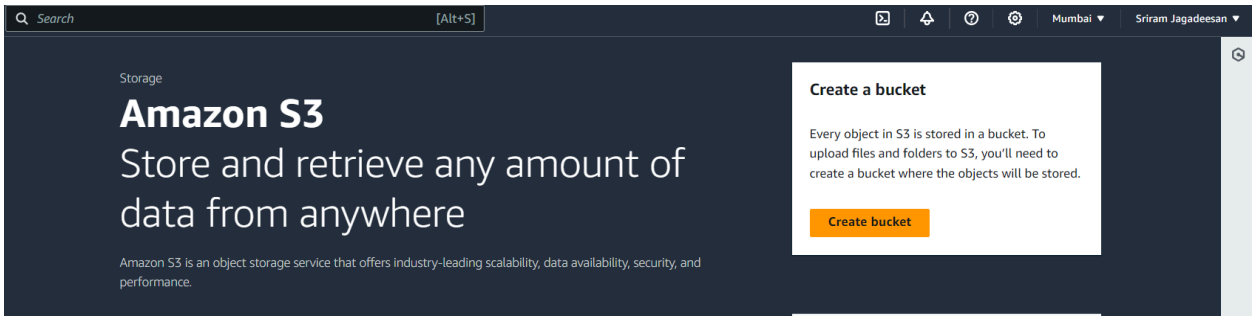
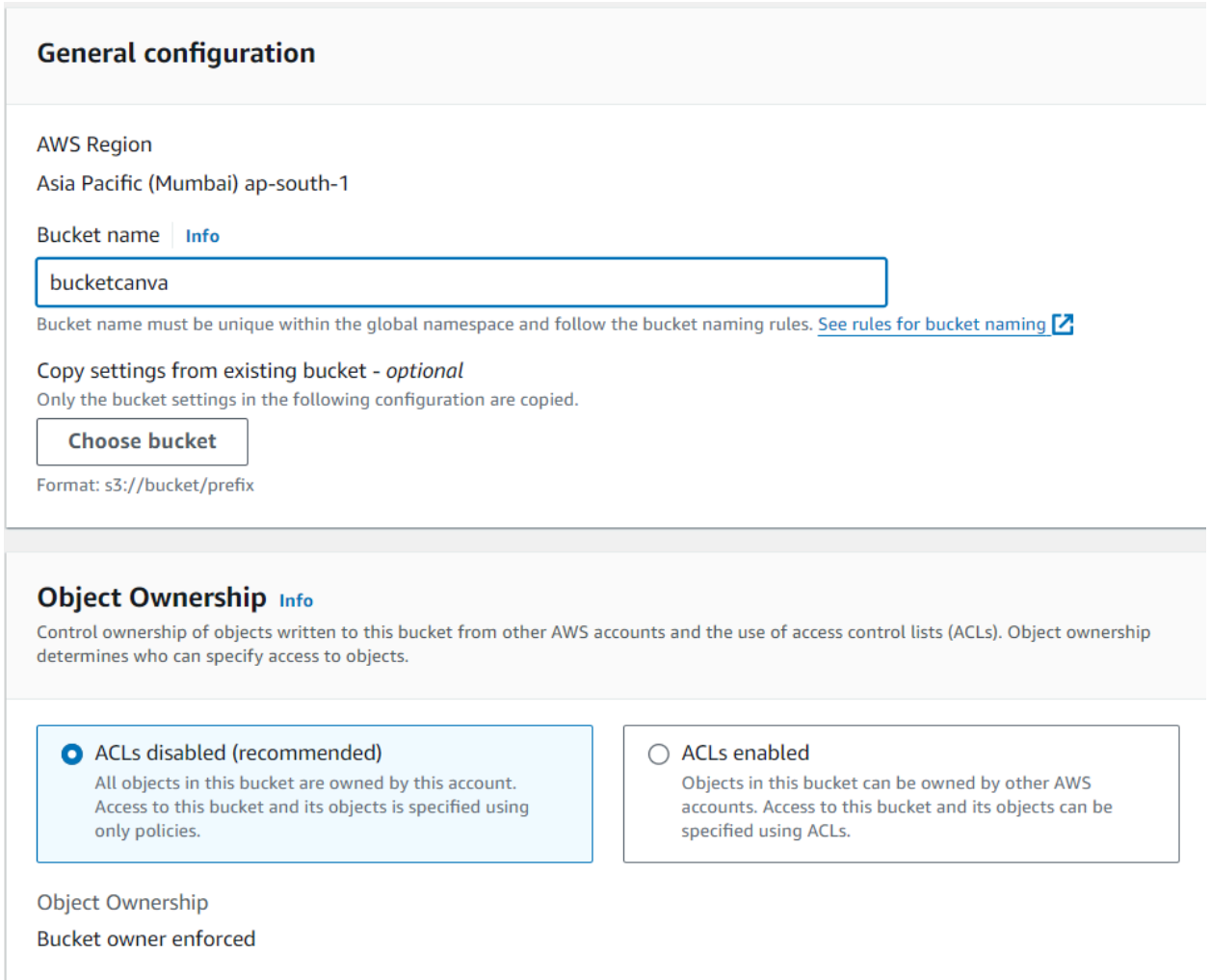
CREATED S3 BUCKET AND UPLOADED FILE TO SEE THE LOGS





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

- [x] **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.

