

**Name: Prashanth Raghavendra Rao**

**Task: AWS 2**

**Date: 03/06/2025**

### **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.

The screenshot shows the 'Create bucket' wizard in the AWS S3 console. The steps are as follows:

- General configuration:** Set AWS Region to Asia Pacific (Mumbai) ap-south-1, Bucket type to General purpose, and Bucket name to guvprashanth. A note says "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".
- Object Ownership:** Set to ACLs disabled (recommended), indicating all objects in this bucket are owned by this account.
- Block Public Access settings for this bucket:** Turned on 'Block all public access'. Options include: Block public access to buckets and objects granted through new access control lists (ACLS), Block public access to buckets and objects granted through any access control lists (ACLS), and Block public access to buckets and objects created through new public bucket or access point policies.
- Bucket Versioning:** Set to Disable.
- Tags - optional (0):** No tags associated with this bucket. An 'Add tag' button is present.
- Default encryption:** Server-side encryption is automatically applied to new objects stored in this bucket. Options include: Server-side encryption with Amazon S3 managed keys (SSE-S3), Server-side encryption with AWS Key Management Service keys (SSE-KMS), and Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS).

Screenshot of the AWS S3 Bucket Creation Wizard:

**Bucket Versioning**  
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Disable  
 Enable

**Tags - optional (0)**  
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.  
[Add tag](#)

**Default encryption** [Info](#)  
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)  
 Server-side encryption with Amazon S3 managed keys (SSE-S3)  
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)  
 Dual-layer server-side encryption with AWS Key Management Service keys (DSS-E-KMS)  
Secure your objects with two separate layers of encryption. For details on pricing, see DSS-E-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

**Bucket Key**  
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSS-E-KMS. [Learn more](#)

Disable  
 Enable

**Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Create bucket](#)

Screenshot of the AWS S3 Buckets List:

**General purpose buckets (1) [Info](#) All AWS Regions**  
Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
guvprashanth	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	June 3, 2025, 18:52:45 (UTC+05:30)

[View details](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Screenshot of the AWS S3 Bucket Properties page for 'guviprashanth'.

**Bucket overview**

- AWS Region: Asia Pacific (Mumbai) ap-south-1
- Amazon Resource Name (ARN): arnaws3::guviprashanth
- Creation date: June 3, 2025, 18:52:43 (UTC+05:30)

**Bucket Versioning**

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

**Bucket Versioning**  
Disabled

**Multi-factor authentication (MFA) delete**  
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

**Tags (0)**  
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

**Default encryption**  
Server-side encryption is automatically applied to new objects stored in this bucket.

**Encryption type** Info  
Server-side encryption with Amazon S3 managed keys (SSE-S3)

**Bucket Key**  
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)  
Enabled

**Intelligent-Tiering Archive configurations (0)**  
Enable objects stored in the Intelligent-Tiering storage class to tier down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#)

**Server access logging**  
Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. [Learn more](#)

**Server access logging**  
Disabled

**AWS CloudTrail data events (0)** Info  
Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](#)

**Event notifications (0)**  
Send a notification when specific events occur in your bucket. [Learn more](#)

**Amazon EventBridge**

S3

Search [Option+S]

Amazon S3 > Buckets > guviprashanthi

Choose Create event notification to be notified when a specific event occurs.

Create event notification

**Amazon EventBridge**

For additional capabilities, use Amazon Eventbridge to build event-driven applications at scale using S3 event notifications. [Learn more](#) or [see EventBridge pricing](#).

**Edit**

**Send notifications to Amazon EventBridge for all events in this bucket**

Off

**Transfer acceleration**

Use an accelerated endpoint for faster data transfers. [Learn more](#).

**Edit**

**Transfer acceleration**

Disabled

**Object Lock**

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#).

**Edit**

**Object Lock**

Disabled

**Requester pays**

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#).

**Edit**

**Requester pays**

Disabled

**Static website hosting**

Use this bucket to host a website or redirect requests. [Learn more](#).

**Edit**

**We recommend using AWS Amplify Hosting for static website hosting**

Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#).

**Create Amplify app**

**S3 static website hosting**

Disabled

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# FILE UPLOAD

The screenshot shows the AWS S3 console after a file has been uploaded. A green success message at the top states "Upload succeeded. For more information, see the Files and folders table." Below this, the "Upload: status" section indicates "Succeeded" with "1 file, 117.2 KB (100.00%)" and "Failed" with "0 files, 0 B (0%)". The "Files and folders" tab is selected, showing a table with one item: "AWS Task-3.docx" (application/vnd.openxmlformats-officedocument.wordprocessingml.document, 117.2 KB, Succeeded). The "Configuration" tab is also present.

