

TASK - 15

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

Creating a S3 bucket with no public access:

The screenshot shows the AWS Management Console interface for creating a new S3 bucket. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and a keyboard shortcut '[Alt+S]'. The breadcrumb trail indicates the path: 'Amazon S3 > Buckets > Create bucket'. The main heading is 'Create bucket' with an 'Info' link. Below this, a note states 'Buckets are containers for data stored in S3.' The 'General configuration' section is expanded, showing the 'AWS Region' as 'Asia Pacific (Mumbai) ap-south-1'. The 'Bucket name' field is populated with 'mys3buc1' and has an 'Info' link. A note below the field states: 'Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)'. There is a 'Copy settings from existing bucket - optional' section with a note: 'Only the bucket settings in the following configuration are copied.' and a 'Choose bucket' button. Below this, the 'Format: s3://bucket/prefix' is shown. The 'Object Ownership' section is also expanded, showing two options: 'ACLs disabled (recommended)' (selected) and 'ACLs enabled'. The 'ACLs disabled' option has a description: 'All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.' The 'ACLs enabled' option has a description: 'Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.' Below these options, the 'Object Ownership' is set to 'Bucket owner enforced'. At the bottom, the 'Block Public Access settings for this bucket' section is partially visible.

aws Services Search [Alt+S]

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](#)

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

aws

Services

Search

[Alt+S]

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.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable

☐ Enable

Tags - optional (0)

aws

Services

Search

[Alt+S]

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-KMS. [Learn more](#)

☐ Disable

☒ Enable

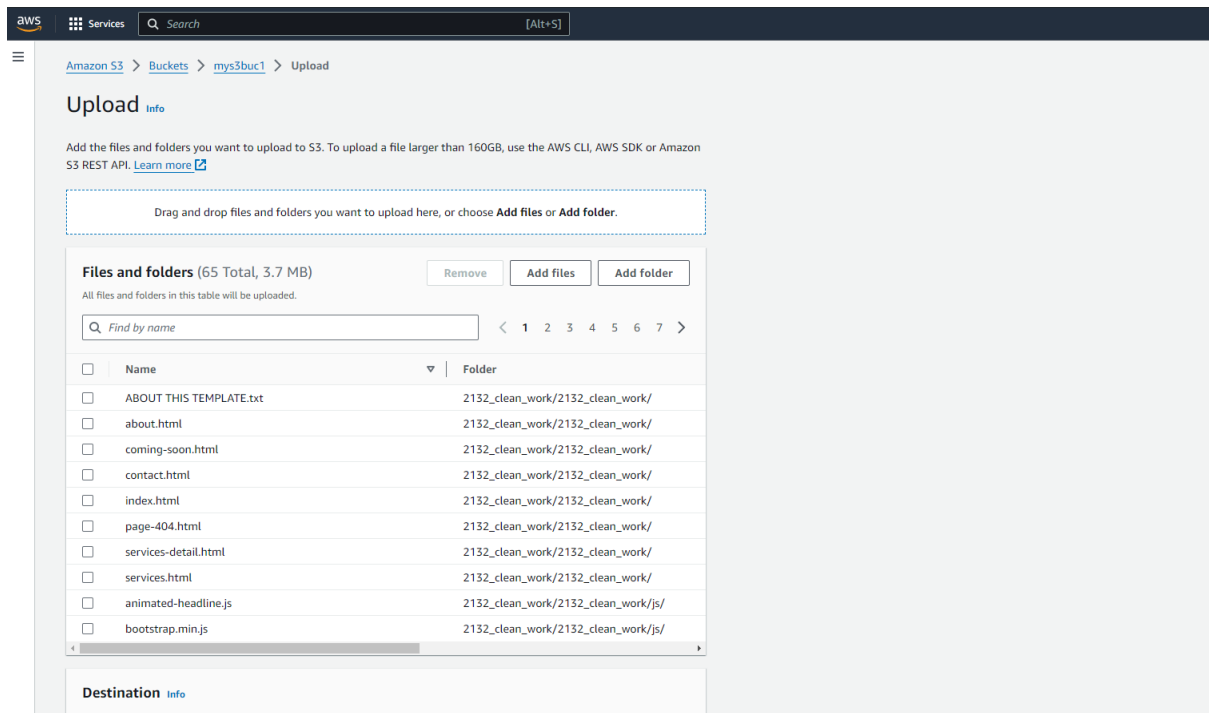
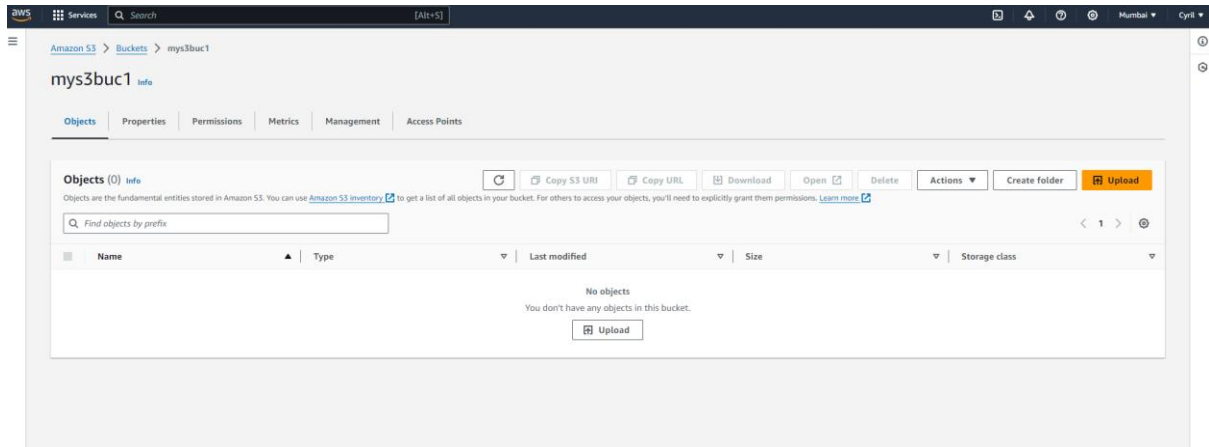
► Advanced settings

