

**aws**

**S3 and ELB**

---

# Create a S3 Bucket

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name Info

myawsbucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

aws Services Search [Alt+S]

Successfully created bucket "gokul-sm-test"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

General purpose buckets

Directory buckets

General purpose buckets (1) Info

Refresh

Copy ARN

Empty

Delete

Create bucket

Find buckets by name

Name	AWS Region	Access	Creation date
<input type="radio"/> gokul-sm-test	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 13, 2024, 11:04:30 (UTC+05:30)

# With No Public Access

awsServicesSearch[Alt+S]

Amazon S3gokul-sm-testCreate access point

Create access pointInfo

Amazon S3 Access points simplify managing data access at scale for shared datasets in S3. Access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations. [Learn more](#)

Properties

Access point name  
accesspoint  
Access point names must be unique within the account for this Region and comply with the [rules for access point naming](#).

Bucket name  
gokul-sm-test

AWS Region  
Region is determined by the bucket's location.  
Asia Pacific (Mumbai) ap-south-1

Network origin  
☒ Virtual private cloud (VPC)  
No internet access. Requests are made over a specified VPC only.  
☐ Internet

The S3 console doesn't support accessing bucket resources using a virtual private cloud (VPC) access point. To access bucket resources from a VPC access point, use the AWS CLI, AWS SDK, or Amazon S3 REST API. [Learn more](#)

VPC ID  
vpc-  
VPC ID must start with vpc-

Block Public Access settings for this Access Point

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. These settings apply only to this Access Point. Before applying these settings, ensure that your applications will work correctly without public access. These settings can't be edited after the Access Point is created. [Learn more](#)

☒ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☒ Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☒ Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☒ Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☒ Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

awsServicesSearch[Alt+S]

point, use the AWS CLI, AWS SDK, or Amazon S3 REST API. [Learn more](#)

VPC ID  
vpc-  
VPC ID must start with vpc-

Block Public Access settings for this Access Point

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. These settings apply only to this Access Point. Before applying these settings, ensure that your applications will work correctly without public access. These settings can't be edited after the Access Point is created. [Learn more](#)

☒ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☒ Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☒ Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☒ Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☒ Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.


Access Point policy - optional

The Access Point policy, written in JSON, provides access to the objects stored in the bucket from this Access Point. Access Point policies don't apply to objects owned by other accounts. [Learn more](#)

Policy examples


No internet access. Requests are made over a specified VPC only.

☐ Internet




The S3 console doesn't support accessing bucket resources using a virtual private cloud (VPC) access point. To access bucket resources from a VPC access point, use the AWS CLI, AWS SDK, or Amazon S3 REST API. [Learn more](#)





VPC ID



VPC ID must not be empty

VPC ID must start with vpc-

 Services  [Alt+S]

    Global  gokul

Successfully created access point "test-assess".

[Amazon S3](#) > [Buckets](#) > gokul-sm-test

## gokul-sm-test

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

### Access Points (1)

Amazon S3 Access Points simplify managing data access at scale for shared datasets in S3. Access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations. An Access Point alias provides the same functionality as an Access Point ARN and can be substituted for use anywhere an S3 bucket name is normally used for data access. [Learn more](#)

1

	Name	Network origin	Access	Bucket owner account ID	Access Point alias
<input type="radio"/>	test-assess	Virtual private cloud (VPC)	VPC (ID: vpc-05fbffcb1fb9c1a33)	488546547125	test-assess-91cjr8jfsbbwyiadufhf9ti76ofyaps3a-s3alias

Amazon S3 > Access Points > test-assess

test-assess

Objects | Properties | Permissions

Permissions overview

Access

VPC (ID: vpc-05fbffcb1fb9c1a33)

Block Public Access settings for this Access Point

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. These settings apply only to this Access Point. Before applying these settings, ensure that your applications will work correctly without public access. These settings can't be edited after the Access Point is created. [Learn more](#)

Block all public access

On

Block public access to buckets and objects granted through new access control lists (ACLs)

On

Block public access to buckets and objects granted through any access control lists (ACLs)

On

Block public access to buckets and objects granted through new public bucket or access point policies

On

Block public and cross-account access to buckets and objects through any public bucket or access point policies