  - [x] **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.

  - [x] **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.

  - [x] **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.

  - [x] **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.

Bucket Versioning

- (●) Disable
- ( ) 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 tag

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

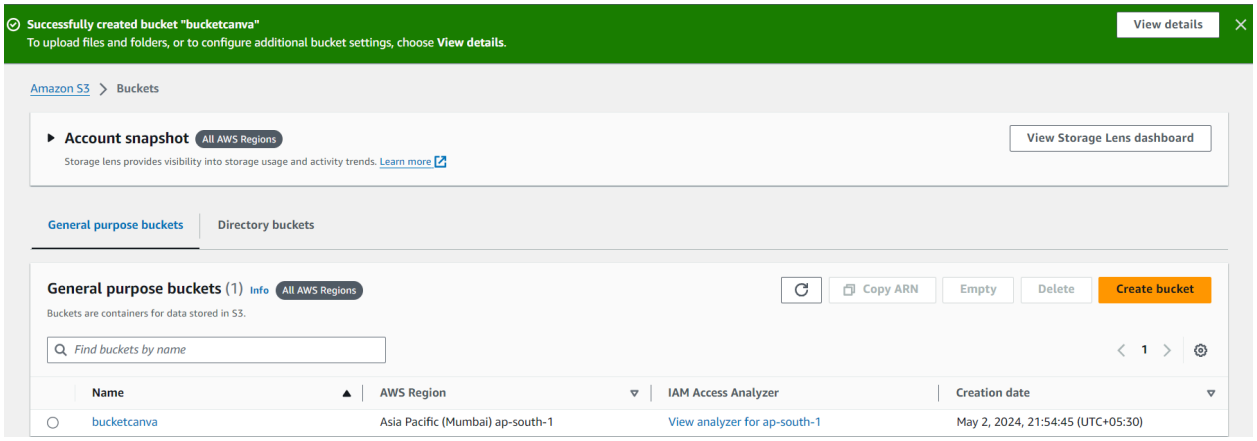
Encryption type Info

- (●) 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)

  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.

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-



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, 215.1 KB)

Remove | Add files | Add folder

All files and folders in this table will be uploaded.

Find by name

1

Name	Folder
package-lock.json	-

Destination Info

Destination

s3://bucketcanva

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://bucketcanva	1 file, 215.1 KB (100.00%)	0 files, 0 B (0%)