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

Cancel

Create bucket

Uploading files to the bucket:



contact.html

2132_clean_work/2132_clean_work/

index.html

2132_clean_work/2132_clean_work/

page-404.html

2132_clean_work/2132_clean_work/

services-detail.html

2132_clean_work/2132_clean_work/

services.html

2132_clean_work/2132_clean_work/

animated-headline.js

2132_clean_work/2132_clean_work/js/

bootstrap.min.js

2132_clean_work/2132_clean_work/js/

Destination

Info

Destination

s3://mys3buc1

► 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.

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

Summary

Destination

s3://mys3buc1

Succeeded

8 files, 161.2 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (8 Total, 161.2 KB)

Find by name

< 1 >

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	41.3 KB	Succeeded	-
services-det...	-	text/html	26.6 KB	Succeeded	-
page-404.ht...	-	text/html	13.5 KB	Succeeded	-
contact.htm...	-	text/html	16.2 KB	Succeeded	-
coming-soo...	-	text/html	14.2 KB	Succeeded	-
about.html	-	text/html	18.1 KB	Succeeded	-
services.htm...	-	text/html	30.9 KB	Succeeded	-
ABOUT THI...	-	text/plain	510.0 B	Succeeded	-

Amazon S3 > Buckets > mys3buc1 > 2132_clean_work/ > 2132_clean_work/

2132_clean_work/

Copy S3 URI

Objects

Properties

Objects (12)