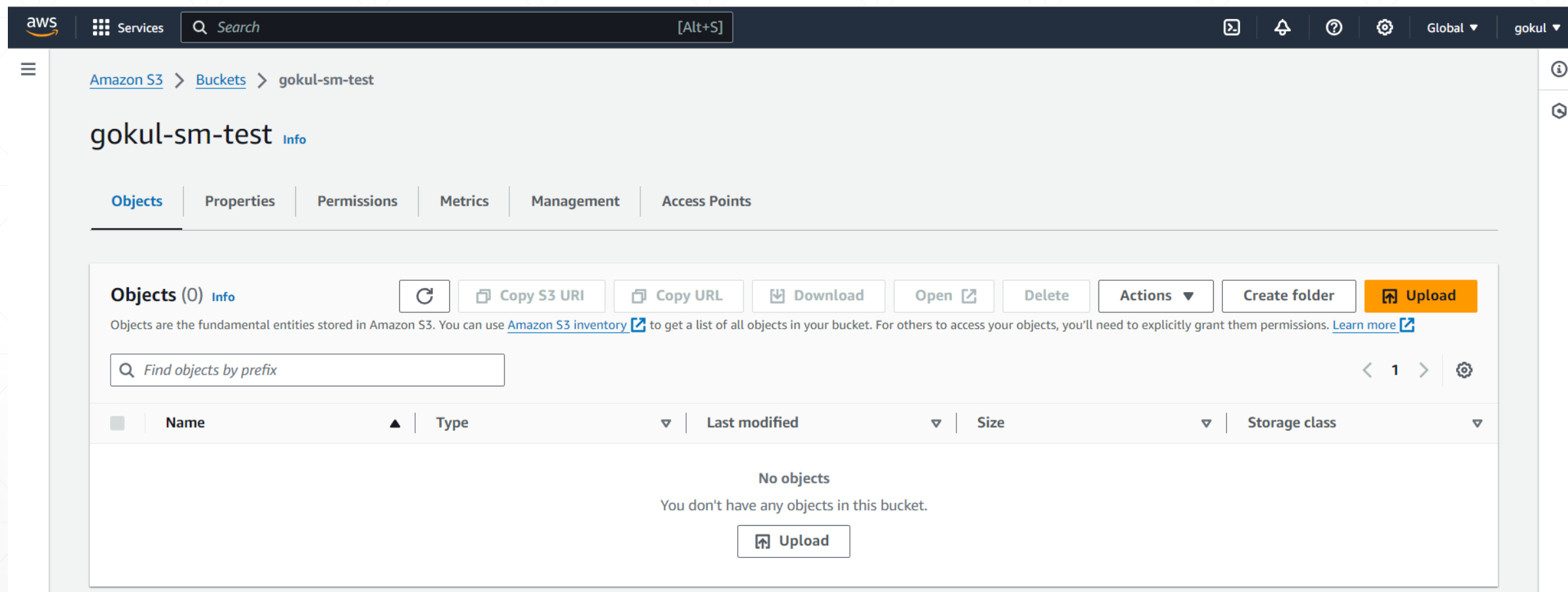
On

Access Point policy

The Access Point policy, written in JSON, provides access to the objects stored in the bucket from this Access Point. Access Point policies don't apply to objects owned by other accounts. [Learn more](#)

EditDelete

# Upload Files To The Bucket



aws

Services

Search

[Alt+S]

Amazon S3 > Buckets > gokul-sm-test > Upload

Upload

Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 40.0 B)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	token.txt	-	text/plain

Destination

Info

Destination

s3://gokul-sm-test

► Destination details

Bucket settings that impact new objects stored in the specified destination.

► Permissions


Grant public access and access to other AWS accounts.

► Properties

Specify storage class, encryption settings, tags, and more.


Cancel

Upload

 Upload succeeded  
View details below.


## Upload: status


Close

 The information below will no longer be available after you navigate away from this page.

### Summary

Destination  
[s3://gokul-sm-test](#)

Succeeded  
 1 file, 40.0 B (100.00%)


Failed  
 0 files, 0 B (0%)

Files and folders | Configuration

### Files and folders (1 Total, 40.0 B)

 Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
token.txt	-	text/plain	40.0 B	 Succeeded	-



**Two ec2-instances And Connect It to a Application Load Balancer**

---

**“Create ec2-instances”**

---



Network

Info

vpc-098c718272cf3dfc7

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-8' 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 (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Summary

Number of instances

Info

2

When launching more than 1 instance, consider EC2 Auto Scaling

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-0449c34f967dbf18a

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 includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

Review commands

EC2 > Instances > Launch an instance

Success  
Successfully initiated launch of instances (i-0a6a1d3dd1f9a0e89, i-0638788680cab1226)

Launch log

Next Steps

What would you like to do next with these instances, for example "create alarm" or "create backup"

< 1 2 3 4 >

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Create billing alerts

Connect to your instance

Once your instance is running, log into it from your local computer.

Learn more

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Connect an RDS database

Create a new RDS database

Learn more

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

Create EBS snapshot policy

Manage detailed monitoring

Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

Manage detailed monitoring

Create Load Balancer

Create a application, network gateway or classic Elastic Load Balancer

Create Load Balancer

Create AWS budget

AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

Create AWS budget

Manage CloudWatch alarms

Create or update Amazon CloudWatch alarms for the instance.

Manage CloudWatch alarms

Disaster recovery for your instances

Recover the instances you just launched into a different Availability Zone or a different Region using AWS Elastic Disaster Recovery (DRS).

Get instance screenshot

Capture a screenshot from the instance and view it as an image. This is useful for troubleshooting an unreachable instance.

Get instance screenshot

Get system log

View the instance's system log to troubleshoot issues.

Get system log

Change shutdown behavior

Change the behavior of the instance for when you initiate a shutdown from the operating system of the instance itself.

Change shutdown behavior

EC2 Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

New

Images

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Instances (2) Info

Find Instance by attribute or tag (case-sensitive)

Running

Name

Instance ID

Instance state

Instance type

Status check

Alarm status

Availability Zone

Public IPv4 DNS

Public IPv4 ...

Elastic IP

IPv6 IPs

TEST-ELB 1

i-0638788680cab1226

Running

t2.micro

Initializing

View alarms

+

ap-south-1b

ec2-3-110-218-207.ap-...

3.110.218.207

-

-

TEST-ELB 2

i-0a6a1d3dd1f9a0e89

Running

t2.micro

Initializing

View alarms

+

ap-south-1b

ec2-3-110-122-47.ap-s...

3.110.122.47

-

-

Select an instance

**“Create application load balancer”**

---

- ▼ Instances
- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations
- [New](#)
- Images
- ▼ 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 [New](#)
- ▼ Auto Scaling
- Auto Scaling Groups

[EC2](#) > Load balancers

### Load balancers

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

	Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
--	------	----------	-------	--------	--------------------	------	--------------

No load balancers

You don't have any load balancers in ap-south-1

Create load balancer

0 load balancers selected

Select a load balancer above.



# 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.

TEST-ZEN

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
- An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)
- ☐ Internal
- An internal load balancer routes requests from clients to targets using private IP addresses.

#### IP address type

Info

Select the type of IP addresses that your subnets use.

- ☒ IPv4
- Recommended for internal load balancers.
- ☐ Dualstack
- Includes IPv4 and IPv6 addresses.

### Network mapping

Info

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

#### VPC

Info

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

-

vpc-098c718272cf3dfc7



- ☒ **IPv4**  
Recommended for internal load balancers.
- ☐ **Dualstack**  
Includes IPv4 and IPv6 addresses.

## Network mapping [Info](#)

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

## VPC | Info

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, [view your target groups](#).

vpc-098c718272cf3dfc7  
IPv4: 172.31.0.0/16

Mappings

Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

- ✓ ap-south-1a (aps1-az1)

Subnet

subnet-0bd2646db75e74b91

IPv4 address

Assigned by AWS

☒ ap-south-1b (aps1-az3)

Subnet

subnet-02f76120e48c2b819

IPv4 address

Assigned by AWS

☐ ap-south-1c (aps1-az2)

## Security groups [Info](#)

**“Create Security Groups”**

---

# Create security group

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

MyWebServerGroup

Name cannot be edited after creation.

