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.

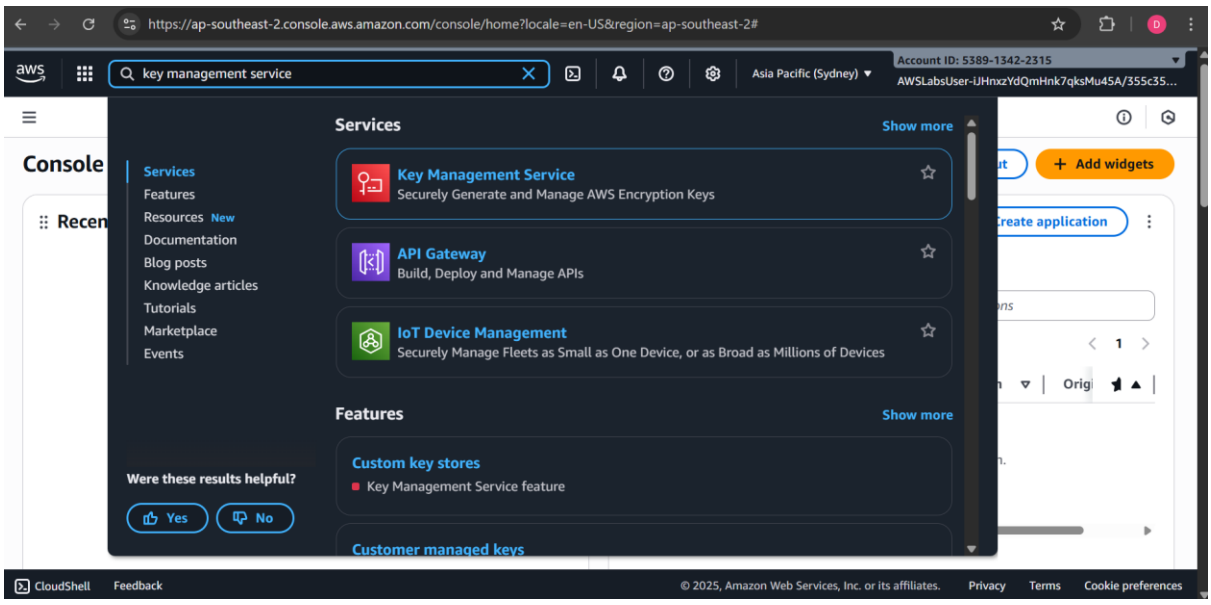
Amazon S3

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.

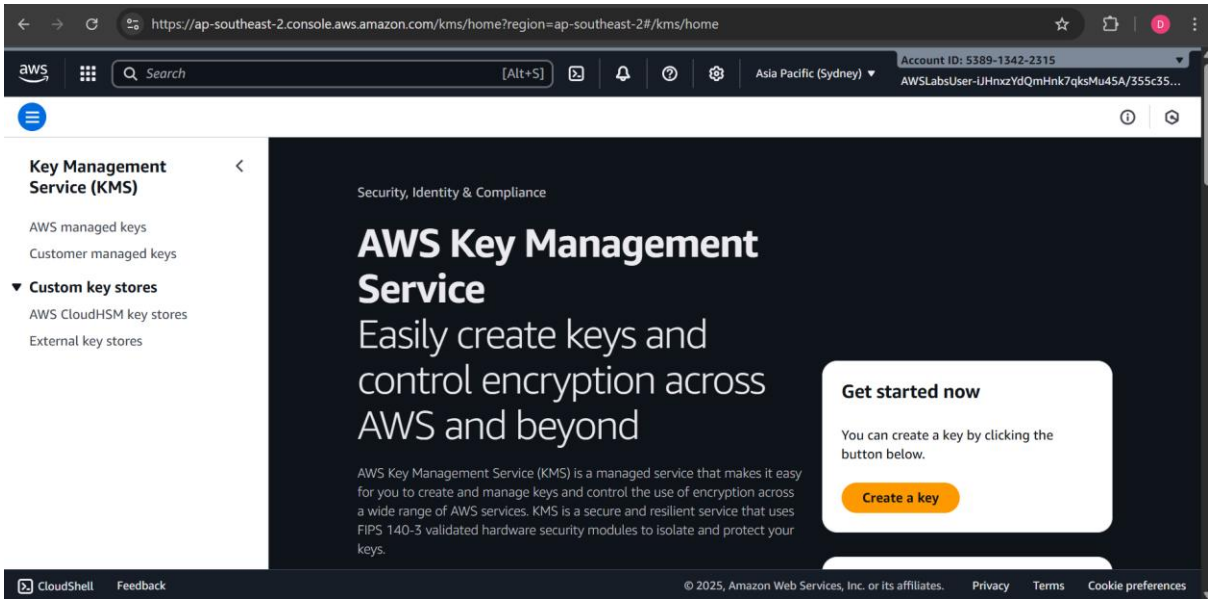
Task 1: Create your KMS master key

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.