Info

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

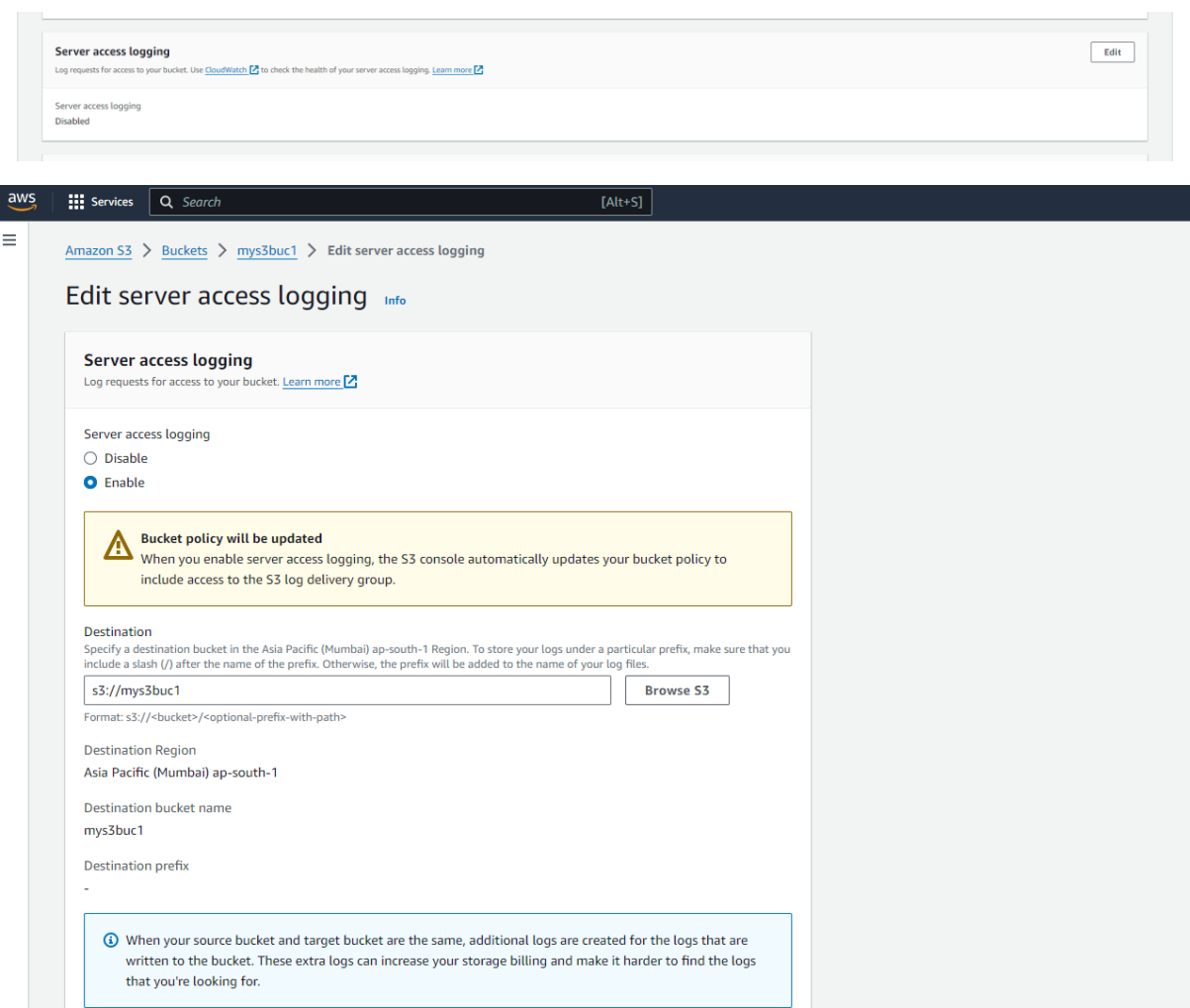
Upload

Find objects by prefix

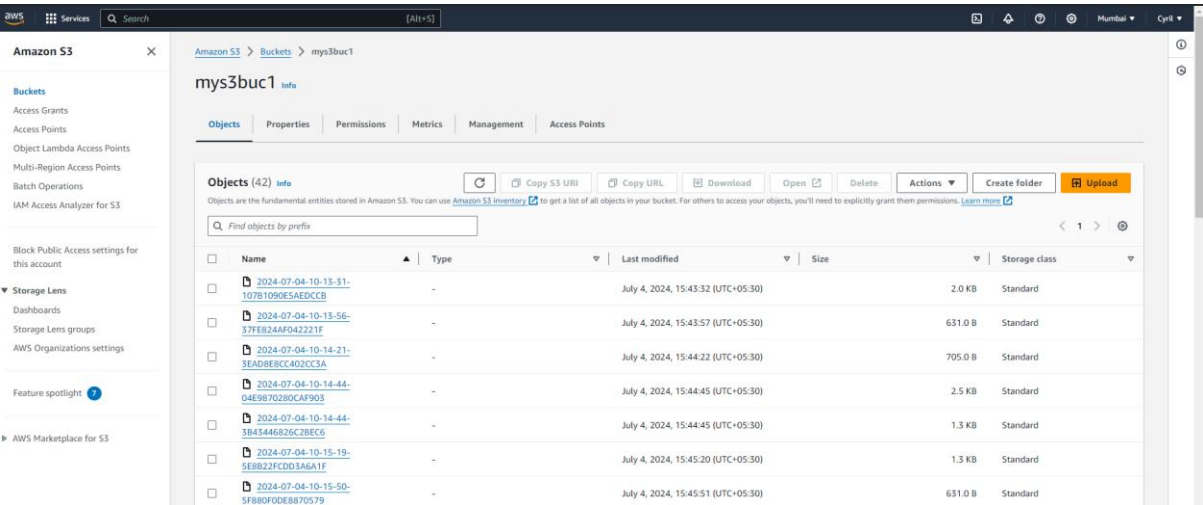
< 1 >

Name	Type	Last modified	Size	Storage class
ABOUT THIS TEMPLATE.txt	txt	July 4, 2024, 14:53:27 (UTC+05:30)	510.0 B	Standard
about.html	html	July 4, 2024, 14:53:28 (UTC+05:30)	18.1 KB	Standard
coming-soon.html	html	July 4, 2024, 14:53:28 (UTC+05:30)	14.2 KB	Standard
contact.html	html	July 4, 2024, 14:53:28 (UTC+05:30)	16.2 KB	Standard
css/	Folder	-	-	-
fonts/	Folder	-	-	-
images/	Folder	-	-	-
index.html	html	July 4, 2024, 14:53:29 (UTC+05:30)	41.3 KB	Standard
js/	Folder	-	-	-
page-404.html	html	July 4, 2024, 14:53:29 (UTC+05:30)	13.5 KB	Standard
services-detail.html	html	July 4, 2024, 14:53:29 (UTC+05:30)	26.6 KB	Standard
services.html	html	July 4, 2024, 14:53:30 (UTC+05:30)	30.9 KB	Standard

Accessing the log of the bucket:



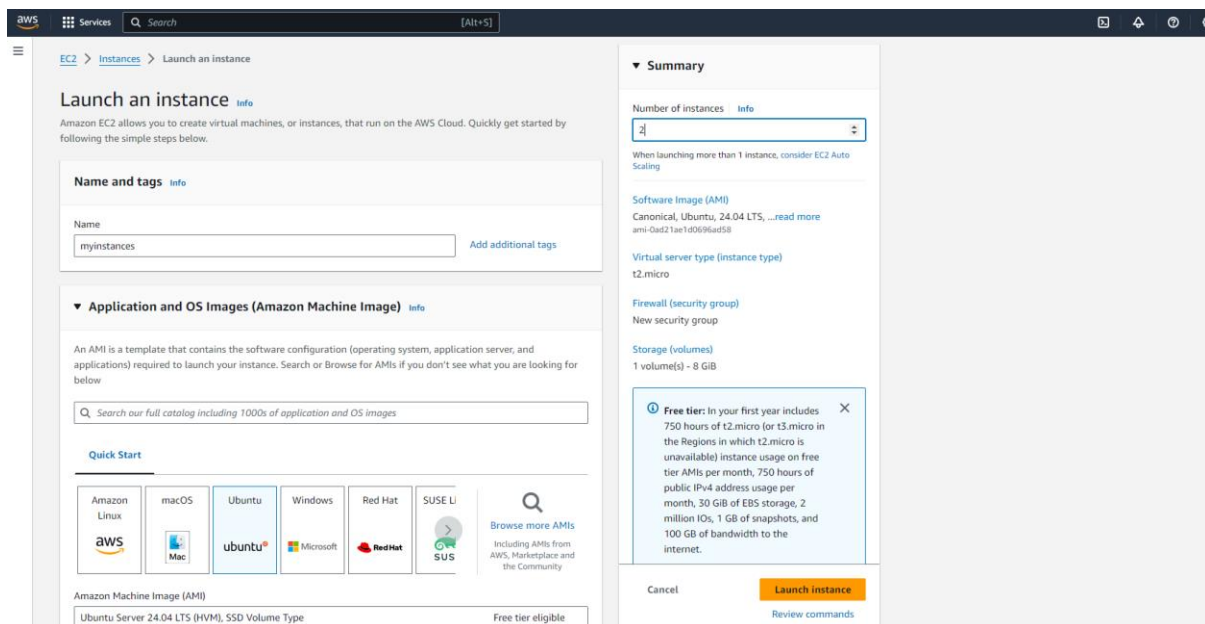
S3 bucket logs:



```
1 fcf1990970127ced4c1aa7fe37b86f7fc1e6c447891650827c021296719027ed7 mys3buc1 [04/Jul/2024:09:33:48 +0000] 120.56.141.9 fcf1990970127ced4c1aa7fe37b86f7fc1e6c447891650827c021296719027ed7 Y3548211P03NOPJS REST.GET.BUCKET - "GET /mys3buc1?list-type=2
&encoding-type=url&max-keys=1000&fetch-owner=true&delimiter=2F&prefix= HTTP/1.1" 200 - 2690 - 12 11 "-" "S3Console/0.4, aus-internal/3 aus-sdk-java/1.12.488 Linux/5.10.218-186.862.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.372-b08 java/1.8.0_
372 vendor/Oracle_Corporation cfg/retry-mode/standard" - H2zA9pC1J5Ja1a5yN2J2rG8agtP74aaA700pyVayVc0teCB1/eV9HfMR+/H9bHfFA1qM6R+ SigV4 TLS_AES_128_GCM_SHA256 AuthHeader s3.ap-south-1.amazonaws.com TLSv1.3 - -
2 fcf1990970127ced4c1aa7fe37b86f7fc1e6c447891650827c021296719027ed7 mys3buc1 [04/Jul/2024:09:33:48 +0000] 120.56.141.9 fcf1990970127ced4c1aa7fe37b86f7fc1e6c447891650827c021296719027ed7 Y3543FAC3MIG6GCE REST.GET.BUCKET - "GET /mys3buc1?list-type=2
&encoding-type=url&max-keys=1000&fetch-owner=true&delimiter=2F&prefix= HTTP/1.1" 200 - 2690 - 23 22 "-" "S3Console/0.4, aus-internal/3 aus-sdk-java/1.12.488 Linux/5.10.218-186.862.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.372-b08 java/1.8.0_
372 vendor/Oracle_Corporation cfg/retry-mode/standard" - /BdHBFQyvaAndRoLfa8L878ra/sbWLA0BSPLFGP1QV1ZC6eJspTe7LZnoG1HTgYUhdFamCs+ SigV4 TLS_AES_128_GCM_SHA256 AuthHeader s3.ap-south-1.amazonaws.com TLSv1.3 - -
3 fcf1990970127ced4c1aa7fe37b86f7fc1e6c447891650827c021296719027ed7 mys3buc1 [04/Jul/2024:09:33:48 +0000] 120.56.141.9 fcf1990970127ced4c1aa7fe37b86f7fc1e6c447891650827c021296719027ed7 Y35AGMHNDFFPBCZ REST.GET.BUCKET - "GET /mys3buc1?list-type=2
&encoding-type=url&max-keys=1000&fetch-owner=true&delimiter=2F&prefix= HTTP/1.1" 200 - 2690 - 9 9 "-" "S3Console/0.4, aus-internal/3 aus-sdk-java/1.12.488 Linux/5.10.218-186.862.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.372-b08 java/1.8.0_
372 vendor/Oracle_Corporation cfg/retry-mode/standard" - PvcovzR02AMC2qUP/LxChpdT3AMJYf173rqc+G2TVYwT302H0K1c988g2P8QV0puznKC0hKQg+ SigV4 TLS_AES_128_GCM_SHA256 AuthHeader s3.ap-south-1.amazonaws.com TLSv1.3 - -
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

Launching 2 EC2 instances with the same application



aws

Services

Search

[Alt+S]

VPC - required

Info

vpc-049bb71bf494e967f

(default)

172.31.0.0/16

Subnet

Info

No preference

Create new subnet

Auto-assign public IP

Info

Enable

Additional charges apply when outside of free tier allowance

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

Security group name - required

launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _~ / ! @ # \$ % & ' () * + , - . : ;

Description - required

Info

launch-wizard-1 created 2024-07-04T09:36:05.818Z

Inbound Security Group Rules

Security group rule 1 (TCP, 22)

Remove

Type

Info

ssh

Protocol

Info

TCP

Port range

Info

22

Source type

Info

