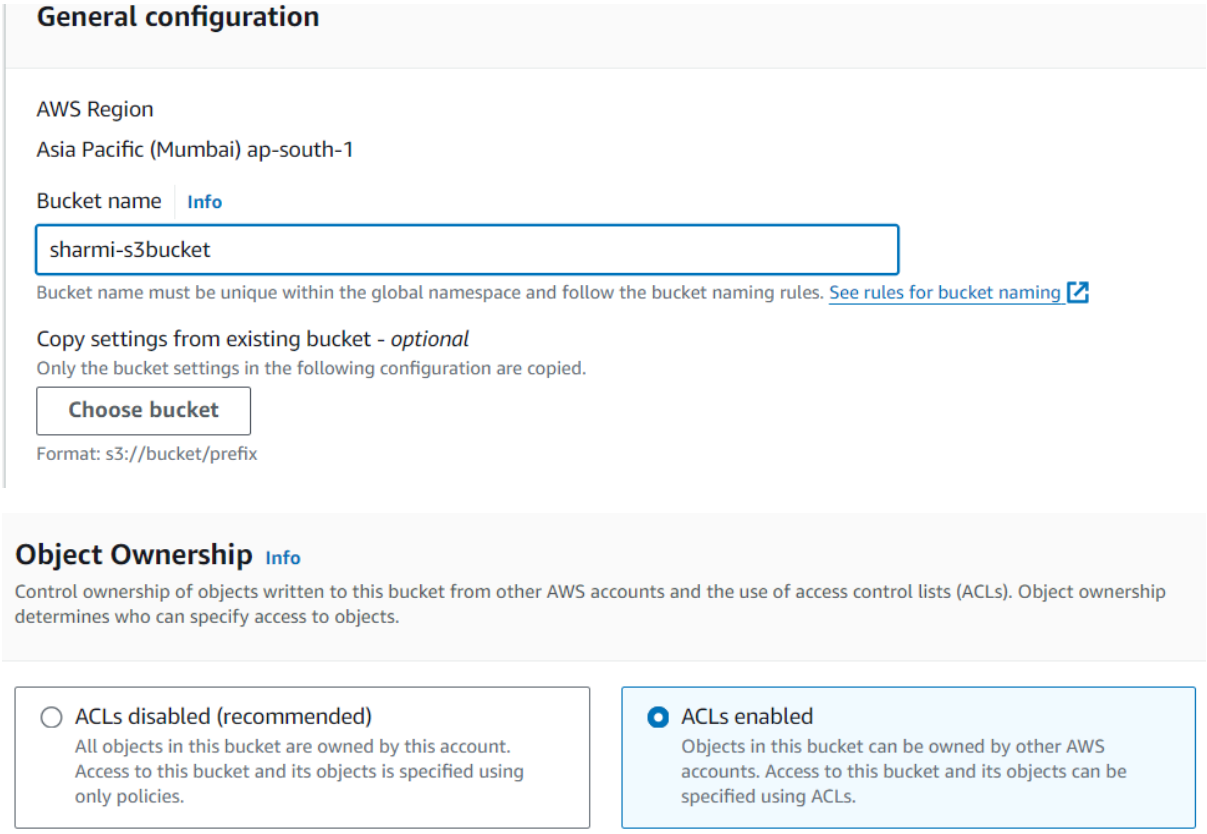
Task 15: Create a S3 bucket, with no public access and upload files to the bucket & view the logs for the uploaded files. Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address.

1. Create a S3 bucket, with no public access & view the logs for the uploaded files:



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 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 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.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the

---

Successfully created bucket "sharmi-s3bucket"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

View details

Amazon S3 > Buckets

▸ **Account snapshot** - *updated every 24 hours* 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.

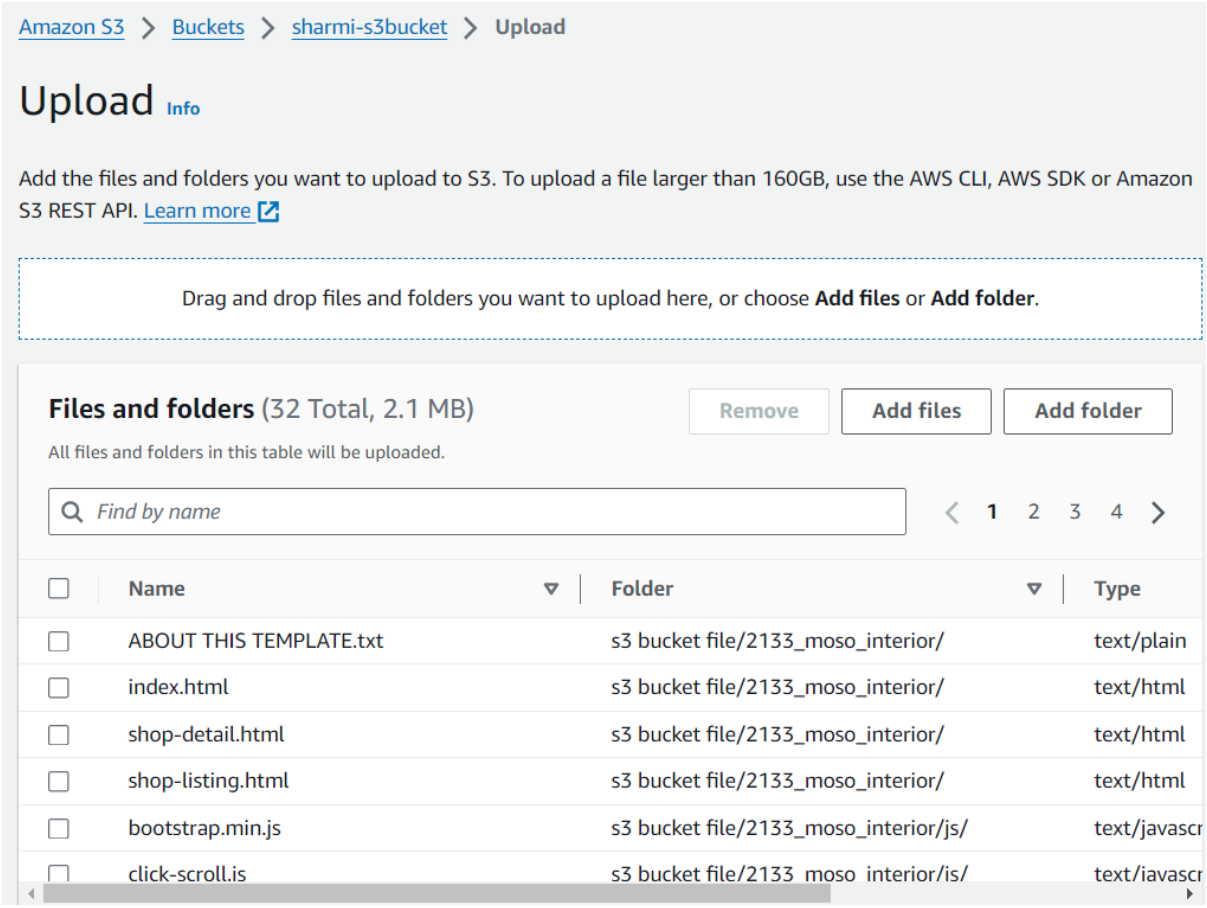
Copy ARN | Empty | Delete | Create bucket

Find buckets by name

1

Name	AWS Region	IAM Access Analyzer	Creation date
sharmi-s3bucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	July 15, 2024, 21:19:39 (UTC+05:30)

2. Upload files to the bucket:



Files and folders (32 Total, 2.1 MB)

Remove | Add files | Add folder

All files and folders in this table will be uploaded.

Find by name

1 2 3 4

Name	Folder	Type
bootstrap.min.js	s3 bucket file/2133_moso_interior/js/	text/javascr
click-scroll.js	s3 bucket file/2133_moso_interior/js/	text/javascr
custom.js	s3 bucket file/2133_moso_interior/js/	text/javascr
jquery.backstretch.min.js	s3 bucket file/2133_moso_interior/js/	text/javascr
jquery.min.js	s3 bucket file/2133_moso_interior/js/	text/javascr
owl.carousel.min.js	s3 bucket file/2133_moso_interior/js/	text/javascr

Destination Info

Destination

s3://sharmi-s3bucket

▶ **Destination details**

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

Upload succeeded

View details below.