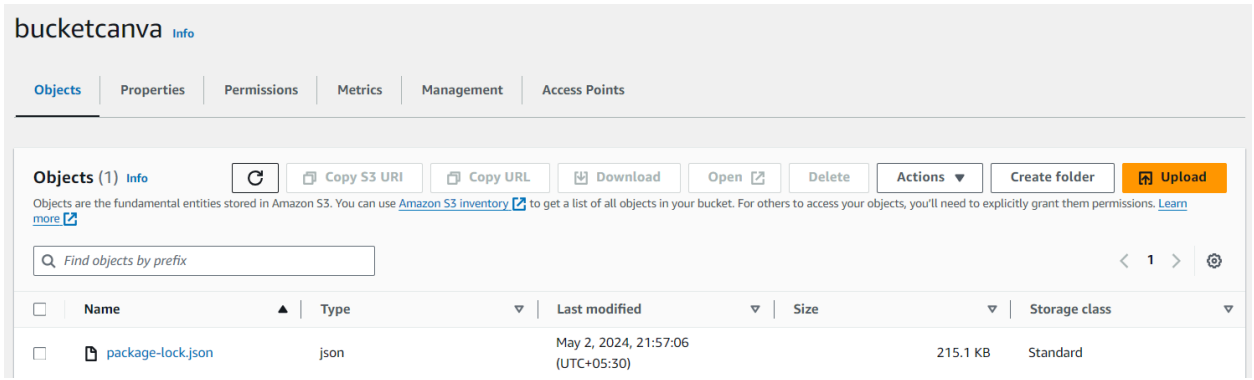
Files and folders | Configuration

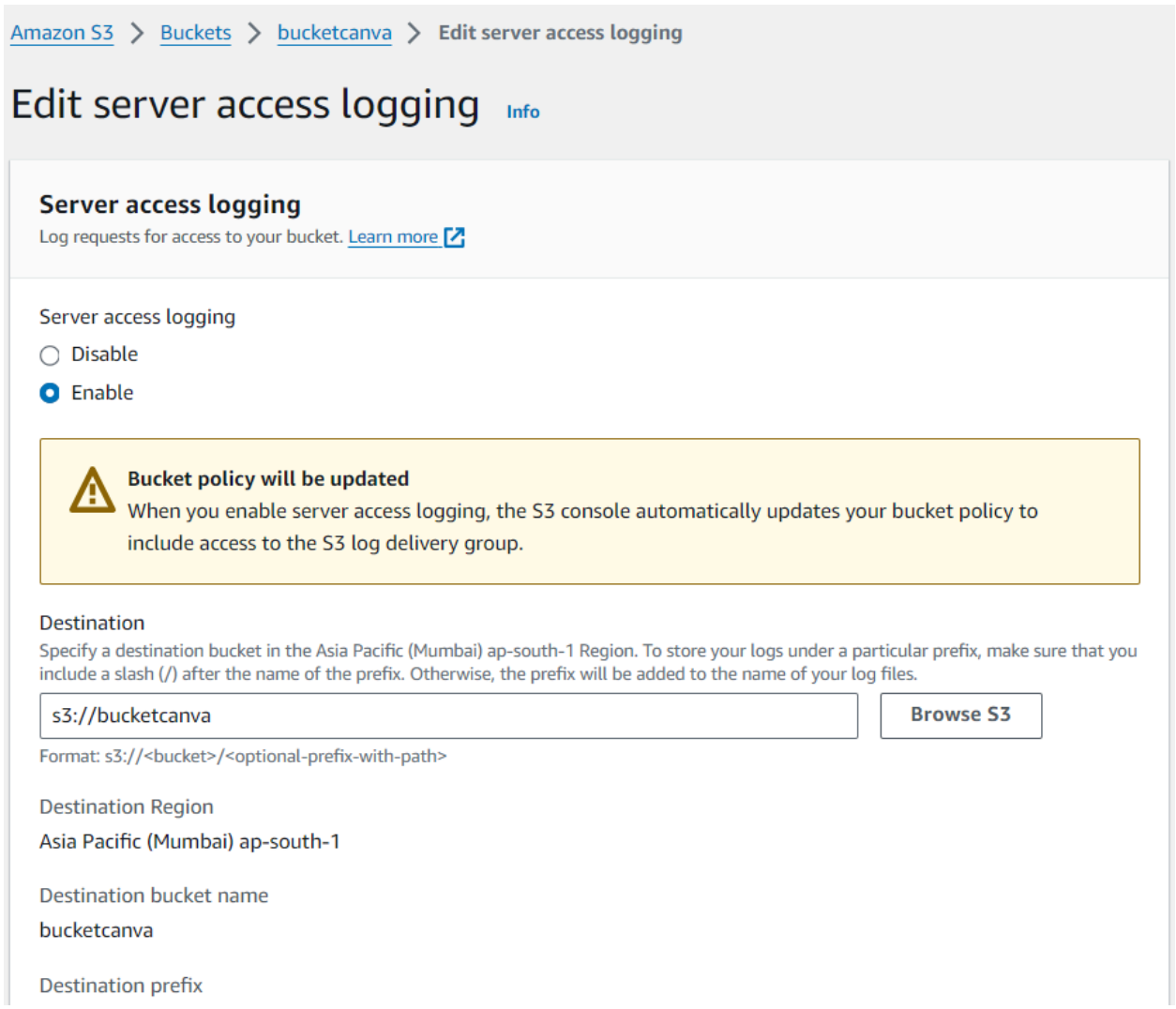
Files and folders (1 Total, 215.1 KB)

Find by name

1

Name	Folder	Type	Size	Status	Error
package-loc...	-	application/...	215.1 KB	Succeeded	-


bucketcanva Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1) 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
Name
Type
Last modified
Size
Storage class
package-lock.json
json
May 2, 2024, 21:57:06 (UTC+05:30)
215.1 KB
Standard


Amazon S3 > Buckets > bucketcanva > 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://bucketcanva
Browse S3
Format: s3://<bucket>/<optional-prefix-with-path>
Destination Region
Asia Pacific (Mumbai) ap-south-1
Destination bucket name
bucketcanva
Destination prefix

Destination Region

Asia Pacific (Mumbai) ap-south-1

Destination bucket name

bucketcanva

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.