Description

Allows SSH access to developers

VPC

vpc-098c718272cf3dfc7

Inbound rules

This security group has no inbound rules.

Add rule

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	
				Delete



## 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](#)

TEST-ELB

Name cannot be edited after creation.

Description [Info](#)

allows ssh access to developers

VPC [Info](#)

vpc-098c718272cf3dfc7

### Inbound rules [Info](#)

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

Source [Info](#)

Description - optional

All TCP

TCP

0 - 65535

Anywhere-I...

0.0.0.0/0

Delete

0.0.0.0/0 X

All UDP

UDP

0 - 65535

Anywhere-I...

0.0.0.0/0

Delete

0.0.0.0/0 X

Add rule



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

### Outbound rules [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Destination <a href="#">Info</a>	Description - optional
HTTP	TCP	80	Anywhere-I... 0.0.0.0/0	<div>0.0.0.0/0 ✕</div>
All TCP	TCP	0 - 65535	Anywhere-I... 0.0.0.0/0	<div>0.0.0.0/0 ✕</div>

Add rule

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

### Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags

Cancel

Create security group

Security group (sg-0836cef1da03ef7e5 | TEST-ELB) was created successfully

Details

EC2 > Security Groups > sg-0836cef1da03ef7e5 - TEST-ELB

sg-0836cef1da03ef7e5 - TEST-ELB

Actions

Details

Security group name

TEST-ELB

Security group ID

sg-0836cef1da03ef7e5

Description

allows ssh access to developers

VPC ID

vpc-098c718272cf3dfc7

Owner

488546547125

Inbound rules count

2 Permission entries

Outbound rules count

2 Permission entries

Inbound rules

Outbound rules

Tags

Inbound rules (2)

Search

Manage tags

Edit inbound rules

< 1 >

	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-0ca66e219002b9b...	IPv4	All UDP	UDP	0 - 65535	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-02a688acc96348be6	IPv4	All TCP	TCP	0 - 65535	0.0.0.0/0	-

☐ ap-south-1c (aps1-az2)

### 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



TEST-ELB

sg-0836cef1da03ef7e5 VPC: vpc-098c718272cf3dfc7



default

sg-0c411a968aa75565f VPC: vpc-098c718272cf3dfc7



### 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

Select a target group

[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



**“Create Target groups”**

---

# 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

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

# 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

< 1 >

	Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID
<input type="checkbox"/>	i-0638788680cab1226	TEST-ELB 1	Running	launch-wizard-8	ap-south-1b	172.31.14.245	subnet-02
<input type="checkbox"/>	i-0a6a1d3dd1f9a0e89	TEST-ELB 2	Running	launch-wizard-8	ap-south-1b	172.31.5.14	subnet-02

0 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Include as pending below

Review targets

Targets (0)

Filter targets

Show only pending

Remove all pending

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



Ports for the selected instances  
Ports for routing traffic to the selected instances.

1-65535 (separate multiple ports with commas)

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

### Targets (2)

🔍 *Filter targets*

< 1 > 

▲

Cancel

[Previous](#)

### Create target group



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

Details

arn:aws:elasticloadbalancing:ap-south-1:488546547125:targetgroup/TEST-ELB-GP/009eb315e29cbaa0

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC <a href="#">vpc-098c718272cf3dfc7</a>		
IP address type IPv4	Load balancer <a href="#">None associated</a>				

2  
Total targets

✔️ 0  
Healthy

0 Anomalous

❌ 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) Info

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

< 1 > ⚙️

<input type="checkbox"/>	Instance ID ▾	Name ▾	Port ▾	Zone ▾	Health status ▾	Health status details
<input type="checkbox"/>	<a href="#">i-0638788680cab1226</a>	TEST-ELB 1	80	ap-south-1b	⏸️ Unused	Target group is not configured to receive traffic from the load balancer
<input type="checkbox"/>	<a href="#">i-0a6a1d3dd1f9a0e89</a>	TEST-ELB 2	80	ap-south-1b	⏸️ Unused	Target group is not configured to receive traffic from the load balancer

ap-south-1c (aps1-az2)

### 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



TEST-ELB

sg-0836cef1da03ef7e5 VPC: vpc-098c718272cf3dfc7



default

sg-0c411a968aa75565f VPC: vpc-098c718272cf3dfc7



### 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

TEST-ELB-GP

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

Review

Review the load balancer configurations and make changes if needed. After you finish reviewing the configurations, choose **Create load balancer**.