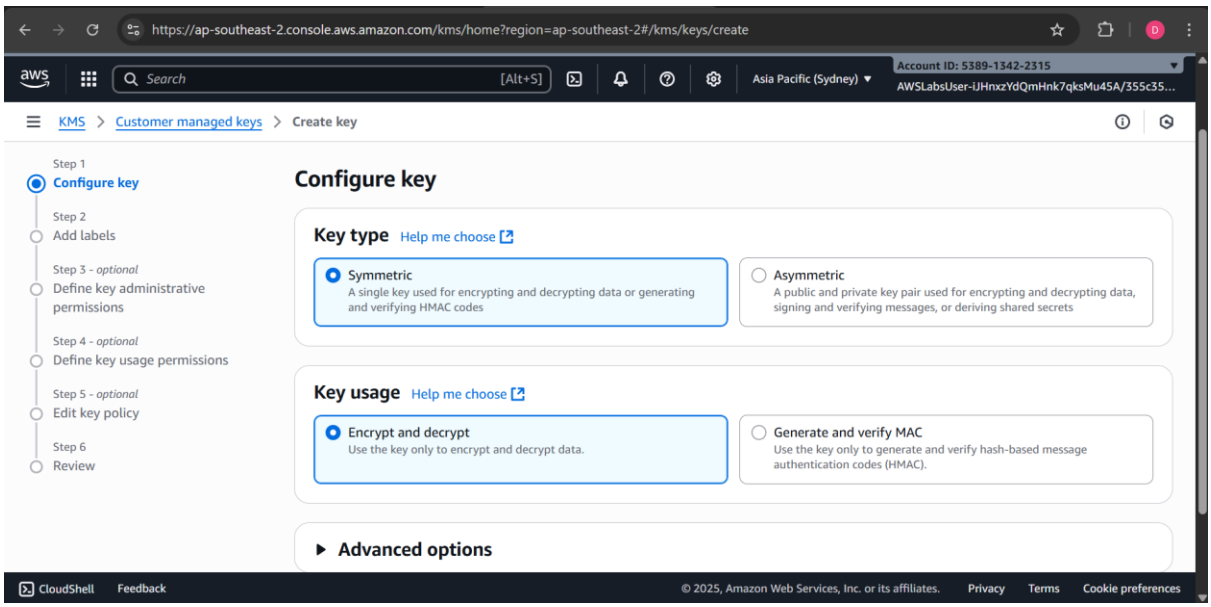
3. At the top of the page, in the unified search bar, search for and choose Key Management Service



