

AWS Task-3

Task-1: Create a S3 bucket, with no public access and upload files to the bucket & view the logs using cloudwatch for the uploaded files.

1. Creating S3 bucket.

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

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

Bucket type: [Info](#)

General purpose Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name: [Info](#) aws-s3-bucket-task3

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn more](#)

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.

Object Ownership

ACLs disabled (recommended) All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using object-level 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.

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 block new buckets and objects using 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 access to buckets and objects granted through new public bucket or access point policies S3 will block new buckets and objects using policies that grant public access to buckets and objects.

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 that define their own public access to buckets and objects.

2. s3 bucket created.

General purpose buckets (1/1) Info		
Create bucket		
Buckets are containers for data stored in S3.		
<input type="text"/> Find buckets by name	Copy ARN	Empty
Name	AWS Region	Creation date
aws-s3-bucket-task3	Asia Pacific (Mumbai) ap-south-1	January 6, 2026, 13:24:33 (UTC+05:30)

3. uploading files to s3 bucket.

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 SDKs 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, 957.0 KB)

All files and folders in this table will be uploaded.

Find by name	Remove	Add files	Add folder
<input type="checkbox"/> Name	Remove	Add files	Add folder
VPC_IoW.pdf			

Destination [Info](#)

Destination: [s3://aws-s3-bucket-task3](#)

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](#)

4. files uploaded.

The screenshot shows the AWS S3 console interface. At the top, a green header bar indicates "Upload succeeded" with a link to the "Files and folders table". Below this, a summary table shows the destination as "s3://aws-s3-bucket-task" with one succeeded file (1 file, 957.0 KB) and zero failed files. The main area displays a table of files under the "Files and folders" tab, showing one entry: "VPC_IGW.pdf" which is an application/pdf file of size 957.0 KB and status "Succeeded".

5. creating cloud trail.

The screenshot shows the "Quick trail create" wizard. In the "Trail details" step, a trail name "s3-activity-trail" is entered. A note states that logs will be stored in a new S3 bucket named "aws-cloudtrail-logs-484733236792-e153ba3e". A note also mentions potential charges for the S3 bucket. At the bottom, there are "Cancel" and "Create trail" buttons.

6. could trail created.

The screenshot shows the "Trails" list page. It displays a single trail named "s3-activity-trail" with the ARN "arn:aws:cloudtrail:ap-south-1:484733236792:trail/s3-activity-trail". The trail is set up for multi-region logging from the "Asia Pacific (Mumbai)" region. It is currently disabled and has no associated S3 bucket or CloudWatch Logs log group. The status is "Logging".

7. adding s3 bucket details in cloud trail under data events.

The screenshot shows the "Edit arn:aws:cloudtrail:ap-south-1:484733236792:trail/s3-activity-trail" configuration page. Under the "Events" section, "Data events" are selected. The "Data events" section shows that advanced event selectors are enabled. The "Data event: S3" section is expanded, showing a dropdown for "Resource type" set to "S3", a "Log selector template" dropdown with "Log all events" selected, and a "Selector name - optional" input field. At the bottom, there are "Cancel" and "Save changes" buttons.

8. send cloud trail logs to cloud watch. Enable cloud watch logs and create log group and IAM role.

CloudWatch Logs - optional
Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. [Learn more](#)

CloudWatch Logs [Info](#)
 Enabled

Log group Info
 New
 Existing

Log group name
/aws/cloudtrail/s3
1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

IAM Role Info
AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.
 New
 Existing

Role name
cloudtrail

9. uploading file again in s3 bucket.

Upload succeeded
For more information, see the [Files and folders table](#).

Upload: status [Close](#)

After you navigate away from this page, the following information is no longer available.

Summary
Destination: s3://aws-s3-bucket-task3
Succeeded: 1 file, 41.6 KB (100.00%)
Failed: 0 files, 0 B (0%)

Files and folders [Configuration](#)

Files and folders (1 total, 41.6 KB)
Find by name
Name | Folder | Type | Size | Status | Error
Raval.pdf | - | application/pdf | 41.6 KB | Succeeded | -

10. checking logs in cloud watch under log groups.

▼	3	2026-01-06T08:52:48.218Z	PutObject	VPC_IGW.pdf
Field		Value		
@entity.KeyAttributes.ResourceType		AWS::CloudTrail::Trail		
@entity.KeyAttributes.Type		AWS::Resource		
@entity.KeyAttributes.Identifier		s3-activity-trail		
@aws.account		484733236792		
@aws.region		ap-south-1		
@data_format		Default		
@data_source_name		aws_cldtrail		
@data_source_type		data		
@entity.Attributes.AWS.Resource.ARN		arn:aws:cloudtrail:ap-south-1:484733236792:trail/s3-activity-trail		
@ingestionTime		1767689568233		
@log		484733236792:/aws/cloudtrail/s3		
@logGroupId		26553a0a-cf2e-4b11-90f8-0f96943b72fc		
@logStream		484733236792_CloudTrail_ap-south-1_2		
@logStreamId		26553a0a-cf2e-4b11-90f8-0f96943b72fc:18de9474b455cbf49338c09a7fd18ef23		
@message		{ "eventVersion": "1.11", "userIdentity": { "type": "Root", "principalId": "484733236792", "arn": "arn:aws:iam::484733236792" }}		

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "cloudtrail.amazonaws.com"
  },
  "eventTime": "2026-01-06T08:51:19Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "ap-south-1",
  "sourceIPAddress": "cloudtrail.amazonaws.com",
  "userAgent": "CloudTrail.amazonaws.com",
  "requestParameters": {
    "bucketName": "aws-cloudtrail-logs-484733236792-e1538a3e",
    "Host": "aws-cloudtrail-logs-484733236792-e1538a3e.s3.ap-south-1.amazonaws.com",
    "x-amz-acl": "bucket-owner-full-control",
    "x-amz-server-side-encryption": "AES256",
    "key": "AWSLogs/484733236792/CloudTrail/us-east-1/2026/01/06/484733236792_CloudTrail_us-east-1_20260106T08502_m9JY1skJdtWczER.json.gz"
  },
  "responseElements": {
    "Back to top ^"
}
```

Task-2: 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. Created two ec2 instances.

<input type="checkbox"/> instances2	i-06fae8b7c631cc8d	Running	Q Q	t3.micro	3/3 checks passed	View alarms +	eu-north-1b	ec2-13-48-4
<input type="checkbox"/> instance1	i-01c88c7433970155	Running	Q Q	t3.micro	3/3 checks passed	View alarms +	eu-north-1b	ec2-51-20-4

2. Install nginx in both instances.

```
NO VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-38-131:~$ sudo systemctl start nginx
ubuntu@ip-172-31-38-131:~$ sudo systemctl enable nginx
Synchronizing state of nginx.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable nginx
ubuntu@ip-172-31-38-131:~$
```

```
ubuntu@ip-172-31-37-10:~$ sudo systemctl enable nginx
Synchronizing state of nginx.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable nginx
ubuntu@ip-172-31-37-10:~$
```

3. creating target groups.

Create target group
A target group can be made up of one or more targets. Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Step 2 - recommended

Target groups

Create **Describe and create**

Create target group

Settings - immutable
Choose a target type for the load balancer and internet will route traffic to your target. These settings can't be modified after target group creation.

Target type
Select the target type you want to target. Only the selected target type can be reported by the target group.

Instances
Instances are targets in Amazon Lambda, AWS Lambda functions, and AWS Lambda layers. You can also target Lambda functions in AWS Lambda managed environments.

IP addresses
IP addresses are targets in Amazon VPC, Direct Connect, and AWS Wavelength. You can also target IP addresses in AWS Lambda managed environments.

Application Load Balancer
Allows use of static IP addresses and instances with an Application Load Balancer. You can also target Application Load Balancers in AWS Lambda managed environments.

Target group name
Name must be unique per Region per AWS account.

Port
Port number where targets receive traffic. Can be overridden for individual targets.

443/443

Address type
Only address types are included if address type is required for this target group.

IPv4
Each target has a default network interface (netif) that is assigned the primary private IPv4 address. The internet primary private IP address is the IP address that can be assigned to the target.

IPv6
Each target has a primary IPv6 address. This is configured as the Internet-facing network interface (netif).

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

vpce-outside-15454807

Protocol
Protocols for communication between the load balancer and targets.

HTTP
Targets receive requests using HTTP/1.1. Supported when the request protocol is set to HTTP/1.1 or all/HTTP.

HTTP2
Targets receive requests using HTTP/2.0. Supported when the request protocol is set to HTTP/2.0 or all/HTTP2.

HTTPS
Targets receive requests using HTTPS. Supported when the request protocol is set to HTTPS or all/HTTPS, but HTTPS-specific features are not available.

Health checks
The Amazon Cloud Load Balancer periodically sends requests, per the setting below, to the registered targets to test their status.

Health check protocol
 HTTP

Health check path
Enter the desired path ("") to perform health checks on the hosts, or specify a custom path if preferred.

Up to 1024 characters allowed.

Advanced health check settings

Target optimizer **optional** **optimal**
Load balancers automatically balance the target traffic based on the target's current concurrency levels.

Target control port
The port number that the load balancer communicates to targets. This value can't be modified after target group creation.

Attributes
 Certain default attributes will be applied for your target group. You can view and edit them after creating the target group.

Tags - optional

Available instances (2)

Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-06fae8b7c631cc08d	instances2	Running	launch-wizard-21	eu-north-1b	172.31.38.131	subnet-0cff70384eae259ca	January 6, 2026, 15:20 (UTC+0:30)
i-01c88c7f433970155	instance1	Running	launch-wizard-20	eu-north-1b	172.31.37.10	subnet-0cff70384eae259ca	January 6, 2026, 15:01 (UTC+0:30)

Review targets

Targets (2)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-06fae8b7c631cc08d	instances2	80	Running	launch-wizard-21	eu-north-1b	172.31.38.131	subnet-0cff70384eae259ca	January 6, 2026, 15:20 (UTC+0:30)
i-01c88c7f433970155	instance1	80	Running	launch-wizard-20	eu-north-1b	172.31.37.10	subnet-0cff70384eae259ca	January 6, 2026, 15:01 (UTC+0:30)

Step 1: Review and create

Step 2: Register targets

Step 3: Review and create

Step 4: Target group details

Target group details

Name: alb	Target type: Instance	Protocol: Port	Protocol version: HTTP1
VPC: vpc-04aa45a7f345246b7	IP address type: IPv4		

Health check details

Health check protocol: HTTP	Health check path: /	Health check port: traffic-port	Interval: 30 seconds
Timeout: 5 seconds	Healthy threshold: 5	Unhealthy threshold: 2	Success codes: 200

Step 2: Register targets

Targets (2)

Instance ID	Name	Port	Zone
i-06fae8b7c631cc08d	instances2	80	eu-north-1b
i-01c88c7f433970155	instance1	80	eu-north-1b

4. target group is created.

Target groups (1/1) [Info](#) | [What's new?](#)

Target group: ALB

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
ALB	arn:aws:elasticloadbalancing:eu-north-1:484733236792:targetgroup/ALB/28187a7b9c6208d0	80	HTTP	Instance	None associated	vpc-04aa45a7f345246b7

Target group: ALB

Target type	Protocol: Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-04aa45a7f345246b7
IP address type	Load balancer		
IPv4	None associated		

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
2	0	0	2	0	0

5. creating 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.

myfirstalb

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

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

 Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- 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.

 Dualstack without public IPv4

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

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](#).

vpc-04aa45a7f345246b7

172.31.0.16

(default) ▾

[Create VPC](#)

IP pools | [Info](#)

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view Pools in the [Amazon VPC IP Address Manager console](#).

 Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets | [Info](#)

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

 eu-north-1a (eu-n1-az1)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-03ad22b085d115448

IPv4 subnet CIDR: 172.31.16.0/20

▼

 eu-north-1b (eu-n1-az2)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

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-09961433307c8ec9

VPC: vpc-04aa45a7f345246b7

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**

Protocol

HTTP

Port

80

1-65535

[Remove](#)

Default action | [Info](#)

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Routing action

 Forward to target groups Redirect to URL Return fixed response

Forward to target group | [Info](#)

Choose a target group and specify routing weight or [create target group](#).

Target group

ALB

Target type: Instance, IPv4 | Target stickiness: Off

HTTP

Weight

1

Percent

100%

+ Add target group

You can add up to 4 more target groups.

Target group stickiness | [Info](#)

Enables the load balancer to bind a user's session to a specific target group. To use stickiness the client must support cookies. If you want to bind a user's session to a specific target, turn on the Target Group attribute Stickiness.

Turn on target group stickiness

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](#)

You can add up to 49 more listeners.

▶ Load balancer tags - optional

6. application load balancer created.

Details

Load balancer type Application	Status Provisioning	VPC vpc-04aa45a7f345246b7	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z23TAZ6LKFNMIO	Availability Zones subnet-0cf70384eae259ca eu-north-1b (eu-n1-az2) subnet-03ad2bb85d113448 eu-north-1a (eu-n1-az1)	Date created January 6, 2026, 15:36 (UTC+05:30)
Load balancer ARN arn:aws:elasticloadbalancing:eu-north-1:484733236792:loadbalancer/app/myfirstalb/745e7069a1ec5b9	DNS name info myfirstalb-2096510666.eu-north-1.elb.amazonaws.com (A Record)		

Listeners and rules (1) [Info](#)

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS	Trust store
HTTP:80	Forward to target group ALB : 1 (100%)	1 rule	ARN	Not applicable	Not applicable	Not applicable	Not applicable
Target group stickiness: Off							

7. Updating ec2 security groups. (adding application load balancer security groups)

Inbound rules (2)

IP version	Type	Protocol	Port range	Source	Description
IPv4	SSH	TCP	22	0.0.0.0/0	-
-	HTTP	TCP	80	sg-09961433307cc8ec9...	-

Inbound rules (2)

group rule ID	IP version	Type	Protocol	Port range	Source	Description
1bd9655fb4b991	-	HTTP	TCP	80	sg-09961433307cc8ec9...	-
71067d43f9f693	IPv4	SSH	TCP	22	0.0.0.0/0	-

8. Installed nginx on one server and installed Apache on another ec2.

```

<h1>Hello from APACHE on Ubuntu</h1>
ubuntu@ip-172-31-37-10:~$ curl localhost
<h1>Hello from APACHE on Ubuntu</h1>
ubuntu@ip-172-31-37-10:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: 
   Active: active (running) since Tue 2026-01-06 10:45:08 UTC; 2min 29s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 3641 (apache2)
      Tasks: 55 (limit: 1008)
     Memory: 6.4M (peak: 6.8M)
        CPU: 51ms
       CGroup: /system.slice/apache2.service
           └─3641 /usr/sbin/apache2 -k start
              ├─3643 /usr/sbin/apache2 -k start
              ├─3644 /usr/sbin/apache2 -k start

Jan 06 10:45:08 ip-172-31-37-10 systemd[1]: Starting apache2.service - The Apache 
Jan 06 10:45:08 ip-172-31-37-10 systemd[1]: Started apache2.service - The Apache 

ubuntu@ip-172-31-37-10:~$ sudo ss -tulpn | grep :80
tcp  LISTEN  0      511          *:80          *:*      users:(("apache2",pid=3644,fd=4),("apache2",pid=3643,fd=4),("apache2",pid=3641,fd=4))
ubuntu@ip-172-31-37-10:~$ 

```

```
OF
<h1>Hello from NGINX on Ubuntu</h1>
buntu@ip-172-31-38-131:~$ curl localhost
!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
  tml { color-scheme: light dark; }
  body { width: 35em; margin: 0 auto;
  font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>
<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>
<p><em>Thank you for using nginx.</em></p>
```

9. Checking load balancer working fine or not. (copy and open ALB dns name in browser).



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

10. By accessing the ALB DNS and observing alternating responses, I confirmed proper load balancing.