This screenshot shows the detailed view of the uploaded file "AWS Task-3.docx". The left sidebar includes links for Amazon S3, General purpose buckets, Storage Lens, and AWS Marketplace for S3. The main content area displays the "Object overview" with details like Owner (4f92632be7b133605172e0eca52b77d895fd2ee6d39240b9a56d8320cc45686), AWS Region (Asia Pacific (Mumbai) ap-south-1), Last modified (June 3, 2025, 18:55:23 (UTC+05:30)), Size (117.2 KB), Type (docx), and Key (AWS Task-3.docx). On the right, there are buttons for Copy S3 URI, Download, Open, and Object actions. The "Object management overview" section notes that Bucket Versioning is disabled and recommends enabling it. The "Management configurations" section includes Replication status, View replication rules, and Expiration rule. The "Expiration date" section indicates the object will be permanently deleted on June 3, 2027.

## EDIT SERVER ACCESS LOGIN

The screenshot shows the 'Edit server access logging' page for the 'guvprashanth' bucket in the AWS S3 console. The 'Server access logging' section is active, with the 'Enable' radio button selected. A note states: 'Bucket policy will be updated When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.' Below this, there's a 'Destination' section where users can specify a destination bucket and prefix. The 'Log object key format' section contains two options: '[DestinationPrefix]{YYYY}{MM}{DD}{hh}{mm}{ss}{UniqueString}' (selected) and '[DestinationPrefix]{SourceAccountId}/{SourceRegion}/{SourceBucket}/{YYYY}/{MM}/{DD}/{YYYY}{MM}{DD}{hh}{mm}{ss}{UniqueString}'. The 'Log object key example' section shows a placeholder. At the bottom right are 'Cancel' and 'Save changes' buttons.

A modal dialog titled 'Choose destination' is displayed, listing a single bucket named 'guvprashanth'. The modal includes a search bar, a table for filtering by name and AWS Region, and buttons for 'Cancel' and 'Choose destination'.

**Edit server access logging**

**Server access logging**

Log requests for access to your bucket. [Learn more](#)

Enable

**Bucket policy will be updated**

When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.

**Destination**

Specify a destination bucket in the Asia Pacific (Mumbai) ap-south-1 Region. To store your logs under a particular prefix, make sure that you include a slash (/) after the name of the prefix. Otherwise, the prefix will be added to the name of your log files.

Format: s3://[bucket]/[optional-prefix-with-path]

[Browse S3](#)

**Destination Region**

Asia Pacific (Mumbai) ap-south-1

**Destination bucket name**

guviprashanth

**Destination prefix**

-

**Log object key format**

[DestinationPrefix]{YYYY}{MM}{DD}{hh}{mm}{ss}{UniqueString}

[DestinationPrefix]{SourceAccountId}/{SourceRegion}/{SourceBucket}/{YYYY}{MM}{DD}{YYYY}{MM}{DD}{hh}{mm}{ss}{UniqueString}

To speed up analytics and query applications, use this format.

**Log object key example**

2025-07-01-10-12-56-[UniqueString]

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

**Successfully edited server access logging.**

**Intelligent-Tiering Archive configurations (0)**

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#)

[View details](#) [Edit](#) [Delete](#) [Create configuration](#)

**Server access logging**

Log requests for access to your bucket. Use [CloudWatch](#) to check the health of your server access logging. [Learn more](#)

**Server access logging**

Enabled

**Destination bucket**

s3://guviprashanth

**Log object key format**

{YYYY}{MM}{DD}{hh}{mm}{ss}{UniqueString}

**AWS CloudTrail data events (0)**

Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](#)

[Configure in CloudTrail](#)

**You don't have permission to get AWS CloudTrail data events details**

You or your AWS administrator must update your IAM permissions to allow `cloudtrail:DescribeTrails`. After you obtain the necessary permission, choose Refresh. Learn more about [Identity and access management in Amazon S3](#)

[Refresh](#) [Diagnose with Amazon Q](#)

**Event notifications (0)**

Send a notification when specific events occur in your bucket. [Learn more](#)

[Create event notification](#)

No event notifications

Choose Create event notification to be notified when a specific event occurs.