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



5. On the **Configure key** page, select **Symmetric**.

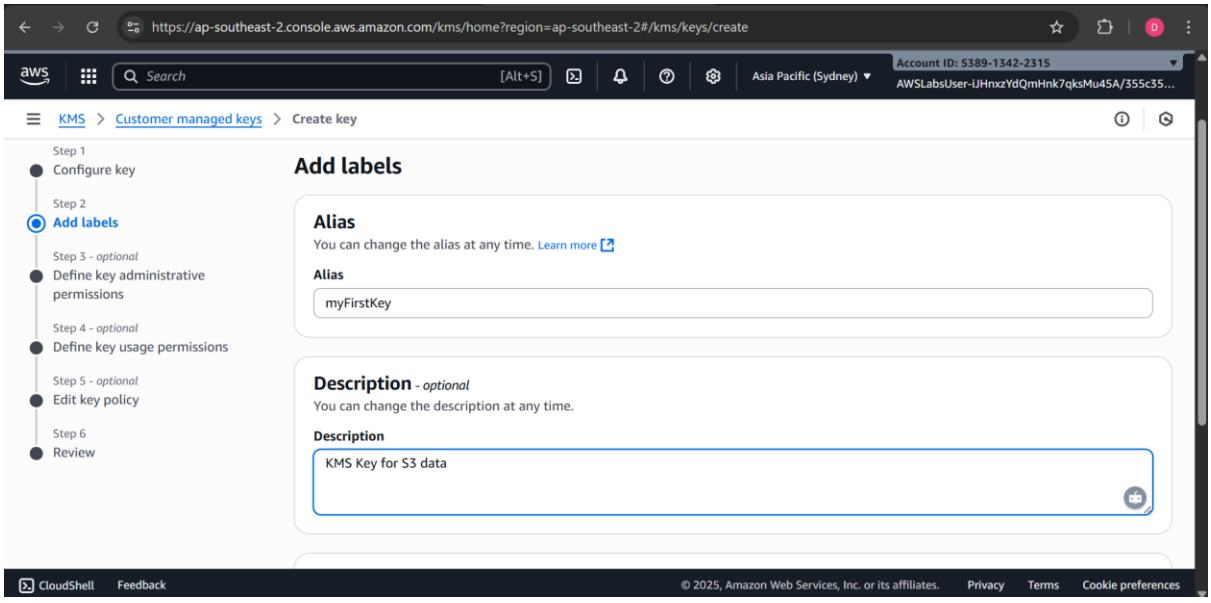


6. Choose **Next**
7. On the **Add labels** page, configure:

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

KMS Key for S3 data

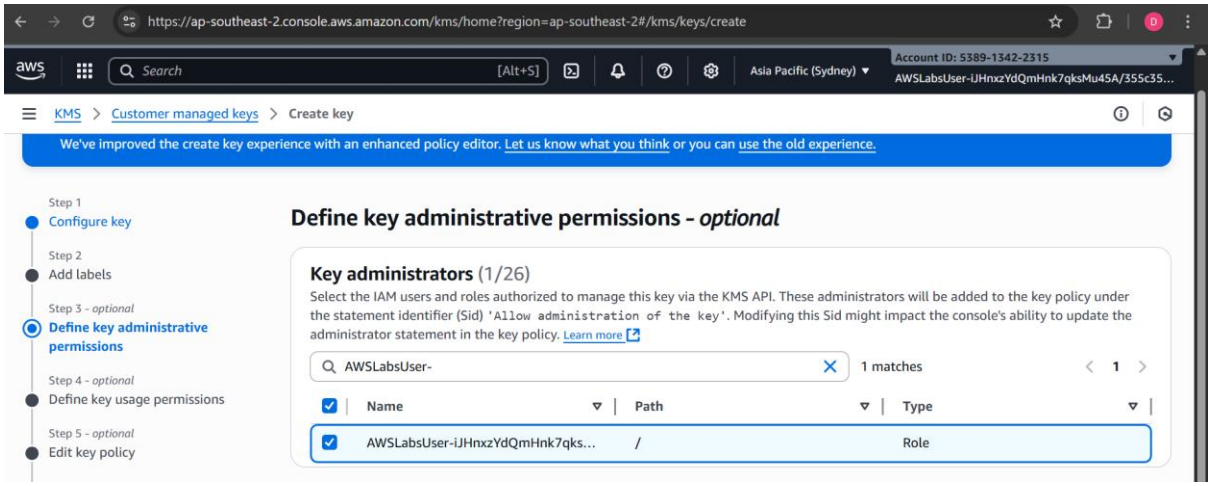
It is a good practice to describe what services the encryption key is associated with.



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-**

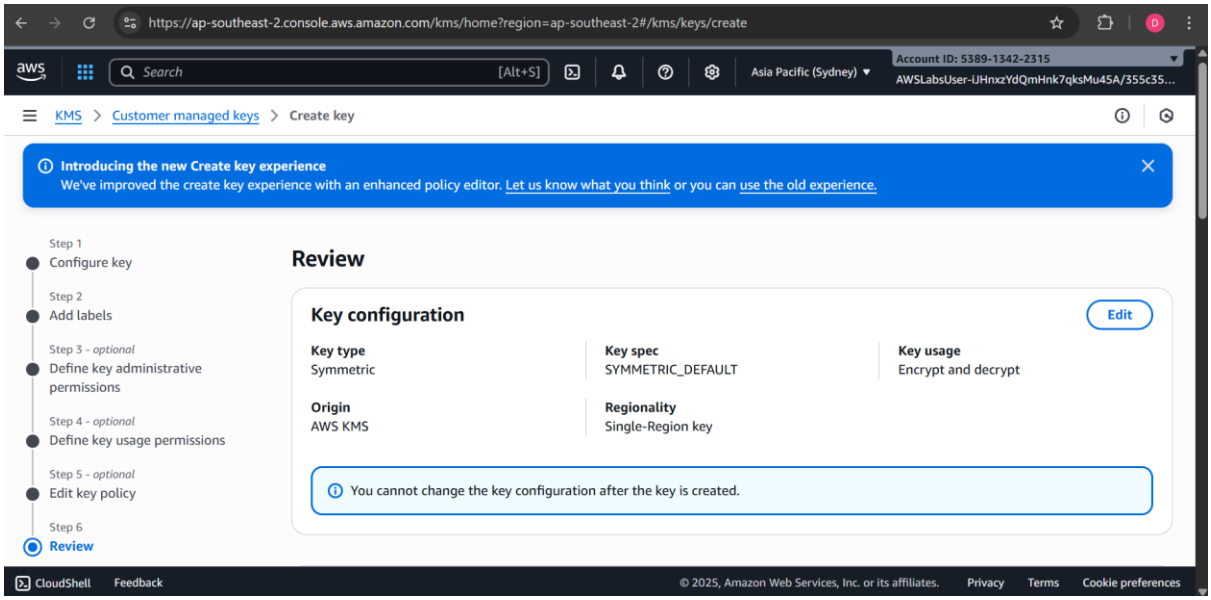
- You can also enter AWSLabsUser- in the search field to find and select the user.

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



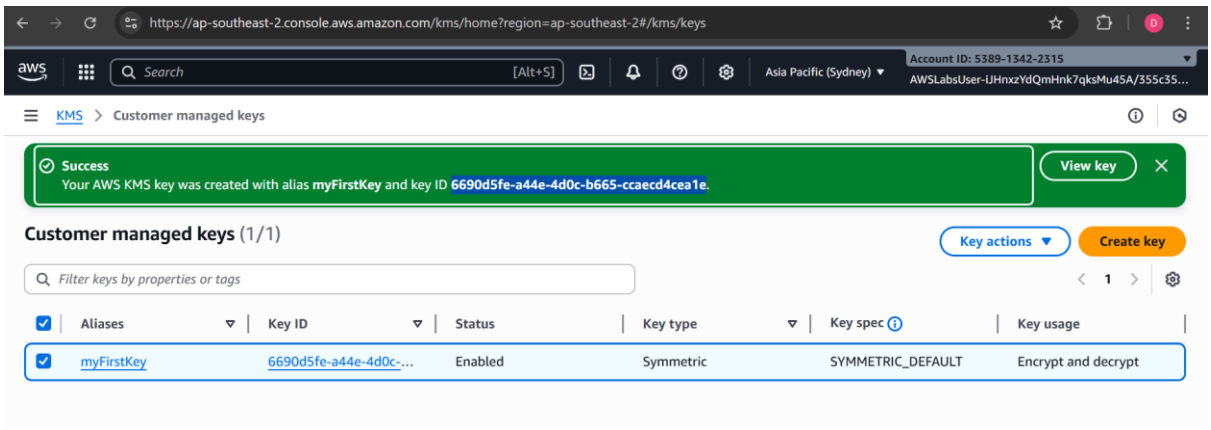
12. Choose **Next**.

