

# Secure Cloud File Storage with IAM and Audit Logging in AWS

Prepared by Mayank Jain

## 1. Project Summary:

"Configured secure file storage in AWS using S3, with strict IAM policies and CloudTrail logging to monitor access and protect data."

## 2. Tools Used:

- AWS S3
- IAM
- Cloudtrail

## 3. Security Features Implemented:

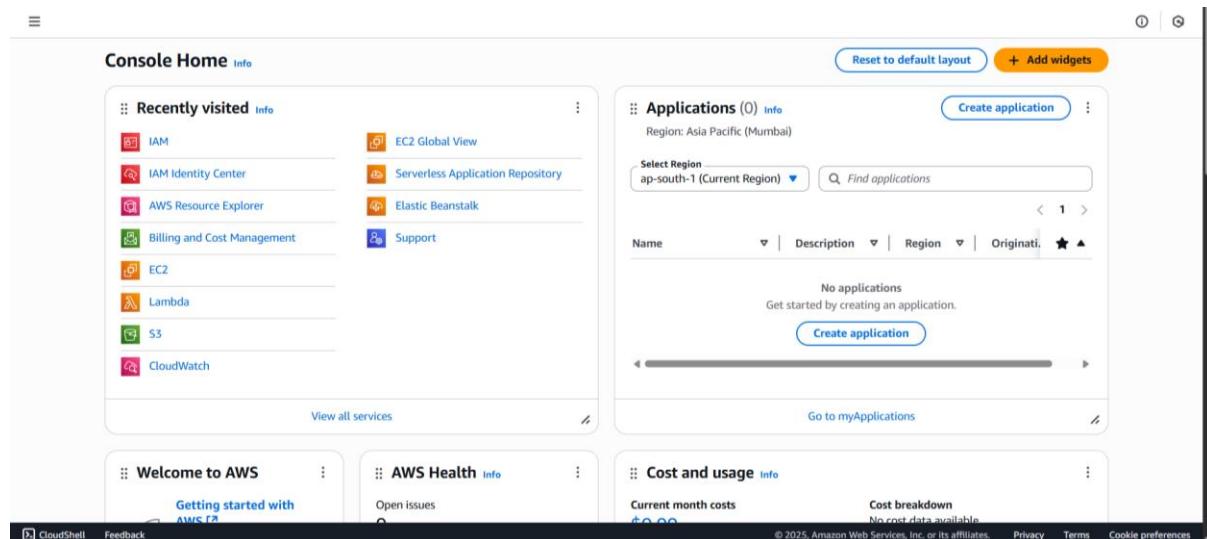
- Private S3 bucket
- IAM-based least-privilege access
- Default encryption
- CloudTrail audit logging

## 4. Outcome:

- Read-only user created
- Unauthorized actions blocked
- Audit logs successfully recorded in CloudTrail

## Steps:

1. Log in to your Amazon AWS account and go to the **S3 service** in the AWS Console



## 2. Click “Create bucket”.

The screenshot shows the Amazon S3 homepage. At the top, there's a dark header with the AWS logo and the word "Storage". Below it, the main title "Amazon S3" is displayed in large, bold letters, followed by the subtitle "Store and retrieve any amount of data from anywhere". A subtext below the subtitle reads: "Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance." To the right of the main content area, there's a white box with the heading "Create a bucket". Inside this box, the text says: "Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored." At the bottom of this box is a yellow "Create bucket" button. Below the main content, there are sections for "How it works" (with a video thumbnail), "Pricing" (mentioning no minimum fees), and "Resources". The footer contains links for CloudShell, Feedback, and various AWS terms like Privacy, Terms, and Cookie preferences.