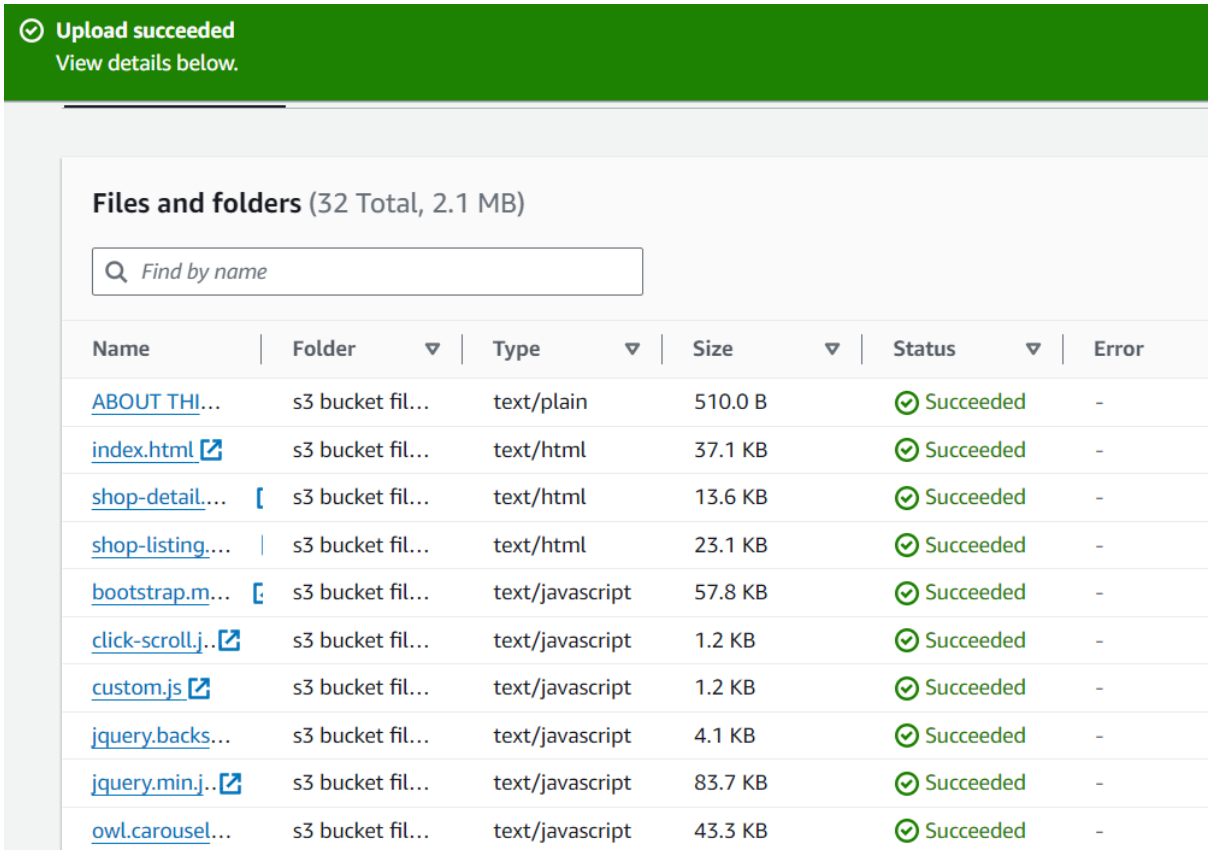
Upload: status

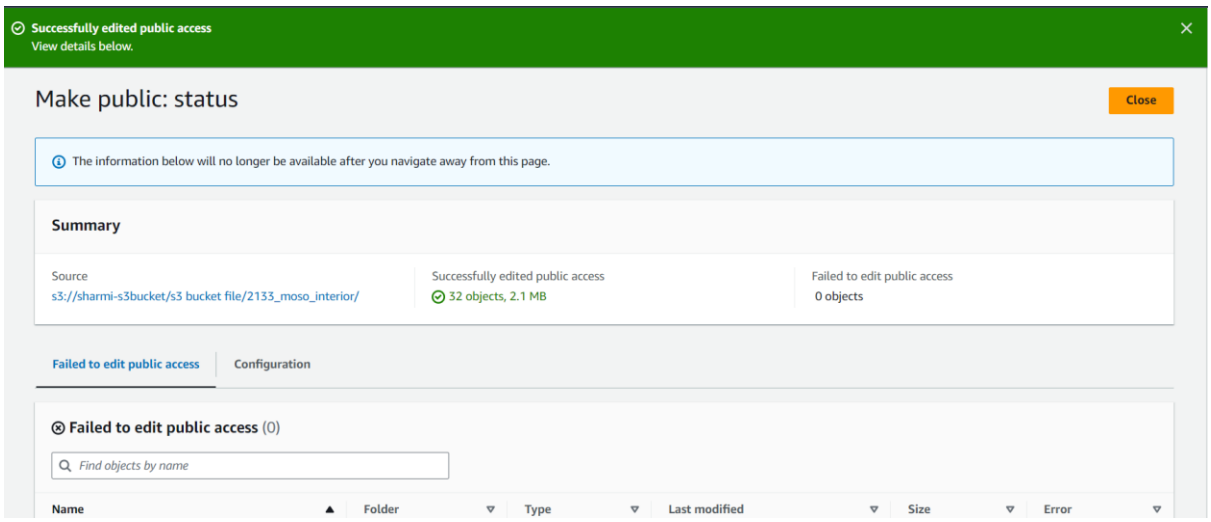
Close

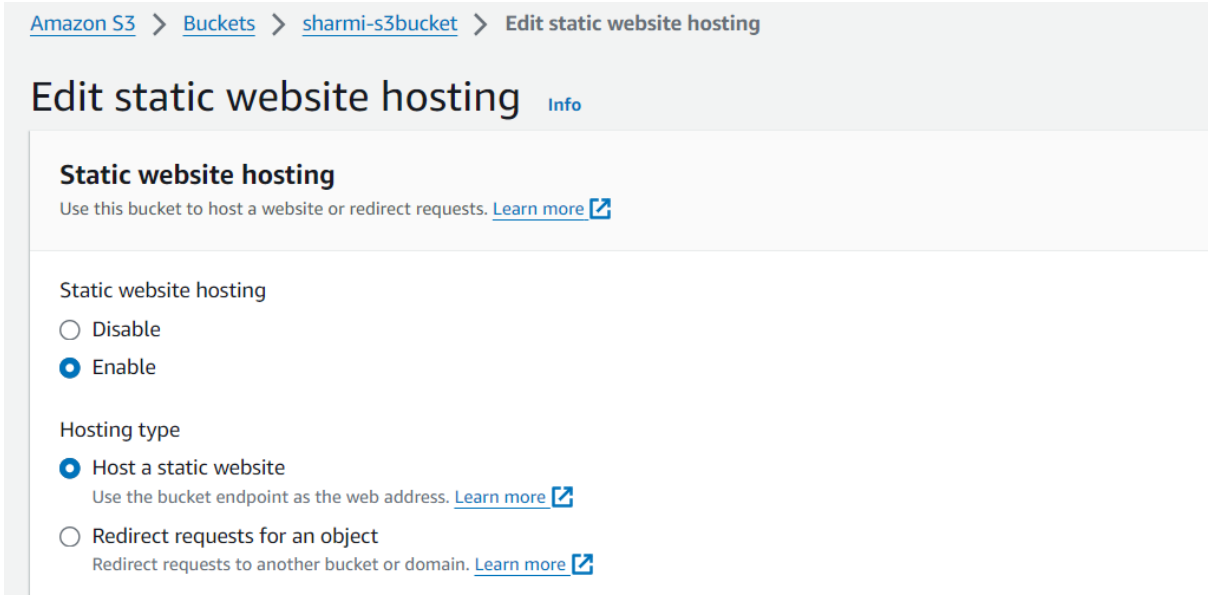
The information below will no longer be available after you navigate away from this page.

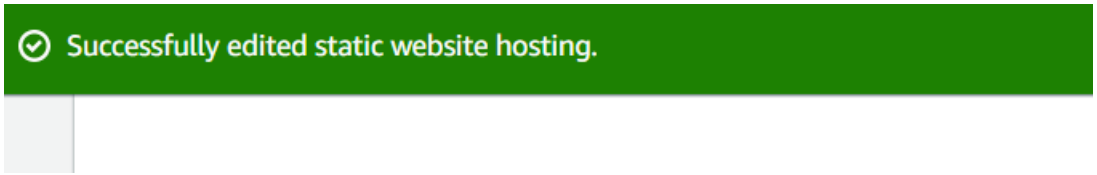
Summary

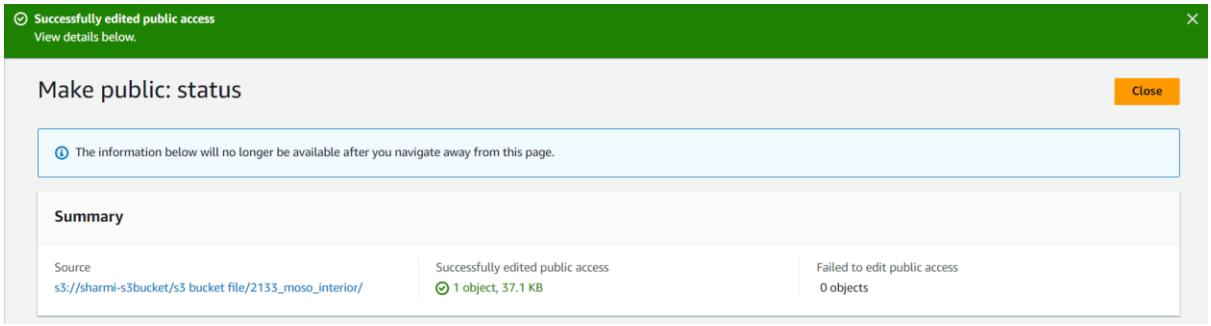
Destination	Succeeded	Failed
s3://sharmi-s3bucket	32 files, 2.1 MB (100.00%)	0 files, 0 B (0%)

