

AWS Task-3

Task Description:

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

S3 Bucket with CloudWatch Logging - Step-by-Step Guide

Task Breakdown & Completion Status:

- Step 1: Created an S3 bucket with no public access.
- Step 2: Uploaded files to the private S3 bucket.
- Step 3: Enabled CloudTrail to track S3 activities.
- Step 4: Configure CloudWatch Logs to store and view logs.
- Step 5: Verified file upload (PutObject) and delete (DeleteObject) logs in CloudWatch.

Step 1: Create an S3 Bucket (Private)

- - Login to AWS Console → Navigate to S3.
- - Click "Create bucket".
- - Enter a Bucket Name (sangeethacloud-my-private-bucket).
- - Choose a Region (same as your AWS resources).
- - Block all public access → Enable (this ensures the bucket remains private).
- - Object Ownership → Keep it ACLs disabled (recommended).
- - Click "Create bucket".
- - Bucket is now created with no public access.

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

sangeethacloud-my-private-bucket

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.

☒ **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

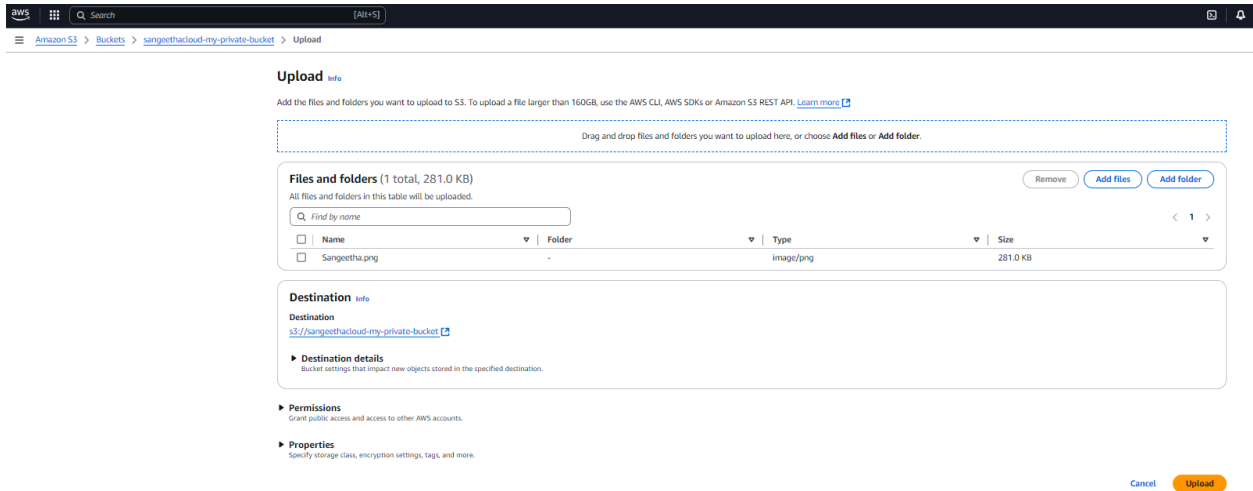
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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 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.

Step 2: Upload Files to S3

- Open S3 → Click on your bucket (sangeethacloud-my-private-bucket).
- Click "Upload" → "Add files".
- Select a file from your system (e.g., an image or text file).
- Click "Upload".
- ☒ File is successfully uploaded to S3.



Step 3: Enable CloudTrail to Log S3 File Activities

To track uploads, downloads, and deletions, we need to enable CloudTrail.

- Go to AWS CloudTrail → Click "Create trail".
- Enter Trail Name: s3-logging-trail.
- Storage Location:
 - Select "Use existing S3 bucket" and choose sangeethacloud-my-private-bucket
 - This will store CloudTrail logs inside your bucket.