## 3. Name it **secure-storage-mayank** and keep default settings for the bucket.

The screenshot shows the "Create bucket" wizard on the "General configuration" step. The top navigation bar shows "Amazon S3 > Buckets > Create bucket". The main section is titled "Create bucket" with a "General configuration" sub-section. It includes fields for "AWS Region" (set to Asia Pacific (Mumbai) ap-south-1), "Bucket type" (set to "General purpose"), and "Bucket name" (set to "secure-storage-mayank"). There are also sections for "Copy settings from existing bucket - optional" and "Object Ownership". The "Object Ownership" section has two options: "ACLs disabled (recommended)" (selected) and "ACLs enabled". The "Block Public Access settings for this bucket" section contains several checkboxes for blocking public access, all of which are checked. The "Bucket Versioning" section is partially visible at the bottom. The footer contains standard AWS links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

4. Click **Create Bucket**.

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

- Default encryption**: Info. Server-side encryption is automatically applied to new objects stored in this bucket.
- Encryption type**: Info. Options include:  Server-side encryption with Amazon S3 managed keys (SSE-S3) (selected),  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). Note: Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-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 DSSE-KMS. [Learn more](#). Options:  Disable (selected),  Enable.
- Advanced settings**: A link to view additional bucket settings after creation.
- Summary**: After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
- Buttons**: 'Cancel' and 'Create bucket' (highlighted in orange).

5. In the list of General purpose buckets, you will be able to see the created S3 bucket **secure-storage-mayank**.

The screenshot shows the 'General purpose buckets' list in the AWS S3 console. The table displays one bucket:

Name	AWS Region	IAM Access Analyzer	Creation date
<a href="#">secure-storage-mayank</a>	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	May 16, 2025, 18:31:54 (UTC+05:30)

Other visible elements include:

- 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](#).
- General purpose buckets** (1) [Info](#) All AWS Regions. Buckets are containers for data stored in S3.
- Actions**: Copy ARN, Empty, Delete, Create bucket.
- Navigation**: Page 1 of 1.
- Footer**: CloudShell, Feedback, © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, Cookie preferences.

The screenshot shows the Amazon S3 console interface. At the top, the navigation bar includes 'Amazon S3 > Buckets > secure-storage-mayank'. Below the navigation is a header with tabs: 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The main content area is titled 'secure-storage-mayank' with a 'Info' link. It displays 'Objects (0)' and a message stating 'No objects'. There is a search bar labeled 'Find objects by prefix' and a toolbar with actions like 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A note at the bottom says 'Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions.' Below the note is a 'Upload' button. The footer of the page includes links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

## 6. Go to IAM.

The screenshot shows the AWS IAM console search results for 'IAM'. The search bar at the top left contains 'IAM'. On the left, a sidebar lists 'Services' (Features, Resources, Documentation, Knowledge articles, Marketplace, Blog posts, Events, Tutorials) and 'Features' (Groups, Roles, Identity providers). The main content area shows three services: 'IAM' (Manage access to AWS resources), 'IAM Identity Center' (Manage workforce user access to multiple AWS accounts and cloud applications), and 'Resource Access Manager' (Share AWS resources with other accounts or AWS Organizations). To the right, there is a 'Create application' section with a 'Create application' button and a 'Cost breakdown' section indicating 'No cost data available'. The footer includes links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

## 7. Click on Users.

The screenshot shows the IAM Dashboard. On the left, a sidebar lists navigation options like Dashboard, Access management, and Access reports. The main area displays security recommendations (Add MFA for root user, Root user has no active access keys), IAM resources (User groups: 0, Users: 0, Roles: 2, Policies: 0, Identity providers: 0), and a 'What's new' section with recent announcements from AWS IAM, CodeBuild, and IAM Roles Anywhere.

## 8. Click on Create User.

The screenshot shows the Users page under the IAM section. The sidebar includes options like Dashboard, Access management (with 'Users' selected), and Access reports. The main content area shows a table header for 'Users (0)' with columns for User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, and Acc. A message indicates 'No resources to display'. A prominent orange 'Create user' button is located in the top right corner.