# CREATE CLOUD TRIAL

The screenshot shows the 'Quick trail create' step of the AWS CloudTrail configuration wizard. The 'Trail details' section is visible, containing a note about simplified logging management and a link to the full 'Create trail' workflow. A 'Trail name' field is filled with 's3-trails'. Below it, a log folder path 'aws-cloudtrail-logs-755937526811-0f4163da' is shown, along with a note that logs will be stored in an S3 bucket. A warning message at the bottom states that charges will be incurred for the S3 bucket used to store logs. At the bottom right are 'Cancel' and 'Create trail' buttons.

The screenshot shows the 'Choose trail attributes' step of the AWS CloudTrail configuration wizard. A yellow error bar at the top indicates an 'AccessDeniedException' occurred, stating that the user 'arn:aws:iam::755937526811:user/guviprashanthgavendra' is not authorized to perform the 'cloudtrailListTrails' action. The 'General details' section shows a note about multi-region trails and a 'Trail name' field containing 's3-guvi-prashanth-logs'. The 'Storage location' section includes options for creating a new S3 bucket or using an existing one; 'Use existing S3 bucket' is selected. Other settings include 'Trail log bucket name' (prefix 'guvi'), 'Log file SSE-KMS encryption' (Enabled), 'Customer managed AWS KMS key' (New), and 'AWS KMS alias' (empty). At the bottom, 'Additional settings' include 'Log file validation' (Enabled). Navigation steps are shown on the left: Step 1 (selected), Step 2, Step 3, and Review and create.

**AccessDeniedException**  
User: arn:aws:iam::755937526811:user/guviprashanthravendra is not authorized to perform: cloudtrail>ListTrails because no identity-based policy allows the cloudtrail>ListTrails action

**Step 1 Choose trail attributes**

- 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.  
**s3-guvi-prashanth-logs**

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

**Storage location** [Info](#)

- Create new S3 bucket**  
Create a bucket to store logs for this trail.
- Use existing S3 bucket**  
Choose an existing bucket to store logs for this trail.

**Trail log bucket name**  
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.  
**guviprashanth** [X](#) [Browse](#)

**Prefix - optional**  
**prefix**  
Logs will be stored in guviprashanth/AWSLogs/755937526811

**Log file SSE-KMS encryption** [Info](#)

**Enabled**

**Customer managed AWS KMS key**

- New**
- Existing**

**AWS KMS alias**  
**Enter KMS alias**  
KMS key and S3 bucket must be in the same region.

**Additional settings**

**Log file validation** [Info](#)

**Enabled**

**SNS notification delivery** [Info](#)

**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** [Info](#)

**Enabled**

**Log group** [Info](#)

- New**
- Existing**

**Log group name**  
**aws-cloudtrail-logs-755937526811-038ac2c6**

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**  
**CloudTrailRoleForCloudWatchLogs\_{trail-name}**

**Policy document**

**Tags - optional** [Info](#)  
You can add one or more tags to help you manage and organize your resources, including trails.

Key	Value - optional
<b>Enter key</b>	<b>Enter value</b>

[Add tag](#)  
You can add 49 more tags

[Cancel](#) [Next](#)

Screenshot of the AWS CloudTrail 'Create trail' wizard Step 2: Choose log events.

**AccessDeniedException**  
User: arn:aws:iam::755937526811:user/guviprashanthraghavendra is not authorized to perform: cloudtrail>ListTrails because no identity-based policy allows the cloudtrail>ListTrails action

**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.

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**

**Cancel** **Previous** **Next**

Screenshot of the AWS CloudTrail 'Create trail' wizard Step 3: Review and create.

**AccessDeniedException**  
User: arn:aws:iam::755937526811:user/guviprashanthraghavendra is not authorized to perform: cloudtrail>ListTrails because no identity-based policy allows the cloudtrail>ListTrails action

**Review and create**

**Step 1: Choose trail attributes**

**General details**

Trail name s3-govi-prashanth-logs	Trail log location guviprashanth/AWSLogs/755937526811	Log file validation Enabled
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled	SNS notification delivery Disabled
Apply trail to my organization Not enabled		

**CloudWatch Logs**

Log group aws-cloudtrail-logs-755937526811-058ac2c6	IAM Role AmazonAPIGatewayPushToCloudWatchLogs
--	--

**Tags**

Key	Value
No tags No tags associated with this trail	

**Step 2: Choose log events**

**Management events**

No additional charges apply to log management events on this trail because this is your first copy of management events.

**Cancel** **Previous** **Next**

**AccessDeniedException**  
User: arn:aws:iam::755937526811:user/guviprashanthraghavendra is not authorized to perform: cloudtrail>ListTrails because no identity-based policy allows the cloudtrail>ListTrails action

User: arn:aws:iam::755937526811:user/guviprashanthraghavendra is not authorized to perform: cloudtrail>CreateTrail on resource: arn:aws:cloudtrail:ap-south-1:755937526811:trail/s3-guvi-prashanth-logs because no identity-based policy allows the cloudtrail>CreateTrail action

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

### Review and create

#### Step 1: Choose trail attributes

General details		
Trail name s3-guvi-prashanth-logs	Trail log location guviprashanth/AWSLogs/755937526811	Log file validation Enabled
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled	SNS notification delivery Disabled
Apply trail to my organization Not enabled		

CloudWatch Logs	
Log group aws-cloudtrail-logs-755937526811-038ac2c6	IAM Role AmazonAPIGatewayPushToCloudWatchLogs

Tags	
Key	Value
No tags No tags associated with this trail	

#### Step 2: Choose log events

#### Management events

**Amazon S3**

- General purpose buckets
- Directory buckets
- Table buckets
- Access Grants
- Access Points for general purpose buckets
- Access Points for directory buckets
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

**Storage Lens**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 11

AWS Marketplace for S3

**Account snapshot - updated every 24 hours** All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

[View Storage Lens dashboard](#)

**General purpose buckets** (2) [Info](#) All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
aws-cloudtrail-logs-755937526811-bf4163da	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	June 3, 2025, 19:05:12 (UTC+05:30)
guviprashanth	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	June 3, 2025, 19:01:50 (UTC+05:30)

[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

**ACCESS DENIED FOR MY IAM**

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

## CREATE INSTANCES

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar navigation includes:

- Dashboard
- EC2 Global View
- Events
- Instances** (selected)
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity Reservations
- Images
- AMI Catalog
- Elastic Block Store
- Volumes
- Snapshots
- Lifecycle Manager
- Network & Security
- Security Groups
- Elastic IPs
- Placement Groups
- Key Pairs
- Network Interfaces
- Load Balancing
- Load Balancers
- Target Groups
- Trust Stores
- Auto Scaling
- Auto Scaling Groups

The main content area displays the "Instances (1/2) Info" table with two rows:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
prash1	i-0dc68e9dea8dfe308	Running	t2.micro	Initializing	View alarms	ap-south-1b	ec2-3-110-40-185.ap-s...
<b>prash2</b>	i-07df530003ff01db1	Running	t2.micro	Initializing	View alarms	ap-south-1b	ec2-13-201-194-246.ap...

The details page for instance **i-07df530003ff01db1 (prash1)** is shown with the following configuration:

- Details** tab selected.
- Instance summary** section:
  - Instance ID: i-07df530003ff01db1
  - IPv6 address: -
  - Hostname type: IP name: ip-172-31-9-155.ap-south-1.compute.internal
  - Answer private resource DNS name: IPv4 (A)
  - Auto-assigned IP address: 13.201.194.246 [Public IP]
- Public IPv4 address**: 13.201.194.246 | open address
- Instance state**: Running
- Private IP DNS name (IPv4 only)**: ip-172-31-9-155.ap-south-1.compute.internal
- Instance type**: t2.micro
- VPC ID**: vpc-0fb93fb8ea61af6e (Default-VPC)
- Private IPv4 addresses**: 172.31.9.155
- Public DNS**: ec2-13-201-194-246.ap-south-1.compute.amazonaws.com | open address
- Elastic IP addresses**: -
- AWS Compute Optimizer finding** (with a note about compute-optimizer:EnrollmentStatus):
  - User: arn:aws:iam::755937526811:user/guviprashanthraghavendra is not authorized to perform: compute-optimizer:GetEnvironmentStatus on resource: \* because no identity-based policy allows the compute-optimizer action on the resource.

