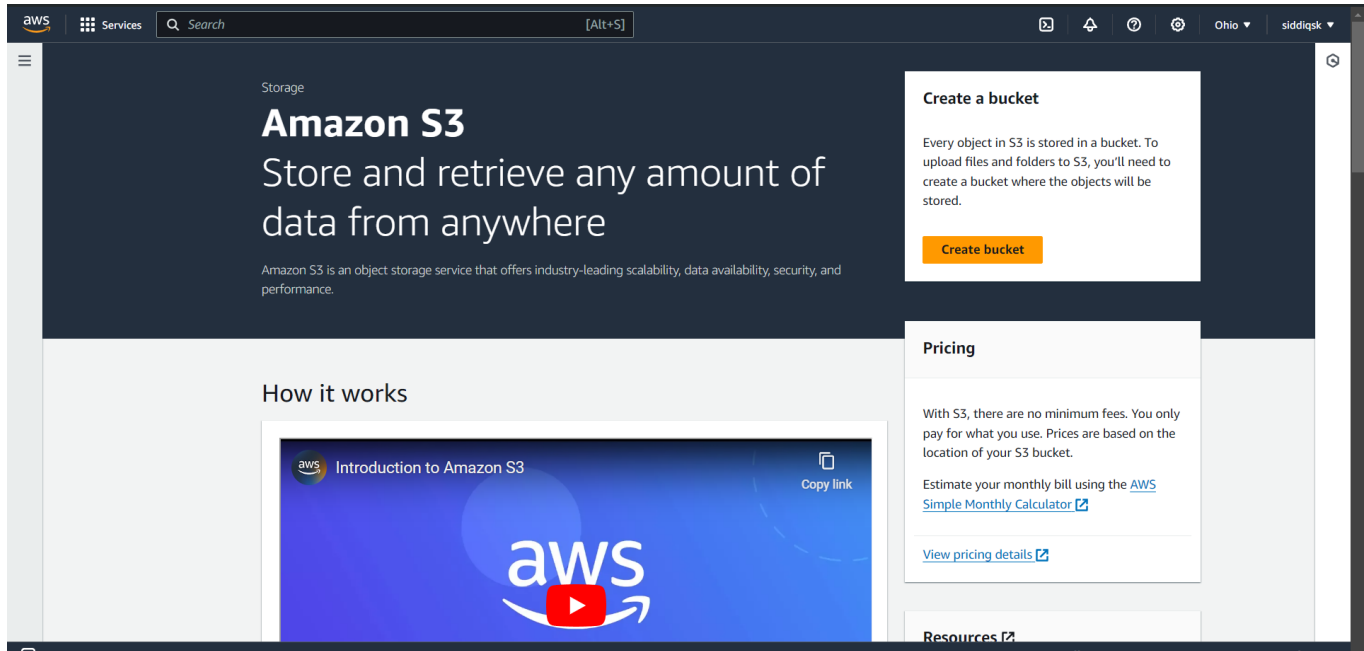


AWS Task-3

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

Create a S3 bucket, with no public access and upload files to the bucket & view the logs for the uploaded files



create the create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (Ohio) us-east-2

Bucket name [Info](#)

siddiq

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


☐ ACLs enabled

Objects in this bucket can be owned by other AWS

accounts. Access to this bucket and its objects can be

enter the unique bucket name.

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 objects within becoming public.

Uncheck "Block all public access"

► Advanced settings



After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

create the bucket

Amazon S3 > Buckets

► **Account snapshot - updated every 24 hours** All AWS Regions View Storage Lens dashboard

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

General purpose buckets | Directory buckets

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

< 1 > ⚙

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	siddiq1	US East (Ohio) us-east-2	View analyzer for us-east-2	July 30, 2024, 15:19:37 (UTC+05:30)