## 9. Enter the username: **readonly-user**.

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

### Specify user details

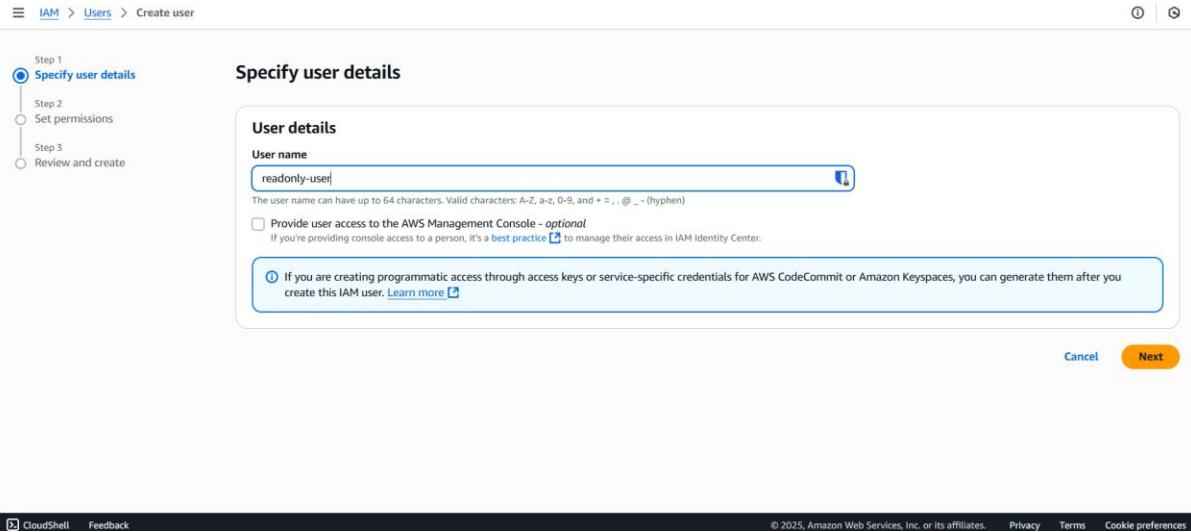
**User details**

User name  

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ \_ - (hyphen)

Provide user access to the AWS Management Console - optional  
If you're providing console access to a person, it's a best practice [Learn more](#). If you're creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

**Cancel** **Next**



10. Click on **Attach policies directly** and then click on **Create Policy** to create your custom policy.

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

### Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Permissions options**

Add user to group  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions  
Copy all group memberships, attached managed policies, and inline policies from an existing user.

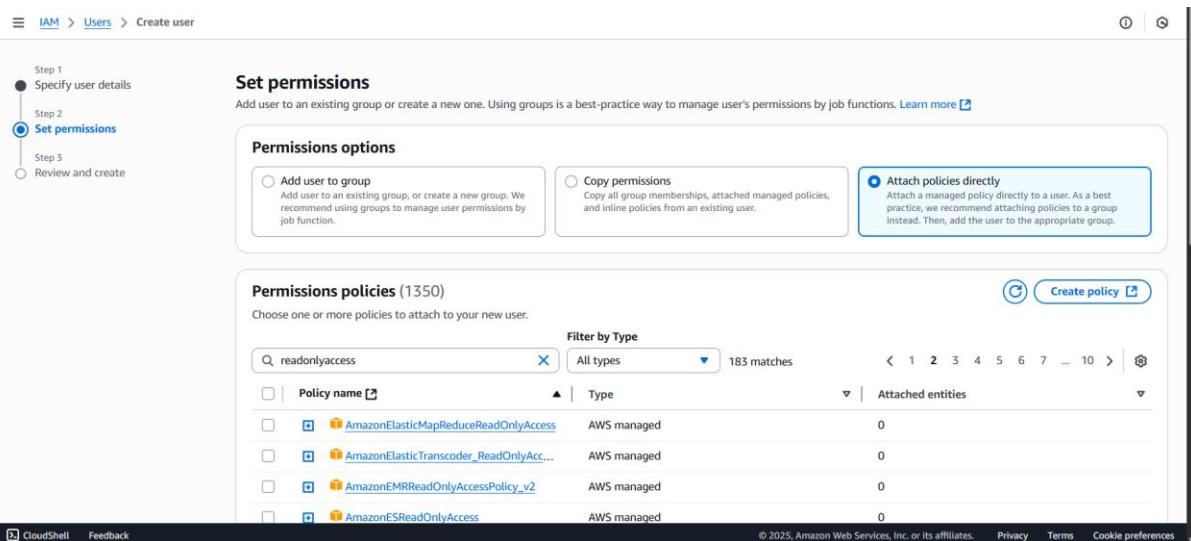
Attach policies directly  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

**Permissions policies (1350)**

Choose one or more policies to attach to your new user.