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



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.



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

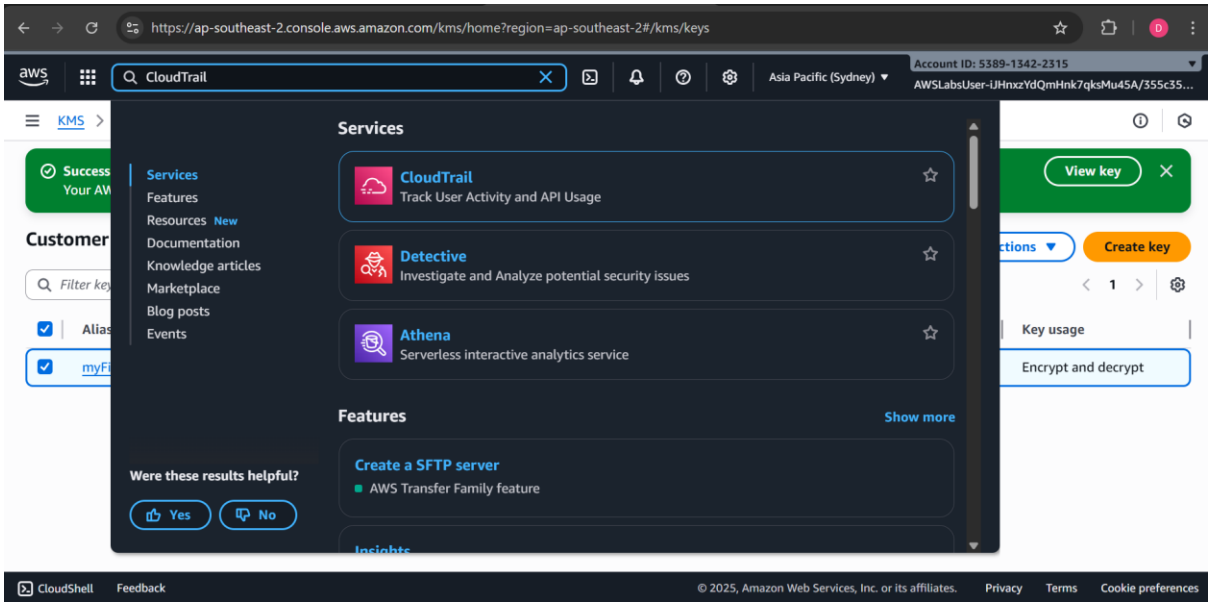
Task 2: Configure CloudTrail to store logs in a new S3 bucket

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

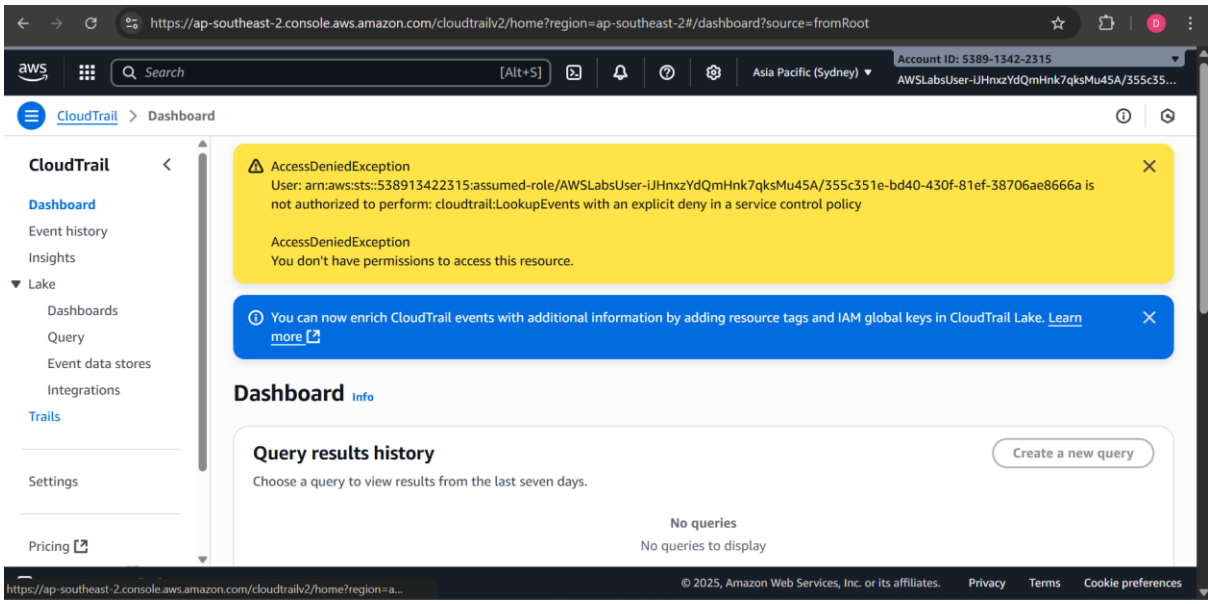
16. At the top of the page, in the unified search bar, search for and choose CloudTrail