created the bucket

siddiq1 Info

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

Objects (0) Info Refresh Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

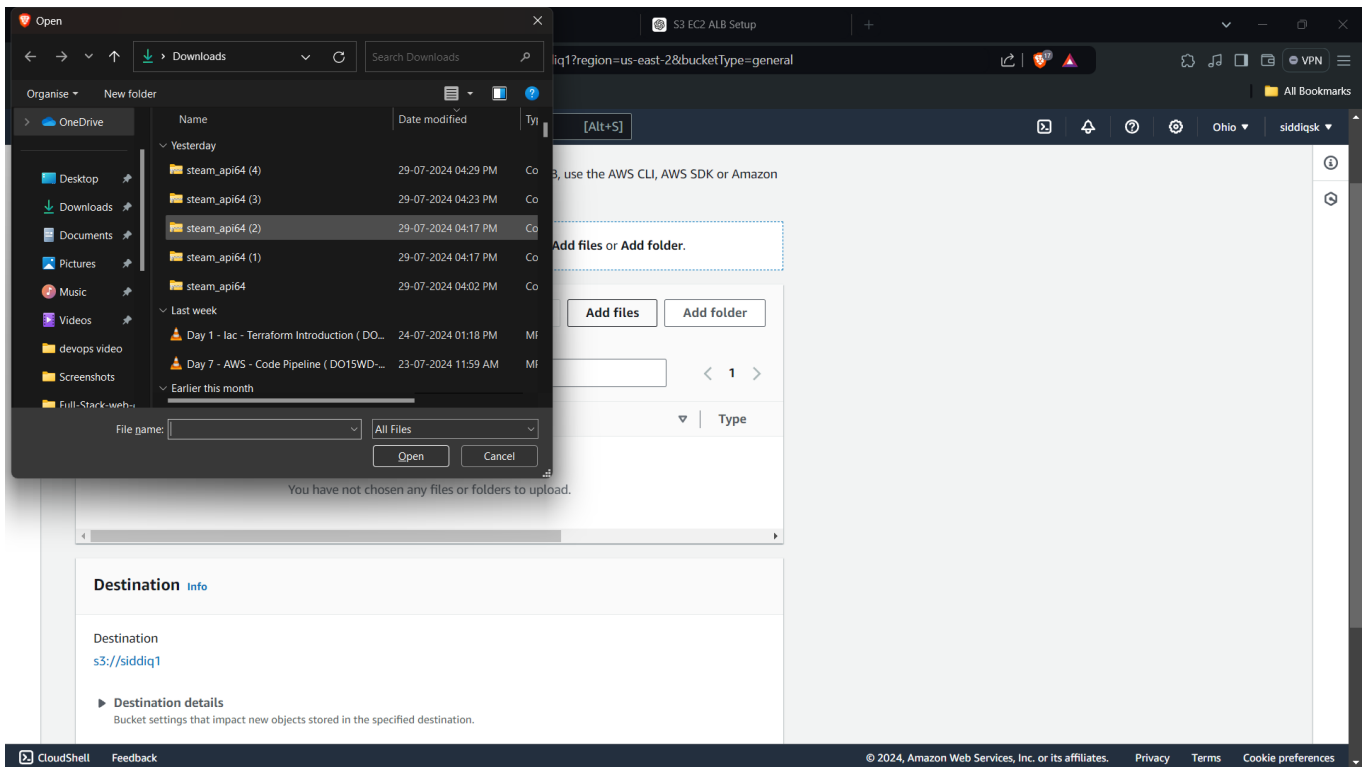
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