Summary

Review and confirm your configurations. [Estimate cost](#)

Basic configuration

TEST-ZEN

- Internet-facing
- IPv4

Security groups

- TEST-ELB
  - [sg-0836cef1da03ef7e5](#)
  - default
    - [sg-0c411a968aa75565f](#)

Network mapping

VPC [vpc-098c718272cf3dfc7](#)

- ap-south-1a
  - [subnet-0bd2646db75e74b91](#)
- ap-south-1b
  - [subnet-02f76120e48c2b819](#)

Listeners and routing

- HTTP:80 defaults to [TEST-ELB-GP](#)

Service integrations

AWS WAF: None

AWS Global Accelerator: None

Tags

None

Attributes

Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Creation workflow and status

► Server-side tasks and status

After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.

Cancel

Create load balancer



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

✔ Successfully created load balancer: TEST-ZEN

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.

EC2

>

Load balancers

>

TEST-ZEN

TEST-ZEN

Actions

Details

Load balancer type

Application

Status

Provisioning

VPC

vpc-098c718272cf3dfc7

IP address type

IPv4

Scheme

Internet-facing

Hosted zone

ZP97RAFLXTNZK

Availability Zones

subnet-02f76120e48c2b819 ap-south-1b (aps1-az3)

subnet-0bd2646db75e74b91 ap-south-1a (aps1-az1)

Date created

February 13, 2024, 23:31 (UTC+05:30)

Load balancer ARN

arn:aws:elasticloadbalancing:ap-south-1:488546547125:loadbalancer/app/TEST-ZEN/b65602c5d40118e5

DNS name

TEST-ZEN-327329226.ap-south-1.elb.amazonaws.com (A Record)

- Listeners and rules
- Network mapping
- Security
- Monitoring
- Integrations
- Attributes
- Tags

Listeners and rules (1)

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.

Filter listeners

Protocol:Port

Default action

Rules

ARN

Security policy

Default SSL/TLS certificate

mTLS

Trust store

HTTP:80

Forward to target group

- TEST-ELB-GP: 1 (100%)
- Group-level stickiness: Off

1 rule

ARN

Not applicable

Not applicable

Not applicable

Not applicable

aws

Services

Search

[Alt+S]

Mumbai

gokul

EC2 Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

New

Images

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

EC2 > Load balancers

Load balancers (1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

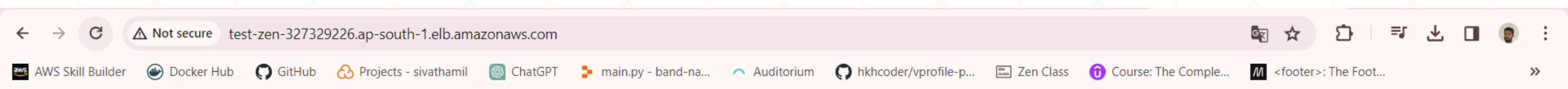
Filter load balancers

< 1 >

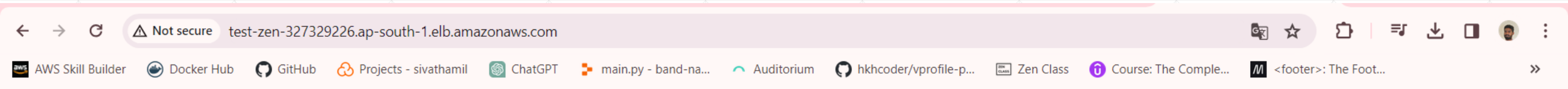
	Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
	TEST-ZEN	TEST-ZEN-327329226.ap-...	Active	vpc-098c718272cf3dfc7	2 Availability Zones	application	February 13, 2024, 23:31 (UTC+05:30)

0 load balancers selected

Select a load balancer above.



**ZEN CLASS ip-172-31-14-245.ap-south-1.compute.internal**



**ZEN CLASS ip-172-31-5-14.ap-south-1.compute.internal**

***Thank You ..***