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

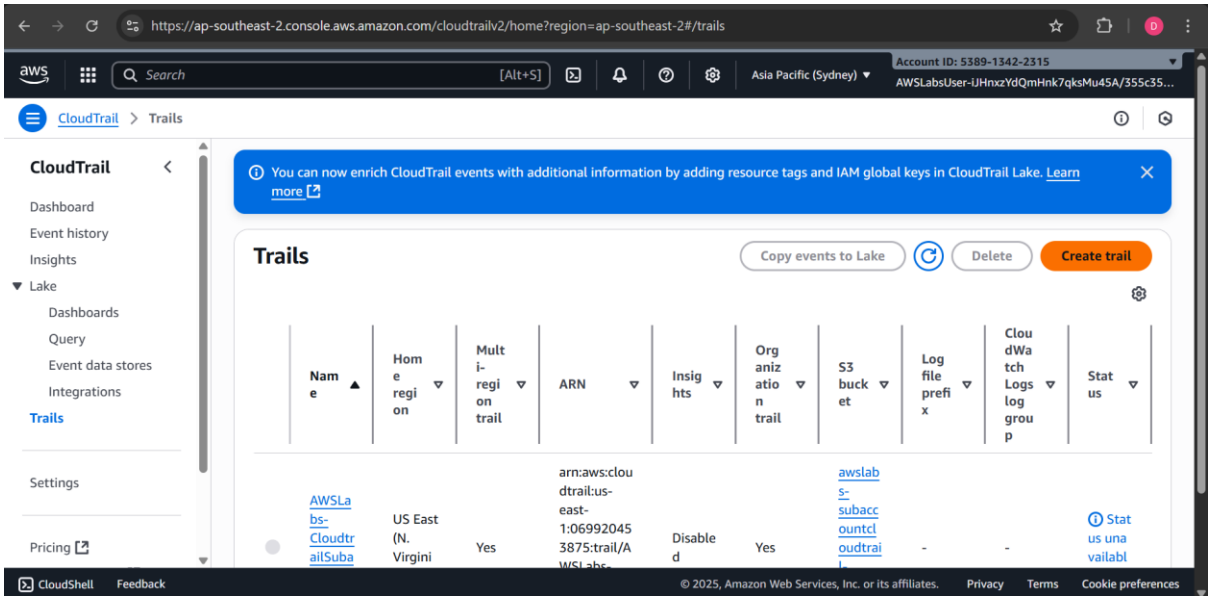
- *The option to create an organization trail is not available for this AWS account…*
- *AccessDeniedExceptions…*
- *You do not have permissions to perform this action….*