< 1 > ⚙

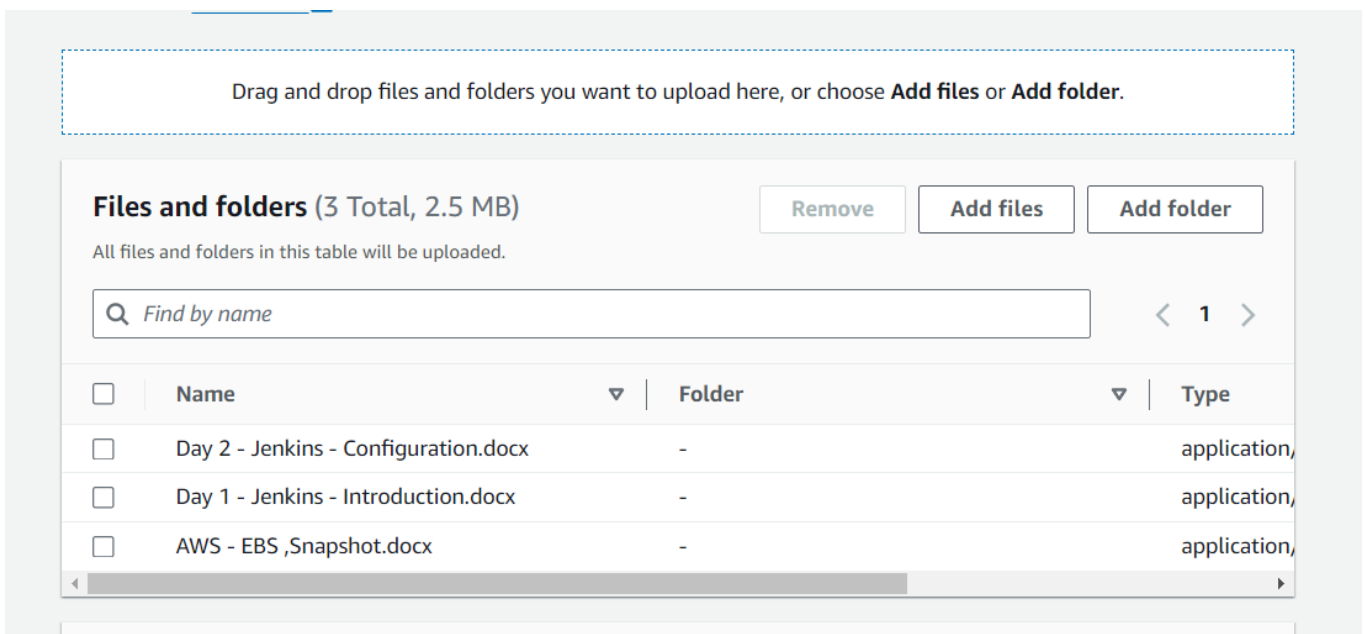
	Name	Type	Last modified	Size	Storage class
No objects					
You don't have any objects in this bucket.					

Upload

upload the demo file.



upload the files



file upload

Files and folders

Configuration

Files and folders (3 Total, 2.5 MB)

Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
Day 2 - Jenk...	-	application/...	604.0 KB	Succeeded	-
Day 1 - Jenk...	-	application/...	1.4 MB	Succeeded	-
AWS - EBS,...	-	application/...	614.8 KB	Succeeded	-

upload successfully

siddiq1

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (3) Info

Refresh

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 > ⚙

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	AWS - EBS_Snapshot.docx	docx	July 30, 2024, 15:21:57 (UTC+05:30)	614.8 KB	Standard
<input type="checkbox"/>	Day 1 - Jenkins - Introduction.docx	docx	July 30, 2024, 15:21:56 (UTC+05:30)	1.4 MB	Standard
<input type="checkbox"/>	Day 2 - Jenkins - Configuration.docx	docx	July 30, 2024, 15:21:54 (UTC+05:30)	604.0 KB	Standard

files

service log

Server access logging

Edit

Log requests for access to your bucket. Use [CloudWatch](#) to check the health of your server access logging. [Learn more](#)

Server access logging

Disabled

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 US East (Ohio) us-east-2 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://siddiq1

Browse S3

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

Destination Region

US East (Ohio) us-east-2

Destination bucket name

siddiq1

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.