Filter by Type		
<input type="text" value="readonlyaccess"/> 	All types 	183 matches
<input type="checkbox"/> Policy name 	Type 	Attached entities 
<input type="checkbox"/>  AmazonElasticMapReduceReadOnlyAccess	AWS managed	0
<input type="checkbox"/>  AmazonElasticTranscoder_ReadOnlyAcc...	AWS managed	0
<input type="checkbox"/>  AmazonEMRReadOnlyAccessPolicy_v2	AWS managed	0
<input type="checkbox"/>  AmazonESReadOnlyAccess	AWS managed	0

 **Create policy** 



11. Choose **Json** as the option and specify the permissions. Paste the following statement in the Policy editor and click on **Next**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::secure-storage-mayank/*"]
    }
  ]
}
```

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": ["s3:GetObject"],
7       "Resource": ["arn:aws:s3:::secure-storage-mayank/*"]
8     }
9   ]
10 }
11

```

## 12. Give the policy name and click on Create Policy.

**Review and create** Info

Review the permissions, specify details, and tags.

**Policy details**

**Policy name**  
Enter a meaningful name to identify this policy.

**Description - optional**  
Add a short explanation for this policy.

**Permissions defined in this policy** Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Service	Access level	Resource	Request condition
Allow (1 of 440 services)			

## 13. Your policy is created message shows.

**Identity and Access Management (IAM)**

**Policies (1351)** Info

A policy is an object in AWS that defines permissions.

**Filter by Type**

Policy name	Type	Used as	Description
<a href="#">AccessAnalyzerServiceRole...</a>	AWS managed	None	
<a href="#">AdministratorAccess</a>	AWS managed - job function	None	
<a href="#">AdministratorAccess-Amplify</a>	AWS managed	None	
<a href="#">AdministratorAccess-AWSEL...</a>	AWS managed	None	
<a href="#">AIOpsAssistantPolicy</a>	AWS managed	None	
<a href="#">AIOpsConsoleAdminPolicy</a>	AWS managed	None	
<a href="#">AIOpsOperatorAccess</a>	AWS managed	None	
<a href="#">AIOpsReadOnlyAccess</a>	AWS managed	None	
<a href="#">AlexaForBusinessDeviceSetup</a>	AWS managed	None	

14. Now we resume the process of giving permission to our user and attach the policy we just created and click on **Next**.

Permissions options

- Add user to group
- Copy permissions
- Attach policies directly**

Permissions policies (1351)

Choose one or more policies to attach to your new user.

Policy name	Type	Attached entities
AWSMarketplaceRead-only	AWS managed	0
Read-onlyaccesstospecificbucket	Customer managed	0

Set permissions boundary - optional

Cancel Previous Next

Permissions options

- Add user to group
- Copy permissions
- Attach policies directly**

Permissions policies (1/1351)

Choose one or more policies to attach to your new user.

Policy name	Type	Attached entities
AWSMarketplaceRead-only	AWS managed	0
Read-onlyaccesstospecificbucket	Customer managed	0

Set permissions boundary - optional

Cancel Previous Next

15. Review the information and permissions for the user and click on **Create User**.

Step 1 Specify user details  
 Step 2 Set permissions  
 Step 3 Review and create

**Review and create**  
 Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details	Console password type	Require password reset
User name read-onlyuser	None	No

**Permissions summary**

Name	Type	Used as
<a href="#">Read-onlyaccessstospecificbucket</a>	Customer managed	Permissions policy

**Tags - optional**  
 Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.  
 No tags associated with the resource.

Add new tag  
 You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

16. User created successfully message appears. You can click on the user to see his information and permissions.

**User created successfully**  
 You can view and download the user's password and email instructions for signing in to the AWS Management Console.