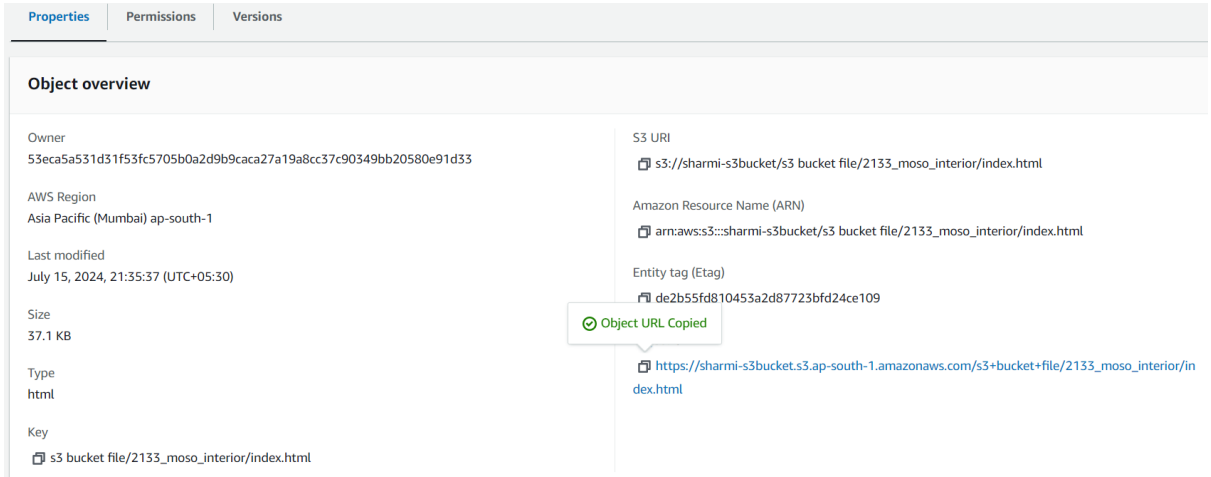

Upload succeeded
View details below.
Files and folders (32 Total, 2.1 MB)
Find by name
Name
Folder
Type
Size
Status
Error
ABOUT THI...
s3 bucket fil...
text/plain
510.0 B
Succeeded
-
index.html
s3 bucket fil...
text/html
37.1 KB
Succeeded
-
shop-detail....
s3 bucket fil...
text/html
13.6 KB
Succeeded
-
shop-listing....
s3 bucket fil...
text/html
23.1 KB
Succeeded
-
bootstrap.m...
s3 bucket fil...
text/javascript
57.8 KB
Succeeded
-
click-scroll.j..
s3 bucket fil...
text/javascript
1.2 KB
Succeeded
-
custom.js
s3 bucket fil...
text/javascript
1.2 KB
Succeeded
-
jquery.backs...
s3 bucket fil...
text/javascript
4.1 KB
Succeeded
-
jquery.min.j..
s3 bucket fil...
text/javascript
83.7 KB
Succeeded
-
owl.carousel...
s3 bucket fil...
text/javascript
43.3 KB
Succeeded
-

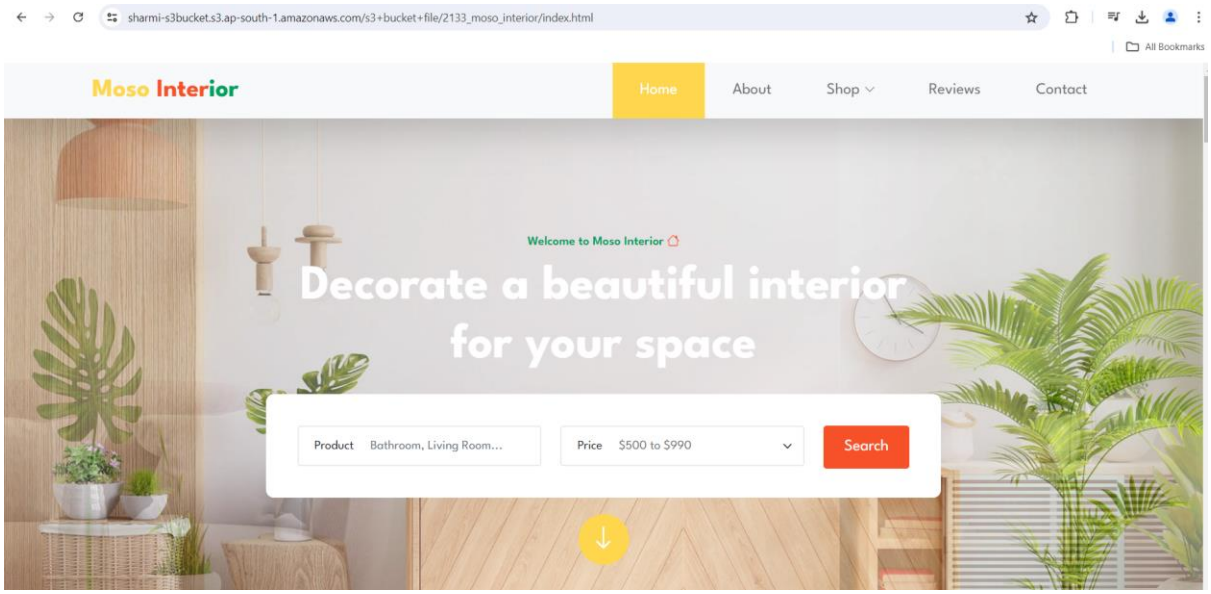

Successfully edited public access
View details below.
Make public: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Source
s3://sharmi-s3bucket/s3 bucket file/2133_moso_interior/
Successfully edited public access
32 objects, 2.1 MB
Failed to edit public access
0 objects
Failed to edit public access
Configuration
Failed to edit public access (0)
Find objects by name
Name
Folder
Type
Last modified
Size
Error


Amazon S3 > Buckets > sharmi-s3bucket > Edit static website hosting
Edit static website hosting Info
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Static website hosting
Disable
Enable
Hosting type
Host a static website
Use the bucket endpoint as the web address. Learn more
Redirect requests for an object
Redirect requests to another bucket or domain. Learn more

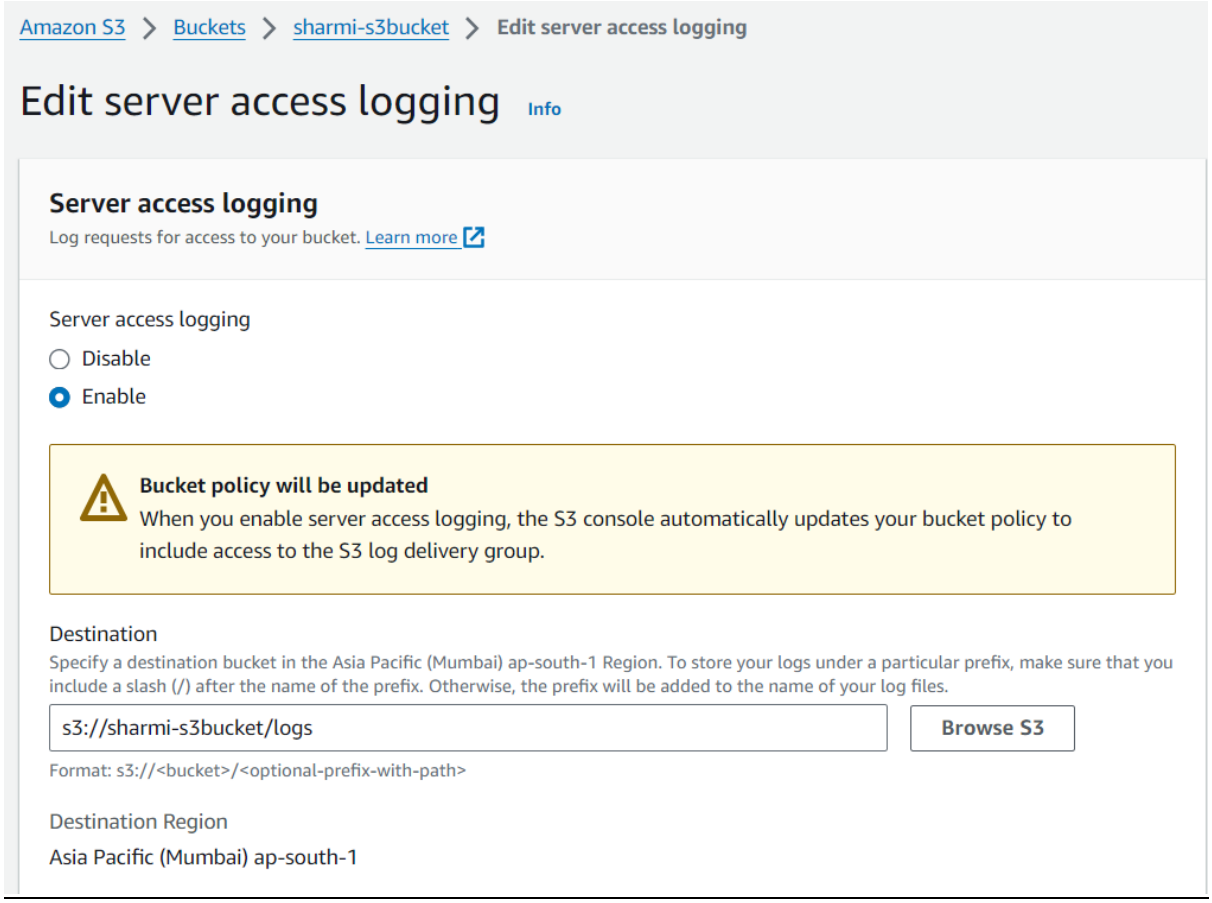

Successfully edited static website hosting.

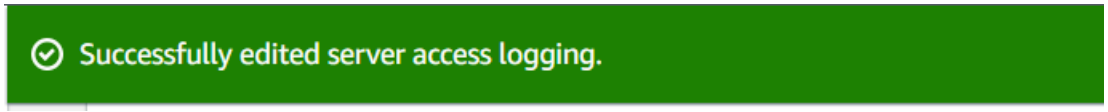

Successfully edited public access
View details below.
Make public: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Source
s3://sharmi-s3bucket/s3 bucket file/2133_moso_interior/
Successfully edited public access
1 object, 37.1 KB
Failed to edit public access
0 objects

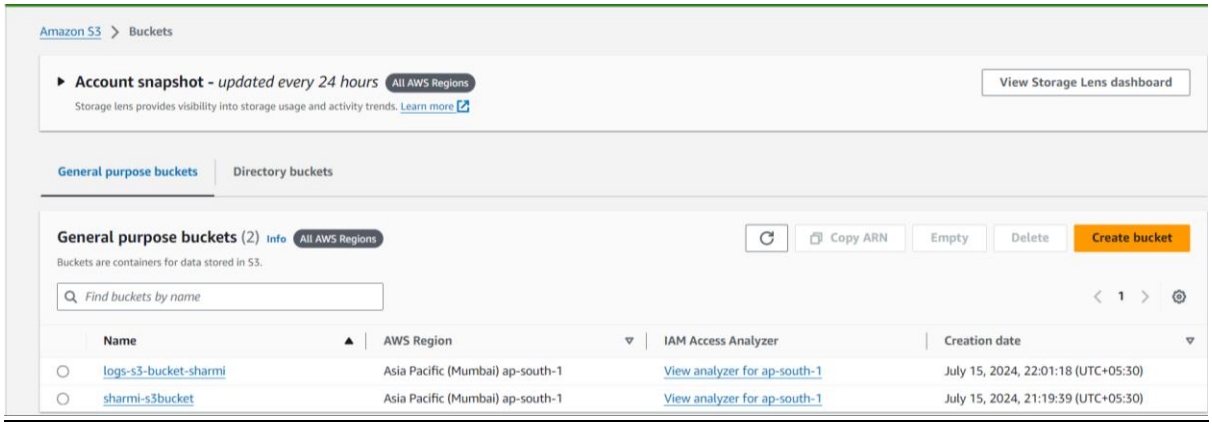

Properties
Permissions
Versions
Object overview
Owner
53eca5a531d31f53fc5705b0a2d9b9caca27a19a8cc37c90349bb20580e91d33
AWS Region
Asia Pacific (Mumbai) ap-south-1
Last modified
July 15, 2024, 21:35:37 (UTC+05:30)
Size
37.1 KB
Type
html
Key
s3 bucket file/2133_moso_interior/index.html
S3 URI
s3://sharmi-s3bucket/s3 bucket file/2133_moso_interior/index.html
Amazon Resource Name (ARN)
arn:aws:s3:::sharmi-s3bucket/s3 bucket file/2133_moso_interior/index.html
Entity tag (Etag)
de2b55fd810453a2d87723bfd24ce109
Object URL Copied
https://sharmi-s3bucket.s3.ap-south-1.amazonaws.com/s3+bucket+file/2133_moso_interior/index.html



3. **<u>View the logs for the uploaded files:</u>**







Objects (642) Info

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

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

Find objects by prefix

1 2 3

Name	Type	Last modified	Size	Storage class
logs2024-07-15-17-13-25-004DF45FFCA78131	-	July 15, 2024, 22:43:26 (UTC+05:30)	663.0 B	Standard
logs2024-07-15-17-15-17-A22F2CDCFDF200C4	-	July 15, 2024, 22:45:18 (UTC+05:30)	652.0 B	Standard
logs2024-07-15-17-17-07-B071D6F4659884E8	-	July 15, 2024, 22:47:08 (UTC+05:30)	1.3 KB	Standard
logs2024-07-15-17-17-55-6313A8D2CE4A1E75	-	July 15, 2024, 22:47:56 (UTC+05:30)	670.0 B	Standard
logs2024-07-15-17-18-13-B86259999C34BAA6	-	July 15, 2024, 22:48:14 (UTC+05:30)	650.0 B	Standard
logs2024-07-15-17-				

