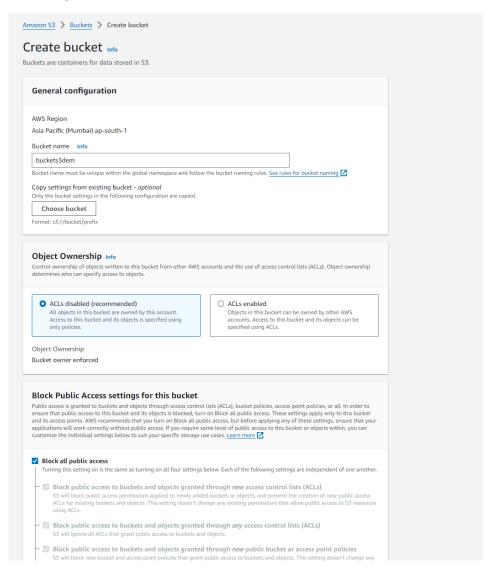# 1.Creating S3 Bucket with No Public Access

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

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

Bucket name Info

buckets3dem

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

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 on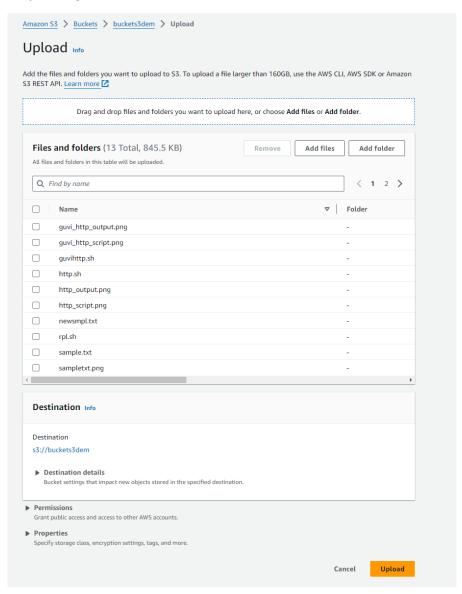ly to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. 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

2.S3 Bucket Created

Successfully created bucket "buckets3dem"
To upload files and folders, or to configure additional bucket settings, choose View details.

View details ✕

Amazon S3 > Buckets

▶ Account snapshot All AWS Regions
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 All AWS Regions
Buckets are containers for data stored in S3.

⟳ | Copy ARN | Empty | Delete | **Create bucket**

Q Find buckets by name

< 1 > ⚙

	Name ▲	AWS Region ▽	IAM Access Analyzer	Creation date ▽
●	buckets3dem	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	April 30, 2024, 19:02:45 (UTC+05:30)

3.Bucket file Uploading page

Amazon S3 > Buckets > buckets3dem

buckets3dem Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (0) Info
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

⟳ | Copy S3 URI | Copy URL | Download | Open | Delete | Actions ▼ | Create folder | **Upload**

Q Find objects by prefix

< 1 > ⚙

	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽

No objects
You don't have any objects in this bucket.

Upload

4.Uploading Files in S3 Bucket

Amazon S3 > Buckets > buckets3dem > 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 (13 Total, 845.5 KB)

Remove   Add files   Add folder

All files and folders in this table will be uploaded.

Find by name   < **1** 2 >

☐	Name ▽	Folder
☐	guvi_http_output.png	-
☐	guvi_http_script.png	-
☐	guvihttp.sh	-
☐	http.sh	-
☐	http_output.png	-
☐	http_script.png	-
☐	newsmpl.txt	-
☐	rpl.sh	-
☐	sample.txt	-
☐	sampletxt.png	-

Destination Info

Destination

s3://buckets3dem

▶ 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

5.Files Uploaded to S3 Bucket

Summary

Destination	Succeeded	Failed
s3://buckets3dem	⊘ 13 files, 845.5 KB (100.00%)	⊘ 0 files, 0 B (0%)

Files and folders   Configuration

Files and folders (13 Total, 845.5 KB)

Find by name

Name	Folder ▽	Type ▽	Size ▽	Status ▽	Error
guvi_http_o...	-	image/png	60.4 KB	⊘ Succeeded	-
guvi_http_s...	-	image/png	59.1 KB	⊘ Succeeded	-
guvihttp.sh	-	text/x-sh	258.0 B	⊘ Succeeded	-
http.sh	-	text/x-sh	217.0 B	⊘ Succeeded	-
http_output...	-	image/png	58.8 KB	⊘ Succeeded	-
http_script....	-	image/png	52.5 KB	⊘ Succeeded	-
newsmpl.txt	-	text/plain	1.1 KB	⊘ Succeeded	-
rpl.sh	-	text/x-sh	111.0 B	⊘ Succeeded	-
sample.txt	-	text/plain	1.1 KB	⊘ Succeeded	-
sampletxt.png	-	image/png	93.9 KB	⊘ Succeeded	-

6.No Public Access for the Bucket we created

Amazon S3 > Buckets > buckets3dem

buckets3dem Info

Objects | Properties | **Permissions** | Metrics | Management | Access Points

---

Permissions overview

Access
View analyzer for ap-south-1

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 blocked, turn on Block all public access. 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 specific storage use cases. Learn more

Block *all* public access
⊘ On
▶ Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

ⓘ **Public access is blocked because Block Public Access settings are turned on for this bucket**
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

No policy to display.