**Users (1) Info**  
 An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID
<a href="#">read-onlyuser</a>	/	0	-	-	-	-	-

[View user](#) [Delete](#) [Create user](#)

**read-onlyuser Info**

**Summary**

ARN <a href="#">arn:aws:iam::992382596209:user/read-onlyuser</a>	Console access Disabled	Access key 1 <a href="#">Create access key</a>
Created May 16, 2025, 18:44 (UTC+05:30)	Last console sign-in -	

**Permissions** [Groups](#) [Tags](#) [Security credentials](#) [Last Accessed](#)

**Permissions policies (1)**  
 Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
<a href="#">Read-onlyaccessstospecificbucket</a>	Customer managed	Directly

**Permissions boundary (not set)**

**Generate policy based on CloudTrail events**

17. Go to Security Credentials and click on Enable Console Access.

Identity and Access Management (IAM)

Users > read-onlyuser

Summary

ARN: arn:aws:iam::992382596209:user/read-onlyuser

Created: May 16, 2025, 18:44 (UTC+05:30)

Console access: Disabled

Last console sign-in: -

Access key 1: Create access key

Permissions Groups Tags Security credentials Last Accessed

Console sign-in

Console sign-in link: https://992382596209.signin.aws.amazon.com/console

Console password: Not enabled

Enable console access

Multi-factor authentication (MFA) (0)

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Type Identifier Certifications Created on

Assign MFA device

18. Click on **Custom Password** for providing a password of your choice and click on **Enable Console Access**.

Identity and Access Management (IAM)

Users > read-onlyuser

Summary

ARN: arn:aws:iam::992382596209:user/read-onlyuser

Created: May 16, 2025, 18:44 (UTC+05:30)

Console access: Disabled

Access key 1: Create access key

Enable console access

Console password:

Autogenerated password

Custom password

User must create new password at next sign-in

Enable console access

Multi-factor authentication (MFA) (0)

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Type Identifier Certifications Created on

Assign MFA device

Identity and Access Management (IAM)

Users > read-onlyuser

Summary

ARN: arn:aws:iam::992382596209:user/read-onlyuser

Created: May 16, 2025, 18:44 (UTC+05:30)

Console access: Disabled

Access key 1: Create access key

Enable console access

Console password:

Autogenerated password

Custom password

.....

Must be at least 8 characters long  
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & \* \_ + - (hyphen) - [ ] { }

Show password

User must create new password at next sign-in

Enable console access

Multi-factor authentication (MFA) (0)

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Type Identifier Certifications Created on

Assign MFA device

The screenshot shows the AWS IAM console under the 'Users' section for a user named 'read-onlyuser'. A modal window titled 'Console password' displays a green success message: 'You have successfully enabled the user's new password. This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.' Below this, the 'Console sign-in URL' is listed as <https://992382596209.signin.aws.amazon.com/console>. The 'User name' is 'read-onlyuser' and the 'Console password' is masked. At the bottom right of the modal is a 'Close' button.

## 19. Now go to Cloudtrail to enable audit logging.

The screenshot shows the AWS search results for 'cloudtrail'. The top result is 'CloudTrail' with the description 'Track User Activity and API Usage'. Other results include 'Detective' (Investigate and Analyze potential security issues), 'Athena' (Serverless interactive analytics service), 'Create a SFTP server' (AWS Transfer Family feature), 'Insights' (CloudTrail feature), and 'Lake' (CloudTrail feature). On the right side of the search results, there is a sidebar for 'Access key 1' with options to 'Create access key', 'Remove', and 'Add permis'. Below the sidebar, it says 'Attached via [ ] Directly'.

## 20. Click on Create a trail.

The screenshot shows the AWS CloudTrail homepage. At the top, there's a banner with the text "Management & Governance" and "AWS CloudTrail". Below the banner, the main heading is "AWS CloudTrail" with the subtext "Continuously log your AWS account activity". A call-to-action button "Create a trail" is visible. To the right, there's a "Pricing" section and a "Getting started" section with links to "What is AWS CloudTrail?", "How AWS CloudTrail works", and "Services that integrate with AWS CloudTrail". At the bottom of the page, there are links for "CloudShell", "Feedback", "© 2025, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".

21. Either create a **Quick Trail** or click on **Create Trail** in the first line to see the full workflow as in this case.

The screenshot shows the "Quick trail create" wizard. The first step, "Trail details", is selected. It contains fields for "Trail name" (set to "s3-access-logs"), "Trail log bucket and folder" (set to "aws-cloudtrail-logs-992382596209-25409363"), and a note about charges. At the bottom are "Cancel" and "Create trail" buttons.

22. Provide the **Trail Name** (s3-access-logs) and choose **Use existing S3 bucket** and choose the bucket we created previously.

The screenshot shows the "Choose trail attributes" step of the "Create trail" wizard. The "Step 1 Choose trail attributes" tab is selected. Under "General details", the "Trail name" is set to "s3-access-logs". Under "Storage location", the "Use existing S3 bucket" option is selected, pointing to the "secure-storage-mayank" bucket. Other options like "Create new S3 bucket" are also shown. At the bottom are "Cancel", "Previous Step", "Next Step", and "Create trail" buttons.

## 23. Provide a key name for the AWS KMS alias to create a new key.

The screenshot shows the 'Create trail' wizard at Step 2: Choose log events. In the 'Events' section, the 'Management events' checkbox is checked. A note below states: 'No additional charges apply to log management events on this trail because this is your first copy of management events.'

## 24. Choose Management and Data events.

The screenshot shows the 'Create trail' wizard at Step 2: Choose log events. Both 'Management events' and 'Data events' checkboxes are checked. A note below states: 'No additional charges apply to log management events on this trail because this is your first copy of management events.'

The screenshot shows the 'Create trail' wizard at Step 2: Choose log events. Both 'Management events' and 'Data events' checkboxes are checked. A note below states: 'No additional charges apply to log management events on this trail because this is your first copy of management events.'

## 25. Choose the events you want to log in Managed events.

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

**API activity**  
Choose the activities you want to log.

Read  Write

Exclude AWS KMS events  
 Exclude Amazon RDS Data API events

**Data events** Info  
Data events show information about the resource operations performed on or within a resource. Additional charges apply

**Advanced event selectors are enabled**  
Use the following fields for fine-grained control over the data events captured by your trail.

**Data event: S3**

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

S3

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

## 26. In Data events, select Resource Type as S3 and Log all events.

**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.

**Data event: S3**

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

S3

**Log selector template**  
Log all events

**Selector name - optional**  
Enter a name  
1,000 character limit

**JSON view**

Add data event type

Cancel Previous Next

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

## 27. Review the information and click on Create Trail.

**Review and create**

**Step 1: Choose trail attributes**

**General details**

Trail name s3-access-logs	Trail log location secure-storage-mayank/AWSLogs/992382596209	Log file validation Enabled
Multi-region trail Yes	Log file SSE-KMS encryption Enabled	SNS notification delivery Disabled
Apply trail to my organization Not enabled	AWS KMS key alias alias/cloudtrail-logs-key	

**CloudWatch Logs**

No CloudWatch Logs log groups  
CloudWatch Logs is not configured for this trail

**Tags**

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

**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.

**API activity**  
All

**Exclude AWS KMS events**  
No  
Exclude Amazon RDS Data API events  
Yes

**Data events**

**Data events: S3**  
Log selector template  
Log all events

**Selector name**  
--

All events

**Insights events**

You can only enable CloudTrail Insights on trails that log management events. [Learn more](#)

**Network activity events**

Network activity event collection is not configured for this trail

28. Trail successfully created message appears.

**Trails**

Trail successfully created

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
s3-access-logs	Asia Pacific (Mumbai)	Yes	arn:aws:cloudtrail:ap-south-1:992382596209:trail/s3-access-logs	Disabled	No	secure-storage-mayank	-	-	Logging

29. Login to the new user that you created (read-onlyuser).

You are currently using the improved sign in UI experience.  
The improved sign in experience will launch soon. During this time, you can still change back to legacy sign in using the dropdown in the upper right corner.

IAM user sign in

Account ID or alias (Don't have?)

Remember this account

IAM username

Password

Show Password Having trouble?

Sign in

aws

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

Learn more

Robot icon giving a thumbs up

Service menu

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 Aurora and RDS Lambda

View all services

Applications (0)

Create application

Select Region: eu-north-1 (Current Region)

Find applications

Name Description Region Originati.

Access denied to servicelogicatalog>ListApplications

Diagnose with Amazon Q

Welcome to AWS

Getting started with AWS F2F

AWS Health

Cost and usage

Cost breakdown

CloudShell Feedback

30. Go to S3 using the new user.

aws

S3

Services

Features

Resources New

Documentation

Knowledge articles

Marketplace

Blog posts

Events

Tutorials

Were these results helpful?