select the S3 Bucket

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

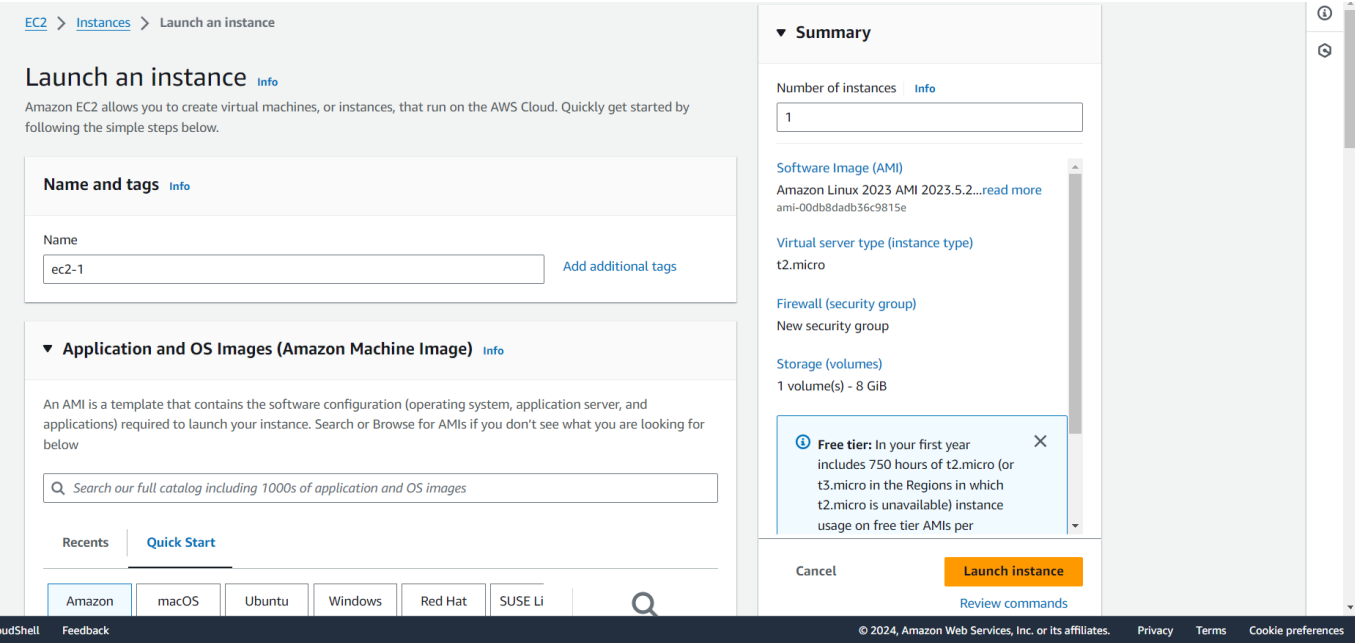
save the changes

logs for the uploaded files.

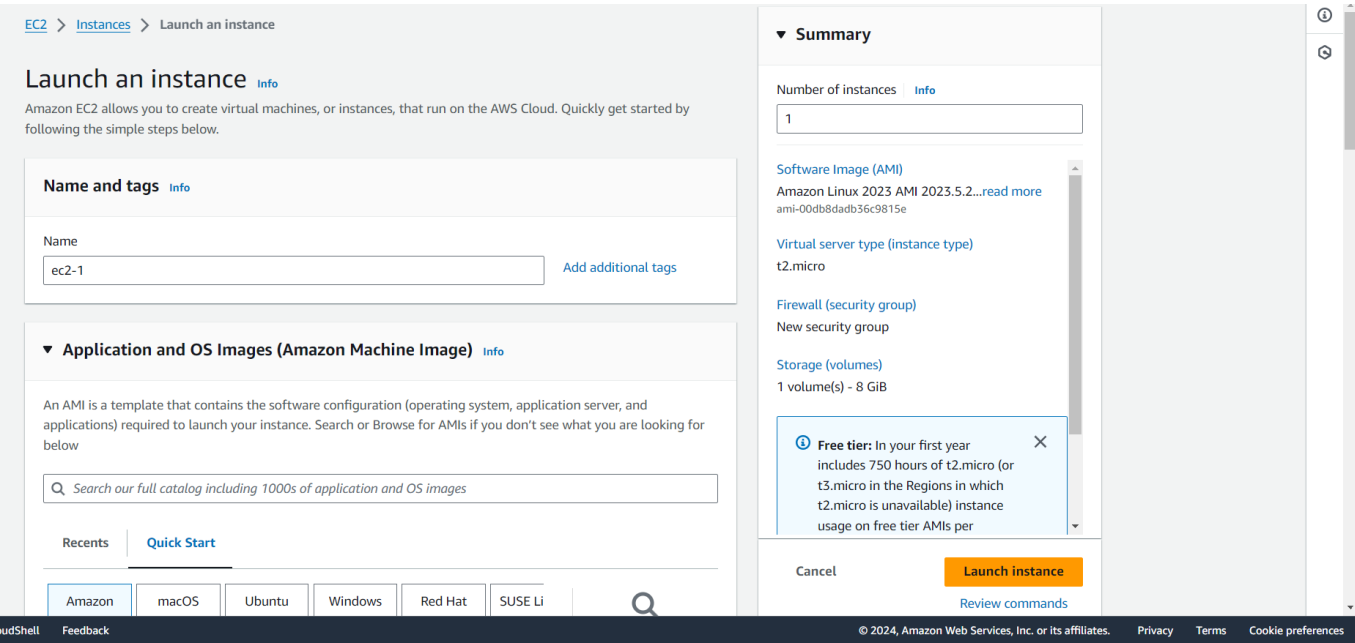
	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	AWS - EBS_Snapshot.docx	docx	July 30, 2024, 15:21:57 (UTC+05:30)	614.8 KB	Standard