Objects (642) Info

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

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

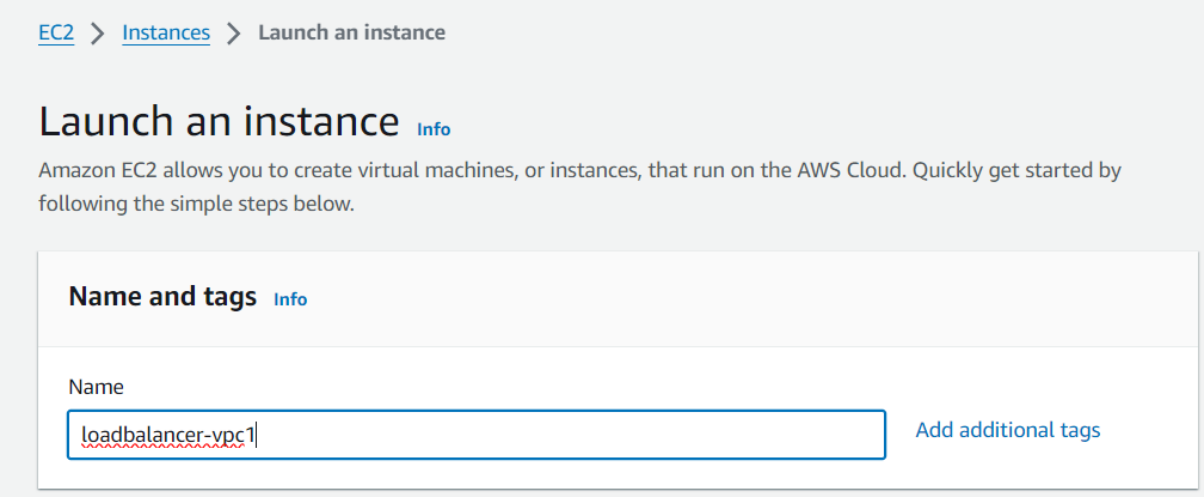
Find objects by prefix

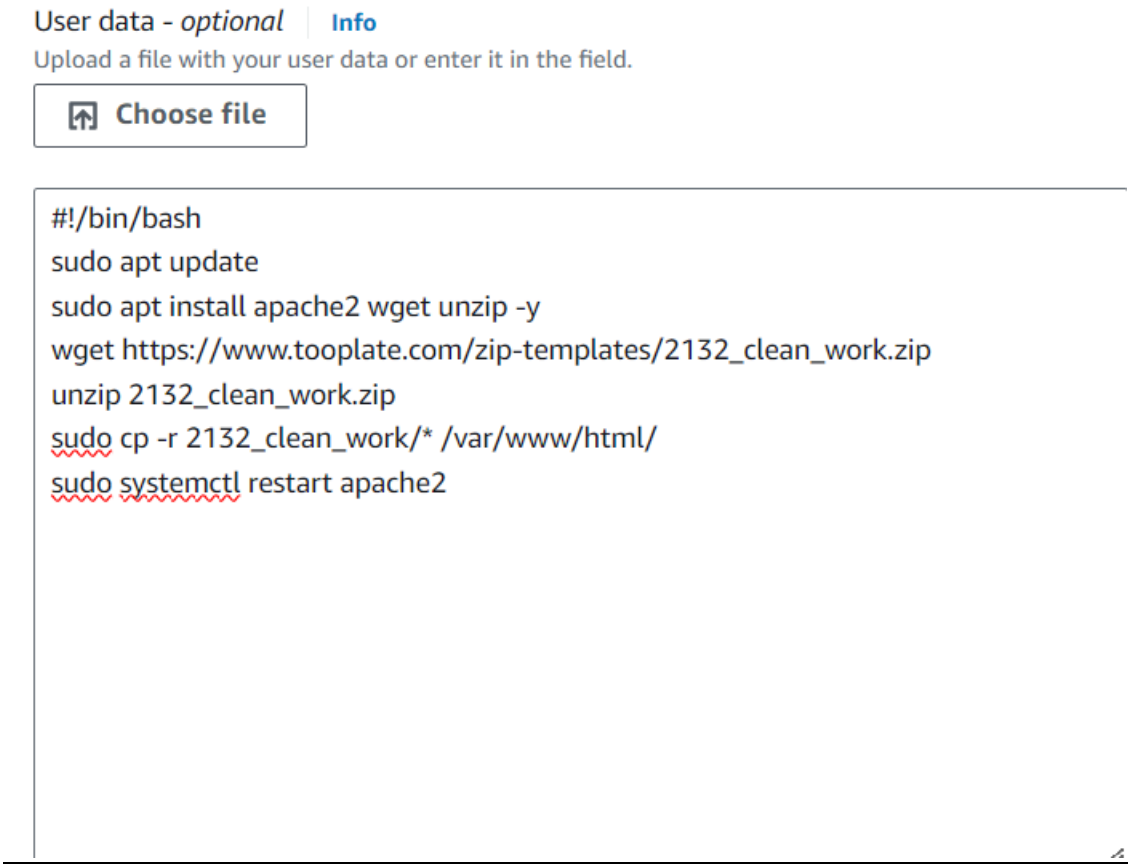
1 2 3

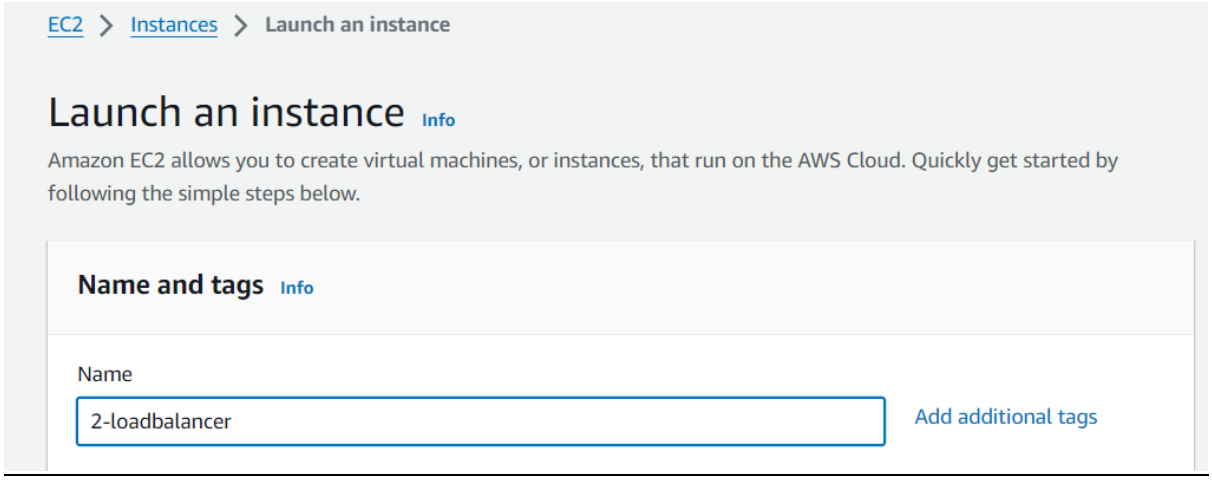
Name	Type	Last modified	Size	Storage class
B86259999C34BAA6				
logs2024-07-15-17-18-17-8E7F270C5F355D19	-	July 15, 2024, 22:48:18 (UTC+05:30)	663.0 B	Standard
logs2024-07-15-17-18-30-FAF0AB4095FE30EE	-	July 15, 2024, 22:48:31 (UTC+05:30)	656.0 B	Standard
logs2024-07-15-17-18-55-1315C76CAB97E986	-	July 15, 2024, 22:48:56 (UTC+05:30)	668.0 B	Standard
logs2024-07-15-17-19-46-4B9330A63CA6404B	-	July 15, 2024, 22:49:47 (UTC+05:30)	638.0 B	Standard
logs2024-07-15-17-22-45-01C6885113452004	-	July 15, 2024, 22:52:46 (UTC+05:30)	731.0 B	Standard
logs2024-07-15-17-				

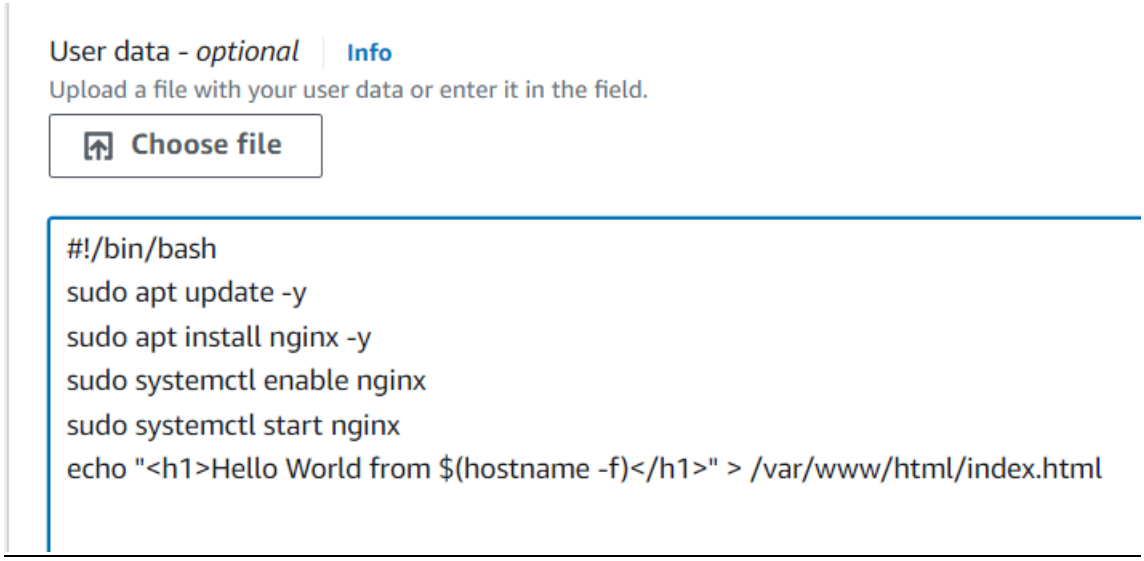
4. Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address:

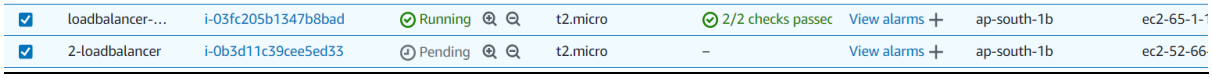
- Launch two ec2-instances:



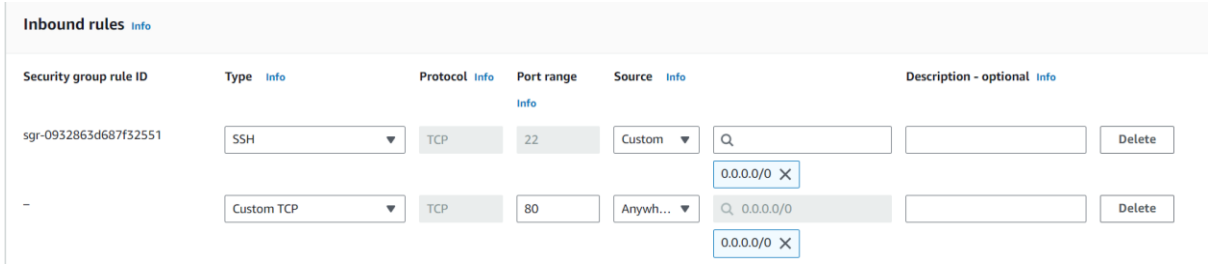


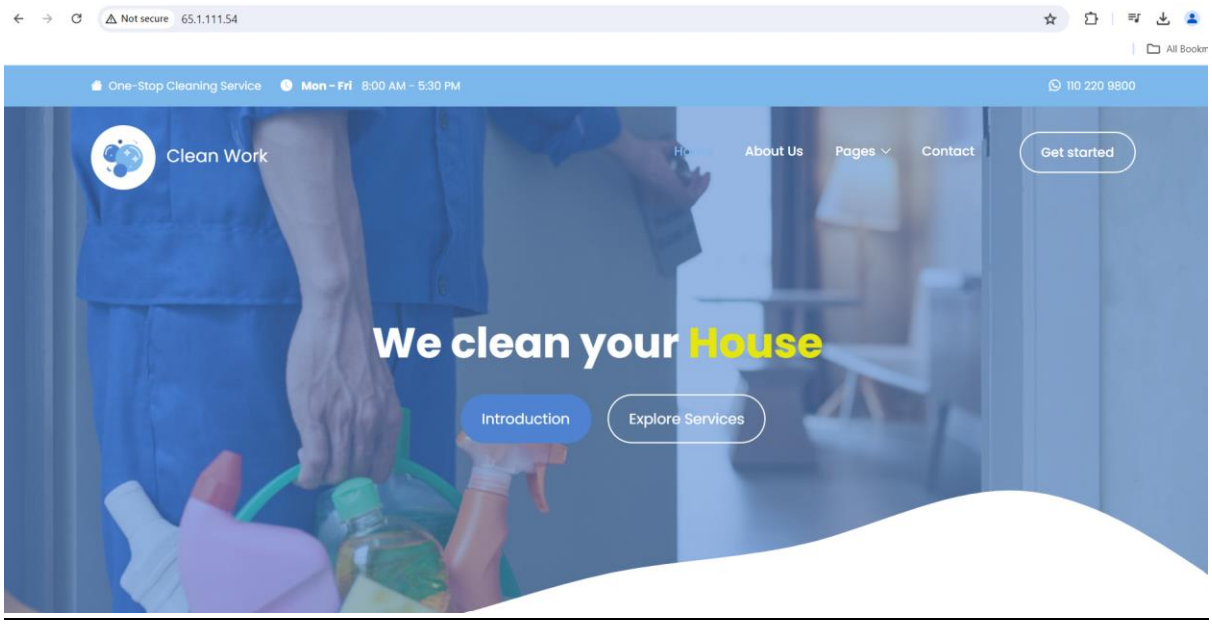






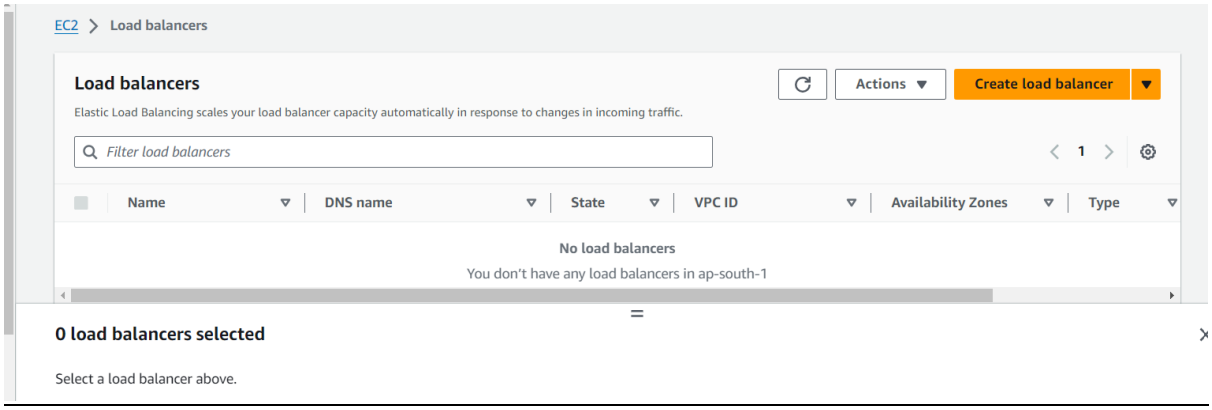
My 2 applications running in port no 80:





Hello World from ip-172-31-9-214.ap-south-1.compute.internal

Create 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.

task-loadbalancer

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. Compatible with the **IPv4** and **Dualstack** IP address types.

Security group (sg-06738f32eab15f1ee | lb-sg) was created successfully ×

▸ **Details**

EC2 > Security Groups > sg-06738f32eab15f1ee - lb-sg

sg-06738f32eab15f1ee - lb-sg

Actions

Details

Security group name	Security group ID	Description	VPC ID
lb-sg	sg-06738f32eab15f1ee	application load balancer	vpc-01ce844a8c44890ec

Owner	Inbound rules count	Outbound rules count
891377228959	1 Permission entry	1 Permission entry

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

lb-sg
sg-06738f32eab15f1ee VPC: vpc-01ce844a8c44890ec

Listeners and routing Info

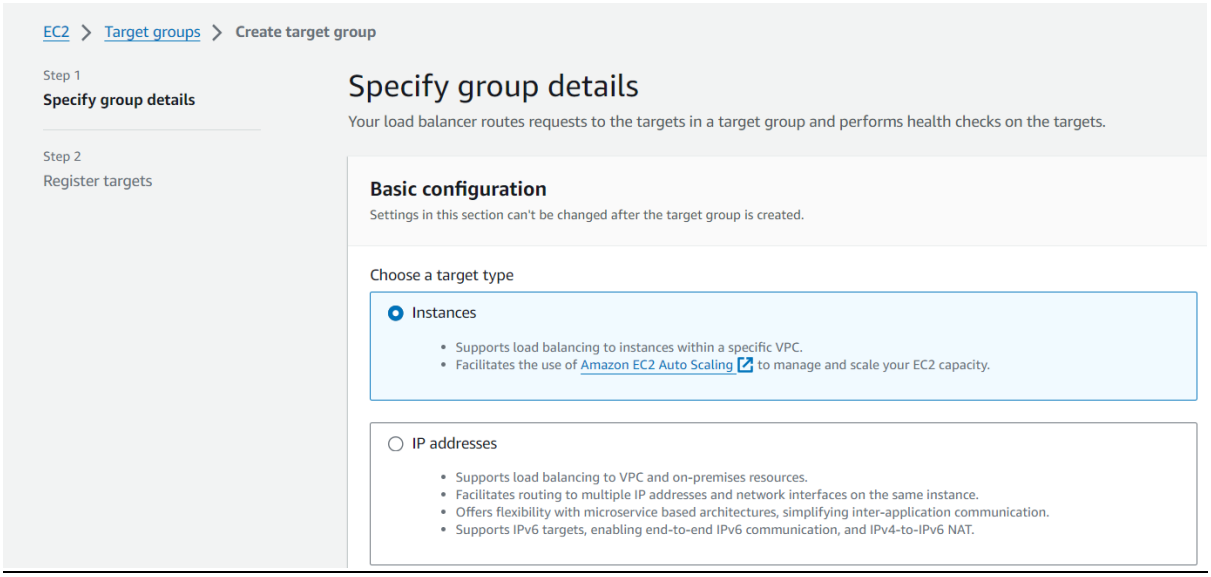
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener **HTTP:80** Remove

Protocol	Port	Default action Info
HTTP	80 (1-65535)	Forward to *Select a target group*

Create target group

Create target group:



Target group name

loadbalancer-tg

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

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP | 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