7.Enabling Server Access Logging details

Amazon S3 > Buckets > buckets3dem > Edit server access logging

Edit server access logging Info

Server access logging
Log requests for access to your bucket. Learn more

Server access logging
○ Disable
● Enable

⚠ **Bucket policy will be updated**
When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.

Destination
Specify a destination bucket in the Asia Pacific (Mumbai) ap-south-1 Region. To store your logs under a particular prefix, make sure that you include a slash (/) after the name of the prefix. Otherwise, the prefix will be added to the name of your log files.

`s3://buckets3dem`   [Browse S3]

Format: s3://<bucket>/<optional-prefix-with-path>

Destination Region
Asia Pacific (Mumbai) ap-south-1

Destination bucket name
buckets3dem

Destination prefix
-

ⓘ When your source bucket and target bucket are the same, additional logs are created for the logs that are written to the bucket. These extra logs can increase your storage billing and make it harder to find the logs that you're looking for.

Log object key format
● [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
○ [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/
[DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
To speed up analytics and query applications, use this format.

Log object key example
2024-07-01-10-12-56-[UniqueString]

[Cancel] [**Save changes**]

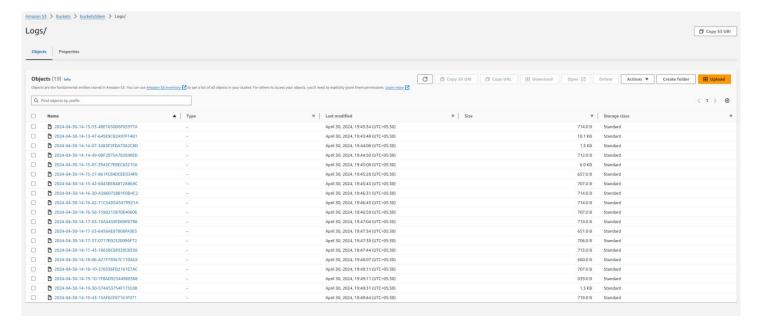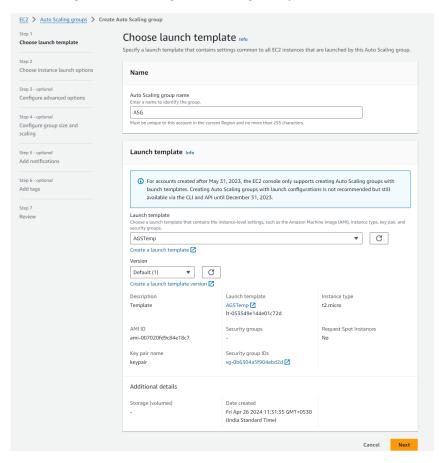## 8. Created New Folder and Moved the files to the folder

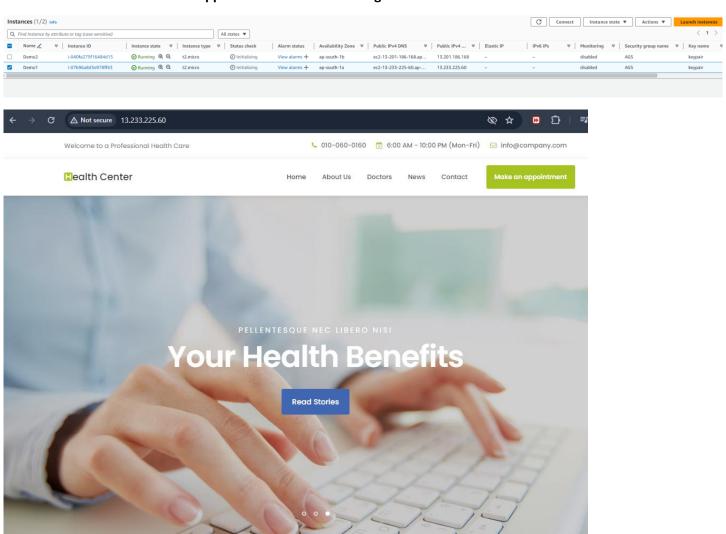## 9.Created Logs Folder for Logs Files to be stored in Logs folder
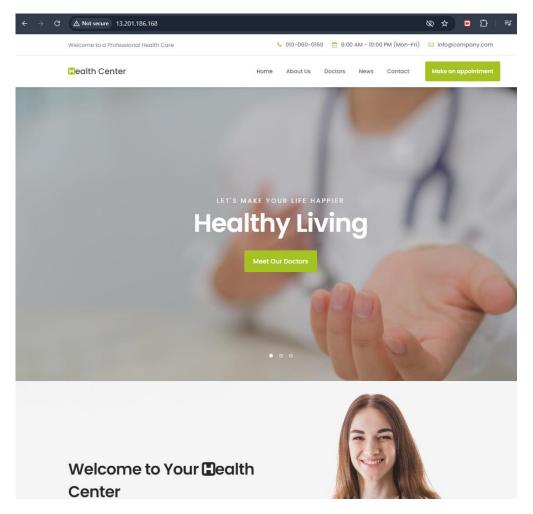