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

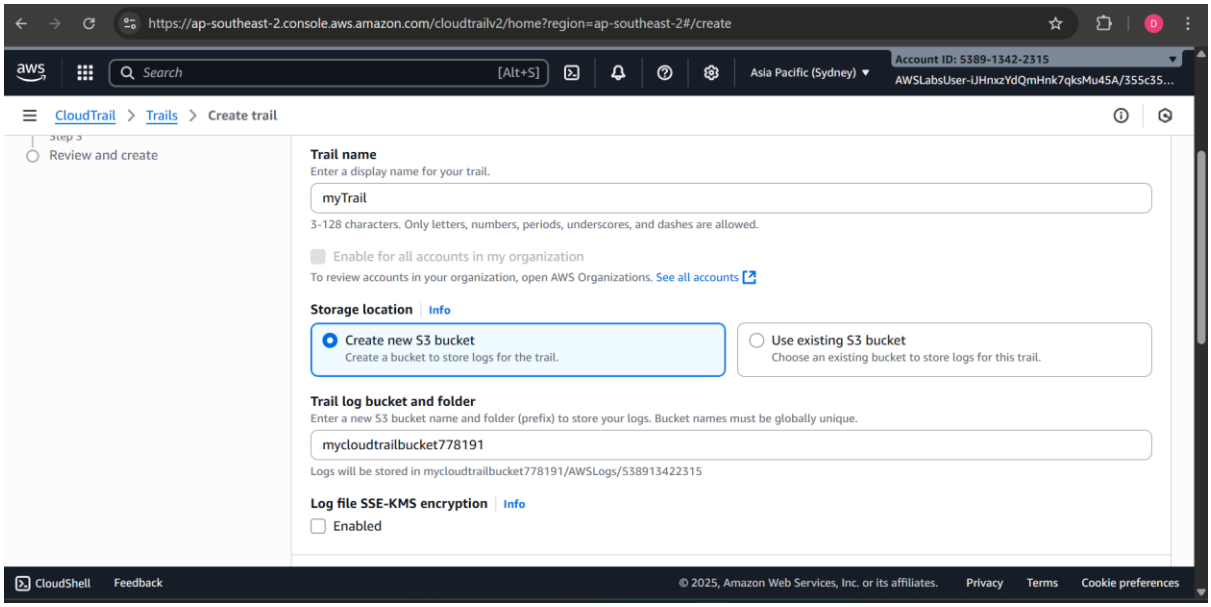


18. Choose **Create trail**.



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

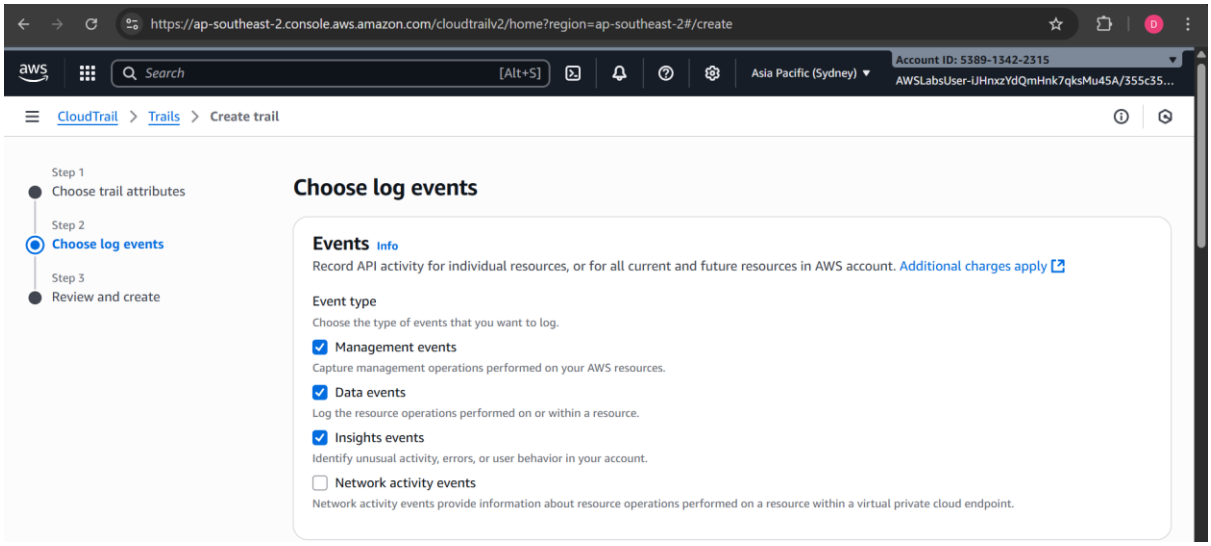
- **Trail name:** myTrail
- **Trail log bucket and folder:** mycloudtrailbucketNUMBER
- Replace **NUMBER** with a random number.
- De-select **Enabled** for **Log file SSE-KMS encryption**.



20. Choose **Next**.

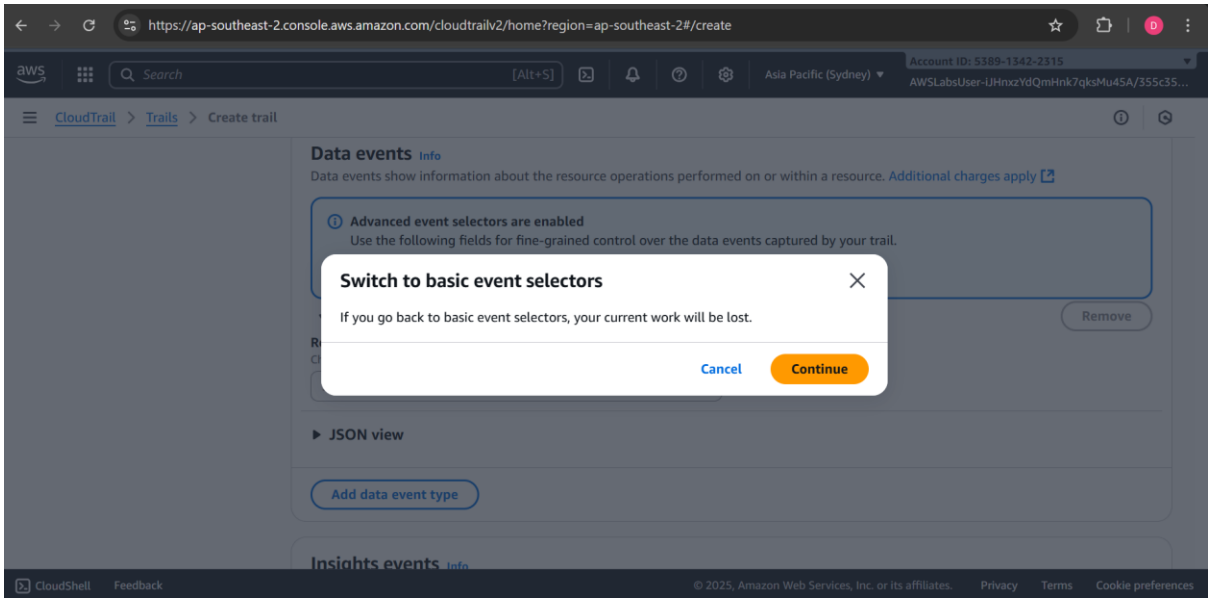
21. On the **Choose log events** page, configure:

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



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

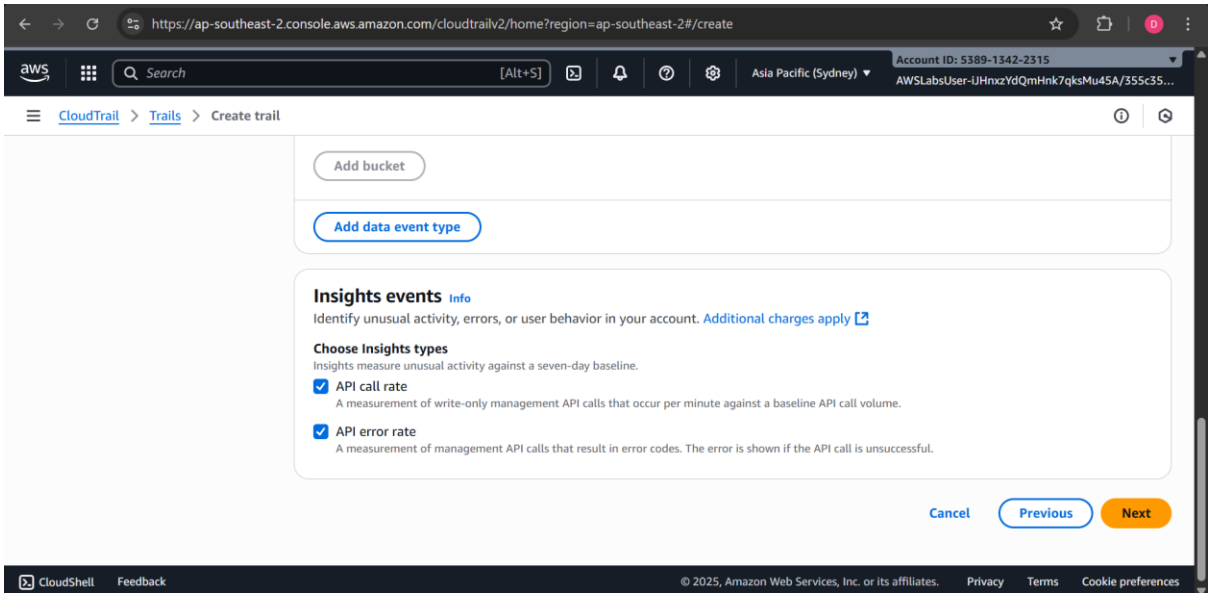
- Then choose **Continue**.



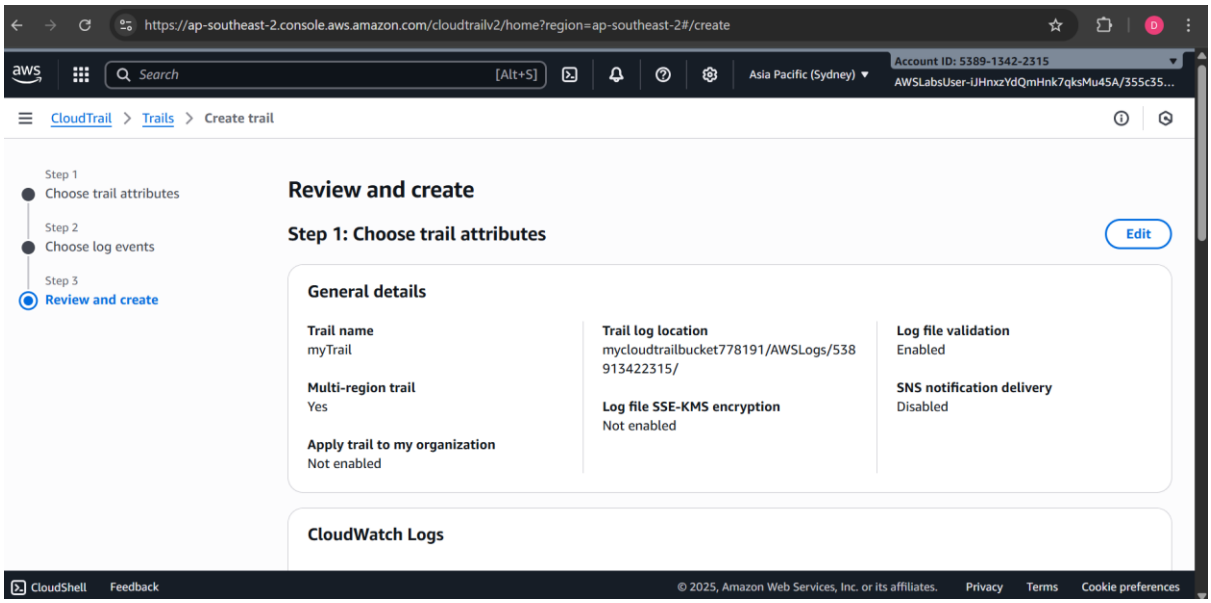
23. In the **Insights events** section, select