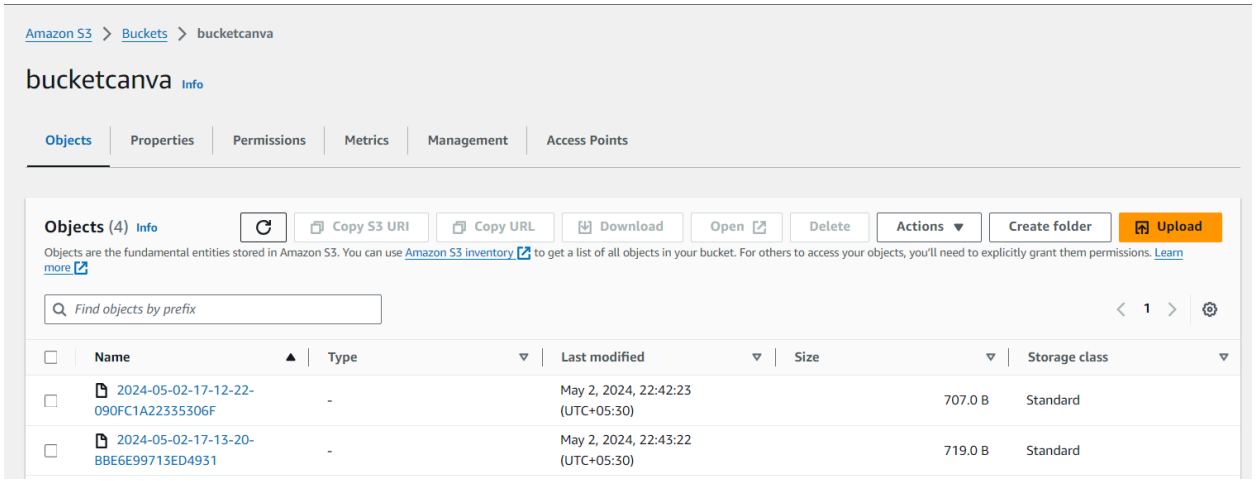
Log object key format

- [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.

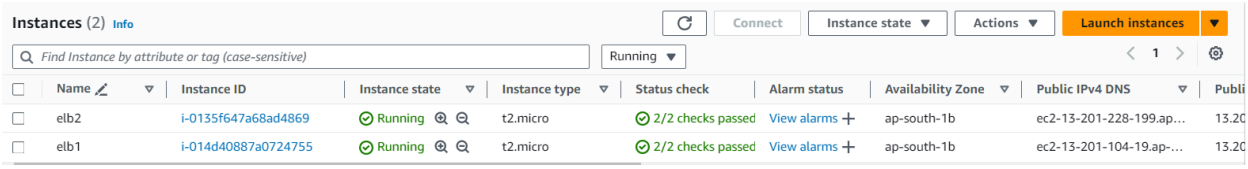
Log object key example

2024-07-01-10-12-56-[UniqueString]

Cancel | Save changes



LAUNCHED 2 EC2 MACHINES AND CONNECT **APPLICATION LOAD BALANCER** TO ACCESS THE APPLICATION BY **LOAD BALANCER IP ADDRESS**



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.

Loadbalancer1

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.

Network mapping Info

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

VPC | Info

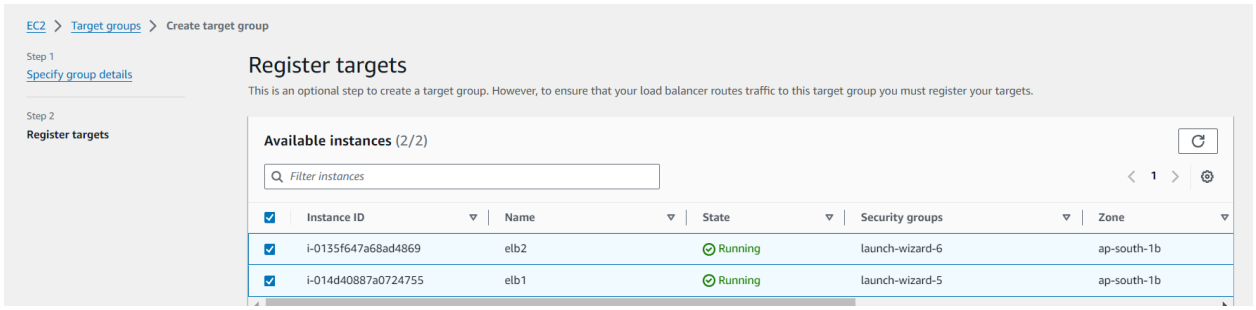
Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.