## SETUP SERVERS

The screenshot shows a terminal window within the AWS CloudShell interface. The terminal is executing a series of commands to set up an Apache web server on an Ubuntu 8.6 system. The output of the commands is displayed below:

```
Setting up libaprutil1-db-dbd-sqlite3:amd64 (1.6.3-1.lubuntu7) ...
Setting up apache2-utils (2.4.58-ubuntu8.6) ...
Setting up apache2 (2.4.58-ubuntu8.6) ...
  enabling module mpm_event...
  enabling module auths_core...
  enabling module auths_host...
  enabling module authn_core...
  enabling module auth_basic...
  enabling module access_compat...
  enabling module authn_file...
  enabling module auths_user...
  enabling module alias...
  enabling module dir...
  enabling module autoindex...
  enabling module env...
  enabling module mime...
  enabling module negotiation...
  enabling module securif...
  enabling module filter...
  enabling module deflate...
  enabling module status...
  enabling module reqtimeout...
  enabling conf charset...
  enabling conf localized-error-pages...
  enabling conf other-hosts-access-log...
  enabling conf security...
  enabling conf serve-cgi-bin...
  enabling site 000-default...
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Scanning processes...
Scanning linux images...
running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-14-38:~$ sudo systemctl enable apache2
[sudo] password for ubuntu:
synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
ubuntu@ip-172-31-14-38:~$ echo "Hello from $(hostname)" | sudo tee /var/www/html/index.html
Hello from ip-172-31-14-38
ubuntu@ip-172-31-14-38:~$
```

At the bottom of the terminal, the command history shows:

```
i-0dc68e9dea8dfe308 (prash-server-1)
PublicIP: 3.110.40.185 PrivateIP: 172.31.14.38
```

Below the terminal, the CloudShell interface includes standard navigation and help links.

# APPLICATION LOAD BALANCER

The screenshot shows the AWS CloudFront console with the following details:

- Region:** Asia Pacific (Mumbai)
- User:** guvprashanthaghavendra @ 7559-3752-6811
- Breadcrumbs:** EC2 > Load balancers > Create Application Load Balancer
- Message:** Application Load Balancers now support public IPv4 IP Address Management (IPAM). You can get started with this feature by configuring IP pools in the Network mapping section.
- Create Application Load Balancer:** Info
- Description:** 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:** A detailed description of how ALBs work, mentioning internal and internet-facing traffic, private and public IP addresses, and DNS resolution.
- Basic configuration:**
  - Load balancer name:** ALB-Prash (Name must be unique within your AWS account and can't be changed after the load balancer is created.)
  - Scheme:** Info (Scheme can't be changed after the load balancer is created)
    - Internet-facing:** Selected. Includes public IP addresses, DNS name resolves to public IPs, and requires a public subnet.
    - Internal:** Unselected. Services internal traffic, has private IP addresses, and DNS name resolves to private IPs.
  - 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:** Selected. Includes only IPv4 addresses.
    - Dualstack:** Unselected. Includes IPv4 and IPv6 addresses.
    - Dualstack without public IPv4:** Unselected. 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. For a new VPC, create a VPC.)
- Default VPC:** vpc-0f893fb8ea61af6e (IPv4 VPC CIDR: 172.31.0.0/16)
- Actions:** cloudShell Feedback

The screenshot shows the AWS EC2 Target Groups page with the following details:

- Region:** Asia Pacific (Mumbai)
- User:** guvprashanthaghavendra @ 7559-3752-6811
- Breadcrumbs:** EC2 > Target groups > ALB1
- Message:** Successfully created the target group: ALB1. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab.
- ALB1:** Details
  - Target type:** Instance
  - Protocol:** Port HTTP:80
  - Protocol version:** HTTP1
  - VPC:** vpc-0f893fb8ea61af6e
  - IP address type:** IPv4
  - Load balancer:** None associated
- Targets:** 2 Total targets
  - 0 Healthy
  - 0 Unhealthy
  - 2 Unused
  - 0 Initial
  - 0 Draining
- Distribution of targets by Availability Zone (AZ):** Select values in this table to see corresponding filters applied to the Registered targets table below.
- Registered targets (2):** Info
  - Anomaly mitigation: Not applicable
  - Filter targets
  - 1 target
  - Instance ID: i-0dc68e9dea8dfe308 (prash-server-1)
  - Instance ID: i-07df530003ff01db1 (prash-server-2)
- Actions:** cloudShell Feedback

aws IAM EC2 VPC S3

EC2 > Load balancers > ALB-Prash

**ALB-Prash**

**Details**

Load balancer type Application	Status Provisioning	VPC <a href="#">vpc-0fb938fb8ea61af6e</a>	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone ZP97RAFLXTNZK	Availability Zones subnet-09fd6fab0bc365232 ap-south-1c (ap1-az2) subnet-0a3863e7fae1d0ea ap-south-1b (ap1-az3) subnet-0f6d05beada3c7095 ap-south-1a (ap1-az1)	Date created June 3, 2025, 20:04 (UTC+05:30)
Load balancer ARN <a href="#">arnaws:elasticloadbalancing:ap-south-1:755937526811:loadbalancer/app/ALB-Prash/53fd78c0b4b4000</a>	DNS name Info <a href="#">ALB-Prash-26655702.ap-south-1.elb.amazonaws.com (A Record)</a>		