Custom

Source

Info

Add CIDR, prefix list or security

Description - optional

Info

e.g. SSH for admin desktop

Add security group rule

Summary

Number of instances

Info

2

When launching more than 1 instance, consider EC2 Auto Scaling

Software Image (AMI)

Canonical, Ubuntu, 24.04 LTS, ...read more

ami-0ad21ae1d0696ad58

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, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel

Launch instance

Review commands

aws

Services

Search

[Alt+S]

V2 only (token required)

For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.

Metadata response hop limit

Info

2

Allow tags in metadata

Info

Select

User data - optional

Info

Upload a file with your user data or enter it in the field.

Choose file

#!/bin/bash
sudo apt update
sudo apt install apache2 wget unzip -y
wget https://www.tooplate.com/zip-templates/2132_clean_work.zip
unzip 2132_clean_work.zip
sudo cp -r 2132_clean_work/* /var/www/html/
sudo systemctl restart apache2

User data has already been base64 encoded

Summary

Number of instances

Info

2

When launching more than 1 instance, consider EC2 Auto Scaling

Software Image (AMI)

Canonical, Ubuntu, 24.04 LTS, ...read more

ami-0ad21ae1d0696ad58

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, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel

Launch instance

Review commands

aws

Services

Search

[Alt+S]

Mumbai

Cyril

EC2 Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Successfully initiated termination of i-0fa7d05aa1f1957ecj-099b71e390f3fab8e

Instances (2)

Info

Find instance by attribute or tag (case-sensitive)

All states

running

Clear filters

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	myinstances1	i-09x92f490093817fb	Running	t2.micro	Initializing	View alarms +	ap-south-1a	ec2-13-233-230-190.ap...	13.233.230.190	-
<input type="checkbox"/>	myinstances2	i-0139394072528343b	Running	t2.micro	Initializing	View alarms +	ap-south-1a	ec2-13-201-32-93.ap-s...	13.201.32.93	-

Creating a Load Balancer:

aws

Services

Search

[Alt+S]

Home

Help

Account

Cyrl


EC2 > Load balancers > Compare and select load balancer type

Compare and select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

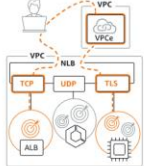
Load balancer types

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.

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-

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

aws

Services

Search

[Alt+S]

Home

Help

Account

Cyrl

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.

mylb

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 type of IP addresses that your subnets use. Public IPv4 addresses have an additional cost.

☒ IPv4

Includes only IPv4 addresses.

☐ Dualstack

Includes IPv4 and IPv6 addresses.

☐ Dualstack without public IPv4

Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

aws

Services

Search

[Alt+S]