- create the trail

CloudTrail

Dashboard

Event history

Insights

Lake

Dashboards

Query

Event data stores

Integrations

Trails

Settings

Pricing

Documentation

Forums

FAQs

What's new: Strengthen your data perimeter and implement better detective controls for your VPC endpoints by enabling Network activity events on your Trail or CloudTrail Lake. [Learn more](#)

Dashboard

Query results history

Trails

CloudTrail Insights

Event history

Query results history

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

No queries

No queries to display

Create a new query

Trails

Name	Status
s3-activity-trail	Logging
s3-activity-trail-s3	Logging

Copy events to Lake

Create trail

CloudTrail Insights

CloudTrail Insights is not enabled

Insights are events that show unusual API activity. After you enable Insights, if unusual activity is logged, Insights events are shown in this table for 90 days. Additional charges apply. [Learn more](#)

Event history

Event name	Event time	Event source
PutBucketEncryption	March 19, 2025, 11:26:38 (UTC+...)	s3.amazonaws.com
CreateBucket	March 19, 2025, 11:26:37 (UTC+...)	s3.amazonaws.com
CreateLogStream	March 17, 2025, 18:54:15 (UTC+...)	logs.amazonaws.com
CreateLogStream	March 17, 2025, 18:53:09 (UTC+...)	logs.amazonaws.com
CreateLogStream	March 17, 2025, 18:52:12 (UTC+...)	logs.amazonaws.com

- Step 1
- Choose trail attributes
- Step 2
- Choose log events
- Step 3
- Review and create

Choose trail attributes

General details

A trail created in the console is a multi-region trail. [Learn more](#)

Trail name

Enter a display name for your trail.

Sangeethacloud01-s3-logging-trail

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. [See all accounts](#)

Storage location

☒ Create new S3 bucket

Create a bucket to store logs for the trail.

☐ Use existing S3 bucket

Choose an existing bucket to store logs for this trail.

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-311141562203-0d0028b5

Logs will be stored in aws-cloudtrail-logs-311141562203-0d0028b5/AWSLogs/311141562203

Log file SSE-KMS encryption

☐ Enabled

Additional settings

Log file validation

☒ Enabled

SNS notification delivery

☐ Enabled

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

aws-cloudtrail-logs-311141562203-778c0327

- Enable Logging for S3:

- Scroll to Data events → Select S3.
- Choose "Specify bucket" and select sangeethacloud-my-private-bucket.
- Enable "Read & Write" (to log uploads & deletions).
- Click "Next", review the settings, and click "Create Trail".
-  CloudTrail is now tracking S3 file activities.

Next step

Step 1

● Choose trail attributes


Step 2

● **Choose log events**

Step 3



● Review and create

Choose log events


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.

 Multiple management events trails detected. Charges apply to duplicated logged management events. [Additional charges apply](#) 

API activity
Choose the activities you want to log.
☒ **Read**
☐ Exclude AWS KMS events
☐ Exclude Amazon RDS Data API events
☒ **Write**

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

 **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

Review and proceed !

Step 1

● Choose trail attributes

Step 2

● Choose log events

Step 3

● **Review and create**

Review and create

Step 1: Choose trail attributes

Edit

General details

Trail name
Sangeethacloud01-s3-logging-trail

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
aws-cloudtrail-logs-311141562203-000028b5/AWSLogs/311141562203

Log file SSE-KMS encryption
Not enabled

Log file validation
Enabled

SNS notification delivery
Disabled

CloudWatch Logs

Log group
aws-cloudtrail-logs-311141562203-778c0327

IAM Role
CloudTrailToCloudWatchLogs

Tags

Key	Value
No tags No tags associated with this trail	

Step 2: Choose log events

Edit

Step 4: Enable CloudWatch Logs for Easy Viewing

- Open AWS CloudTrail → Click on your trail (s3-logging-trail).
- Click "Edit" → Scroll to CloudWatch Logs.
- Enable CloudWatch Logs → Choose "Create new Log Group" (e.g., S3-Log-Group).
- Click "Save Changes".
- ☒ Now, S3 logs will be visible in CloudWatch Logs.

CloudTrail > Trails > [arn:aws:cloudtrail:ap-south-1:311141562203:trail/s3-logging-trail](#) > Edit

Edit [arn:aws:cloudtrail:ap-south-1:311141562203:trail/s3-logging-trail](#) [Info](#)

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

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

► Policy document

[Cancel](#) [Save changes](#)

CloudTrail > Trails > [arn:aws:cloudtrail:ap-south-1:311141562203:trail/s3-logging-trail](#) > Edit

Edit [arn:aws:cloudtrail:ap-south-1:311141562203:trail/s3-logging-trail](#) [Info](#)

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

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

► Policy document

[Cancel](#) [Save changes](#)

Step 5: View Logs in CloudWatch

- Go to AWS CloudWatch → Click "Log Groups".
- Open the Log Group (S3-Log-Group).
- Click on the latest Log Stream.
- Search for event types:
 - "PutObject" → When a file is uploaded
 - "DeleteObject" → When a file is deleted
 - "GetObject" → When a file is downloaded
- ☒ Now, you can track all file activities in CloudWatch.

CloudWatch

Log groups

53-Log-Group

311141562203_CloudTrail_ap-south-1_4

Alarms

Logs

Log groups

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

Metrics

X-Ray traces

Events

Application Signals

Network Monitoring

Insights

Settings

Getting Started

What's new

Log events

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](#)

DeleteObject

Clear

1m

30m

1h

12h

Custom

UTC timezone

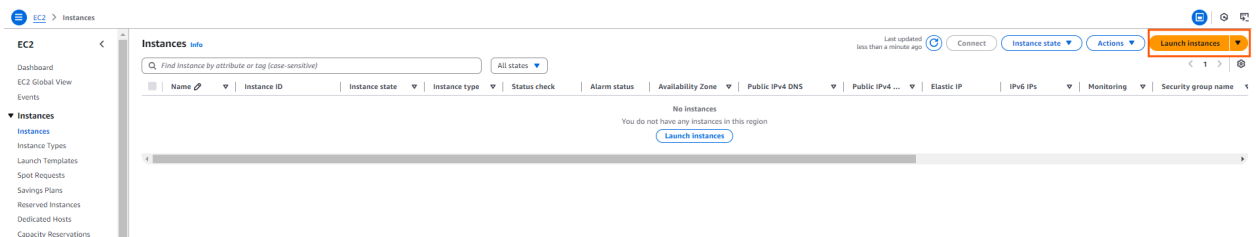
Display

Timestamp	Message
2025-03-20T06:33:16.932Z	<pre>{ "eventVersion": "1.11", "userIdentity": { "type": "Root", "principalId": "A11141562203", "arn": "arn:aws:iam::111141562203:root", "accountId": "111141562203", "accessKeyId": "AKIAQJL3ON7UAC10N7", "userName": "sangeethacloud", "sessionContext": { "attributes": { "creationDate": "2025-03-20T06:30:21Z", "mfaAuthenticated": "false" } } }, "eventTime": "2025-03-20T06:30:21Z", "eventSource": "s3.amazonaws.com", "eventName": "DeleteObject", "awsRegion": "ap-south-1", "sourceIPAddress": "1803.08.12.12", "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6.0 Safari/537.36", "requestParameters": { "bucketName": "sangeethacloud-my-private-bucket", "key": "sangeethacloud-my-private-bucket.x3.ap-south-1.amazonaws.com", "object": "" }, "responseElements": null, "additionalEventData": { "signatureVersion": "signature", "cipherSuite": "TLS_AES_128_GCM_SHA256", "bytesTransferred": 0, "authenticationMethod": "Authenticator", "aws-iam-2": "signatureVersion=20250320063021Zkey=111141562203secret=AKIAQJL3ON7UAC10N7signature=sangeethacloud-my-private-bucket", "requestID": "H0AB3C1604W25TV", "eventID": "H0B0ab08-765f-46cf-8765-60808054612a", "readOnly": false, "resources": [{ "type": "AWs::S3::Object", "arnPrefix": "arn:aws:s3:::sangeethacloud-my-private-bucket/" }, { "accountId": "111141562203", "type": "AWs::S3::Bucket", "ARN": "arn:aws:s3:::sangeethacloud-my-private-bucket" }] }, "eventType": "AwsApiCall", "managementEvent": false, }</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

1 Create Two EC2 Instances

1. Navigate to **AWS EC2 Console**.
2. Click **Launch Instance** and configure the following:
 - Choose **Amazon Linux 2** as the AMI.
 - Select **t2.micro** instance type.
 - Configure instance details and ensure both instances are in the same **VPC**.
 - Add **User Data** to install a web server:
 - `#!/bin/bash`
 - `yum update -y`
 - `yum install -y httpd`
 - `echo "<h1>Welcome to Web Server 1</h1>" > /var/www/html/index.html`
 - `systemctl start httpd`
 - `systemctl enable httpd`
 - Repeat the process for the second instance, but modify the HTML content:
 - `echo "<h1>Welcome to Web Server 2</h1>" > /var/www/html/index.html`
3. **Configure Security Group:**
 - Allow **HTTP (Port 80) from Anywhere (0.0.0.0/0)**.
 - Allow **SSH (Port 22) from Your IP**.
4. **Launch the Instances** and note their **Public IPs**.



It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

Do not show me this message again

Take a walkthrough

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

web-server-1

[Add additional tags](#)

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Recents

[Quick Start](#)



[Browse more AMIs](#)
Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-08fe5144a4659a3b3 (64-bit (x86)) / ami-dbf9265d789594735 (64-bit (ARM))
Virtualization: hvm | ENA: enabled: true | Root device type: ebs

Free tier eligible

Description

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemD 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Amazon Linux 2 Kernel 5.10 AMI 2.0.20250305.0 x86_64 HVM gp2

Architecture

64-bit (x86)

AMI ID

ami-08fe5144a4659a3b3

Publish Date

2025-03-05

Username

ec2-user

Verified provider

Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI... [read more](#)
ami-08fe5144a4659a3b3

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 of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

[Preview code](#)

Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Family: t2 | 1 vCPU | 1 GiB Memory | Current generation: true | On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour | On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour | On-Demand SUSE base pricing: 0.0124 USD per Hour

Free tier eligible

☐ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

SangeethaCloud01

[Create new key pair](#)

Network settings [Info](#)

[Edit](#)

Network [Info](#)

vpc-01118fb0ecfe7f2dc

Subnet [Info](#)

No preference (Default subnet in any availability zone)

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

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

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere

0.0.0.0/0

☐ 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.

Create instance 2

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

web-server-2

Add additional tags

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-08fe5144e4659a3b3 (64-bit (x86)) / ami-0bf9265d7d9594735 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

Description

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Amazon Linux 2 Kernel 5.10 AMI 2.0.20250305.0 x86_64 HVM gp2

Architecture

AMI ID

Publish Date

Username

64-bit (x86) ▼

ami-08fe5144e4659a3b3

2025-03-05

ec2-user

Verified provider

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour On-Demand SUSE base pricing: 0.0124 USD per Hour

☐ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

SangeethaCloud01

[Create new key pair](#)

▼ Network settings [Info](#)

[Edit](#)

Network | [Info](#)

vpc-01118fb0ecfe7f2dc

Subnet | [Info](#)

No preference (Default subnet in any availability zone)

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

We'll create a new security group called 'launch-wizard-2' with the following rules:

☒ Allow SSH traffic from
Helps you connect to your instance

Anywhere
0.0.0.0/0

☐ 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.

2 Verify Web Server is Running

1. Connect to the instances using SSH:

```
ssh -i "your-key.pem" ec2-user@<EC2-Public-IP>
```

2. Check if the web server is running:

```
curl http://localhost
```

Expected Output:

<h1>Welcome to Web Server 1</h1> OR <h1>Welcome to Web Server 2</h1>

3. Open the **Public IP** in a browser and check if the webpage is displaying correctly.

The screenshot shows the AWS Management Console 'Instances' page with two instances listed: 'web-server-2' and 'web-server-1'. Below the table, a browser window is open to the public IP of 'web-server-1' (13.233.251.29), displaying 'Welcome to Web Server 1'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring	Secu
web-server-2	i-017d86ec24e42f03e	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-15-206-179-64.ap-...	15.206.179.64	-	-	disabled	laun
web-server-1	i-0c784b6b4836a4be4	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-13-233-251-29.ap-...	13.233.251.29	-	-	disabled	laun

The screenshot shows the 'Details' tab for instance 'i-0c784b6b4836a4be4 (web-server-1)'. The 'Public IPv4 address' is highlighted as 13.233.251.29. The instance state is 'Running'.

Instance summary

- Instance ID: i-0c784b6b4836a4be4
- IPv6 address: -
- Hostname type: IP name: ip-172-31-3-133.ap-south-1.compute.internal
- Answer private resource DNS name (IPv4 (A)): 13.233.251.29 (Public IP)
- Auto-assigned IP address: 13.233.251.29 (Public IP)
- IAM Role: -

Public IPv4 address: 13.233.251.29 | open address

Instance state: Running

Private IP DNS name (IPv4 only): ip-172-31-3-133.ap-south-1.compute.internal

Instance type: t2.micro

VPC ID: vpc-0118f0b0ecf7f2dc

Subnet ID: subnet-0493c4d8b760e8b4c

The screenshot shows the AWS Management Console 'Instances' page with two instances listed: 'web-server-2' and 'web-server-1'. Below the table, a browser window is open to the public IP of 'web-server-2' (15.206.179.64), displaying 'Welcome to Web Server 2'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring	Secu
web-server-2	i-017d86ec24e42f03e	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-15-206-179-64.ap-...	15.206.179.64	-	-	disabled	laun
web-server-1	i-0c784b6b4836a4be4	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-13-233-251-29.ap-...	13.233.251.29	-	-	disabled	laun

The screenshot shows the 'Details' tab for instance 'i-017d86ec24e42f03e (web-server-2)'. The 'Public IPv4 address' is highlighted as 15.206.179.64. The instance state is 'Running'.

Instance summary

- Instance ID: i-017d86ec24e42f03e
- IPv6 address: -
- Hostname type: IP name: ip-172-31-0-17.ap-south-1.compute.internal
- Answer private resource DNS name (IPv4 (A)): 15.206.179.64 (Public IP)
- Auto-assigned IP address: 15.206.179.64 (Public IP)
- IAM Role: -

Public IPv4 address: 15.206.179.64 | open address

Instance state: Running

Private IP DNS name (IPv4 only): ip-172-31-0-17.ap-south-1.compute.internal

Instance type: t2.micro

VPC ID: vpc-0118f0b0ecf7f2dc

Subnet ID: subnet-0493c4d8b760e8b4c

3 Create an Application Load Balancer (ALB)

1. Go to **AWS Load Balancers Console**.
2. Click **Create Load Balancer** → Select **Application Load Balancer**.
3. Configure:
 - **Scheme**: Internet-facing.
 - **IP Address Type**: IPv4.
 - **Availability Zones**: Select at least **two subnets**.
4. **Configure Security Group**:
 - Allow **HTTP (Port 80)** from **Anywhere**.
5. **Create a Target Group**:
 - Choose **Instance Type** as target.
 - **Port**: 80.
 - **Health Check Path**: `/index.html` (change from `/` to avoid failure).
6. **Register Targets (EC2 Instances)**:
 - Select both instances and register them.

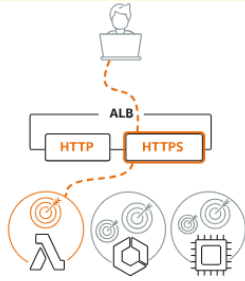
[EC2](#) > [Load balancers](#) > Compare and select load balancer type

Compare and select load balancer type

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

Load balancer types

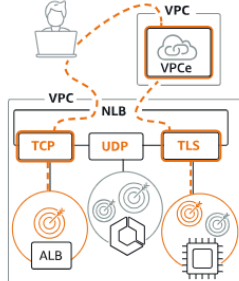
Application Load Balancer [Info](#)



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.

[Create](#)


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-low latencies.

[Create](#)

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.

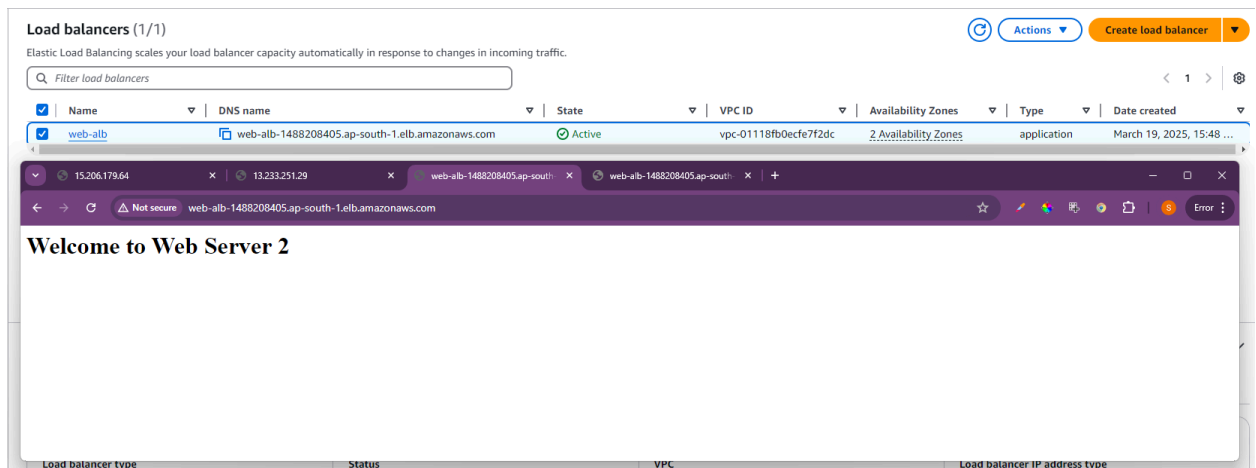
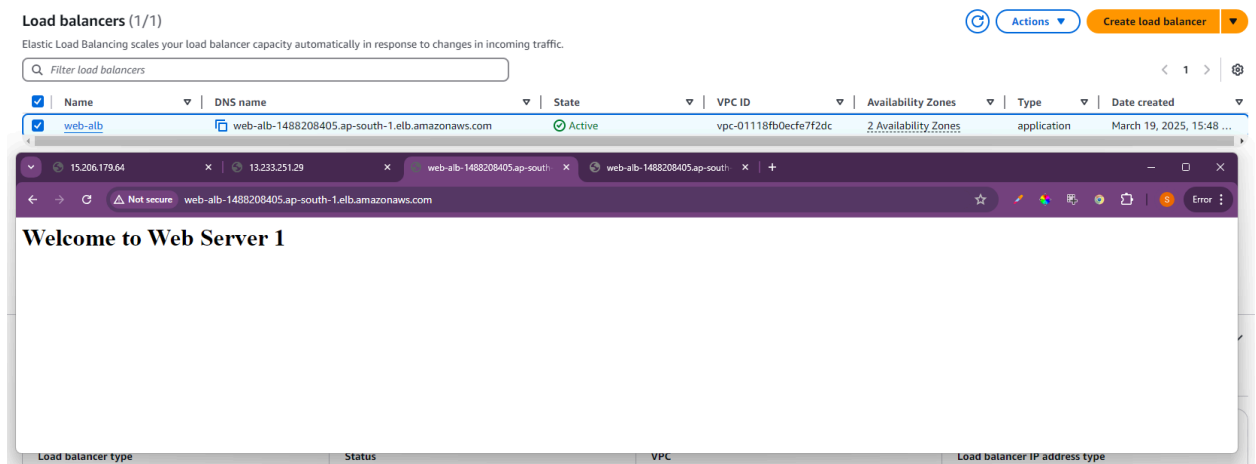
[Create](#)

► **Classic Load Balancer - previous generation**

[Close](#)

4 Testing the Load Balancer

1. Wait for the **ALB status to become Active**.
2. Open the **Load Balancer DNS Name** in a browser.
– <http://web-alb-xxxxxx.ap-south-1.elb.amazonaws.com/>
3. **Expected Output:**
 - Refresh multiple times, and you should see responses alternating between:
 - Welcome to Web Server 1
 - Welcome to Web Server 2



🎯 Final Confirmation

- ✓ Web Servers are running
- ✓ Load Balancer is distributing traffic
- ✓ DNS is accessible and responding correctly