**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
HTTP:80	Forward to target group • ALB1: 1 (100%) • Target group stickiness: Off	1 rule	<a href="#">ARN</a>	Not applicable	Not applicable	Not applicable

The following NEW packages will be installed:

```

nginx nginx-common
0 upgraded, 0 newly installed, 0 to remove and 101 not upgraded.
Need to get 551 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx-common all 1.24.0-2ubuntu7.3 [31.2 kB]
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx amd64 1.24.0-2ubuntu7.3 [520 kB]
Fetched 551 kB in 0s (24.5 MB/s)
Preconfiguring packages ...
Purging nginx-common (1.24.0-2ubuntu7.3) ...
Unpacking nginx-common (1.24.0-2ubuntu7.3) ...
Selected previously unselected package nginx.
Preparing to unpack .../nginx_1.24.0-2ubuntu7.3_amd64.deb ...
Unpacking nginx (1.24.0-2ubuntu7.3) ...
Setting up nginx-common (1.24.0-2ubuntu7.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /usr/lib/systemd/system/nginx.service.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-9-155:~$ sudo systemctl start nginx
ubuntu@ip-172-31-9-155:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-06-03 15:59:45 UTC; 22s ago
     Docs: man:nginx(8)
  Process: 2307 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
  Process: 2308 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Main PID: 2310 (nginx)
    Tasks: 2 (limit: 1129)
   Memory: 1.79M (peak: 1.98M)
      CPU: 10ms
     CGroup: /system.slice/nginx.service
             └─2311 nginx worker process

Jun 03 15:59:45 ip-172-31-9-155 systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server...
Jun 03 15:59:45 ip-172-31-9-155 systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server.
ubuntu@ip-172-31-9-155:~$ 
```

i-07df530003f01db1 (prash-server-2)

PublicIPs: 13.201.194.246 PrivateIPs: 172.31.9.155

**Load balancers (1/1)**

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
ALB-Prash	ALB-Prash-26655702.ap-so...	Active	vpc-0f8938fb8ea61af6e	3 Availability Zones	application	June 3, 2025, 20:04 (UTC+05:30)

**Load balancer: ALB-Prash**

**Details**

Load balancer type Application	Status <span style="color: green;">Active</span>	VPC vpc-0f8938fb8ea61af6e	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone ZP97RAFLXTNZK	Availability Zones	Date created June 3, 2025, 20:04 (UTC+05:30)
Load balancer ARN arn:aws:elasticloadbalancing:ap-south-1:755937526811:loadbalancer/app/ALB-Prash/53fd78c0b4b b4000		DNS name Info ALB-Prash-26655702.ap-south-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
HTTP:80	Forward to target group • ALB-2 (100%) • Target group stickiness: Off	1 rule	ARN	Not applicable	Not applicable	Not applicable

Screenshot of the AWS EC2 Target Groups interface showing the configuration for ALB-2.

**Details:**

- Protocol: Port - HTTP: 80
- Protocol version: HTTP1
- VPC: [vpc-0fb938fb8ea61af6e](#)

**Targets:**

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

**Distribution of targets by Availability Zone (AZ):**

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.

**Registered targets (2) [Info](#)**

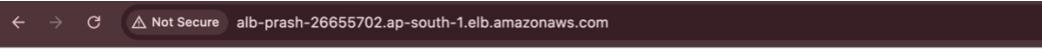
Instance ID	Name	Port	Zone	Health status	Health status details	Admini...	Overri...	Launch...
<a href="#">i-0dc68e9dea8dfc308</a>	prash-server-1	80	ap-south-1b (a...	Healthy	-	<input type="radio"/> No override.	<input type="radio"/> No overri...	June 3, 20...
<a href="#">i-07df530003ff01db1</a>	prash-server-2	80	ap-south-1b (a...	Healthy	-	<input type="radio"/> No override.	<input type="radio"/> No overri...	June 3, 20...

**Actions:**

- Anomaly mitigation: Not applicable
- Deregister
- Register targets

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## RESPONSE FROM LOADBALANCER WHEN REFRESHED POINTS TO TWO SERVERS



Hello from ip-172-31-9-155

←

→



Not Secure

alb-prash-26655702.ap-south-1.elb.amazonaws.com

Hello from ip-172-31-14-38