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-049bb71bf494e967f

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)**

Subnet

subnet-07aeb170ff4b5e49

IPv4 address

Assigned by AWS

☒ **ap-south-1b (aps1-az3)**

Subnet

subnet-027f12a2fc673cfac

IPv4 address

Assigned by AWS

☒ **ap-south-1c (aps1-az2)**

Subnet

subnet-03dd3bb40c1821259

IPv4 address

Assigned by AWS

Creating Security Group for the load balancer:

aws

Services

Search

[Alt+S]

Mumbai

Cyrl

EC2

Security Groups

Create security group

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

mysg

Name cannot be edited after creation.

Description Info

mysg

VPC Info

vpc-049bb71bf494e967f

Inbound rules Info

Type Info

Custom TCP

Protocol Info

TCP

Port range Info

80

Source Info

Anywhere-I...

Description - optional

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.

X

Creating Target Group:

Services

Search

[Alt+S]

• 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

mylbtarget

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

Register targets

Step 2

Available instances (2)

Instance ID	Name	State	Security groups	Zone	Private IPv4 address
i-09a92f490093817fb	myinstances1	Running	launch-wizard-1	ap-south-1a	172.31.42.121
i-0139394072528343b	myinstances2	Running	launch-wizard-1	ap-south-1a	172.31.46.199

0 selected

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

80

1-65535 (separate multiple ports with comma)

Include as pending below

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

Review targets

Targets (2)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-09a92f490093817fb	myinstances1	80	Running	launch-wizard-1	ap-south-1a	172.31.42.121	subnet-07aecb170ff4b5e49	July 4, 2024, 15:09 (UTC+05:30)
i-0139394072528343b	myinstances2	80	Running	launch-wizard-1	ap-south-1a	172.31.46.199	subnet-07aecb170ff4b5e49	July 4, 2024, 15:09 (UTC+05:30)

Continuation of Load Balancer Creation:

aws

Services

Search

[Alt+S]

msg

sg-08712423635593051

VPC: vpc-049bb71bf494e967f

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

Forward to

mylbtarget

HTTP

⌂

1-65535

Target type: Instance, IPv4

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

► Load balancer tags - optional

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Optimize with service integrations - optional

Optimize your load balancing architecture by integrating AWS services with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the load balancer's "Integrations" tab.

aws

Services

Search

[Alt+S]

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

mylb

Internet-facing

IPv4

Security groups

msg

sg-08712423635593051

Network mapping

VPC

vpc-049bb71bf494e967f

ap-south-1a

subnet-07a6cb170ff4b5e49

ap-south-1b

subnet-027f12a2fc673cfac

ap-south-1c

subnet-03dd3bb40c1821259

Listeners and routing

HTTP:80 defaults to

mylbtarget

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

Connecting to the instance through the load balancer DNS name:

