

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

The screenshot shows the AWS S3 console interface. At the top left, there's a navigation bar with a blue circular icon containing three horizontal lines, followed by the text "Amazon S3 > Buckets". Below this is the main content area:

- Amazon S3** (with a back arrow)
- Buckets** (selected category)
- General purpose buckets** (sub-category)
- Directory buckets**
- Table buckets**
- Vector buckets**
- Access management and security** (category)
- Access Points**
- Access Points for FSx**
- Access Grants**
- IAM Access Analyzer**
- Storage management and insights** (category)
- Storage Lens**
- Batch Operations**

Below the sidebar, the main content area has a header "General purpose buckets" with a "All AWS Regions" button. It also includes a search bar labeled "Find buckets by name" and a table with two entries:

Name
aws-cloudtrail-logs-085980781930-bc98e782
demo01-data-bucket

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

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 enable CloudWatch Metrics Insights, CloudWatch Metrics Insights automatically analyzes your CloudTrail log files for unusual API activity and generates CloudWatch Metrics Insights events.

Event history Info

Event name	Event time	Event source
CreateLogStream	December 02, 2025, 11:53:21 (U...	logs.amazonaws.com
DeleteLogGroup	December 02, 2025, 11:52:20 (U...	logs.amazonaws.com
CreateLogStream	December 02, 2025, 11:49:41 (U...	logs.amazonaws.com
CreateLogStream	December 02, 2025, 11:49:00 (U...	logs.amazonaws.com

Log groups (1)

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



Filter log groups or try pattern search



| Log group



| Log class



| Anomaly detection



[aws-cloudtrail-logs-085980781930-361933aa](#)

Standard

[Configure](#)

aws-cloudtrail-logs-085980781930-361933aa

▼ Log group details

Log class | [Info](#)

Standard

Metric filters

0

ARN

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

Subscription filters

0

Creation time

36 minutes ago

Contributor Insights

-

Retention

Never expire

KMS key ID

-

Stored bytes

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

Metric filters

0

ARN

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

Subscription filters

0

Creation time

21 minutes ago

Contributor Insights

-

Retention

Never expire

KMS key ID

-

Stored bytes

-

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 CloudWatch 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.

 Put

	Timestamp	Message
▼	2025-12-02T06:22:43.291Z	<pre>{"eventVersion": "1.11", "userIdentity": {"type": "IAMUser", "principalId": "AIDARIBG2TVVWMC4ZFXR6", "arn": "arn:aws:iam::085980781930:user/powerUser", "accountId": "085980781930", "accessKeyId": "ASIAIRIBG2TVVAXR7XTT0", "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, like Gecko) Chrome/120.0.0.0 Safari/537.36]", "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-amz-content-sha256;x-amz-expire", "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": {}}</pre>

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					
<input type="text"/> Find Instance by attribute or tag (case-sensitive)				All states ▼	
<input type="checkbox"/> Instance state = running X		Clear filters			
	Name 🔗	Instance ID	Instance state	Instance type	Status check
<input type="checkbox"/>	demo server 1	i-04e9bed462a07ae90	Running Q Q	t3.micro	3/3 checks passed View alarms +
<input type="checkbox"/>	demo server 2	i-037b898a262001de3	Running Q Q	t3.micro	3/3 checks passed View alarms +

Inbound rules of Instances

<input type="checkbox"/>	Name 🔗	Instance ID	Instance state	Instance type	Status check	Alarm status	A
<input checked="" type="checkbox"/>	demo server 1	i-04e9bed462a07ae90	Running Q Q	t3.micro	3/3 checks passed View alarms +	us-	
<input type="checkbox"/>	demo server 2	i-037b898a262001de3	Running Q Q	t3.micro	3/3 checks passed View alarms +	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)								
▼ Inbound rules								
<input type="text"/> 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								
<input type="text"/> 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

Protocol : Port

HTTP: 80

IP address type

IPv4

Load balancer

[None associated](#)

2

Total targets

0

Healthy

0

Unhealthy

0 Anomalous

► 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](#)

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status
<input type="checkbox"/>	i-04e9bed462a07ae90	demo server 1	80	us-west-2b (us...)	Unused
<input type="checkbox"/>	i-037b898a262001de3	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, Lambda functions, or IP addresses. It evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the targets defined in the rule.

▶ 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
• 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 protocols.

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 (default/vpc)
172.31.0.0/16

IP pools [Info](#)
You can optionally choose to configure an IPAM pool as the preferred source for your load balancer's IP addresses. Create or view Pools in the [AWS 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 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 fail over between zones.

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-0518f8ea7fa289dd
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-2c (usw2-az3)
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.

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-0e1b98de84a35b169 [X](#)

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 tell the listener what to do with each request.

▼ Listener HTTP:80

Protocol	Port
HTTP	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 applies to all traffic that matches the listener's rules.

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 healthy.

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

demo-ALB-load-Balancer

Ip's Redirecting

The image shows two separate browser windows side-by-side. Both windows have a URL bar indicating they are not secure (**Not secure**) and are pointing to the same endpoint: `demo-alb-load-balancer-1647634222.us-east-1.elb.amazonaws.com`. The top window displays the text **Instance Private IP: 172.31.80.8**. The bottom window displays the text **Instance Private IP: 172.31.81.36**.

Listner rules

Rules | Tags

Listener rules (2) Info

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the highest priority rule at the top.

Filter rules

<input type="checkbox"/>	Name tag	Priority	Conditions (If)	Actions (Then)
<input type="checkbox"/>	error	3	Path Pattern is /error	Return fixed response <ul style="list-style-type: none">• Response code:• Response body:• Response content:
<input type="checkbox"/>	Default	Last (default)	If no other rule applies	Forward to target <ul style="list-style-type: none">• demo-alb-target• Target group settings

