

# AWS Task-3

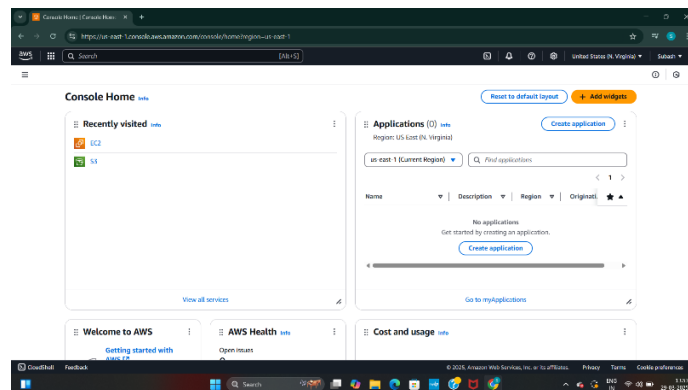
## TASKS

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

### Step 1: Create an S3 Bucket (No Public Access)

#### ✓ Log in to AWS Management Console:

- Go to [AWS Console] (<https://aws.amazon.com/console/>), and log in with your credentials.



#### ✓ Navigate to S3:

- In the search bar at the top, type S3 and click on it.

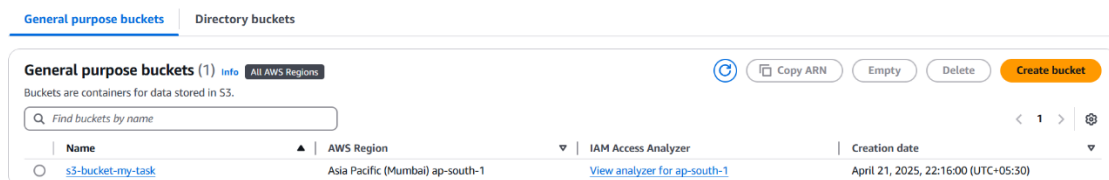
#### ✓ Create Bucket:

- Click the orange “Create bucket” button.

#### ✓ Configure Bucket Settings:

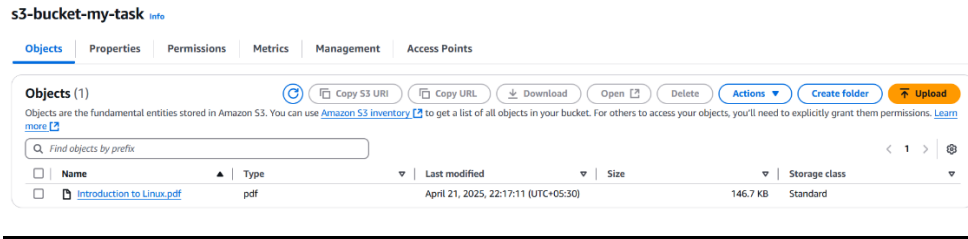
- Bucket name: Choose a unique name (e.g., s3-bucket-my-task)
- Region: Pick the region closest to you or your app
- Uncheck the "Block all public access" checkbox? NO! Leave it checked — this ensures your bucket stays private.
- Keep default settings for versioning, tags, encryption unless you need them.

#### ✓ Click "Create bucket" at the bottom.



### Step 2: Upload Files to the Bucket

- ✓ From the list of buckets, click on your bucket name (e.g., s3-bucket-my-task).
- ✓ Click the “Upload” button.
- ✓ Drag and drop your file or click “Add files”.
- ✓ Click “Upload” .



### Step 3: Enable Logging for File Uploads Using CloudTrail & View in CloudWatch

S3 doesn't log directly to CloudWatch for uploads. You need to use CloudTrail, which sends logs to CloudWatch Logs.

#### Step 3.1: Create a CloudTrail Trail

- ✓ Go to CloudTrail from the AWS Console (search "CloudTrail").
- ✓ Click on "Trails" in the sidebar → then click "Create trail"
- ✓ Give your trail a name (e.g., my-s3-uploads-trail)
- ✓ Choose "Create a new S3 bucket" or choose an existing one for the logs.
- ✓ **Scroll down and enable CloudWatch Logs:**
  - Check "Enabled"
  - Choose a log group (or create one)
  - Create a new IAM role when prompted (CloudTrail will create permissions for you)

#### 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

☒ Enabled

##### Log group

☒ New

☐ Existing

##### Log group name

my-cloudwatch

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

##### IAM Role

AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

☒ New

☐ Existing

##### Role name

my-role

- ✓ **Click Next → Select "Management events":**
  - Read and Write events: Choose Write-only (since you're interested in uploads)
  - Select S3 as the data resource
  - Add your bucket

## Events [Info](#)

Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

### Event type

Choose the type of events that you want to log.

☒ Management events

Capture management operations performed on your AWS resources.

☒ Data events

Log the resource operations performed on or within a resource.

☐ Insights events

Identify unusual activity, errors, or user behavior in your account.

☐ Network activity events

Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.

## Management events [Info](#)

Management events show information about management operations performed on resources in your AWS account.

[i](#) No additional charges apply to log management events on this trail because this is your first copy of management events.

### API activity

Choose the activities you want to log.

☐ Read

☒ Write

☐ Exclude AWS KMS events

☐ Exclude Amazon RDS Data API events

## Data events [Info](#)

Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

[i](#) Advanced event selectors are enabled  
Use the following fields for fine-grained control over the data events captured by your trail.

[Switch to basic event selectors](#)

### ▼ Data event: S3

[Remove](#)

#### Resource type

Choose the resource type for which you want to log data events.

S3

#### Log selector template

Log all events

✓ Click through the rest of the steps and Create Trail.

### my-s3-uploads-trail

[Delete](#)

[Stop logging](#)

#### General details

[Edit](#)

##### Trail logging

☒ Logging

##### Trail name

my-s3-uploads-trail

##### Multi-region trail

Yes

##### Apply trail to my organization

Not enabled

##### Trail log location

my-cloudtrail-subash/AWSLogs/039612867666

##### Last log file delivered

-

##### Log file SSE-KMS encryption

Not enabled

##### Log file validation

Enabled

##### Last file validation delivered

-

##### SNS notification delivery

Disabled

##### Last SNS notification

-

#### CloudWatch Logs

[Edit](#)

##### Log group

my-cloudwatch

##### IAM Role

arn:aws:iam::039612867666:role/service-role/my-role

## Step 3.2: Upload a File to Test the Logs

- Go back to S3 and upload a file again.
- Wait a few minutes (CloudTrail takes a bit of time to process events).

### Upload: status

[Close](#)

[i](#) After you navigate away from this page, the following information is no longer available.

#### Summary

Destination  
s3://s3-bucket-my-task

##### Succeeded

☒ 1 file, 231.5 KB (100.00%)

##### Failed

☐ 0 files, 0 B (0%)

#### Files and folders

#### Configuration

#### Files and folders (1 total, 231.5 KB)

Name	Folder	Type	Size	Status	Error
Basic Commands.pdf	-	application/pdf	231.5 KB	<input checked="" type="checkbox"/> Succeeded	-

## Step 4: View Logs in CloudWatch

- ✓ Go to CloudWatch from the AWS Console.
- ✓ In the sidebar, click “Logs” → then “Log groups”
- ✓ Find the log group from your trail (e.g., /aws/cloudtrail/logs)
- ✓ Click the latest log stream (you’ll see one with today's date).

**Log groups (1)** [Actions](#) [View in Logs Insights](#) [Start tailing](#) [Create log group](#)

By default, we only load up to 10000 log groups.

☐ Exact match

<input type="checkbox"/>	Log group	Log class	Anomaly d...	Data pr...	Sensitiv...	Retention	Metric fl...
<input type="checkbox"/>	<a href="#">my-cloudwatch</a>	Standard	<a href="#">Configure</a>	-	-	Never expire	-

< 1 > ⚙

---

< **Log streams** Tags Anomaly detection Metric filters Subscription filters Contributor Insights Data protection Field >

**Log streams (2)** [Delete](#) [Create log stream](#) [Search all log streams](#)

☐ Exact match ☐ Show expired [Info](#)

<input type="checkbox"/>	Log stream	Last event time
<input type="checkbox"/>	<a href="#">039612867666_CloudTrail_ap-south-1_4</a>	2025-04-21 17:06:57 (UTC)
<input type="checkbox"/>	<a href="#">039612867666_CloudTrail_ap-south-1</a>	-

< 1 > ⚙

---

**Log events** [Actions](#) [Start tailing](#) [Create metric filter](#)

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

[Clear](#) [1m](#) [30m](#) [1h](#) [12h](#) [Custom](#) [UTC timezone](#)

[Display](#) ⚙

▶	Timestamp	Message
		No older events at this moment. <a href="#">Retry</a>
▶	2025-04-21T17:06:57.471Z	{\"eventVersion\":\"1.11\",\"userIdentity\":{\"type\":\"Root\",\"principalId\":\"039612867666\",\"arn\":\"arn:aws:iam:039612867666:root\",\"accountId...
▶	2025-04-21T17:06:57.471Z	{\"eventVersion\":\"1.11\",\"userIdentity\":{\"type\":\"Root\",\"principalId\":\"039612867666\",\"arn\":\"arn:aws:iam:039612867666:root\",\"accountId...
▶	2025-04-21T17:06:57.471Z	{\"eventVersion\":\"1.11\",\"userIdentity\":{\"type\":\"AWSService\",\"invokedBy\":\"cloudtrail.amazonaws.com\"},\"eventTime\":\"2025-04-21T17:06:38...
		No newer events at this moment. Auto retry paused. <a href="#">Resume</a>

## 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.

### Step 1: Launch Two EC2 Instances

- ✓ Go to EC2 → Launch Instance.
- ✓ AMI: Amazon Linux 2.
- ✓ Instance type: t2.micro (for free tier) or anything else.
- ✓ **Network settings:**
  - Select VPC(default) and Subnet .
  - Auto-assign Public IP: Enable.
- ✓ **Security Group:**
  - Allow HTTP (80) and SSH (22) inbound from your IP (for admin) and the Load Balancer's security group.

**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

We'll create a new security group called 'launch-wizard-1' with the following rules:

- ☒ Allow SSH traffic from Anywhere  
0.0.0.0/0  
Helps you connect to your instance
- ☒ Allow HTTPS traffic from the internet  
To set up an endpoint, for example when creating a web server
- ☒ Allow HTTP traffic from the internet  
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ×

- Launch two instances. Name them Server-1 and Server-2.

**Instance summary for i-0b1daa02eeaf80119 (Server-1)** [Info](#) Connect Instance state ▼ Actions ▼

Updated less than a minute ago

<b>Instance ID</b> i-0b1daa02eeaf80119	<b>Public IPv4 address</b> 44.208.21.23   <a href="#">open address</a>	<b>Private IPv4 addresses</b> 172.31.88.75
<b>IPv6 address</b> -	<b>Instance state</b> Running	<b>Public IPv4 DNS</b> ec2-44-208-21-23.compute-1.amazonaws.com   <a href="#">open address</a>
<b>Hostname type</b> IP name: ip-172-31-88-75.ec2.internal	<b>Private IP DNS name (IPv4 only)</b> ip-172-31-88-75.ec2.internal	<b>Elastic IP addresses</b> -
<b>Answer private resource DNS name</b> IPv4 (A)	<b>Instance type</b> t2.micro	<b>AWS Compute Optimizer finding</b> Opt-in to AWS Compute Optimizer for recommendation s.   <a href="#">Learn more</a>
<b>Auto-assigned IP address</b> 44.208.21.23 [Public IP]	<b>VPC ID</b> vpc-02e1ac48114ace71d	<b>Auto Scaling Group name</b> -
<b>IAM Role</b> -	<b>Subnet ID</b> subnet-0d0ba5953b19d0f25 (my-subnet)	<b>Managed</b> false
<b>IMDSv2</b> Required	<b>Instance ARN</b> arn:aws:ec2:us-east-1:039612867666:instance/i-0b1daa02eeaf80119	

**Instance summary for i-0e19b3b580714af56 (Server-2)** [Info](#) Connect Instance state ▼ Actions ▼

Updated less than a minute ago

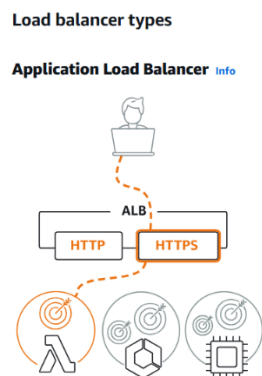
<b>Instance ID</b> i-0e19b3b580714af56	<b>Public IPv4 address</b> 3.86.59.242   <a href="#">open address</a>	<b>Private IPv4 addresses</b> 172.31.85.106
<b>IPv6 address</b> -	<b>Instance state</b> Running	<b>Public IPv4 DNS</b> ec2-3-86-59-242.compute-1.amazonaws.com   <a href="#">open address</a>
<b>Hostname type</b> IP name: ip-172-31-85-106.ec2.internal	<b>Private IP DNS name (IPv4 only)</b> ip-172-31-85-106.ec2.internal	<b>Elastic IP addresses</b> -
<b>Answer private resource DNS name</b> IPv4 (A)	<b>Instance type</b> t2.micro	<b>AWS Compute Optimizer finding</b> Opt-in to AWS Compute Optimizer for recommendation s.   <a href="#">Learn more</a>
<b>Auto-assigned IP address</b> 3.86.59.242 [Public IP]	<b>VPC ID</b> vpc-02e1ac48114ace71d	<b>Auto Scaling Group name</b> -
<b>IAM Role</b> -	<b>Subnet ID</b> subnet-0d0ba5953b19d0f25 (my-subnet)	<b>Managed</b> false
<b>IMDSv2</b> Required	<b>Instance ARN</b> arn:aws:ec2:us-east-1:039612867666:instance/i-0e19b3b580714af56	

## Step 2: Install Web Server on Each Instance

- ✓ Install an web server on both instance. To install an web server the command is:
  - `sudo yum update -y`
  - `sudo yum install httpd -y`
  - `sudo systemctl start httpd`
  - `sudo systemctl enable httpd`
- ✓ And, now you can host an webpage you want ,move the index.html file to the below location.
  - `/var/www/html/index.html`.

## Step 3: Create an Application Load Balancer

- ✓ Go to EC2 → Load Balancers → Create Load Balancer → Application Load Balancer.



### ✓ Basic Configuration:

- Name: My-ALB
- Scheme: Internet-facing
- IP address type: IPv4

#### 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.

### ✓ Network Mapping:

- VPC: Select your existing VPC (or default).
- Availability Zones: Select 2 AZs where your EC2s are.

#### 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.

##### ☒ us-east-1a (use1-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-0c33a792e0a1f6bd7

IPv4 subnet CIDR: 172.31.0.0/20

##### ☒ us-east-1b (use1-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.

subnet-06fce0720d766fa86

IPv4 subnet CIDR: 172.31.80.0/20

##### ☐ us-east-1c (use1-az4)

##### ☐ us-east-1d (use1-az6)

##### ☐ us-east-1e (use1-az3)

##### ☐ us-east-1f (use1-az5)

## ✓ Security Groups:

- Create or select one allowing **HTTP (80)** inbound.

### 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](#)

## ✓ Listeners and Routing:

- Listener: Port 80 → Forward to **Target Group**.

### 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

Port

Default action

Forward to

My-Targetgroup

HTTP

HTTP

:

80

1-65535

Forward to

My-Targetgroup

Target type: Instance, IPv4

HTTP

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.

## ✓ Create a Target Group:

- Target type: **Instance**
- Protocol: **HTTP**
- Port: **80**
- Health checks: HTTP on /
- Register both EC2 instances to the Target Group.

Registered targets (2) <a href="#">Info</a>									
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.									
<input type="text" value="Filter targets"/>									
<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Admini...	Overri...	
<input type="checkbox"/>	i-0e19b3b580714af56	Server-2	80	us-east-1b (us...	⊖ Unused	Target group is not co...	-	-	
<input type="checkbox"/>	i-0b1daa02eaf80119	Server-1	80	us-east-1b (us...	⊖ Unused	Target group is not co...	-	-	

## ✓ Finalize and Create Load Balancer.

### My-ALB

▼ Details

Load balancer type

Application

Scheme

Internet-facing

Status

⊖ Provisioning

Hosted zone

Z35SXDOTRQ7X7K

VPC

vpc-02e1ac48114ace71d

Availability Zones

subnet-049fe7c6a0eac5e67 us-east-1a (use1-az1)

subnet-0d0ba5953b19d0f25 us-east-1b (use1-az2)

Load balancer IP address type

IPv4

Date created

April 26, 2025, 22:40 (UTC+05:30)

Load balancer ARN

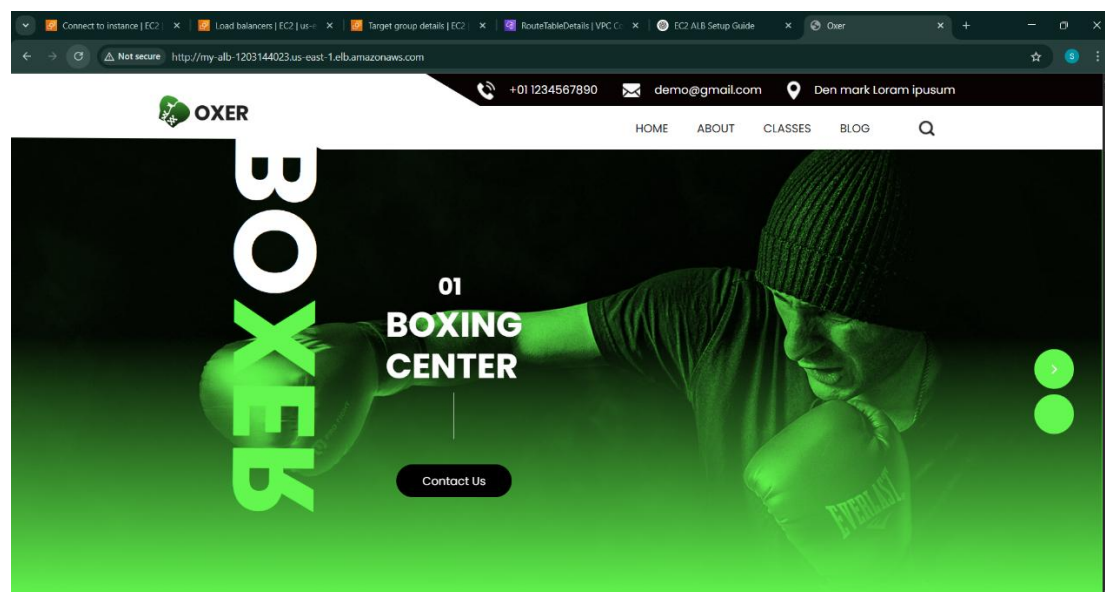
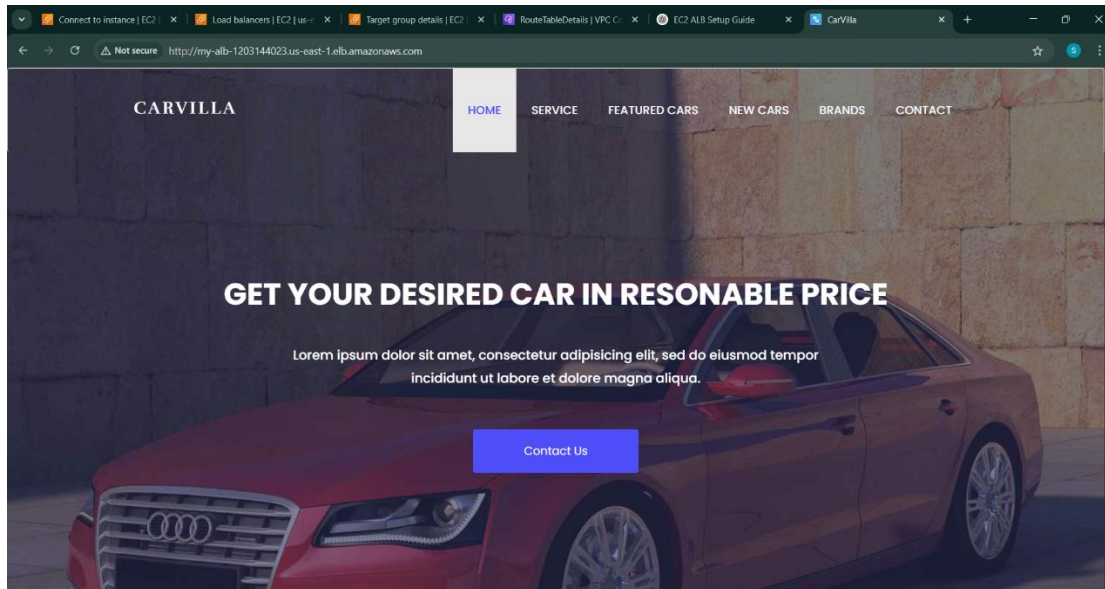
arn:aws:elasticloadbalancing:us-east-1:039612867666:loadbalancer/app/My-ALB/f2c779c108fae3fb

DNS name

My-ALB-1203144023.us-east-1.elb.amazonaws.com (A Record)

#### Step 4: Test the Setup

- ✓ Find your ALB DNS name (something like My-ALB-1203144023.us-east-1.elb.amazonaws.com).
- ✓ Open the ALB DNS name in browser:
  - Refresh multiple times → you should see responses switching between Server 1 and Server 2 (round robin).



\*\*\*\*\* TASK COMPLETED \*\*\*\*\*