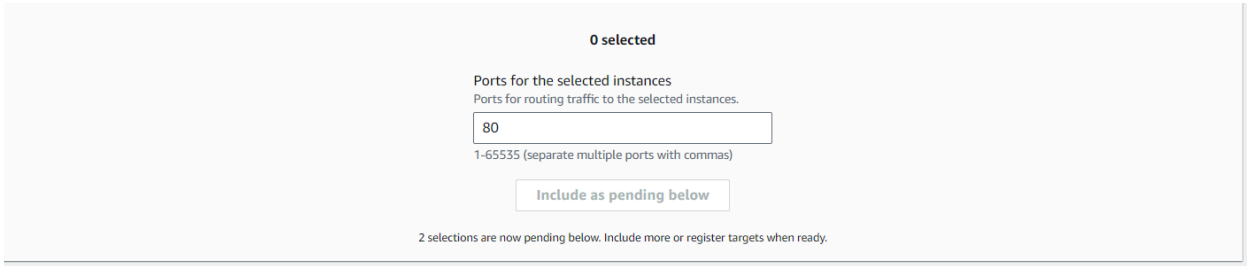
-
vpc-055cb9231e6edf043
IPv4 VPC CIDR: 172.31.0.0/16

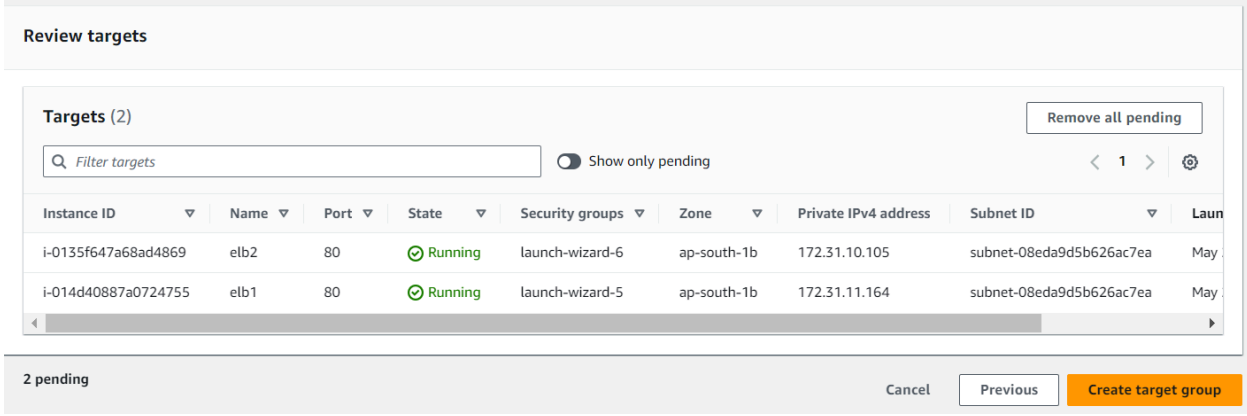
Mappings | Info

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.

- [x] **ap-south-1a (aps1-az1)**
  Subnet
  subnet-039fe4ecec97386a3
  IPv4 address
  Assigned by AWS
- [x] **ap-south-1b (aps1-az3)**
  Subnet
  subnet-08eda9d5b626ac7ea
  IPv4 address
  Assigned by AWS
- [x] **ap-south-1c (aps1-az2)**
  Subnet


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
Security groups
Zone
i-0135f647a68ad4869
elb2
Running
launch-wizard-6
ap-south-1b
i-014d40887a0724755
elb1
Running
launch-wizard-5
ap-south-1b


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
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
1
Instance ID
Name
Port
State
Security groups
Zone
Private IPv4 address
Subnet ID
i-0135f647a68ad4869
elb2
80
Running
launch-wizard-6
ap-south-1b
172.31.10.105
subnet-08eda9d5b626ac7ea
i-014d40887a0724755
elb1
80
Running
launch-wizard-5
ap-south-1b
172.31.11.164
subnet-08eda9d5b626ac7ea
2 pending
Cancel
Previous
Create target group

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-0597197ad9de7d23d VPC: vpc-055cb9231e6edf043

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 TG-LB, Target type: Instance, IPv4, HTTP

Create target group

Summary

Review and confirm your configurations. Estimate cost

Basic configuration Edit

Loadbalancer1

- Internet-facing
- IPv4

Security groups Edit

- LB-SG
  sg-0597197ad9de7d23d

Network mapping Edit

VPC vpc-055cb9231e6edf043

- ap-south-1a
  subnet-039fe4ecec97386a3
- ap-south-1b
  subnet-08eda9d5b626ac7ea
- ap-south-1c
  subnet-04107044f11d77b0a

Listeners and routing Edit

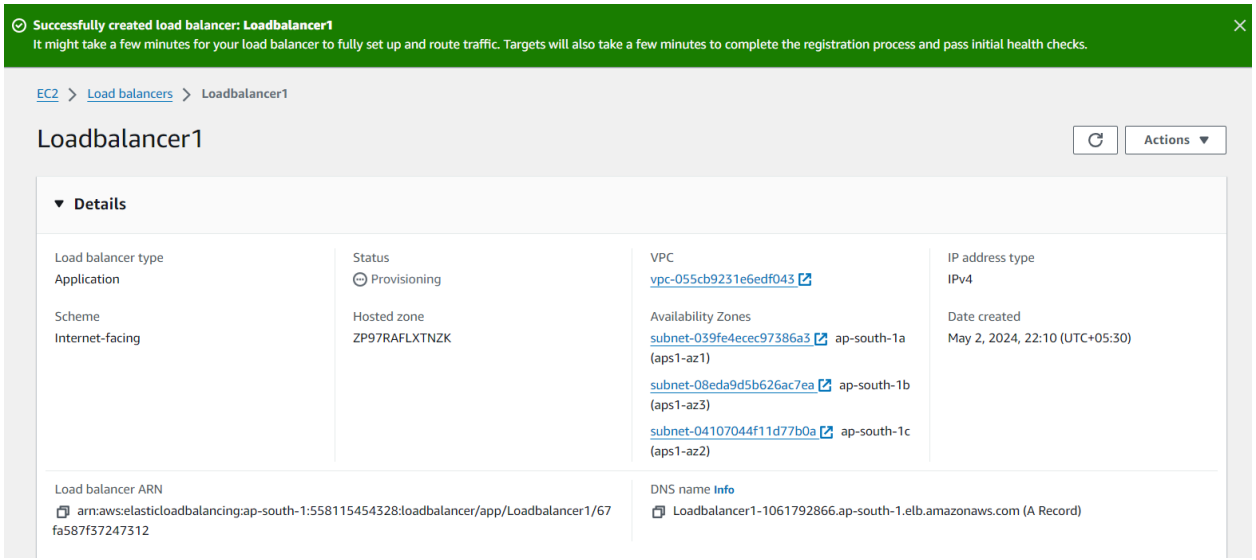
- HTTP:80 defaults to
  TG-LB

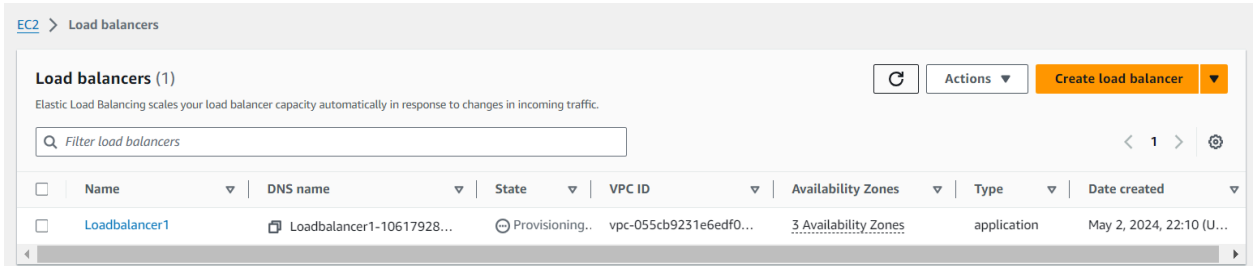
Service integrations Edit

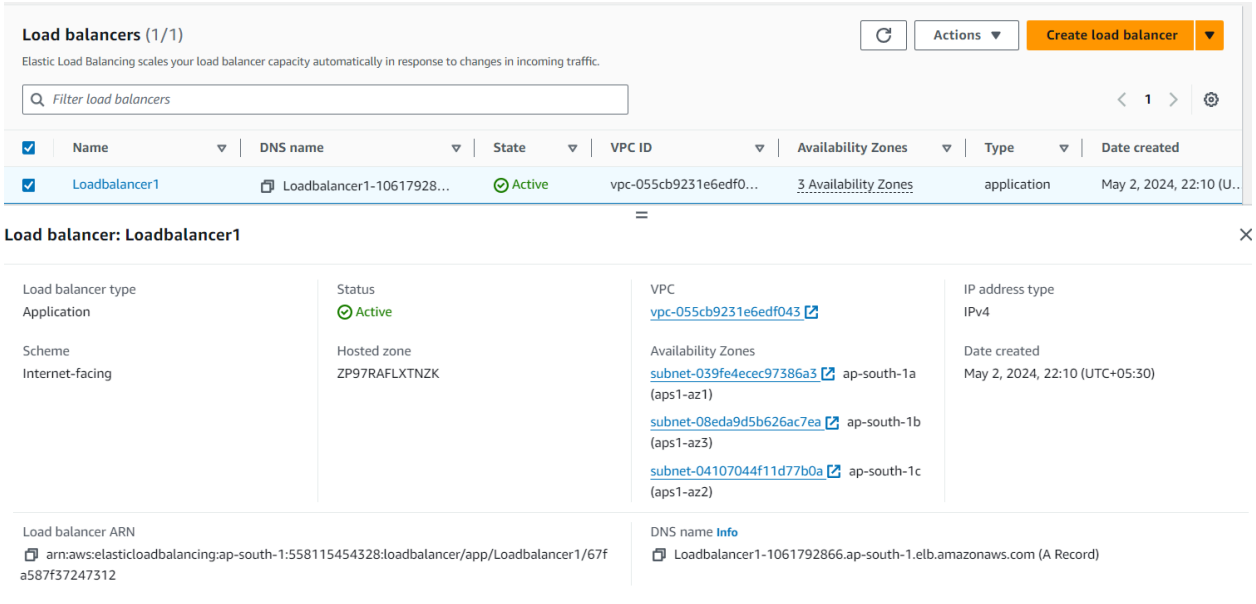
AWS WAF: *None*
AWS Global Accelerator: *None*

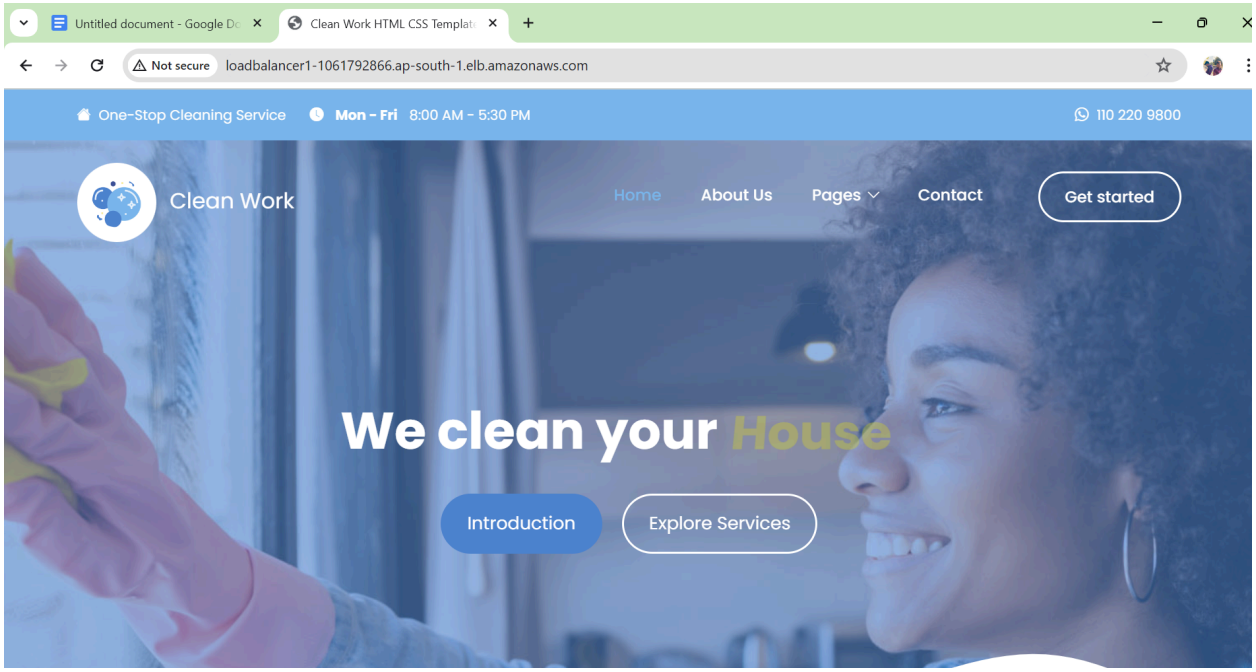
Tags Edit

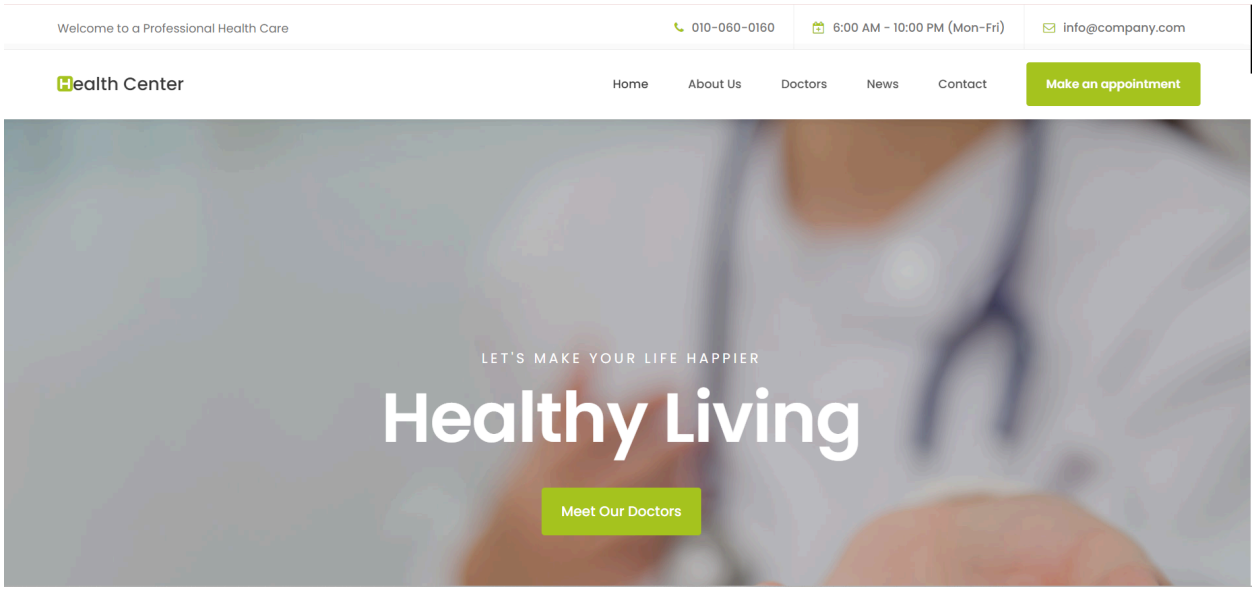
None


Successfully created load balancer: Loadbalancer1
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 > Loadbalancer1
Loadbalancer1
Actions
Details
Load balancer type
Application
Status
Provisioning
VPC
vpc-055cb9231e6edf043
IP address type
IPv4
Scheme
Internet-facing
Hosted zone
ZP97RAFLXTNZK
Availability Zones
subnet-039fe4ecec97386a3 ap-south-1a (aps1-az1)
subnet-08eda9d5b626ac7ea ap-south-1b (aps1-az3)
subnet-04107044f11d77b0a ap-south-1c (aps1-az2)
Date created
May 2, 2024, 22:10 (UTC+05:30)
Load balancer ARN
arn:aws:elasticloadbalancing:ap-south-1:558115454328:loadbalancer/app/Loadbalancer1/67fa587f37247312
DNS name Info
Loadbalancer1-1061792866.ap-south-1.elb.amazonaws.com (A Record)


EC2 > Load balancers
Load balancers (1)
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.
Actions
Create load balancer
Filter load balancers
1
Name
DNS name
State
VPC ID
Availability Zones
Type
Date created
Loadbalancer1
Loadbalancer1-10617928...
Provisioning..
vpc-055cb9231e6edf0...
3 Availability Zones
application
May 2, 2024, 22:10 (U...


Load balancers (1/1)
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.
Actions
Create load balancer
Filter load balancers
1
Name
DNS name
State
VPC ID
Availability Zones
Type
Date created
Loadbalancer1
Loadbalancer1-10617928...
Active
vpc-055cb9231e6edf0...
3 Availability Zones
application
May 2, 2024, 22:10 (U...
Load balancer: Loadbalancer1
Load balancer type
Application
Status
Active
VPC
vpc-055cb9231e6edf043
IP address type
IPv4
Scheme
Internet-facing
Hosted zone
ZP97RAFLXTNZK
Availability Zones
subnet-039fe4ecec97386a3 ap-south-1a (aps1-az1)
subnet-08eda9d5b626ac7ea ap-south-1b (aps1-az3)
subnet-04107044f11d77b0a ap-south-1c (aps1-az2)
Date created
May 2, 2024, 22:10 (UTC+05:30)
Load balancer ARN
arn:aws:elasticloadbalancing:ap-south-1:558115454328:loadbalancer/app/Loadbalancer1/67fa587f37247312
DNS name Info
Loadbalancer1-1061792866.ap-south-1.elb.amazonaws.com (A Record)


Untitled document - Google D
Clean Work HTML CSS Templat
Not secure
loadbalancer1-1061792866.ap-south-1.elb.amazonaws.com
One-Stop Cleaning Service
Mon - Fri 8:00 AM - 5:30 PM
110 220 9800
Clean Work
Home
About Us
Pages
Contact
Get started
We clean your House
Introduction
Explore Services


Welcome to a Professional Health Care
010-060-0160
6:00 AM - 10:00 PM (Mon-Fri)
info@company.com
Health Center
Home
About Us
Doctors
News
Contact
Make an appointment
LET'S MAKE YOUR LIFE HAPPIER
Healthy Living
Meet Our Doctors