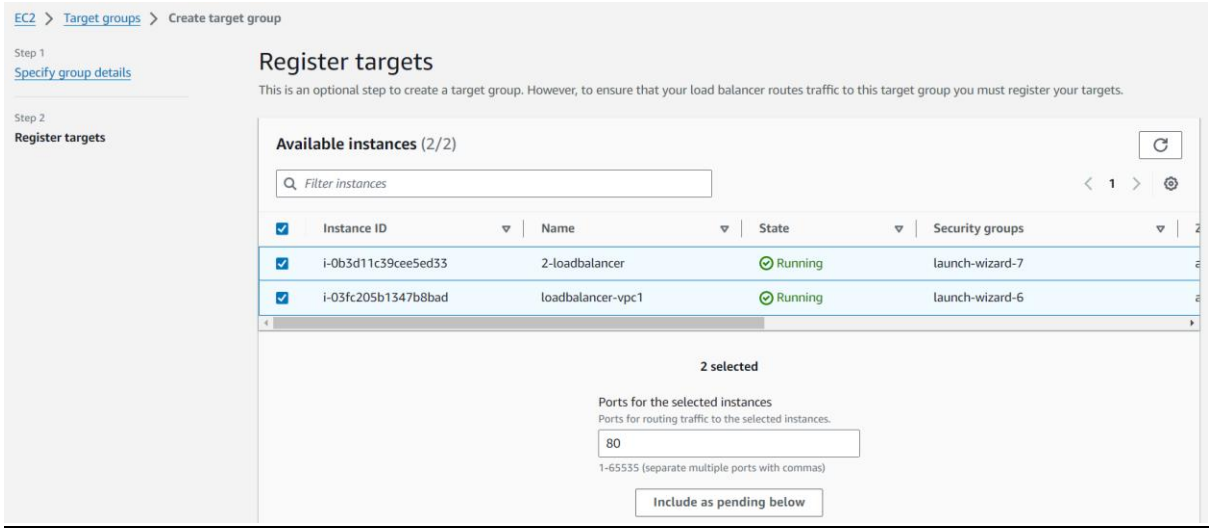
VPC

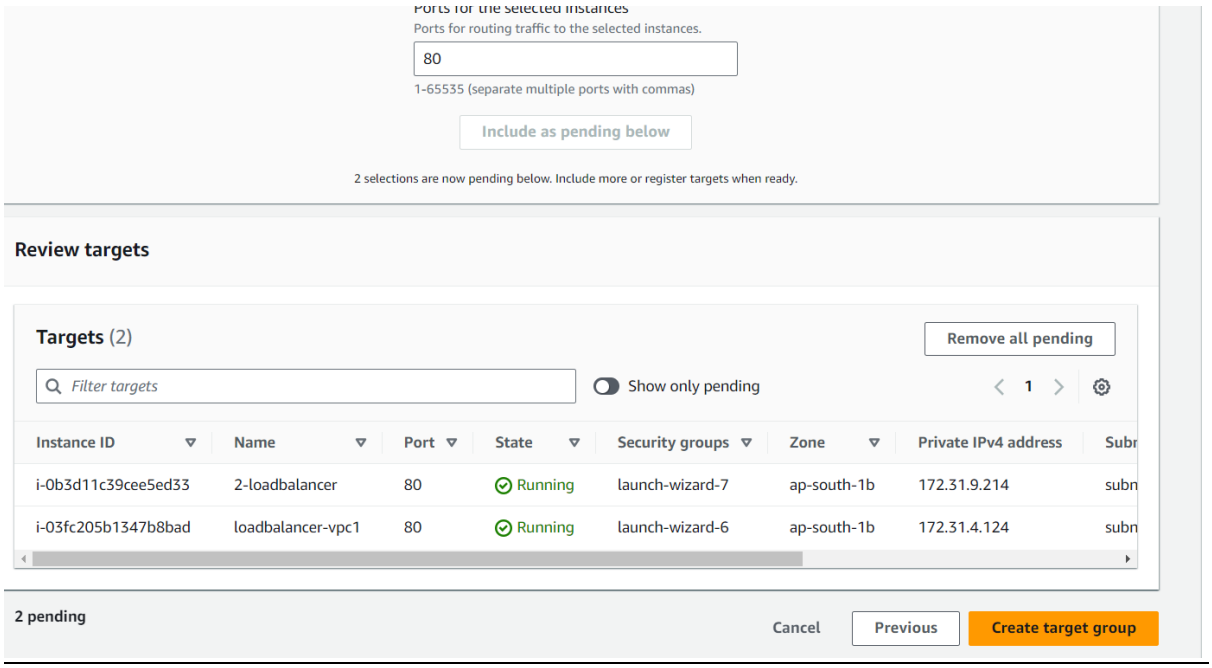
Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

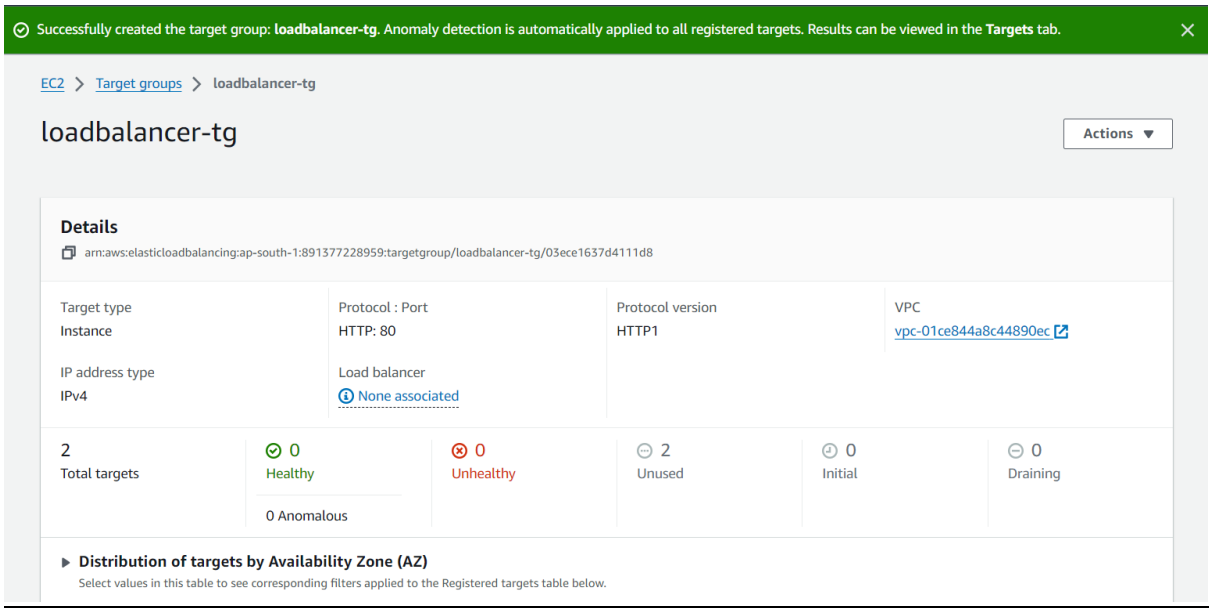
-
vpc-01ce844a8c44890ec
IPv4 VPC CIDR: 172.31.0.0/16

Protocol version

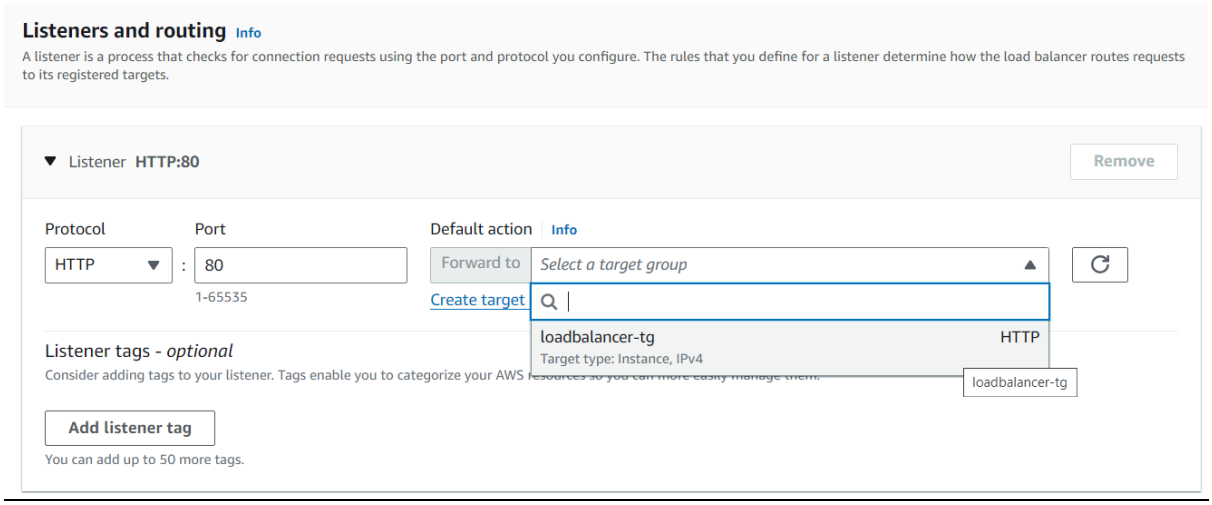
- HTTP1

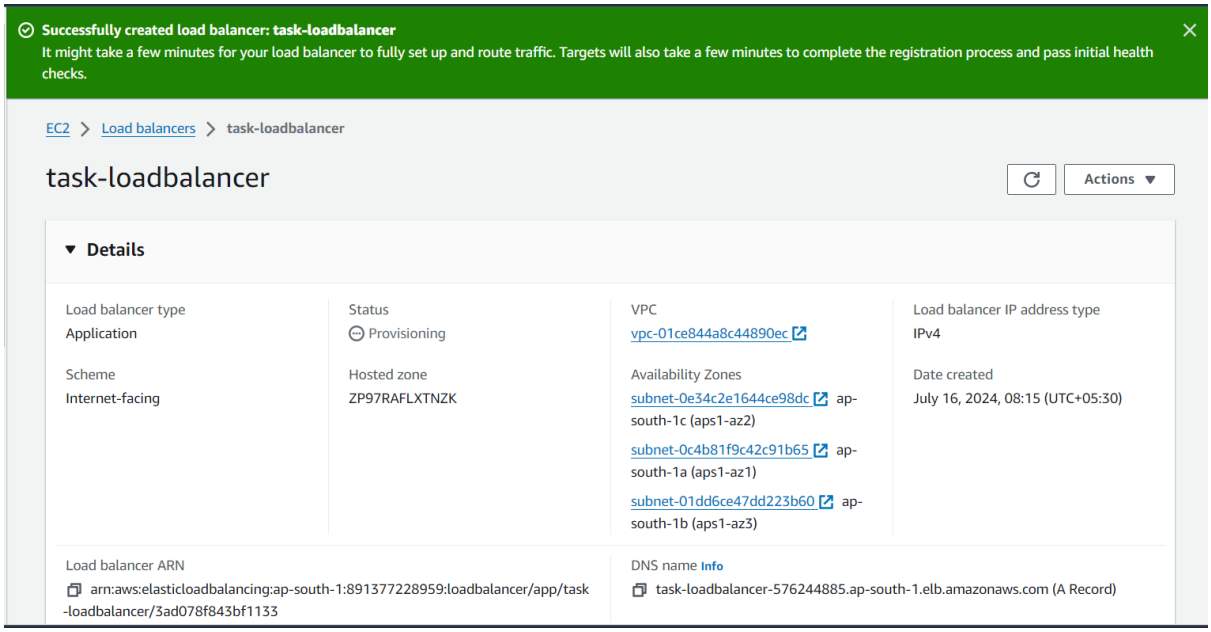

EC2 > Target groups > Create target group
Step 1
Specify group details
Step 2
Register targets
Register targets
This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.
Available instances (2/2)
Filter instances
Instance ID
Name
State
Security groups
i-0b3d11c39cee5ed33
2-loadbalancer
Running
launch-wizard-7
i-03fc205b1347b8bad
loadbalancer-vpc1
Running
launch-wizard-6
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

