verifying : nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch 5/7  
Verifying : nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch 6/7  
Verifying : nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch 7/7  
  
Installed:  
generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64  
libunwind-1.4.0-5.amzn2023.0.3.x86_64 nginx-1:1.28.0-1.amzn2023.0.2.x86_64  
nginx-core-1:1.28.0-1.amzn2023.0.2.x86_64 nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch  
nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch  
  
Complete!  
[root@ip-10-0-132-218 ec2-user]#  
[root@ip-10-0-132-218 ec2-user]#  
[root@ip-10-0-132-218 ec2-user]# systemctl start nginx  
[root@ip-10-0-132-218 ec2-user]# systemctl enable nginx  
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /usr/lib/systemd/system/nginx.service.  
[root@ip-10-0-132-218 ec2-user]#  
[root@ip-10-0-132-218 ec2-user]# |
```



Search



root@ip-10-0-132-218:/home/

generic-logos-nginx-18.0.0-12.amzn2023.0.3.noarch
libunwind-1.4.0-5.amzn2023.0.3.x86_64
nginx-core-1:1.28.0-1.amzn2023.0.2.x86_64
nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch

gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64
nginx-1:1.28.0-1.amzn2023.0.2.x86_64
nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch

Complete!

```
[root@ip-10-0-132-218 ec2-user]#  
[root@ip-10-0-132-218 ec2-user]#  
[root@ip-10-0-132-218 ec2-user]# systemctl start nginx  
[root@ip-10-0-132-218 ec2-user]# systemctl enable nginx  
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /usr/lib/systemd/system/nginx.service.  
[root@ip-10-0-132-218 ec2-user]#  
[root@ip-10-0-132-218 ec2-user]# systemctl status nginx  
● nginx.service - The nginx HTTP and reverse proxy server  
  Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: disabled)  
  Active: active (running) since Tue 2025-12-23 12:37:52 UTC; 57s ago  
    Main PID: 26457 (nginx)  
      Tasks: 3 (limit: 1067)  
     Memory: 3.2M  
       CPU: 55ms  
      CGroup: /system.slice/nginx.service  
          ├─26457 "nginx: master process /usr/sbin/nginx"  
          ├─26458 "nginx: worker process"  
          └─26459 "nginx: worker process"
```

```
Dec 23 12:37:52 ip-10-0-132-218.ap-south-1.compute.internal systemd[1]: Starting nginx.service - The nginx HTTP and rev>  
Dec 23 12:37:52 ip-10-0-132-218.ap-south-1.compute.internal nginx[26455]: nginx: the configuration file /etc/nginx/nginx>  
Dec 23 12:37:52 ip-10-0-132-218.ap-south-1.compute.internal nginx[26455]: nginx: configuration file /etc/nginx/nginx.co>  
Dec 23 12:37:52 ip-10-0-132-218.ap-south-1.compute.internal systemd[1]: Started nginx.service - The nginx HTTP and reve>
```

lines 1-16/16 (END)



Search



GNU nano 8.3

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>
<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>
<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

[Read 23 lines]

^G Help
^X Exit

^O Write Out
^R Read File

^F Where Is
^ Replace

^K Cut
^U Paste

^T Execute
^J Justify

^C Location
^/ Go To Line

M-U Undo
M-E Redo

M-A Set Mark
M-G Copy

```
Main PID: 26457 (nginx)
Tasks: 3 (limit: 1067)
Memory: 3.2M
CPU: 55ms
CGroup: /system.slice/nginx.service
└─26457 "nginx: master process /usr/sbin/nginx"
  ├─26458 "nginx: worker process"
  └─26459 "nginx: worker process"

Dec 23 12:37:52 ip-10-0-132-218.ap-south-1.compute.internal systemd[1]: Starting nginx.service - The nginx HTTP and rev>
Dec 23 12:37:52 ip-10-0-132-218.ap-south-1.compute.internal nginx[26455]: nginx: the configuration file /etc/nginx/nginx>
Dec 23 12:37:52 ip-10-0-132-218.ap-south-1.compute.internal nginx[26455]: nginx: configuration file /etc/nginx/nginx.co>
[root@ip-10-0-132-218 ec2-user]# 

root@ip-10-0-132-218 ec2-user]# systemctl restart nginx
root@ip-10-0-132-218 ec2-user]# curl localhost
!DOCTYPE html>
html>
head>
<title>Private EC2 Website</title>
/head>
body>
<h1>Welcome to My Private Linux Server</h1>
<p>This website is hosted on a private EC2 instance.</p>
<p>Accessed securely via Application Load Balancer.</p>
/body>
/html>
root@ip-10-0-132-218 ec2-user]# |
```

 Search

[Alt+S]

Ask Amazon Q



Asia Pacific (Mumbai) ▾

mani (3869-9964-4139) ▾

mani

[☰](#) [EC2](#) > [Security Groups](#) > [sg-09bbebdf768ad8400 - SG-for-Private-host](#) > [Edit inbound rules](#)

Edit inbound rules Info

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

Inbound rules Info

Security group rule ID	Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
------------------------	--------------------------	------------------------------	--------------------------------	----------------------------	--

sgr-0364a33a68e5452e4	SSH	TCP	22	Cus... ▾	SG-bastion	<button>Delete</button>
-----------------------	-----	-----	----	----------	------------	-------------------------

sg-
044f14d920349d4a
3

sgr-0b8172b95128eb7cd	HTTP	TCP	80	Cus... ▾	SG-ALB	<button>Delete</button>
-----------------------	------	-----	----	----------	--------	-------------------------

sg-
0dae3d92edf1d48f
9

[Add rule](#)[CloudShell](#)[Feedback](#)[Console Mobile App](#)

© 2025, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)[Terms](#)[Cookie preferences](#)

Create Target Group:

aws | [Alt+S] Ask Amazon Q | Asia Pacific (Mumbai) mani (3869-9964-4139) mani

Search | EC2 > Target groups > Create target group

Include as pending below

1 selection is now pending below. Include more or register targets when ready.

Review targets

Targets (1)

Show only pending < 1 >

Instance ID	Name	Port	State	Security groups	Zone	Private I
i-0b9566561c5c3c261	Private-Server	80	Running	SG-for-Private-host	ap-south-1a	10.0.132

1 pending



Search

[Alt+S]

Ask Amazon Q



Asia Pacific (Mumbai) ▾

mani (3869-9964-4139) ▾

mani



EC2 > Target groups

Private-ALB-TG



▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

▼ Load Balancing

Load Balancers

Target Groups

Trust Stores

▼ Auto Scaling

Auto Scaling Groups

Settings

✓ Successfully created the target group: Private-ALB-TG. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab.



Give feedback



Private-ALB-TG

Actions ▾

Details

arn:aws:elasticloadbalancing:ap-south-1:386999644139:targetgroup/Private-ALB-TG/2c6d1d0ea2da3e54

Target type

Instance

Protocol : Port

HTTP: 80

Protocol version

HTTP1

VPC

vpc-037a353fbbae8dec3 ↗

IP address type

IPv4

Load balancer

None associated

1	0	0	1	0	0
Total targets	Healthy	Unhealthy	Unused	Initial	Draining
	0 Anomalous				

0

Healthy

0

Unhealthy

1

Unused

0

Initial

0

Draining

Create ALB:

aws | Search [Alt+S] Ask Amazon Q | ☰ | 🔔 | ⓘ | ⚙️ | Asia Pacific (Mumbai) ▾ mani (3869-9964-4139) ▾ mani

☰ EC2 > Load balancers > Create Application Load Balancer ⓘ 🔍 ⚙️

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.

Private-ALB

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.

Choose two public subnets in different Azs:

aws |  Search [Alt+S] Ask Amazon Q |     Asia Pacific (Mumbai) mani (3869-9964-4139) mani

EC2 > Load balancers > Create Application Load Balancer

IP pools | [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 the [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-05cf5c48e54c6c69a PROJECT-1-VPC-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-07039b0d0eee34347 Public-subnet-2-1b
IPv4 subnet CIDR: 10.0.16.0/20

Choose the SG of ALB:

The screenshot shows the AWS Lambda function configuration page. The top navigation bar includes the AWS logo, search bar, Ask Amazon Q button, and account information (mani (3869-9964-4139) in Asia Pacific (Mumbai)). The main content area shows the function name 'HelloWorld' and its ARN. The 'Handler' section is expanded, showing the code editor with the provided Python script. The 'Configuration' tab is selected.

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

SG-For-ALB
sg-0dae3d92edf1d48f9 VPC: vpc-037a353fbbae8dec3

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** Remove

Protocol	Port
HTTP	80 1-65535

Default action Info

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

 Search

[Alt+S]

Ask Amazon Q

Asia Pacific (Mumbai) ▾
mani

mani (3869-9964-4139) ▾

mani

☰ EC2 > Load balancers > Create Application Load Balancer

ⓘ 🔍 ⚙

▼ Listener HTTP:80

Protocol

HTTP

Port

80

1-65535

Remove

Default action | [Info](#)

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Routing action

 Forward to target groups Redirect to URL Return fixed responseForward to target group | [Info](#)

Choose a target group and specify routing weight or [create target group](#) ↗.

Target group

Private-ALB-TG

HTTP ▾

Target type: Instance, IPv4 | Target stickiness: Off



Weight

1

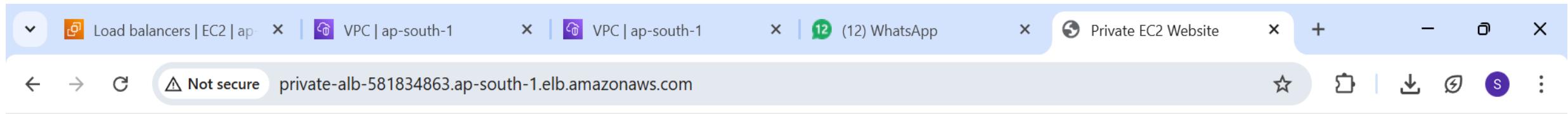
0-999

Percent

100%

+ Add target group

Copy the DNS of ALB into the Browser:



Welcome to My Private Linux Server

This website is hosted on a private EC2 instance.

Accessed securely via Application Load Balancer.

Mount EFS on private subnet:

Create SG for EFS

aws | Search [Alt+S] | Asia Pacific (Mumbai) | mani (3869-9964-4139) | mani

EC2 > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

SG-FOR-EFS

Name cannot be edited after creation.

Description Info

EFS access from private ec2

VPC Info

vpc-037a353fbuae8dec3 (PROJECT-1-VPC-vpc)

Inbound rules Info

Type <small>Info</small>	Protocol	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
Info				

Allow NFS port, source: sg for private instance:

Screenshot of the AWS EC2 Security Groups page showing the creation of a new security group rule.

The rule configuration is as follows:

- Type:** NFS
- Protocol:** TCP
- Port range:** 2049
- Source:** sg-09bbebdf768 (selected from a dropdown)
- Description - optional:** allow private EC2

A modal window displays the selected source security group details:

- sg-09bbebdf768ad840
- 0

An "Add rule" button is visible at the bottom left.

Outbound rules Info

The Outbound rules section shows one rule:

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - optional <small>Info</small>
All traffic	All	All	Cus... ▾	0.0.0.0/0 <small>X</small>

An "Add rule" button is visible at the bottom left.

Create file system (EFS):

aws | Search [Alt+S] Ask Amazon Q | Asia Pacific (Mumbai) ▾ mani (3869-9964-4139) ▾ mani

[Amazon EFS](#) > [File systems](#) > fs-07701a5204ba93ddc

Elastic File System

[File systems](#)
[Access points](#)

[AWS Backup ↗](#)
[AWS DataSync ↗](#)
[AWS Transfer ↗](#)

[Documentation ↗](#)

General

Amazon resource name (ARN)
arn:aws:elasticfilesystem:ap-south-1:386999644139:file-system/fs-07701a5204ba93ddc

Performance mode
General Purpose

Throughput mode
Bursting

Lifecycle management
Transition into Infrequent Access (IA): 30 day(s) since last access
Transition into Archive: None
Transition into Standard: None

Availability zone
Regional

Automatic backups
Disabled

Encrypted
No

File system state
Available

DNS name
fs-07701a5204ba93ddc.efs.ap-south-1.amazonaws.co
m

Replication overwrite protection
Enabled

 Search

[Alt+S]

Ask Amazon Q

Asia Pacific (Mumbai) ▾
mani

mani (3869-9964-4139) ▾

mani



Amazon EFS



File systems

fs-07701a5204ba93ddc

Network access



Elastic File System



File systems

Access points

AWS Backup ↗

AWS DataSync ↗

AWS Transfer ↗

Documentation ↗

ap-south-1a

subnet-056fd5f73baa15cc1

IPv4 only

IPv4 address

10.0.139.224

IPv6 address

-

Security groups

Choose security groups ▾

sg-0e15679d3a1b19f83 X
SG-FOR-EFS**Remove**

Availability zone

Subnet ID

IP address type

ap-south-1b

subnet-07039b0d0eee34347

IPv4 only

IPv4 address**IPv6 address****Security groups**

10.0.24.20

-

Choose security groups ▾

sg-0e15679d3a1b19f83 X
SG-FOR-EFS

```
root@ip-10-0-132-218:/home/ 13.127.126.141

2025-12-23 15:32:49 UTC - WARNING - Error connecting to 127.0.0.1:20770, [Errno 111] Connection refused
2025-12-23 15:32:49 UTC - INFO - Executing: "/sbin/mount.nfs4 127.0.0.1:/ /mnt/efs -o rw,nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,port=20770" with 15 sec time limit.
2025-12-23 15:33:04 UTC - ERROR - Mounting fs-07701a5204ba93ddc.efs.ap-south-1.amazonaws.com to /mnt/efs failed due to timeout after 15 sec, mount attempt 1/3, wait 0 sec before next attempt.
2025-12-23 15:33:04 UTC - INFO - Executing: "/sbin/mount.nfs4 127.0.0.1:/ /mnt/efs -o rw,nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,port=20770" with 15 sec time limit.
2025-12-23 15:33:19 UTC - ERROR - Mounting fs-07701a5204ba93ddc.efs.ap-south-1.amazonaws.com to /mnt/efs failed due to timeout after 15 sec, mount attempt 2/3, wait 0 sec before next attempt.
2025-12-23 15:33:19 UTC - INFO - Executing: "/sbin/mount.nfs4 127.0.0.1:/ /mnt/efs -o rw,nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,port=20770"
2025-12-23 15:36:19 UTC - ERROR - Failed to mount fs-07701a5204ba93ddc.efs.ap-south-1.amazonaws.com at /mnt/efs: returncode=32, stderr="b'mount.nfs4: Connection timed out'"
2025-12-23 15:37:16 UTC - INFO - version=2.4.1 options={'rw': None, 'tls': None}
2025-12-23 15:37:16 UTC - INFO - binding 21018
2025-12-23 15:37:16 UTC - INFO - Starting efs-proxy: "/sbin/efs-proxy /var/run/efs/stunnel-config.fs-07701a5204ba93ddc.mnt.efs.21018 --tls"
2025-12-23 15:37:16 UTC - INFO - Started efs-proxy, pid: 31666
2025-12-23 15:37:16 UTC - WARNING - Error connecting to 127.0.0.1:21018, [Errno 111] Connection refused
2025-12-23 15:37:16 UTC - INFO - Executing: "/sbin/mount.nfs4 127.0.0.1:/ /mnt/efs -o rw,nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,port=21018" with 15 sec time limit.
2025-12-23 15:37:19 UTC - INFO - Successfully mounted fs-07701a5204ba93ddc.efs.ap-south-1.amazonaws.com at /mnt/efs
[root@ip-10-0-132-218 ec2-user]#
[root@ip-10-0-132-218 ec2-user]#
[root@ip-10-0-132-218 ec2-user]#
[root@ip-10-0-132-218 ec2-user]# echo "EFS WORKING" | sudo tee /mnt/efs/test.txt
cat /mnt/efs/test.txt
EFS WORKING
EFS WORKING
[root@ip-10-0-132-218 ec2-user]#
```



Search



ENG
IN



3:42 PM
12/23/2025