Yes No

Scalable Storage in the Cloud

Buckets Storage Lens dashboards Batch Operations S3 Express One Zone S3 Access Grants

Archive Storage in the Cloud

Large Scale Data Transport

Imports from S3

DynamoDB feature

Feature spotlight

S3 feature

S3 Access Grants

Cost breakdown

Access denied

https://eu-north-1.console.aws.amazon.com/s3/home?region=eu-north-1

31. You will see that the **Access Denied** message, as the user does not have permission.

The screenshot shows the AWS S3 buckets interface. On the left, there's a sidebar with options like General purpose buckets, Directory buckets, Table buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. Below that is a section for Block Public Access settings. Under Storage Lens, there are Dashboards, Storage Lens groups, and AWS Organizations settings. A Feature spotlight section is also present. The main content area has tabs for General purpose buckets and Directory buckets, with General purpose buckets selected. It displays an account snapshot updated every 24 hours. A search bar allows finding buckets by name. The table lists buckets by Name, AWS Region, IAM Access Analyzer, and Creation date. One entry is highlighted with a red border and labeled 'Error' with the message 'Access Denied'. There are buttons for Copy ARN, Empty, Delete, and Create bucket. A 'View Storage Lens dashboard' button is also visible.

32. Now go to the root user and then go to **Event History** in Cloudtrail to see the audit logs from root user and read-onlyuser.

The screenshot shows the AWS CloudTrail Event history page. The left sidebar includes CloudTrail (selected), Dashboard, Event history (selected), Insights, Lake (Dashboards, Query, Event data stores, Integrations, Trails), Settings, Pricing, Documentation, Forums, and FAQs. The main content area shows the Event history (15) table. The table has columns for Event name, Event time, User name, Event source, Resource type, and Resource name. The events listed are: StartLogging, CreateTrail, PutEventSelectors, PutBucketPolicy, CreateAlias, CreateKey, DeleteTrail, and PutEventSelectors. All events were performed by the root user on May 16, 2025, at various times. The event sources include cloudtrail.amazonaws.com and s3.amazonaws.com. The resource types include AWS::CloudTrail::Trail and AWS::S3::Bucket. The resource names are arn:aws:cloudtrail:ap-s... and arn:aws:s3-access-logs:arn:aws:s... respectively. There are buttons for Download events, Create Athena table, Filter by date and time, and Clear filter. A message at the bottom says '0 / 5 events selected'.

CloudTrail
Dashboard
<b>Event history</b>
Insights
▼ Lake
Dashboards
Query
Event data stores
Integrations
Traits
Settings
Pricing
Documentation
Forums
FAQs

## Event history (25) Info

Event history shows you the last 90 days of management events.

Lookup attributes

User name	Event name	Event time	User name	Event source	Resource type	Resource name
	<a href="#">ListBuckets</a>	May 16, 2025, 19:28:24 (UTC+0...)	read-onlyuser	s3.amazonaws.com	-	-
	<a href="#">ListBuckets</a>	May 16, 2025, 19:28:21 (UTC+0...)	read-onlyuser	s3.amazonaws.com	-	-
	<a href="#">ListNotificationHubs</a>	May 16, 2025, 19:28:21 (UTC+0...)	read-onlyuser	notifications.amazonaws.com	-	-
	<a href="#">DescribeRegions</a>	May 16, 2025, 19:28:20 (UTC+0...)	read-onlyuser	ec2.amazonaws.com	-	-
	<a href="#">ListNotificationHubs</a>	May 16, 2025, 19:28:17 (UTC+0...)	read-onlyuser	notifications.amazonaws.com	-	-
	<a href="#">ListApplications</a>	May 16, 2025, 19:28:16 (UTC+0...)	read-onlyuser	servicecatalog-appregistry.amazonaws.com	-	-
	<a href="#">DescribeRegions</a>	May 16, 2025, 19:28:16 (UTC+0...)	read-onlyuser	ec2.amazonaws.com	-	-
	<a href="#">ListBuckets</a>	May 16, 2025, 19:27:44 (UTC+0...)	read-onlyuser	s3.amazonaws.com	-	-

0 / 5 events selected



Download events

Create Athena table