

# Secure Web Hosting on AWS using EC2, S3, IAM Roles, and Application Load Balancer

## S3 Bucket (Static Files: logo.png, style.css)

- Go to S3 → Create bucket → Name: `my-lab-private-static-files`
- Region: ap-south-1 (Mumbai)
- Block all public access: ON (recommended)
- ACLs: Disabled, Object Ownership: Bucket owner enforced
- Default encryption: SSE-S3 or SSE-KMS (recommended for production, optional for this lab)
- After creation: Upload your `logo.png` and `style.css` files to the bucket

The screenshot shows the 'Create bucket' page in the AWS Management Console. The page is titled 'Create bucket' with a sub-header 'Buckets are containers for data stored in S3.' The 'General configuration' section is active, showing the 'AWS Region' as 'Asia Pacific (Mumbai) ap-south-1'. Under 'Bucket type', 'General purpose' is selected, with a description: 'Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.' The 'Bucket name' field contains 'my-lab-private-static-files'. Below this, there is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button. The 'Object Ownership' section shows 'ACLs disabled (recommended)' selected, with a description: 'All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.' The 'Block Public Access settings for this bucket' section is also visible, with a note about blocking public access.

**Create bucket** [info](#)  
Buckets are containers for data stored in S3.

**General configuration**

**AWS Region**  
Asia Pacific (Mumbai) ap-south-1

**Bucket type** [info](#)

☒ **General purpose**  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

**Bucket name** [info](#)  
my-lab-private-static-files  
Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

**Copy settings from existing bucket - optional**  
Only the bucket settings in the following configuration are copied.  
[Choose bucket](#)  
Format: s3://bucket/prefix

**Object Ownership** [info](#)  
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**Object Ownership**  
Bucket owner enforced

**Block Public Access settings for this bucket**  
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of

Amazon S3 > Buckets > Create bucket

☐ Enable

**Tags - optional** (0)  
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add new tag](#)  
You can add up to 50 tags.

**Default encryption** [info](#)  
Server-side encryption is automatically applied to new objects stored in this bucket.

**Encryption type** [info](#)  
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage tab](#) of the [Amazon S3 pricing page](#).

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)  
☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)  
☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

**Bucket Key**  
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable  
☒ Enable

► **Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

## IAM Role (EC2 Instance Profile with S3 Read Permissions)

- Go to IAM → Roles → Create Role
- Trusted Entity: AWS Service → EC2
- Attach policy:
  - For full S3 read (lab/demo): `AmazonS3ReadOnlyAccess`
- Name: `iamroleforsep1` (or similar)
- Save role and assign to EC2 at launch

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

IAM Identity Center

AWS Organizations

Roles (5)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	<a href="#">AWSServiceRoleForElasticLoadBalancing</a>	AWS Service: elasticloadbalancing	21 hours ago
<input type="checkbox"/>	<a href="#">AWSServiceRoleForRDS</a>	AWS Service: rds	3 days ago
<input type="checkbox"/>	<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor	-
<input type="checkbox"/>	<a href="#">rds-monitoring-role</a>	AWS Service: monitoring.rds	-

Roles Anywhere

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

IAM > Roles > Create role

Step 1: Select trusted entity

Trusted entity type

☒ AWS service

☐ AWS account

☐ Web identity

☐ SAML 2.0 federation

☐ Custom trust policy

Use case

Service or use case

EC2

Choose a use case for the specified service.

☒ EC2

☐ EC2 Role for AWS Systems Manager

☐ EC2 Spot Fleet Role

☐ EC2 - Spot Fleet Auto Scaling

☐ EC2 - Spot Fleet Tagging

☐ EC2 - Spot Instances

☐ EC2 - Spot Fleet

Step 1: Select trusted entity

Step 2: Add permissions

Permissions policies (1/1073)

Choose one or more policies to attach to your new role.

Filter by Type

amazonS3

All types

8 matches

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	<a href="#">AmazonS3FullAccess</a>	AWS managed	Provides full access to all buckets via the ...
<input type="checkbox"/>	<a href="#">AmazonS3ObjectLambdaExecutionRolePolicy</a>	AWS managed	Provides AWS Lambda functions permissi...
<input type="checkbox"/>	<a href="#">AmazonS3OutpostsFullAccess</a>	AWS managed	Provides full access to Amazon S3 on Out...
<input type="checkbox"/>	<a href="#">AmazonS3OutpostsReadOnlyAccess</a>	AWS managed	Provides read only access to Amazon S3 o...
<input checked="" type="checkbox"/>	<a href="#">AmazonS3ReadOnlyAccess</a>	AWS managed	Provides read only access to all buckets vi...
<input type="checkbox"/>	<a href="#">AmazonS3TablesFullAccess</a>	AWS managed	Provides full access to all S3 table buckets.
<input type="checkbox"/>	<a href="#">AmazonS3TablesLakeFormationServiceRole</a>	AWS managed	This managed policy grants AWS Lake For...
<input type="checkbox"/>	<a href="#">AmazonS3TablesReadOnlyAccess</a>	AWS managed	Provides read only access to all S3 table b...

Set permissions boundary - optional

Cancel

Previous

Next

iam > Roles > Create role

Step 1  
Select trusted entity

Step 2  
Add permissions

Step 3  
Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

iamroleforsepf1

Maximum 64 characters. Use alphanumeric and "+,=,@,-,\_" characters.

Description

Add a short explanation for this role.

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: ".,@-/\_!#\$%&'()\*~+-=,;:'"[]{}|^`"~"

Step 1: Select trusted entities

Edit

Trust policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "sts:AssumeRole"
8       ],
9       "Principal": {
10        "Service": {
11          "ec2.amazonaws.com"
12        }
13      }
14    }
15  ]
16 }
```

Edit

Step 2: Add permissions

Edit

Permissions policy summary

Policy name	Type	Attached as
AmazonS3ReadOnlyAccess	AWS managed	Permissions policy

Step 3: Add tags

Add tags - optional

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create role

# EC2 Instance Setup (Linux + Nginx + AWS CLI)

Launch two EC2 instances with:

- AMI: Amazon Linux 2/2023
- Instance Type: t3.micro (free tier/demo)
- Security Group: Allow TCP 80 (HTTP), 22 (SSH)
- IAM Role: Choose the one created above (e.g. `iamroleforsepl` as in screenshot)

**EC2** > **Instances** > Launch an instance

**Name and tags** [Info](#)

Name:  [Add additional tags](#)

**Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

**Recents** **Quick Start**

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

**Amazon Machine Image (AMI)**

Amazon Linux 2023 kernel-6.1 AMI  
ami-0861f4e788f5069dd (64-bit (x86), uefi-preferred) / ami-0fad8318b9405c6fb (64-bit (Arm), uefi)  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Description**

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.8.20250818.0 x86\_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username
64-bit (x86)	uefi-preferred	ami-0861f4e788f5069dd	2025-08-13	ec2-user

[Verified provider](#)

**Summary**

Number of instances: 1

Software Image: Amazon Linux 2023 kernel-6.1 AMI

Virtual server type: t3.micro

Firewall (security group): New security group

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

[Cancel](#)

EC2 > Instances > Launch an instance

**EC2**

- Dashboard
- EC2 Global View
- Events
- ▼ **Instances**
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity Reservations
- ▼ **Images**
  - AMIs
  - AMI Catalog
- ▼ **Elastic Block Store**
  - Volumes
  - Snapshots
  - Lifecycle Manager
- ▼ **Network & Security**
  - Security Groups
  - Elastic IPs
  - Placement Groups
  - Key Pairs
  - Network Interfaces
- ▼ **Load Balancing**

**t3.micro**  
Family: t3 2 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0112 USD per Hour  
On-Demand SUSE base pricing: 0.0112 USD per Hour On-Demand Windows base pricing: 0.0204 USD per Hour  
On-Demand Ubuntu Pro base pricing: 0.0147 USD per Hour On-Demand RHEL base pricing: 0.04 USD per Hour

Free tier eligible

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ **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*

Harry

Create new key pair

▼ **Network settings** [Info](#) [Edit](#)

**Network** [Info](#)

vpc-099026679a4aa54c6

**Subnet** [Info](#)

No preference (Default subnet in any availability zone)

**Auto-assign public IP** [Info](#)

Enable

**Firewall (security groups)** [Info](#)

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

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-10' with the following rules:

☒ Allow SSH traffic from

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

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

CloudShell Feedback

0 x File systems

**Advanced details** [Info](#)

**Domain join directory** [Info](#)

Select Create new directory

**IAM instance profile** [Info](#)

iamroleforsep1 [Create new IAM profile](#)

**Hostname type** [Info](#)

IP name

**DNS Hostname** [Info](#)

☐ Enable IP name IPv4 (A record) DNS requests  
☒ Enable resource-based IPv4 (A record) DNS requests  
☐ Enable resource-based IPv6 (AAAA record) DNS requests

**Instance auto-recovery** [Info](#)

Select

**Shutdown behavior** [Info](#)

Stop

**Stop - Hibernate behavior** [Info](#)

Select

**Termination protection** [Info](#)

Select

**Summary**

Number of instances [Info](#)

1

**Software image (AMI)**  
Amazon Linux 2023 AMI 2023.8.2...read more  
ami-0861f4c780f5069d0

**Virtual server type (Instance type)**  
t3.micro

**Firewall (security group)**  
New security group

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

Cancel Launch instance Preview code

- User Data (Paste during launch):

```
#!/bin/bash
yum update -y
yum install -y nginx awscli
systemctl enable --now nginx
```

```
# Create web root
```

```
mkdir -p /usr/share/nginx/html
```

```
# Download static assets from S3
```

```
aws s3 cp s3://my-lab-private-static-files/logo.png /usr/share/nginx/html/
```

```
aws s3 cp s3://my-lab-private-static-files/style.css /usr/share/nginx/html/
```

```
# Create dynamic index.html using hostname
```

```
cat <<EOF > /usr/share/nginx/html/index.html
```

```
<!doctype html>
```

```
<html>
```

```
<head>
```

```
<title>EC2 + S3 + IAM Lab</title>
```

```
<link rel="stylesheet" href="style.css">
```

```
</head>
```

```
<body>
```

```
<h1>Hello from $(hostname)</h1>
```

```

```

```
<p>Static files securely served from S3 using IAM Role</p>
```

```
</body>
```

```
</html>
```

```
EOF
```

- Launch both instances in the same VPC/public subnet

Metadata version | Info

V2 only (token required)

⚠ For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.

Metadata response hop limit | Info

2

Allow tags in metadata | Info

Select

User data - optional | Info

Upload a file with your user data or enter it in the field.

Choose file

```
yum update -y
yum install -y nginx awscli
systemctl enable --now nginx
mkdir -p /usr/share/nginx/html
aws s3 cp s3://my-lab-private-static-files1/logo.png /usr/share/nginx/html/
aws s3 cp s3://my-lab-private-static-files1/style.css /usr/share/nginx/html/
cat <<EOF > /usr/share/nginx/html/index.html
<!doctype html>
<html>
<head>
<title>EC2 + S3 + IAM Lab</title>
<link rel="stylesheet" href="style.css">
</head>
<body>
<h1>Hello from $(hostname)</h1>
```

☐ User data has already been base64 encoded

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices.

Take a walkthrough | Do not show me this message again.

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name

ec2z

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

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

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI  
ami-08b1f46788f5069d3 (64-bit (x86), uefi-preferred) / ami-0fad8318b9405c6fb (64-bit (ARM), uefi)  
Virtualization: hvm | ENA enabled: true | Root device type: ebs

Description

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Summary

Number of instances | Info

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.8.2...read more  
ami-08b1f46788f5069d3

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel | Launch instance | Preview code



Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-0861f4e788f5069dd

Publish Date

2025-08-15

Username

ec2-user

Verified provider

▼ Instance type

info | Get advice

Instance type

t3.micro

Free tier eligible

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ 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

Harry

Create new key pair

▼ Network settings

info

Edit

Network

info

vpc-099026679a4aa54c6

Subnet

info

No preference (Default subnet in any availability zone)

Auto-assign public IP

info

Enable

Firewall (security groups)

info

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

EC2 > Instances > Launch an instance

▼ Network settings

info

Edit

Network

info

vpc-099026679a4aa54c6

Subnet

info

No preference (Default subnet in any availability zone)

Auto-assign public IP

info

Enable

Firewall (security groups)

info

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

Create security group

Select existing security group

We'll create a new security group called 'launch-wizard-11' with the following rules:

Allow SSH traffic from

Helps you connect to your instance

Anywhere

0.0.0.0/0

Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ Configure storage

info

Advanced

1x

8

GIB

gp3

Root volume, 3000 IOPS, Not encrypted

Add new volume

Click refresh to view backup information

▼ Summary

info

Number of instances

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.8.2...read more

ami-0861f4e788f5069dd

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

Preview code

0 x File systems

Edit

▼ Advanced details [Info](#)

Domain join directory [Info](#)

Select

Create new directory

IAM instance profile [Info](#)

iamroleforsep1  
arn:aws:iam::395938233552:instance-profile/iamroleforsep1

Create new IAM profile

Hostname type [Info](#)

IP name

DNS Hostname [Info](#)

☒ Enable IP name IPv4 (A record) DNS requests  
☒ Enable resource-based IPv4 (A record) DNS requests  
☐ Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery [Info](#)

Select

Shutdown behavior [Info](#)

Stop

Stop - Hibernate behavior [Info](#)

Select

Termination protection [Info](#)

Select

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.8.2...[read more](#)  
ami-08b1f4c788f5069dcf

Virtual server type (Instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

[Preview code](#)

Metadata version [Info](#)

V2 only (token required)

⚠ For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.

Metadata response hop limit [Info](#)

2

Allow tags in metadata [Info](#)

Select

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

Choose file

```

yum update -y
yum install -y nginx awscli
systemctl enable --now nginx
mkdir -p /usr/share/nginx/html
aws s3 cp s3://my-lab-private-static-files1/logo.png /usr/share/nginx/html/
aws s3 cp s3://my-lab-private-static-files1/style.css /usr/share/nginx/html/
cat <<EOF > /usr/share/nginx/html/index.html
<doctype html>
<html>
<head>
<title>EC2 + S3 + IAM Lab</title>
<link rel="stylesheet" href="style.css">
</head>
<body>
<h1>Hello from $(hostname)</h1>

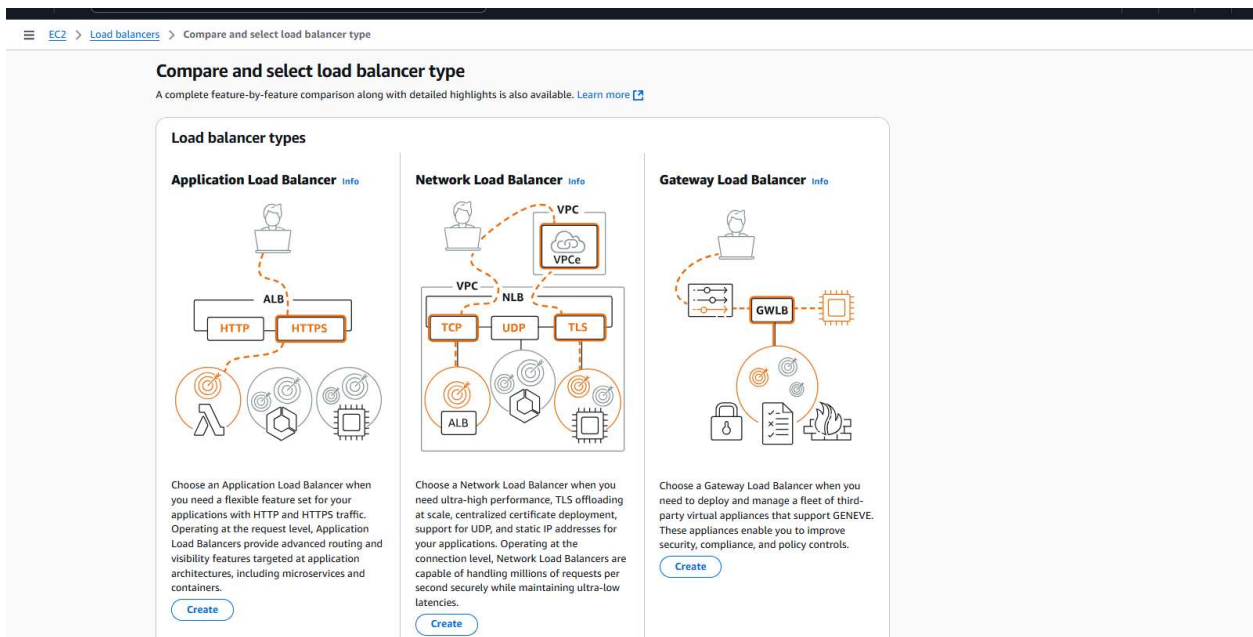
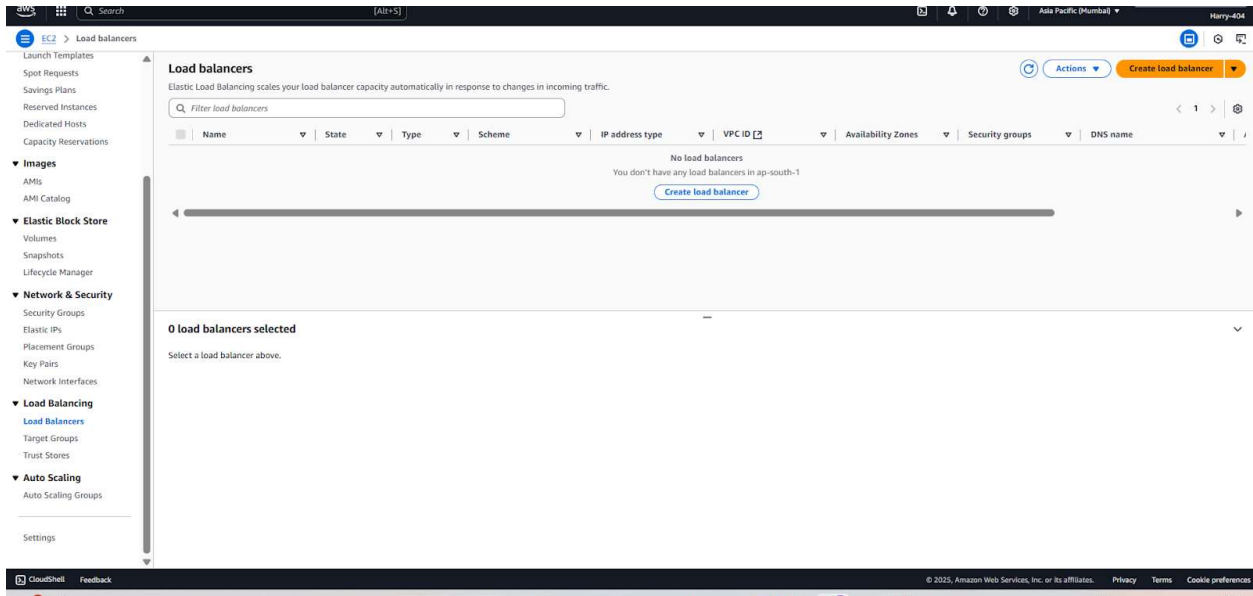
```

☐ User data has already been base64 encoded

## Application Load Balancer (ALB)

- Go to EC2 → Load Balancers → Create Load Balancer
- Type: Application Load Balancer
- Scheme: Internet-facing
- Listener: HTTP (port 80)
- Network mapping: Select at least two subnets in different AZs for HA (as shown in your screenshot)

- Security Groups: Open port 80 inbound
- Target Group: New, Type: Instance, Protocol: HTTP, Port: 80
- Register both EC2 instances as targets
- After creation: Get the DNS name of the ALB (e.g., `alb1-xxxx.ap-south-1.elb.amazonaws.com`)



### 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.

alb1

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.

### 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.

alb1

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



- 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

tg-web-80

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.

#### Port

Port number where targets receive traffic. Can be overridden for individual targets during registration.

#### 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.

- ☒ IPv4
  - Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.
- ☐ IPv6
  - Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

#### VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

vpc-099026679a4aa54c6 (default)

#### Protocol version

- ☒ HTTP1
  - Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
- ☐ HTTP2
  - Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
- ☐ gRPC
  - Send requests to targets using gRPC. Supported when the request protocol is gRPC.

## Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

#### Health check protocol

HTTP

#### Health check path

Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.

/

EC2 > Target groups > Create target group

Step 2  
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)

Filter instances

<input type="checkbox"/>	Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID
<input type="checkbox"/>	i-0fedfb9bb42e22ca6	ec22	Running	launch-wizard-11	ap-south-1a	172.31.34.151	subnet-0b6ce01347fb83f
<input type="checkbox"/>	i-027a27b48e7802c6b	ec2ins	Running	launch-wizard-10	ap-south-1a	172.31.47.177	subnet-0b6ce01347fb83f

0 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

1-65535 (separate multiple ports with commas)

Include as pending below

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

Review targets

Targets (2)

Filter targets

Show only pending

Remove all pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-0fedfb9bb42e22ca6	ec22	80	Running	launch-wizard-11	ap-south-1a	172.31.34.151	subnet-0b6ce01347fb83f	September 1, 2025, 12:44 (UTC+05:30)
i-027a27b48e7802c6b	ec2ins	80	Running	launch-wizard-10	ap-south-1a	172.31.47.177	subnet-0b6ce01347fb83f	September 1, 2025, 12:34 (UTC+05:30)

EC2 > Target groups > tg-web-80

EC2

Dashboard

EC2 Global View

Events

Instances

Instances Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

tg-web-80

Actions

Details

arn:aws:elasticloadbalancing:ap-south-1:395938233352:targetgroup/tg-web-80/9988fdb943cee83

Target type

Instance

Protocol : Port

HTTP: 80

Protocol version

HTTP1

VPC

vpc-099026679a4aa54c6

IP address type

IPv4

Load balancer

None associated

2

Total targets

0

Healthy

0

Unhealthy

2

Unused

0

Initial

0

Draining

Distribution of targets by Availability Zone (AZ)

Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets

Monitoring

Health checks

Attributes

Tags

Registered targets (2)

Anomaly mitigation: Not applicable

Deregister

Register targets

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Filter targets

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Administrative override	Override details
<input type="checkbox"/>	i-0fedfb9bb42e22ca6	ec22	80	ap-south-1a (a...	Unused	Target group is not co...	-	-
<input type="checkbox"/>	i-027a27b48e7802c6b	ec2ins	80	ap-south-1a (a...	Unused	Target group is not co...	-	-

**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**  
HTTP

**Port**  
80  
1-65535

**Default action** info  
Forward to tg-web-80  
Target type: Instance, IPv4  
HTTP

[Create target group](#)

**Listener tags - optional**

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

[Add listener tag](#)

You can add up to 50 more tags.

[Add listener](#)

You can add up to 49 more listeners.

**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.

EC2

Load balancers

alb1

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups

Trust Stores

Auto Scaling

Successfully created load balancer: alb1

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.

alb1

Actions

Details

Load balancer type

Application

Status

Provisioning

VPC

vpc-099026679a4aa54c6

Load balancer IP address type

IPv4

Scheme

Internet-facing

Hosted zone

ZP97RAFLXTNZK

Availability Zones

subnet-0b6ce01347fb83f6d

ap-south-1a (aps1-a21)

subnet-0a6950512b0783fb91

ap-south-1c (aps1-a22)

subnet-0f6c157912b4a9650

ap-south-1b (aps1-a25)

Date created

September 1, 2025, 13:00 (UTC+05:30)

Load balancer ARN

arn:aws:elasticloadbalancing:ap-south-1:39593823352:loadbalancer:app/alb1/b85212008cf0c11e

DNS name

alb1-158734687.ap-south-1.elb.amazonaws.com (A Record)

Listeners and rules

Network mapping

Resource map

Security

Monitoring

Integrations

Attributes

Capacity

Tags

Listeners and rules (1)

Manage rules

Manage listener

Add listener

Filter listeners

Protocol:Port

Default action

Rules

ARN

Security policy

Default SSL/TLS certificate

mTLS

Trust store

HTTP:80

Forward to target group

tg-web-80 (2: 1 (100%))

Target group stickiness: Off

1 rule

ARN

Not applicable

Not applicable

Not applicable

Not applicable

Test

- Open the ALB DNS in your browser:
  - Should display "Hello from ..." with each EC2 instance’s hostname when refreshed
  - logo.png and styling should load (fetched from S3 privately, thanks to EC2 IAM role)—no public S3 access!



Hello from ip-172-31-34-151.ap-south-1.compute.internal



Static files securely served from S3 using IAM Role

## Summary Table: Location and Usage

Step	File Needed	AWS Service	Config/Code	Purpose
S3 Storage	logo.png, style.css	S3	Upload to bucket, block public	Secure static assets
IAM Role	None	IAM	S3 GetObject policy	Least-privilege EC2 S3 access
EC2 UserData	logo.png, style.css	EC2	aws s3 cp, HTML snippet	Serve dynamic/static web content
HTML Output	logo.png	Nginx	<pre>&lt;img src="logo.png" ...&gt;</pre>	Display image on index.html