

- Step 1: create a S3 bucket with no public access.

Step 2 : Click add files → select files→ Click open to upload the files.

[Amazon S3](#) > [Buckets](#) > [guvi-s3-task](#)

guvi-s3-task

[info](#)

[Objects](#)

[Properties](#)

[Permissions](#)

[Metrics](#)

[Management](#)

[Access Points](#)

Permissions overview

Access

[Bucket and objects not public](#)

Block public access (bucket settings)

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 all your S3 buckets and objects is disabled, turn on all settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your app.

Block all public access

On

Individual Block Public Access settings for this bucket

Public access is blocked for the S3 bucket.

2. Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address

Step 1 : create two Ec2 instances with User data for installing apache web server

EC2 > Instances > Launch an instance

Launch an instance

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

Name and tags

Name

Web_Server1

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE L

Browse more AMIs

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-03f487875434977f (64-bit x86) / ami-077885f99cb77b84 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-12-07

Architecture

AMI ID

ami-03f487875434977f

Verified provider

Specify CPU options

The selected instance type does not support CPU options.

Metadata accessible

Enabled

Metadata transport

Select

Metadata version

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

2

Allow tags in metadata

Select

User data - optional

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

Choose file

```
#!/bin/bash
apt-get update
apt-get install -y apache2
systemctl start apache2
systemctl enable apache2
```

☐ User data has already been base64 encoded

EC2 > Instances > Launch an instance

Launch an instance

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

Name and tags

Name

Web_Server2

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE L

Browse more AMIs

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-03f487875434977f (64-bit x86) / ami-077885f99cb77b84 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-12-07

Architecture

AMI ID

ami-03f487875434977f

Verified provider

Select

Specify CPU options

The selected instance type does not support CPU options.

Metadata accessible

Enabled

Metadata transport

Select

Metadata version

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

2

Allow tags in metadata

Select

User data - optional

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

Choose file

```
#!/bin/bash
apt-get update
apt-get install -y apache2
systemctl start apache2
systemctl enable apache2
```

☐ User data has already been base64 encoded

Step 5 : select both instances → click include Pending → create target group.

The screenshot shows the 'Register targets' step in the AWS Management Console. It displays a list of available EC2 instances and a 'Review targets' section where two instances are selected and added to the target group. The 'Registered targets' table shows the following details:

Instances	Name	Size	Port	State	Security group	Zone	Private IP address	Subnet ID	Launch time
1	i-026227b7b0a	M5_Smallest	80	Pending	launch-wizard-1	ap-south-1a	172.31.41.16	subnet-00b7123d1f16217c	January 21, 2024, 10:03:54
2	i-01778b0a388a4	M5_Smallest	80	Pending	launch-wizard-1	ap-south-1a	172.31.32.17	subnet-00b7123d1f16217c	January 21, 2024, 10:03:54

Step 6: create Application load balancer → select newly created target group → click create load balancer

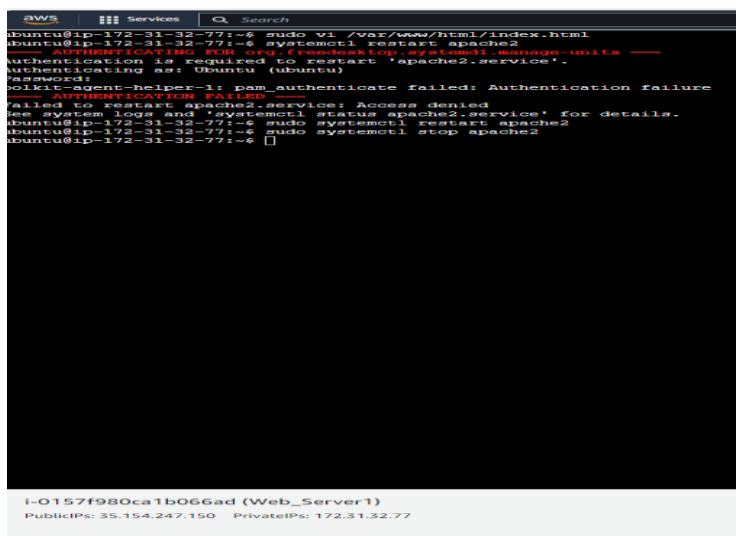
The screenshot shows the 'Create Application Load Balancer' wizard in the AWS Management Console. It includes the following sections:

- Basic configuration:** Load balancer name (WEB-ALB), Scheme (Internet-facing), IP address type (IPv4), and Network mapping (VPC).
- Security groups:** Launch-wizard-1.
- Listeners and routing:** HTTP-80 listener configured to forward traffic to the target group.
- Add-on services:** AWS Global Accelerator.
- Tags:** None.
- Summary:** Overview of the configuration.

Step 7: Use the Load balancer DNS name to in browser to check the web application



Step 8 : stop web server in server 1 .



Step 9: refresh the browser and check the status the web application.