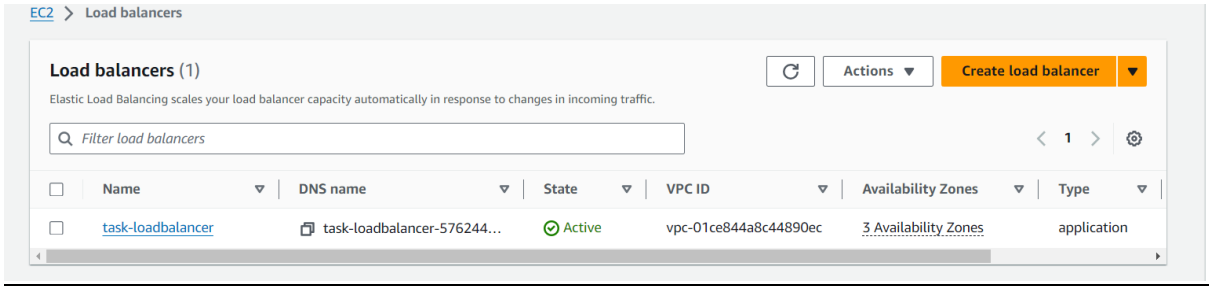

Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)
Include as pending below
2 selections are now pending below. Include more or register targets when ready.
Review targets
Targets (2)
Remove all pending
Filter targets
Show only pending
Instance ID
Name
Port
State
Security groups
Zone
Private IPv4 address
i-0b3d11c39cee5ed33
2-loadbalancer
80
Running
launch-wizard-7
ap-south-1b
172.31.9.214
i-03fc205b1347b8bad
loadbalancer-vpc1
80
Running
launch-wizard-6
ap-south-1b
172.31.4.124
2 pending
Cancel
Previous
Create target group

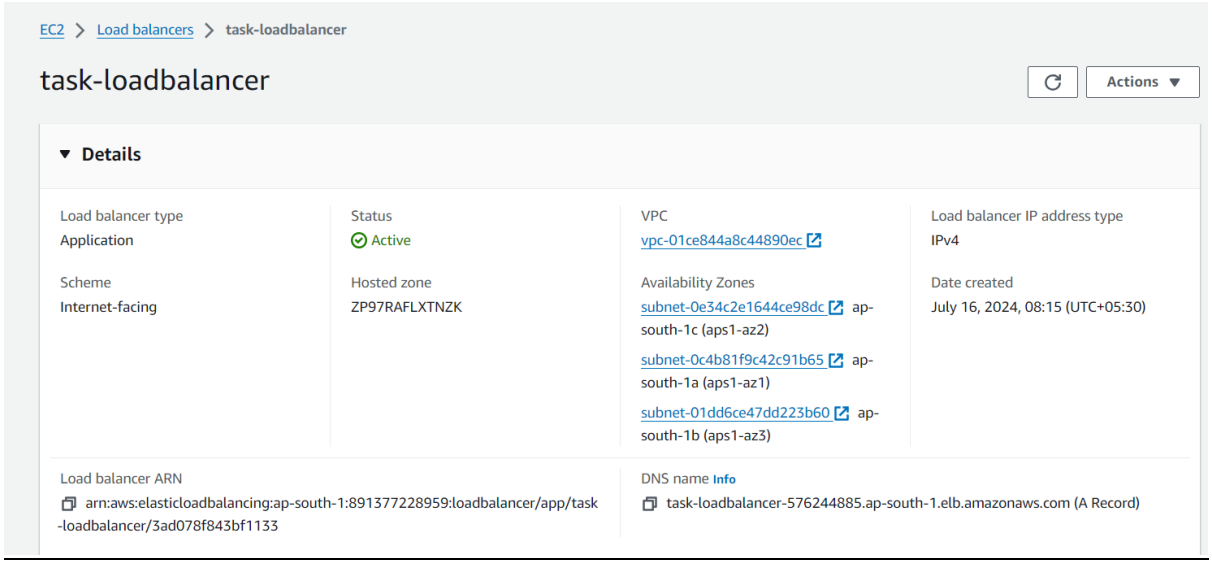

Successfully created the target group: loadbalancer-tg. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab.
EC2 > Target groups > loadbalancer-tg
loadbalancer-tg
Actions
Details
arn:aws:elasticloadbalancing:ap-south-1:891377228959:targetgroup/loadbalancer-tg/03ece1637d4111d8
Target type
Instance
Protocol : Port
HTTP: 80
Protocol version
HTTP1
VPC
vpc-01ce844a8c44890ec
IP address type
IPv4
Load balancer
None associated
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.

Select the created target group:

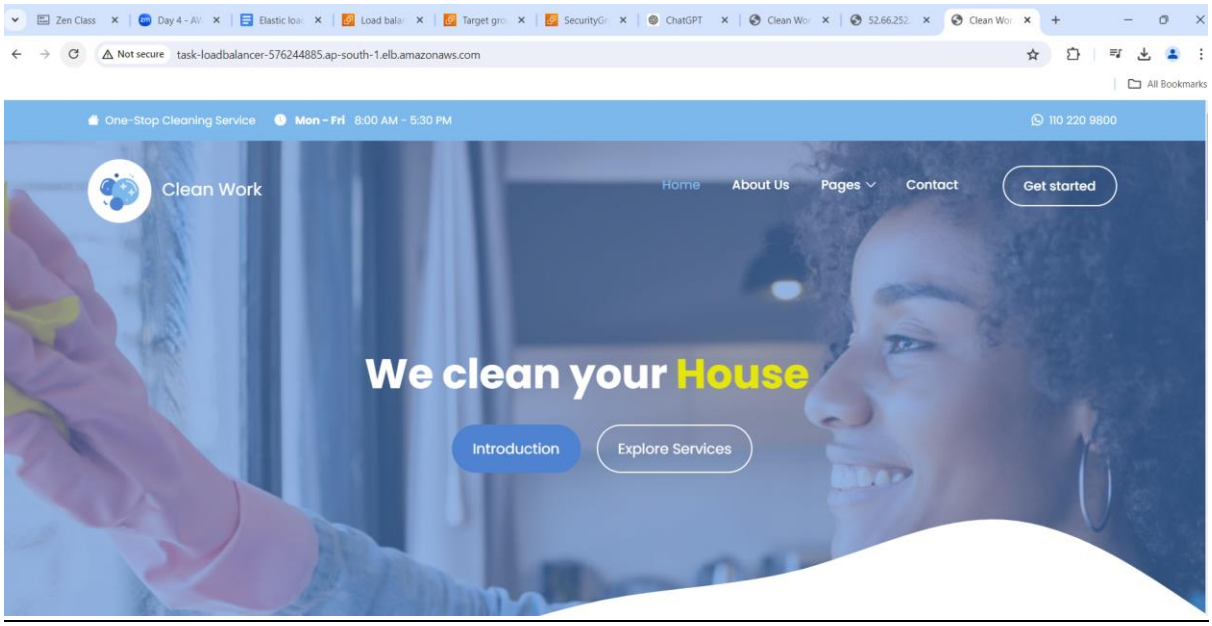


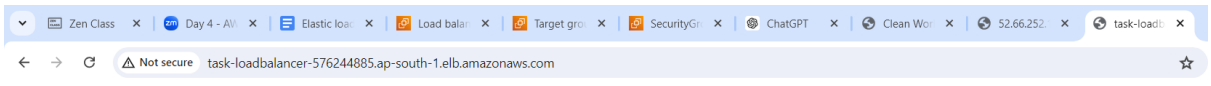






5. application load balancer, where the output traffic from the server must be an load balancer IP address:





Hello World from ip-172-31-9-214.ap-south-1.compute.internal