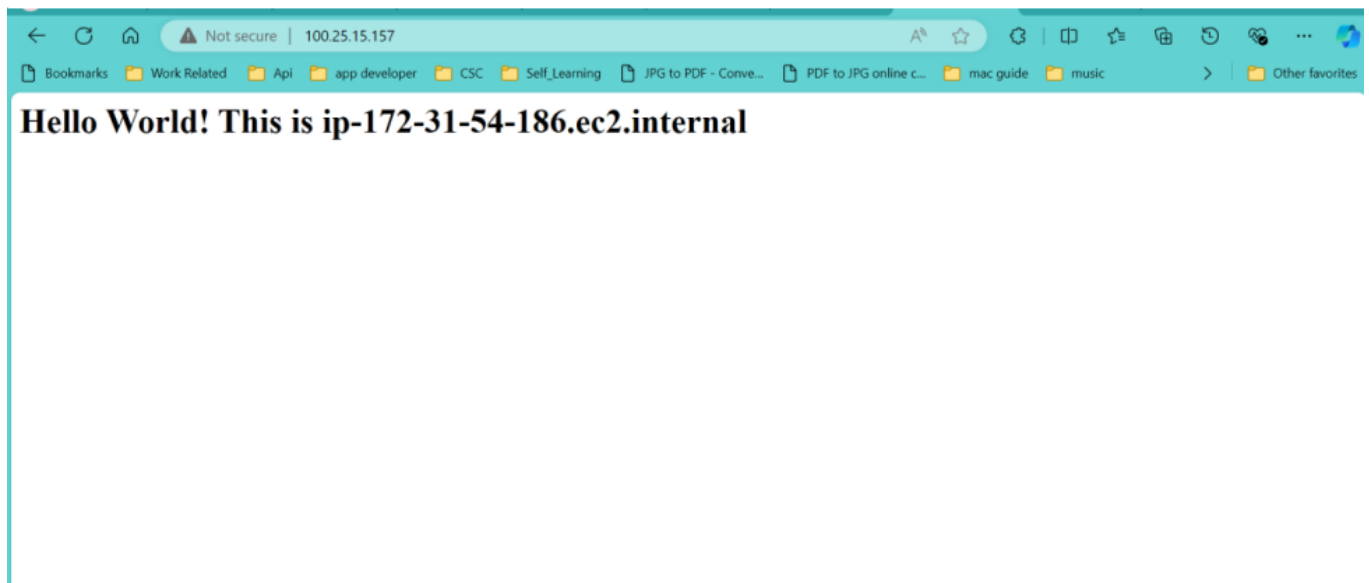
Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address

EC2 -1 CREATED



EC2 -2 CREATED

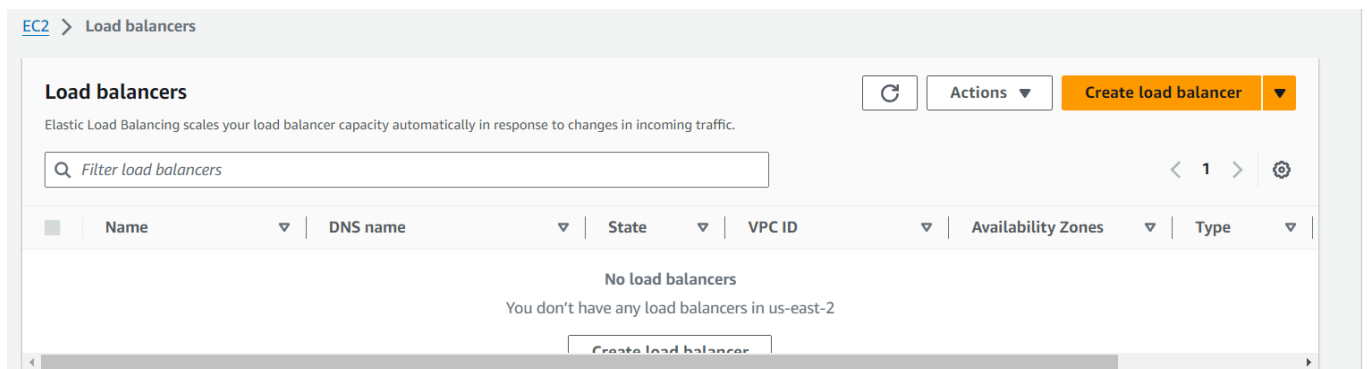




instance -1



instance -2

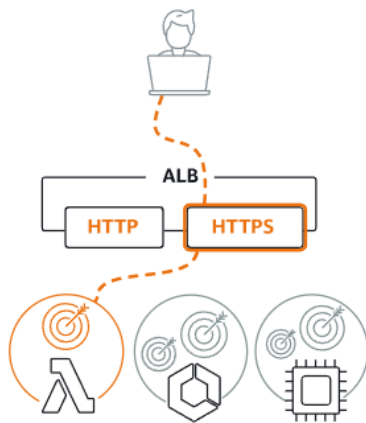


0 load balancers selected

Create the Load Balancers.

Application Load Balancer

[Info](#)

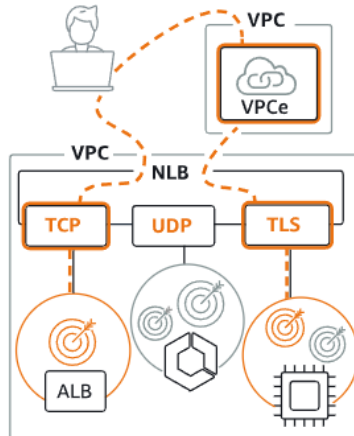


Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create

Network Load Balancer

[Info](#)



Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Gateway Load Balancer

[Info](#)



Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

create the Application Load Balancer.

► 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.

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.

Load balancer IP address type [Info](#)

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

☒ **IPv4**

Includes only IPv4 addresses.

☐ **Dualstack**



Includes IPv4 and IPv6 addresses.

load balancer name.

Network mapping [Info](#)

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

VPC [Info](#)

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#) . For a new VPC, [create a VPC](#) .

-
vpc-0c0040953cf84e9ab
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.

Availability Zones

☒ **us-east-2a (use2-az1)**

Subnet

subnet-0648fa965663af044
IPv4 subnet CIDR: 172.31.0.0/20



IPv4 address
Assigned by AWS

☐ **us-east-2b (use2-az2)**

☐ **us-east-2c (use2-az3)**

vpc and availability Zones

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

default

sg-0913b27e02114b2f7 VPC: vpc-0c0040953cf84e9ab

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.

select the security group.

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

Basic configuration [Edit](#)

kesavan sk

- Internet-facing
- IPv4

Security groups [Edit](#)

- default
[sg-0913b27e02114b2f7](#)

Network mapping [Edit](#)

VPC [vpc-0c0040953cf84e9ab](#)

- us-east-2a
[subnet-0648fa965663af044](#)

Listeners and routing [Edit](#)

- HTTP:80 defaults to
Target group not defined

Service integrations [Edit](#)

AWS WAF: None

AWS Global Accelerator: None

Tags [Edit](#)

None

Attributes

[i](#) 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

create the load balancer.

Target groups (1) [Info](#)

[Refresh](#)

Actions

Create target group

Filter target groups

< 1 > [Settings](#)

<input type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer
<input type="checkbox"/>	newtarget	arn:aws:elasticloadbalanci...	80	HTTP	Instance	None associated

target group

EC2 > Load balancers > kesavan

kesavan

↻

Actions ▾

▼ Details

Load balancer type

Application

Status

⌚ Provisioning

VPC

[vpc-0c0040953cf84e9ab](#)

Load balancer IP address type

IPv4

Scheme

Internet-facing

Hosted zone

Z3AADJGX6K TTL2

Availability Zones

[subnet-08dfd0dc787a5ef76](#) us-east-2b (use2-az2)
[subnet-0648fa965663af044](#) us-east-2a (use2-az1)

Date created

July 30, 2024, 15:52 (UTC+05:30)

Load balancer ARN

arn:aws:elasticloadbalancing:us-east-2:730335547691:loadbalancer/app/kesavan/5136c146f41cb729

DNS name [Info](#)

kesavan-1891297029.us-east-2.elb.amazonaws.com (A Record)

load balancer created.

Target group: newtarget

×

Details

TARGETS

Monitoring

Health checks

Attributes

Tags

Registered targets (0) [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.

Q Filter targets

< 1 > ⚙

Instance ID

▼

Name

▼

Port

▼

Zone

▼

Health status

▼

Health status details

Launch ...

▲

register targets.

Include as pending below

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

Review targets

Targets (2)

[Remove all pending](#)

Q Filter targets

☐ Show only pending

< 1 > ⚙

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-04b2b299294dcb147	EC2-2	80	Running	launch-wizard-3	us-east-2a	172.31.11.118	subnet-0648fa965663af044	July 30, 2024, 15:36 (UTC+05:30)
i-0291c3cf9e29898db	ec2-1	80	Running	launch-wizard-2	us-east-2a	172.31.15.15	subnet-0648fa965663af044	July 30, 2024, 15:35 (UTC+05:30)

2 pending

Cancel

Register pending targets

register targets.

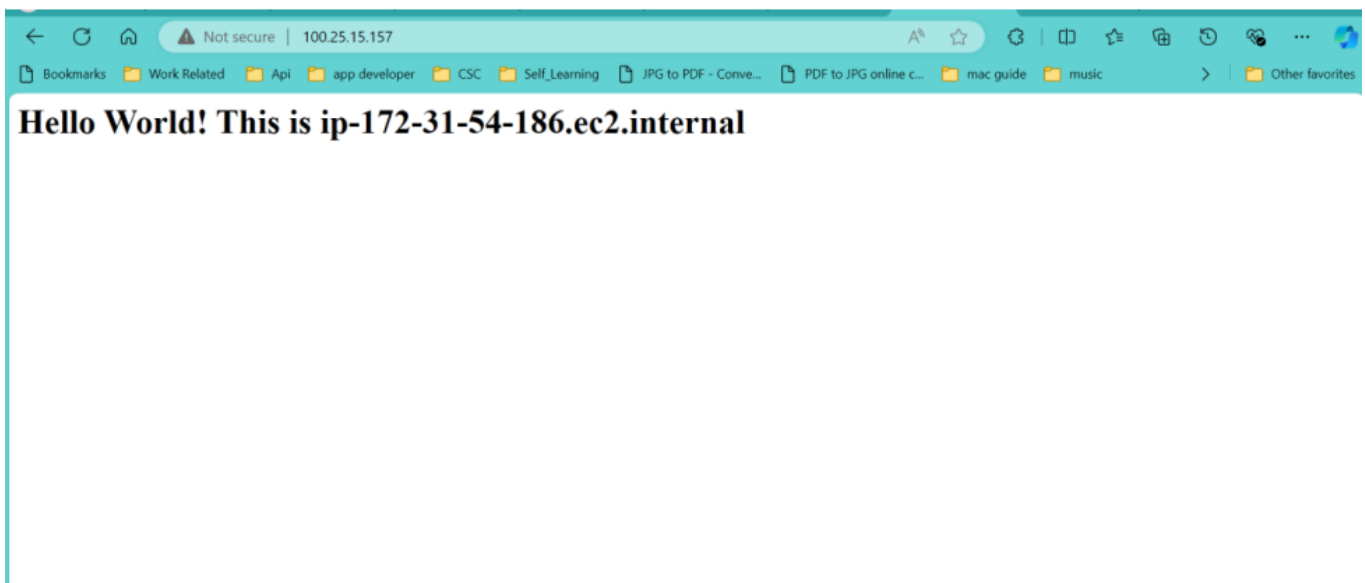
kesavan



Actions ▾

▼ Details

Load balancer type Application	Status ✔ Active	VPC vpc-0c0040953cf84e9ab	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z3AADJGX6KTTL2	Availability Zones subnet-08dfd0dc787a5ef76 us-east-2b (use2-az2) subnet-0648fa965663af044 us-east-2a (use2-az1)	Date created July 30, 2024, 15:52 (UTC+05:30)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-2:730335547691:loadbalancer/app/kesavan/5136c146f41cb729		DNS name Info kesavan-1891297029.us-east-2.elb.amazonaws.com (A Record)	



after reload:

