

Introduction to AWS Key Management Service

Lab overview

This lab introduces you to AWS Key Management Service (AWS KMS). The lab demonstrates the basic steps required to get started with AWS KMS, creating keys, assigning management and usage permissions for the keys, encrypting data and monitoring the access and usage of keys.

Objectives

By the end of this lab, you should be able to do the following:

- Create an Encryption Key
- Create an Amazon Simple Storage Service (Amazon S3) bucket with AWS CloudTrail logging functions
- Encrypt data stored in an Amazon S3 bucket using an encryption key
- Monitor encryption key usage using CloudTrail
- Manage encryption keys for users and roles

Technical knowledge prerequisites

Some familiarity with access control management.

It is strongly recommended to complete this lab using the Google Chrome web browser. If you cannot use Google Chrome then use a utility on your computer that can open gzip compressed files (*.gz).

Start lab

1. To launch the lab, at the top of the page, choose **Start Lab**.

Caution: You must wait for the provisioned AWS services to be ready before you can continue.

2. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

Warning: Do not change the **Region** unless instructed.

Services used in this lab

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data, and uses Hardware Security Modules (HSMs) to protect the security of your keys. AWS Key Management Service is integrated with several other AWS services to help you protect the data you store with these services. AWS Key Management Service is also integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

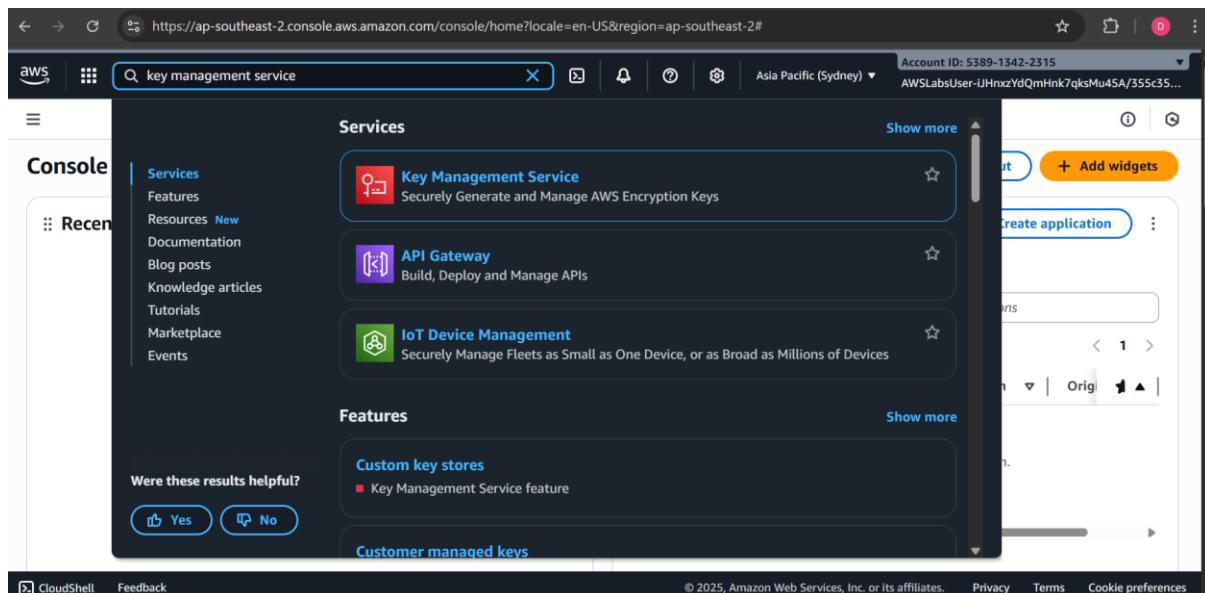
Amazon S3

Companies today need the ability to simply and securely collect, store, and analyze their data at a massive scale. Amazon S3 is object storage built to store and retrieve any amount of data from anywhere – web sites and mobile apps, corporate applications, and data from IoT sensors or devices. It is designed to deliver 99.999999999% durability, and stores data for millions of applications used by market leaders in every industry. S3 provides comprehensive security and compliance capabilities that meet even the most stringent regulatory requirements. It gives customers flexibility in the way they manage data for cost optimization, access control, and compliance. S3 is the only cloud storage solution with query-in-place functionality, allowing you to run powerful analytics directly on your data at rest in S3. And Amazon S3 is the most supported storage platform available, with the largest ecosystem of ISV solutions and systems integrator partners.

Task 1: Create your KMS master key

In this task you create a KMS master key. A KMS master key enables you to easily encrypt your data across AWS services and within your own applications.

3. At the top of the page, in the unified search bar, search for and choose Key Management Service



4. In the **Key Management Service** page , choose **Create a key**.

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services. KMS is a secure and resilient service that uses FIPS 140-3 validated hardware security modules to isolate and protect your keys.

5. On the Configure key page, select Symmetric.

Key type [Help me choose](#)

Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

Asymmetric
A public and private key pair used for encrypting and decrypting data, signing and verifying messages, or deriving shared secrets

Key usage [Help me choose](#)

Encrypt and decrypt
Use the key only to encrypt and decrypt data.

Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

6. Choose Next

7. On the Add labels page, configure:

- **Alias:** myFirstKey
- **Description - optional:**

KMS Key for S3 data

It is a good practice to describe what services the encryption key is associated with.

The screenshot shows the AWS KMS 'Create key' wizard at Step 2: Add labels. On the left, a vertical navigation bar lists steps from 1 to 6. Step 2, 'Add labels', is highlighted. The main area is titled 'Add labels'. It contains two sections: 'Alias' and 'Description'. The 'Alias' section has a note: 'You can change the alias at any time.' with a 'Learn more' link. The 'Alias' input field contains 'myFirstKey'. The 'Description' section has a note: 'You can change the description at any time.' with a 'Description' input field containing 'KMS Key for S3 data'.

9. On the **Define key administrative permissions** page, select the user or role you're signed into the Console with. The user is displayed at the top of the page, to the right of the AWS region. It starts with the characters **AWSLabsUser-**
 - You can also enter **AWSLabsUser-** in the search field to find and select the user.

Key Administrators are users or roles that manage access to the encryption key

The screenshot shows the AWS KMS 'Create key' wizard at Step 4: Define key administrative permissions - optional. The left navigation bar shows steps 1 through 6. Step 4 is selected. The main area is titled 'Define key administrative permissions - optional'. It features a 'Key administrators (1/26)' section with a note: 'Select the IAM users and roles authorized to manage this key via the KMS API. These administrators will be added to the key policy under the statement identifier (Sid) "Allow administration of the key". Modifying this Sid might impact the console's ability to update the administrator statement in the key policy.' Below this is a search interface with a search bar containing 'AWSLabsUser-', a results count of '1 matches', and a table showing one result: 'AWSLabsUser-iJHnxzYdQmHnk7qks... / Role'.

12. Choose **Next**.

13. In the **Review** page, take a brief moment to review the parameters of the KMS configuration.

Introducing the new Create key experience
We've improved the create key experience with an enhanced policy editor. [Let us know what you think](#) or you can [use the old experience](#).

Review

Key configuration

Key type	Symmetric	Key spec	SYMMETRIC_DEFAULT	Key usage	Encrypt and decrypt
Origin	AWS KMS	Regionality	Single-Region key		

You cannot change the key configuration after the key is created.

14. Choose **Finish**.

15. In the **Customer managed keys** page, the new key - myFirstKey is listed. Copy the **Key ID** value to a text editor. The value is located under the Key ID column.

Later in the lab, you use the **Key ID** value when reviewing the activity log for this KMS key.

Success
Your AWS KMS key was created with alias **myFirstKey** and key ID **6690d5fe-a44e-4d0c-b665-ccae0d4cea1e**.

Customer managed keys (1/1)

Aliases	Key ID	Status	Key type	Key spec	Key usage
<input checked="" type="checkbox"/> myFirstKey	6690d5fe-a44e-4d0c-b665-ccae0d4cea1e...	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt

Task complete: You have successfully created a KMS master key.

Task 2: Configure CloudTrail to store logs in a new S3 bucket

In this task you configure CloudTrail to store log files in a new S3 bucket.

16. At the top of the page, in the unified search bar, search for and choose CloudTrail

Note: You can safely ignore any of the following messages if they appear:

- *The option to create an organization trail is not available for this AWS account...*
- *AccessDeniedExceptions...*
- *You do not have permissions to perform this action....*

The screenshot shows the AWS CloudTrail service page. In the left navigation pane, under the 'Customer' section, the 'CloudTrail' link is selected. The main content area displays the 'Services' section with three items: CloudTrail (Track User Activity and API Usage), Detective (Investigate and Analyze potential security issues), and Athena (Serverless interactive analytics service). Below this is the 'Features' section, which includes a 'Create a SFTP server' option and a note about it being an AWS Transfer Family feature. A feedback poll at the bottom asks 'Were these results helpful?' with 'Yes' and 'No' buttons. On the right side, there is a sidebar with a 'View key' button, a 'Create key' button, and sections for 'Key usage' and 'Encrypt and decrypt'. The top right corner shows the account ID: 5389-1342-2315, the region: Asia Pacific (Sydney), and the user: AWSLabsUser-iJHnxzYdQmHnk7qksMu45A/355c35...

17. In the left navigation pane, choose **Trails**.

The screenshot shows the AWS CloudTrail Dashboard page. The left navigation pane has 'CloudTrail' selected, with 'Dashboard' also highlighted. The main content area features a yellow warning box stating: 'AccessDeniedException User: arn:aws:sts::538913422315:assumed-role/AWSLabsUser-iJHnxzYdQmHnk7qksMu45A/355c351e-bd40-430f-81ef-38706ae8666a is not authorized to perform: cloudtrail:LookupEvents with an explicit deny in a service control policy'. Below this is another yellow box: 'AccessDeniedException You don't have permissions to access this resource.' At the bottom, there is a blue info box: 'You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. [Learn more](#)'.

18. Choose **Create trail**.

The screenshot shows the AWS CloudTrail Trails page. A modal at the top right says, "You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more". Below the modal, there's a table titled "Trails" with columns: Name, Home region, Multi-region trail, ARN, Insights, Organization trail, S3 bucket, Log file prefix, CloudWatch Logs log group, and Status. One row is visible: "AWSLogs-us-east-1-3875trail/AWSLogs" under "AWSLogsSub". The "Status" column shows "Disabled". The "Log file SSE-KMS encryption" checkbox is checked.

19. In the **Choose trail attributes** page, configure:

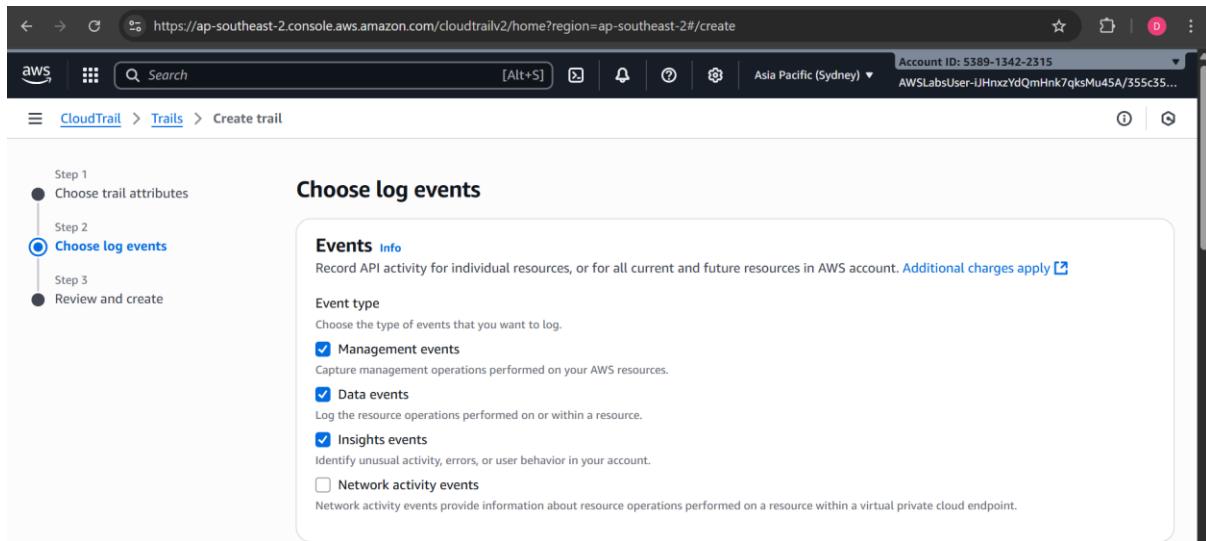
- Trail name:** myTrail
- Trail log bucket and folder:** mycloudtrailbucketNUMBER
- Replace **NUMBER** with a random number.
- De-select **Enabled for Log file SSE-KMS encryption**.

The screenshot shows the "Create trail" configuration page. It's on the "Review and create" step. The "Trail name" field is filled with "myTrail". Under "Storage location", the "Create new S3 bucket" option is selected. The "Trait log bucket and folder" field contains "mycloudtrailbucket778191". The "Log file SSE-KMS encryption" checkbox is unchecked.

20. Choose **Next**.

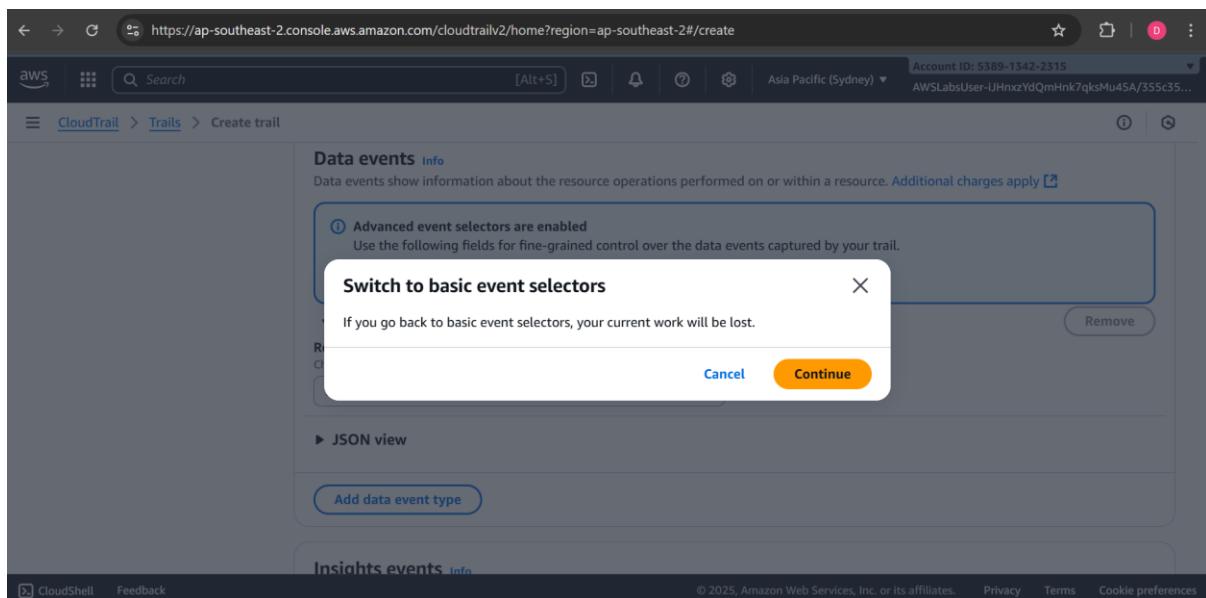
21. On the **Choose log events** page, configure:

- Select **Management events**
- Select **Data events**
- Select **Insights events**



22. In the **Data events** section, choose **Switch to basic event selectors**

- Then choose **Continue**.



23. In the **Insights events** section, select

- Select **API call rate**
- Select **API error rate**

24. Choose **Next**.

The screenshot shows the 'Create trail' configuration page for CloudTrail. In the 'Insights events' section, 'API call rate' and 'API error rate' are selected. Buttons for 'Cancel', 'Previous', and 'Next' are visible at the bottom.

25. In the **Review and create** page, take a brief moment to review the parameters of the **Trail** configuration.

The screenshot shows the 'Review and create' configuration page. The 'Step 1: Choose trail attributes' section is displayed. The 'General details' table includes:

Attribute	Value
Trail name	myTrail
Multi-region trail	Yes
Apply trail to my organization	Not enabled
Trail log location	mycloudtrailbucket778191/AWSLogs/538913422315/
Log file SSE-KMS encryption	Not enabled
Log file validation	Enabled
SNS notification delivery	Disabled

26. Choose **Create trail**.

The trail is created even though it is not listed due to permission controls - in the lab environment.

The screenshot shows the AWS CloudTrail console with a green success message at the top: "Trail successfully created". Below it is a blue info message: "You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more [?]."

The main table lists the trail details:

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
AWSLabs-CloudtrailSubaccountAudit	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:06992045:3875:trail/AWSLabs-CloudtrailSubaccountAudit	Disabled	Yes	awslogs-subaccount-cloudtrail-06992045-7075fa	-	-	Status unavailable

At the bottom, there are links for CloudShell, Feedback, and a copyright notice: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

Task complete: You have successfully configured CloudTrail.

Task 3: Upload an image to your S3 bucket and encrypt it

In this task, you upload an image file to your S3 bucket and encrypt it using the encryption key (*myFirstKey*) you created earlier.

27. At the top of the page, in the unified search bar, search for and choose S3
28. Choose *mycloudtrailbucket**.

The screenshot shows the AWS S3 console with the sidebar menu expanded. The "General purpose buckets" tab is selected, showing three buckets:

Name	AWS Region	Creation date
awslabs-resources-krxqqla59sui8d-us-east-1-538913422315	US East (N. Virginia) us-east-1	October 9, 2020, 20:31:25 (UTC+05:30)
awslabs-resources-r5b3y6ojjszcap-us-east-1-538913422315	US East (N. Virginia) us-east-1	October 3, 2023, 00:14:10 (UTC+05:30)
mycloudtrailbucket778191	Asia Pacific (Sydney) ap-southeast-2	September 19, 2025, 15:34:43 (UTC+05:30)

At the bottom, there are links for Account snapshot, View dashboard, External access summary - new, and a copyright notice: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

29. From the Objects tab, choose Upload.

mycloudtrailbucket778191 [Info](#)

Objects [Actions](#) [Create folder](#) [Upload](#)

Objects (1)

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. [Learn more](#)

Find objects by prefix

Name	Type	Last modified	Size	Storage class
AWSLogs/	Folder	-	-	-

30. Choose Add files.

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

Files and folders (0)

All files and folders in this table will be uploaded.

Find by name

Name	Type	Size
No files or folders		

You have not chosen any files or folders to upload.

31. Browse to and select an image file on your computer.

32. At the bottom of the screen, expand **Properties**.

33. In the **Server-side encryption settings** section, select **Specify an encryption key**.

34. For **Encryption settings**, select **Override bucket settings for default encryption**.

35. For **Encryption type**, select **Server-side encryption with AWS Key Management Service keys (SSE-KMS)**.

36. For **AWS KMS key**, select **Choose from your AWS KMS keys**.

37. From the **Available AWS KMS keys** drop down menu, select **myFirstKey**.

38. Scroll to the bottom of the screen, then choose **Upload**.

The screenshot shows the AWS S3 console at the URL <https://ap-southeast-2.console.aws.amazon.com/s3/upload/mycloudtrailbucket778191?region=ap-southeast-2>. The page displays the 'Server-side encryption' configuration for a bucket. It includes sections for 'Server-side encryption key' (with 'Specify an encryption key' selected), 'Encryption settings' (with 'Override bucket settings for default encryption' selected), and 'Encryption type' (with 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)' selected). The 'AWS KMS key' section is also visible.

The screenshot shows the AWS S3 console at the same URL. This time, the 'AWS KMS key' configuration is being set. It shows 'Choose from your AWS KMS keys' selected, and the dropdown lists 'arn:aws:kms:ap-southeast-2:538913422315:key/6690d5fe-a44e-4d0c-b665-cca...' and a 'Create a KMS key' button. Below this, the 'Bucket Key' section is shown with '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.' and an 'Enable' radio button selected.

39. In the **Upload: status** page, a message shows the image was successfully uploaded.

- Choose **Close**.

40. In the **mycloudtrailbucket*** page, choose the **Objects** tab.

41. From the row that lists the image you uploaded, record the **Last modified** timestamp to a text editor. Later in the lab, you use the **Last modified** timestamp to review CloudTrail logs.

The screenshot shows the AWS S3 'Objects' page at the URL <https://ap-southeast-2.console.aws.amazon.com/s3/upload/mycloudtrailbucket778191?region=ap-southeast-2>. A green toast notification at the top left says 'Upload succeeded'. The main table shows one file: 'HappyFace.jpg' (1 file, 128.2 KB (100.00%)). The 'Status' column indicates it is 'Succeeded'. The 'Files and folders' tab is selected, showing the file details.

Name	Folder	Type	Size	Status	Error
HappyFace.jpg	-	image/jpeg	128.2 KB	Succeeded	-

mycloudtrailbucket778191 [Info](#)

Objects Properties Permissions Metrics Management Access Points

Objects (2) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

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. [Learn more](#)

Name	Type	Last modified	Size	Storage class
AWSLogs/	Folder	-	-	-
HappyFace.jpg	jpg	September 19, 2025, 15:39:45 (UTC+05:30)	128.2 KB	Standard

Task complete: You have successfully uploaded an image to S3, and encrypted it as well.

Task 4: Access the encrypted image

In this task, you try to access the encrypted image through both the AWS Management Console, and the S3 link.

42. In the **Objects** tab, select the image name and then choose **Open**.

The image opens in a new tab/window.



Amazon S3 and AWS KMS perform the following actions when you request that your data be decrypted.

- Amazon S3 sends the encrypted data key to AWS KMS

- AWS KMS decrypts the key by using the appropriate master key and sends the plaintext key back to Amazon S3
- Amazon S3 decrypts the ciphertext and removes the plaintext data key from memory as soon as possible

43. Close the window/tab that displays your image.

44. With the image selected, choose **Copy URL**, and paste the URL to a text editor.

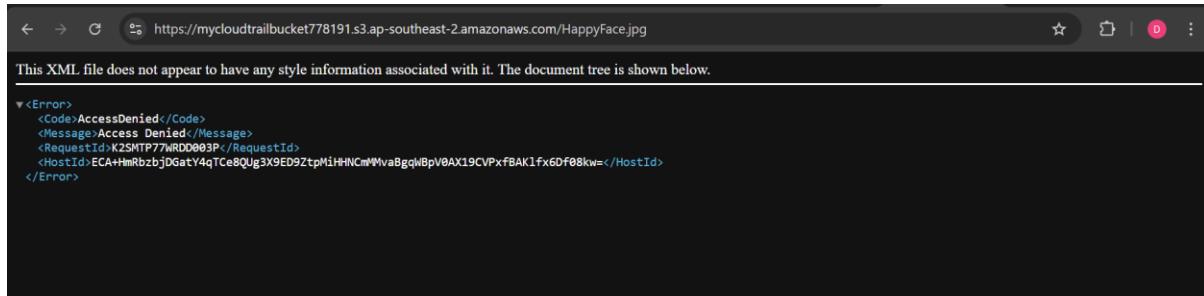
The URL should look similar to <https://mycloudtrailbucket10619.s3-us-west-2.amazonaws.com/Eiffel.jpg>

45. Paste the S3 Object URL that you copied into a new browser/window.

46. Press **Enter**.

47. What does the page show?

It shows *Access Denied*. This is because, by default public access is not allowed.



48. Return to the AWS Management Console.

49. In the **mycloudtrailbucket*** page, choose the **Permissions** tab.

50. In the **Block public access (bucket settings)** section, choose **Edit**.

51. De-select **Block all public access**.

52. Choose **Save changes** then:

- Enter confirm
- Choose **Confirm**.

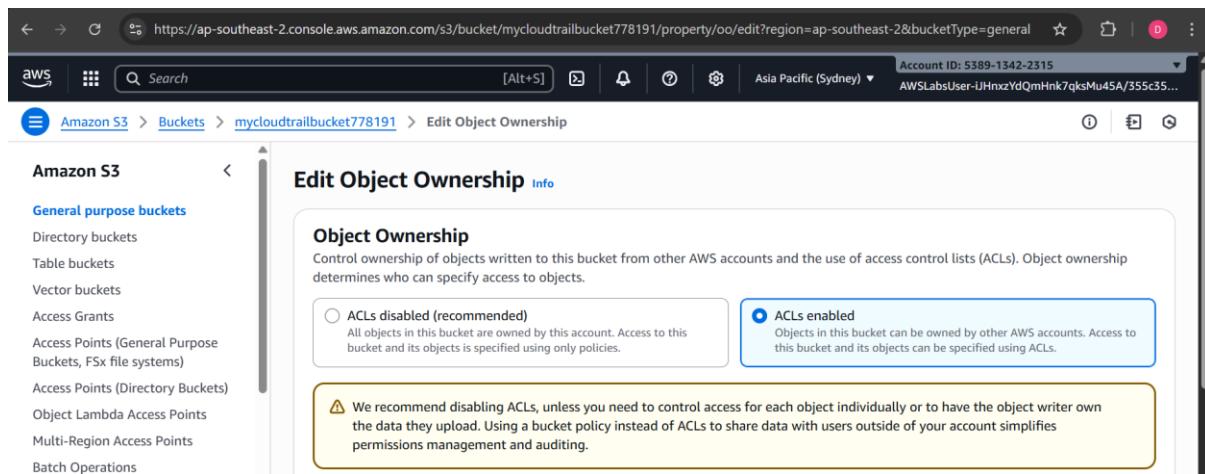
The screenshot shows the 'Edit Block public access (bucket settings)' page for the bucket 'mycloudtrailbucket778191'. On the left, there's a sidebar with 'Amazon S3' and 'General purpose buckets' sections. The main area displays the 'Block public access (bucket settings)' configuration. It includes a detailed description of what each setting does and five checkboxes for 'Block all public access', '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)', 'Block public access to buckets or objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. At the bottom right are 'Cancel' and 'Save changes' buttons.

This screenshot shows a modal dialog titled 'Edit Block public access (bucket settings)'. It contains a warning message: 'Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.' Below it, a text input field is labeled 'To confirm the settings, enter confirm in the field.' with the word 'confirm' typed into it. At the bottom of the dialog are 'Cancel' and 'Confirm' buttons. The background of the dialog is semi-transparent, showing the 'Edit Block public access (bucket settings)' page from the previous screenshot.

53. Scroll to the Object Ownership section, choose **Edit**.

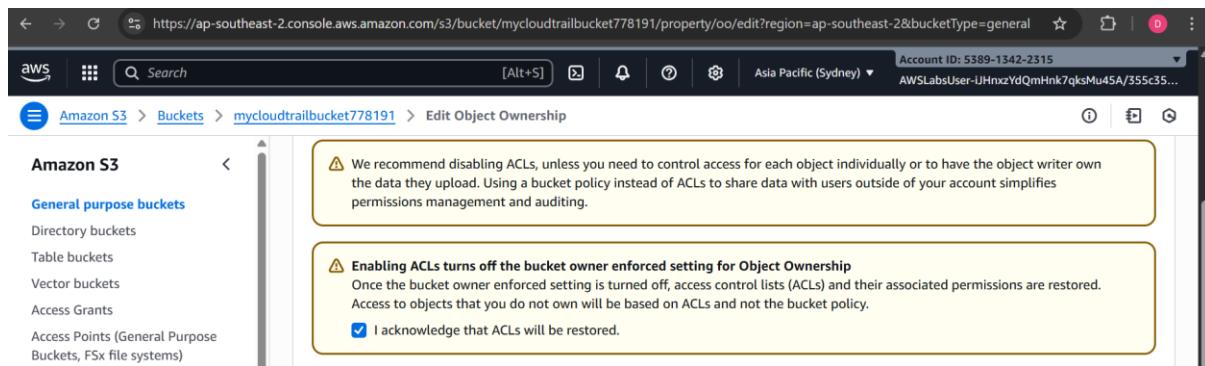
The screenshot shows the 'Object Ownership' section of the 'Permissions' tab for the bucket 'mycloudtrailbucket778191'. The sidebar on the left has a 'General purpose buckets' section. The main area shows the 'Object Ownership' configuration, which is currently set to 'Bucket owner enforced'. A note states: '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.' At the bottom right of the 'Object Ownership' box is a blue 'Edit' button.

54. Select **ACLs enabled.**



The screenshot shows the 'Edit Object Ownership' page for an S3 bucket. On the left, there's a sidebar with 'Amazon S3' and 'General purpose buckets' sections. The main area has a heading 'Object Ownership' with a sub-section about controlling ownership from other accounts. Two radio buttons are shown: 'ACLs disabled (recommended)' and 'ACLs enabled'. The 'ACLs enabled' option is selected and highlighted with a blue border. Below it, a note says: 'We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.'

55. For *Enabling ACLs turns off the bucket owner enforced setting for Object Ownership*, select - I acknowledge that ACLs will be restored.



This screenshot shows the same 'Edit Object Ownership' page as the previous one, but with additional notes. At the top, a note says: 'We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.' Below that, another note says: 'Enabling ACLs turns off the bucket owner enforced setting for Object Ownership. Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.' A checkbox labeled 'I acknowledge that ACLs will be restored.' is checked.

56. Choose **Save changes.**

57. In the **Object tab, select your image.**

58. Choose **Actions**

- From the drop-down menu, select **Make public using ACL**.

The screenshot shows the AWS S3 console with the URL <https://ap-southeast-2.console.aws.amazon.com/s3/buckets/mycloudtrailbucket778191?region=ap-southeast-2&bucketType=general&tab=objects>. The left sidebar lists 'General purpose buckets' with various options like Directory buckets, Table buckets, Vector buckets, Access Grants, etc. The main area shows 'Objects (1/2)' with a single item: 'AWSLogs/' (Folder) and 'HappyFace.jpg' (jpg). A context menu is open over 'HappyFace.jpg', with the 'Actions' dropdown expanded. The 'Make public using ACL' option is highlighted.

59. Choose **Make public**.

The screenshot shows the 'Make public' status page for the 'HappyFace.jpg' object. The URL is https://ap-southeast-2.console.aws.amazon.com/s3/buckets/mycloudtrailbucket778191/object/edit_public_read_access?region=ap-southeast-2&buck.... The page displays a message: 'Successfully edited public access' and 'View details below.' Below this, there's a summary table:

Summary	Successfully edited public access	Failed to edit public access
Source s3://mycloudtrailbucket778191	1 object, 128.2 KB	0 objects

60. In the **Make public: status** page, a message shows the access change was successful.

- Choose **Close**.

The screenshot shows the 'Make public: status' page. The URL is https://ap-southeast-2.console.aws.amazon.com/s3/buckets/mycloudtrailbucket778191/object/edit_public_read_access?region=ap-southeast-2&buck.... A green message bar at the top says 'Successfully edited public access' and 'View details below.' Below this, there's a summary table:

Summary	Successfully edited public access	Failed to edit public access
Source s3://mycloudtrailbucket778191	1 object, 128.2 KB	0 objects

61. Navigate to the browser tab/window with the **S3 Object URL**.

62. Refresh the tab/window.

63. What do you see?

Because the image is encrypted, you are **not** able to view it using the public link. You should see a message saying *Requests specifying Server Side Encryption with AWS KMS managed keys require AWS Signature Version 4.*

```
<Error>
<Code>InvalidArgument</Code>
<Message>Requests specifying Server Side Encryption with AWS KMS managed keys require AWS Signature Version 4.</Message>
<ArgumentName>Authorization</ArgumentName>
<RequestId>Y20RGZTF64SACA9Z</RequestId>
<HostId>UXEgwUQ9X85VzffSgsFvxX6pjjEIQSoKvX+JK+i4A/mcZG3rnx3jodLhqDETZuvTkbeQrgq/gW8tXvqobbzG+gqdglk6PEh5</HostId>
```

If you are uploading or accessing objects encrypted by SSE-KMS, you need to use AWS Signature Version 4 for added security. Signature Version 4 is the process to add authentication information to AWS requests. When you use the AWS Command Line Interface (AWS CLI) or one of the AWS SDKs to make requests to AWS, these tools automatically sign the requests for you with the access key that you specify when you configure the tools. When you use these tools, you don't need to learn how to sign requests yourself. For more information on this process read this blog post: [blog post](#)

64. Close the **S3 Object URL** tab/window.

Task complete: You have attempted to access the S3 object through both the AWS Management Console, and the S3 link.

Task 5: Monitor KMS activity using CloudTrail logs

In this task, you access CloudTrail log files and review logs related to your encryption operations.

65. In the **mycloudtrailbucket*** page, choose the **Objects** tab.

66. Drill-down through the AWSLogs/ folders till you get to a folder that contains log file(s).

Name	Type	Last modified	Size	Storage class
AWSLogs/	Folder	-	-	-
HappyFace.jpg	jpg	September 19, 2025, 15:39:45 (UTC+05:30)	128.2 KB	Standard

The path should look similar to: *Amazon S3 > AWSLogs/ > 197167081626/ > CloudTrail/ > Region > 2024 > 02 > 01*

In the above example, **Region** is the AWS region where your lab is currently running from. The region should match with the **LabRegion** value to the left of these instructions.

If you don't see any log files, choose the **refresh** button every few seconds till you see a log file.

Objects (20) Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

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. [Learn more](#)

Name	Type	Last modified	Size	Storage class
538913422315_CloudTrail_ap-southeast-2_20250919T1010Z_7LUFZhfsf1wvgNbS.json.gz	gz	September 19, 2025, 15:42:32 (UTC+05:30)	833.0 B	Standard

The log files have a **.json.gz** extension.

67. Do you see a log file that has a **Last modified** timestamp that is later than the timestamp for the image file you downloaded? (*In an earlier step, you copied the image upload timestamp to a text editor, use that timestamp when identifying the log files to review*).

- If yes, continue to the next step.
- If no, continue to choose the **refresh** button every few seconds till there is.

Objects (20) Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

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. [Learn more](#)

Name	Type	Last modified	Size	Storage class
538913422315_CloudTrail_ap-southeast-2_20250919T1010Z_7LUFZhfsf1wvgNbS.json.gz	gz	September 19, 2025, 15:42:32 (UTC+05:30)	833.0 B	Standard
538913422315_CloudTrail_ap-southeast-2_20250919T1010Z_BfohrdKHqgmye4tN.json.gz	gz	September 19, 2025, 15:37:39 (UTC+05:30)	7.6 KB	Standard

Note: It can take up to 5 minutes to see a log file that has a **Last modified** time stamp that is greater than the time stamp of the image file that you uploaded.

68. Select the log file that has the *closest* time after the **Last modified** of the image you uploaded.

69. Choose **Open** .

This opens a log file in a new browser tab.

70. If you see a pop-up security warning, confirm that you want to open the file. If not, continue to the next step.

Note: Your browser security settings may simply ignore the pop-up. If you do not see any file being opened and do not see a pop-up alert, you should enable pop-ups within in your browser's settings section.

If you are not using Google Chrome or Firefox, you may need to download and decompress the gz compressed file using a local utility on your own computer. Once the .gz file is decompressed - open it in a text editor.

The log file is in a JSON format and contains each API call that has been logged by CloudTrail. Depending upon the browser you are using the log file might look slightly different.

71. Search for the following in your log file:

- The encryption Key ID that you copied to your text editor
 - The name of the file that you upload. (*You should see name of the file in the same log file that contains your encryption Key ID*)

If you cannot locate the items above, try either one of the following:

- Perhaps the log file you have open - was generated before the **Last modified** timestamp of the image you uploaded. In this case, navigate to the S3 console, and open to search a log file that has a timestamp with the closest time after the **Last modified** of the image you uploaded.

- If you still don't see the image name or the encryption Key ID, open the next file after the one you just checked, and try searching again. Please note, you might have to repeat this action for consecutive log files until you locate your image (or the encryption Key ID). Typically, you should be able to find your image or the encryption Key ID in one of the files that was generated **around 5 minutes** after the timestamp of the **Last modified** time of the image you uploaded.

Task complete: You have monitored KMS activity using CloudTrail logs.

Task 6: Manage encryption keys

In this task you manage encryption keys for users and roles.

72. Navigate to the browser tab/window S3 service.
 73. At the top of the page, in the unified search bar, search for and choose Key Management Service
 74. In the left navigation panel, choose **Customer managed keys**.

The screenshot shows the AWS KMS home page. On the left, there's a sidebar with navigation links: 'Key Management Service (KMS)', 'AWS managed keys', 'Customer managed keys', and 'Custom key stores'. Under 'Custom key stores', there are links for 'AWS CloudHSM key stores' and 'External key stores'. The main content area has a dark background with the title 'AWS Key Management Service' in large white letters. Below it, a sub-section says 'Easily create keys and control encryption across AWS and beyond'. A call-to-action button labeled 'Create a key' is visible. At the bottom of the page, there's a footer with links for 'Privacy', 'Terms', and 'Cookie preferences'.

77. Choose myFirstKey.

The screenshot shows the 'Customer managed keys' list page. The sidebar on the left is identical to the previous screenshot. The main area displays a table with one row for 'myFirstKey'. The columns include 'Aliases' (empty), 'Key ID' (6690d5fe-a44e-4d0c-b665-ccaecd4cea1e), 'Status' (Enabled), 'Key type' (Symmetric), 'Key spec' (SYMMETRIC_DE...), and 'Key usage' (Encrypt a...). There are buttons for 'Key actions' and 'Create key' at the top right of the table.

This opens a page where you can make changes to the KMS settings. One of the configurable setting is **Add or Remove** - key administrators, and key users.

The screenshot shows the 'General configuration' page for the key '6690d5fe-a44e-4d0c-b665-ccaecd4cea1e'. The sidebar on the left is the same. The main content area has a section titled 'General configuration' with the following details:

Alias myFirstKey	Status Enabled	Creation date Sep 19, 2025 15:28 GMT+5:30
ARN arn:aws:kms:ap-southeast-2:538913422315:key/6690d5fe-a44e-4d0c-b665-ccaecd4cea1e	Description KMS Key for S3 data	Regionality Single Region
Current key material ID 4919652906112fa3dc6faad0ce88796eaaf0e0c256c9058ca634a8a584f376a2		

Below this, there are tabs for 'Key policy', 'Cryptographic configuration', 'Tags', 'Key material and rotations', and 'Aliases'. At the bottom, there are links for 'CloudShell', 'Feedback', 'Privacy', 'Terms', and 'Cookie preferences'.

78. In the **Key users** section, select the user or role that you are signed in with.

The screenshot shows the AWS KMS console with a key ID of 6690d5fe-a44e-4d0c-b665-ccaecd4cea1e. In the 'Key users (1/1)' section, there is one entry: 'AWSLabsUser-IJHnxzYdQmHnk7qksMu45A/355c35...'. A blue border highlights this row. At the top right of this section are 'Add' and 'Remove' buttons. Below the table, there is a note: 'The following IAM users and roles can use this key for cryptographic operations. They can also allow AWS services that are integrated with KMS to use the key on their behalf.' A 'Learn more' link is provided.

77. Choose **Remove**.

Immediately, the user's permission to use this key is removed.

78. In the **Key users** section, choose **Add** then:

- Search and select the user or role that you are signed in with.

The user starts with the characters **AWSLabsUser-**

- Choose **Add**.

Immediately, the user's permission to use this key is restored.

The screenshot shows the 'Add key users' dialog box overlying the main KMS interface. The dialog title is 'Add key users'. It contains a search bar with 'AWSLabsUs' and a note: 'The following IAM users and roles can use this key to encrypt and decrypt data from within applications and when using AWS services integrated with KMS.' Below the search bar is a table with one entry: 'AWSLabs... / Role'. The 'Add' button at the bottom right of the dialog is highlighted with a yellow border.

This shows how you can control which IAM users or roles can use KMS Keys that you create. The same process can be used to control which IAM users can manage KMS keys.

Task complete: You have managed encryption keys user permissions.

Conclusion

You have successfully done the following:

- Created an Encryption Key
- Created an S3 bucket with CloudTrail logging functions
- Encrypted an image and stored it in your S3 bucket
- Viewed the encrypted image using the AWS Management Console
- Monitored encryption key usage using CloudTrail
- Managed encryption keys for users and roles

End lab

Follow these steps to close the console and end your lab.

79. Return to the **AWS Management Console**.
80. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
81. Choose **End Lab** and then confirm that you want to end your lab.

Additional Resources

- [Amazon Key Management Service](#)
- [Amazon S3](#)