

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

Amazon S3

> Buckets

Amazon S3

<

▼ Buckets

General purpose buckets

Directory buckets

Table buckets

Vector buckets

▼ Access management and security

Access Points

Access Points for FSx

Access Grants

IAM Access Analyzer

▼ Storage management and insights

Storage Lens

Batch Operations

Account and organization settings

► AWS Marketplace for S3

General purpose buckets

All AWS Regions


Directory buckets

General purpose buckets (2) Info

Buckets are containers for data stored in S3.

Find buckets by name

	Name	
<input type="radio"/>	<a href="#">aws-cloudtrail-logs-085980781930-bc98e782</a>	
<input type="radio"/>	<a href="#">demo01-data-bucket</a>	

 You can now enrich CloudTrail events with additional information by adding resource tags and IAM glob

## Dashboard [Info](#)

### Query results history

Choose a query to view results from the last seven days.

No queries

No queries to display

### CloudTrail Insights [Info](#)

Insights are events that show unusual API activity. After you en

### Event history [Info](#)

Event name	Event time	Event source
<a href="#">CreateLogStream</a>	December 02, 2025, 11:53:21 (U...	logs.amazonaws.com
<a href="#">DeleteLogGroup</a>	December 02, 2025, 11:52:20 (U...	logs.amazonaws.com
<a href="#">CreateLogStream</a>	December 02, 2025, 11:49:41 (U...	logs.amazonaws.com
<a href="#">CreateLogStream</a>	December 02, 2025, 11:49:00 (U...	logs.amazonaws.com

# Log groups (1)

By default, we only load up to 10,000 log groups.

<input type="checkbox"/>	Log group	▼	Log class	▼	Anomaly c
<input type="checkbox"/>	<a href="#">aws-cloudtrail-logs-085980781930-361933aa</a>		Standard		<a href="#">Configure</a>



# aws-cloudtrail-logs-085980781930-361933aa

## ▼ Log group details

Log class | [Info](#)  
Standard

ARN  
 `arn:aws:logs:us-west-2:085980781930:log-group:aws-cloudtrail-logs-085980781930-361933aa:*`

Creation time  
36 minutes ago

Retention  
Never expire


Stored bytes  
-

Metric filters  
0

Subscription filter  
0

Contributor Insights  
-

KMS key ID  
-

Deletion protection  
 Off

[Log streams](#)

[Tags](#)

[Anomaly detection](#)

[Metric filters](#)

[Subscription filters](#)

## Log streams (4)

By default, we only load the most recent log streams.




- ☐ | Log stream
- ☐ [085980781930\\_CloudTrail\\_us-west-2\\_3](#)
- ☐ [085980781930\\_CloudTrail\\_us-west-2\\_4](#)
- ☐ [085980781930\\_CloudTrail\\_us-west-2](#)

## ▼ Log group details

**Log class** | [Info](#)  
Standard

**ARN**

 `arn:aws:logs:us-west-2:085980781930:log-group:aws-cloudtrail-logs-085980781930-361933aa:*`

**Creation time**

21 minutes ago

**Retention**

Never expire

**Stored bytes**

-

**Metric filters**

0

**Subscription filters**

0

**Contributor Insights**

-

**KMS key ID**

-

**Deletion protection**

⊖ Off

### Log streams

### Tags

### Anomaly detection

### Metric filters

### Subscription filters

## Log streams (4)

By default, we only load the most recent log streams.

 *Filter log streams or try prefix search*

☐ | **Log stream**

☐ [085980781930\\_CloudTrail\\_us-west-2\\_3](#)

☐ [085980781930\\_CloudTrail\\_us-west-2\\_2](#)

☐ [085980781930\\_CloudTrail\\_us-west-2](#)

☐ [085980781930\\_CloudTrail\\_us-west-2\\_4](#)

Log events on cloud watch after uploading a new file event

1.

## Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events.

Q Put

► | Timestamp | Message

▼ 2025-12-02T06:22:43.291Z

{"eventVersion":"1.11","userIdentity":{"type":"I

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDARIBG2TVVMHC4ZFXR6",
    "arn": "arn:aws:iam::085980781930:user/powerUser",
    "accountId": "085980781930",
    "accessKeyId": "ASIARIBG2TVVAXR7XTT0",
    "userName": "powerUser",
    "sessionContext": {
      "attributes": {
        "creationDate": "2025-12-02T04:38:21Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2025-12-02T06:19:59Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "36.255.17.230",
  "userAgent": "[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  "requestParameters": {
    "X-Amz-Date": "20251202T061959Z",
    "bucketName": "demo01-data-bucket",
    "X-Amz-Algorithm": "AWS4-HMAC-SHA256",
    "x-amz-acl": "bucket-owner-full-control",
    "X-Amz-SignedHeaders": "content-type;host;x-amz-acl;x-amz-checksum-crc64nvme;x-
    "Host": "demo01-data-bucket.s3.us-west-2.amazonaws.com",
    "X-Amz-Content-Sha256": "UNSIGNED-PAYLOAD",
    "X-Amz-Expires": "300",
    "key": "file4.txt",
    "x-amz-storage-class": "STANDARD"
  },
  "responseElements": {
```

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

Instances (2) Info

Find Instance by attribute or tag (case-sensitive)

All states ▼

Instance state = running X

Clear filters

<input type="checkbox"/>	Name	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status
<input type="checkbox"/>	demo server 1	i-04e9bed462a07ae90	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>
<input type="checkbox"/>	demo server 2	i-037b898a262001de3	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>

## Inbound rules of Instances

<input type="checkbox"/>	Name	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Av
<input checked="" type="checkbox"/>	demo server 1	i-04e9bed462a07ae90	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>	us
<input type="checkbox"/>	demo server 2	i-037b898a262001de3	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>	us

### i-04e9bed462a07ae90 (demo server 1)

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

▼ Security details

IAM Role

-

Security groups

sg-0c43f050a519601f2 (launch-wizard-5)

Owner ID

085980781930

▼ Inbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Source
-	sgr-0d960c2432d90a348	22	TCP	0.0.0.0/0
-	sgr-0eac723b8ea0e8182	80	TCP	0.0.0.0/0

▼ Outbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Destination
-	sgr-09a50349a5d4d4d68	All	All	0.0.0.0/0

Target Group created

# demo-alb-target-group

Details

arn:aws:elasticloadbalancing:us-west-2:085980781930:targetgroup/demo-alb-target-group/170e3c571acb877b

Target type

Instance

IP address type

IPv4

Protocol : Port

HTTP: 80

Load balancer

None associated

2

Total targets

0

Healthy

0 Anomalous

0

Unhealthy

Distribution of targets by Availability Zone (AZ)

Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets

Monitoring

Health checks

Attributes

Tags

Registered targets (2)

Info

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Filter targets

	Instance ID	Name	Port	Zone	Health status
<input type="checkbox"/>	<a href="#">i-04e9bed462a07ae90</a>	demo server 1	80	us-west-2b (us...)	Unused
<input type="checkbox"/>	<a href="#">i-037b898a262001de3</a>	demo server 2	80	us-west-2b (us...)	Unused

Load balancer creation



us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#CreateALBWizard:

aws

Search

[Alt+S]

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. 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.

► 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.

demo-ALB-load-balancer

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 type.

☒ 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 using VPC peering. To confirm the VPC for your targets, view [target groups](#).

vpc-0e1b98de84a35b169 (defaultVpc)  
172.31.0.0/16

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 IPAM 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 Amazon.

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 be scaled across the selected subnets.

☒ us-west-2a (usw2-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.

subnet-0518f8ea7fa289dad  
IPv4 subnet CIDR: 172.31.32.0/20

☒ us-west-2b (usw2-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.

subnet-0ee62e4a782d249db  
IPv4 subnet CIDR: 172.31.16.0/20

us-west-2a (usw2-az2)

Security Group attached on the load balancer

## 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 one.

### Security groups

Select up to 5 security groups

demo-alb-project-sg  
sg-0412bc39d92f73dda VPC: vpc-0e1b98dc84a35b169

## 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 determine how the traffic is routed.

### ▼ Listener HTTP:80

#### Protocol

HTTP

#### Port

80

1-65535

#### 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 [Info](#)

Use fixed-response actions to drop client requests and return a custom HTTP response. When a fixed-response action is taken, the action and response code are required.

#### Response code

The type of message you want to send.

503

2xx, 4xx, 5xx

#### Content type

The format of your message.

text/plain

#### Response body - optional

Enter your response message.

This is an error page

1024 character maximum

#### 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.

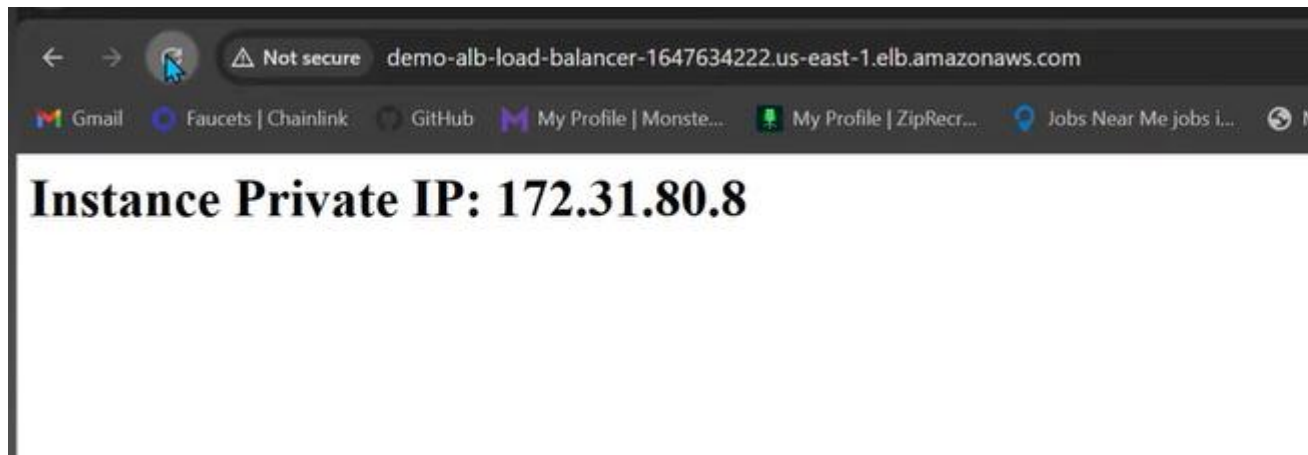
## ✓ Successfully created load balancer: demo-ALB-load-Balancer

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 become available.

[EC2](#) > [Load balancers](#) > demo-ALB-load-Balancer

# demo-ALB-load-Balancer

ip's Redirecting



Listener rules

Rules					Tags
<b>Listener rules (2)</b> <a href="#">Info</a>					
Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the top of the list.					
<input type="text" value="Filter rules"/>					
<input type="checkbox"/>	Name tag	Priority ▲	Conditions (If)	Actions (Then)	
<input type="checkbox"/>	error	3	Path Pattern is /error	<b>Return fixed response</b> <ul style="list-style-type: none"><li>Response code:</li><li>Response body:</li><li>Response content type:</li></ul>	
<input type="checkbox"/>	Default	Last (default)	If no other rule applies	<b>Forward to target group</b> <ul style="list-style-type: none"><li><a href="#">demo-alb-target-group</a></li><li>Target group stickiness</li></ul>	