10. Logs files stored separately in Logs Folder
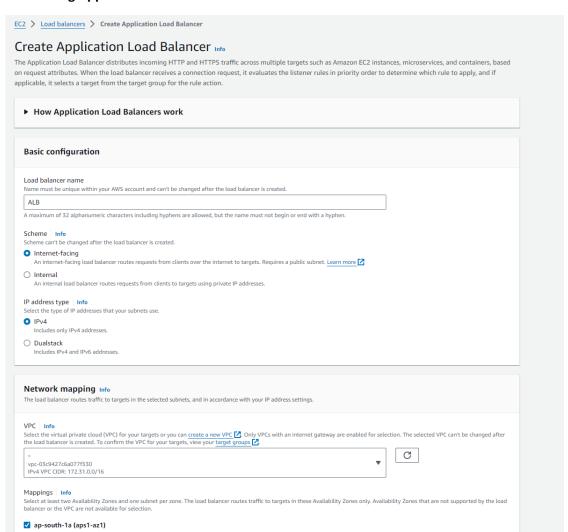
11. Creating Instances using Auto Scaling Group

12. Two instances Created with Applications. Both are running in Different IP
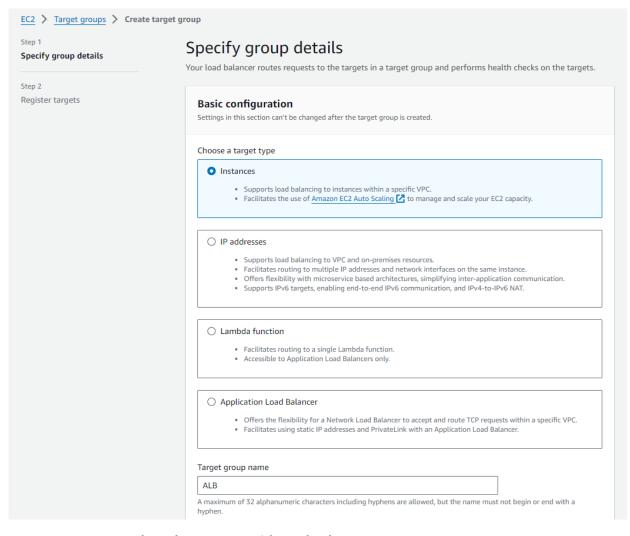
13.Creating Applications Load Balancer

EC2 > Load balancers > Create Application Load Balancer

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.

```
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
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
Includes only IPv4 addresses.

⚪ 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-03c9427c6a077f330                                    ▼
IPv4 VPC CIDR: 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)**

14. Creating Target Group for App Load Balancer

EC2 > Target groups > Create target group

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

ALB

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

15.Target Instances selected to connect with Load Balancer

EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

Register targets

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

Available instances (2/2)

Filter instances

< 1 > ⚙

	Instance ID ▽	Name ▽	State
☑	i-040fa275f16484d15	Demo2	⊘ Running
☑	i-07b96a8d3e978ff43	Demo1	⊘ Running

2 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

16. Two Instances initialized and Running Healthy in Target Group

✓ 2 targets registered successfully to ALB.   ✕

EC2 > Target groups > ALB

ALB   [Actions ▼]

Details
🗋 arn:aws:elasticloadbalancing:ap-south-1:339712699389:targetgroup/ALB/e9d5fe7bd5b2c270

Target type	Protocol : Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-03c9427c6a077f330 ↗
IP address type	**Load balancer**		
IPv4	ⓘ None associated		

2	⊘ 2	⊗ 0	⊖ 0	⊕ 0	⊖ 0
Total targets	Healthy	Unhealthy	Unused	Initial	Draining
	0 Anomalous				

▶ **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 >   ⚙

☐	Instance ID ▽	Name ▽	Port ▽	Zone ▽	Health status ▽	Health status details	Launch... ▲	Anomaly detection result ▽
☐	i-040fa275f16484d15	Demo2	80	ap-south-1b	⊘ Healthy	-	April 30, 2...	⊘ Normal
☐	i-07b96a8d3e978ff43	Demo1	80	ap-south-1a	⊘ Healthy	-	April 30, 2...	⊘ Normal

17. Summary of App Load Balancer .Both Instances are connected with Load Balancer by Target Group

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 Edit

ALB
- Internet-facing
- IPv4

Security groups Edit
- AGS
  sg-0b6304a5f904ebd2d ↗

Network mapping Edit

VPC vpc-03c9427c6a077f330 ↗
- ap-south-1a
  subnet-0ec72037d1a5511ff ↗
- ap-south-1b
  subnet-03a4e3762c3961ada ↗
- ap-south-1c
  subnet-05a6cce13c7248957 ↗

Listeners and routing Edit
- HTTP:80 defaults to
  ALB ↗

Service integrations Edit

AWS WAF: *None*
AWS Global Accelerator: *None*

Tags Edit

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**]

18. App Load Balancer is Running

19.Application Output traffics from the server to Load Balancer IP