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

24. Choose **Next**.

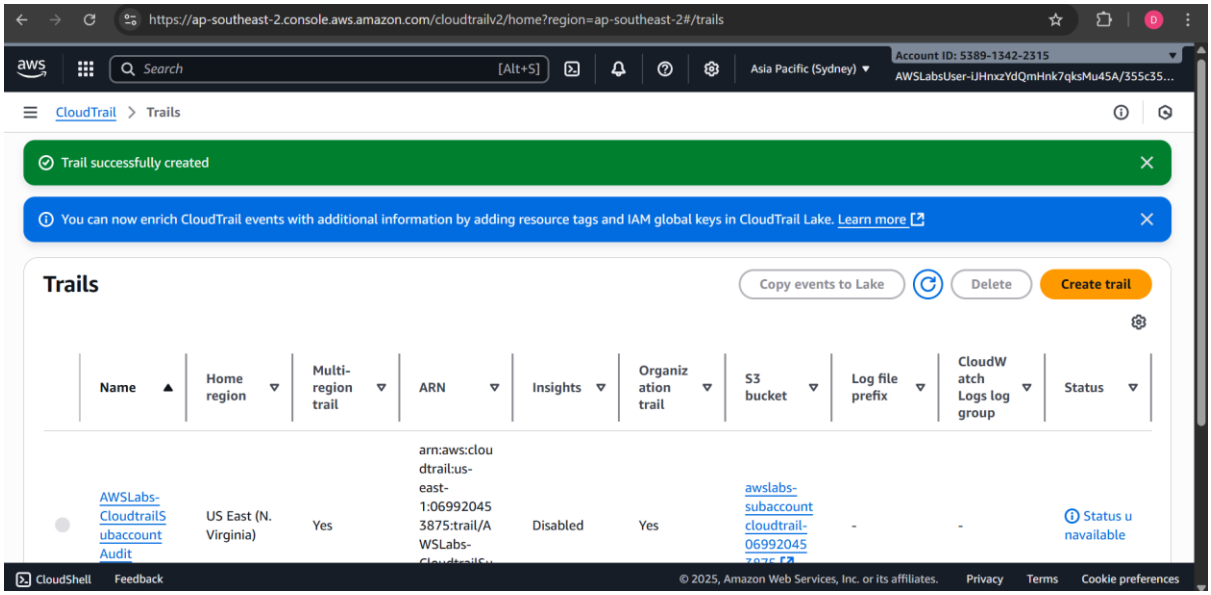


25. In the **Review and create** page, take a brief moment to review the parameters of the **Trail** configuration.



26. Choose **Create trail**.

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

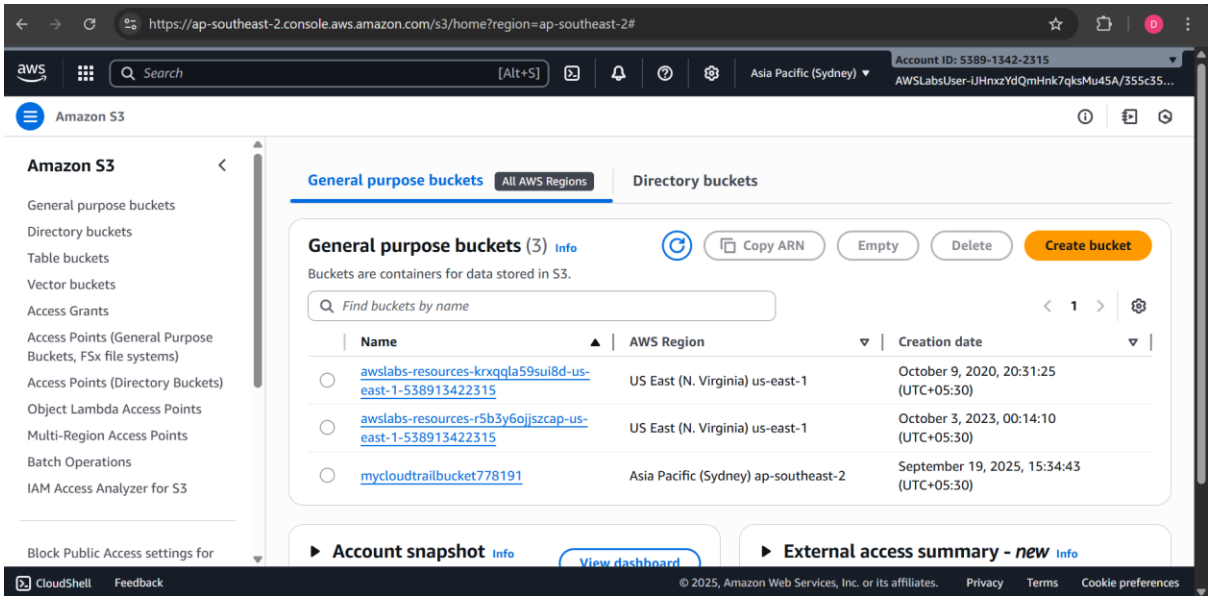


Task complete: You have successfully configured CloudTrail.

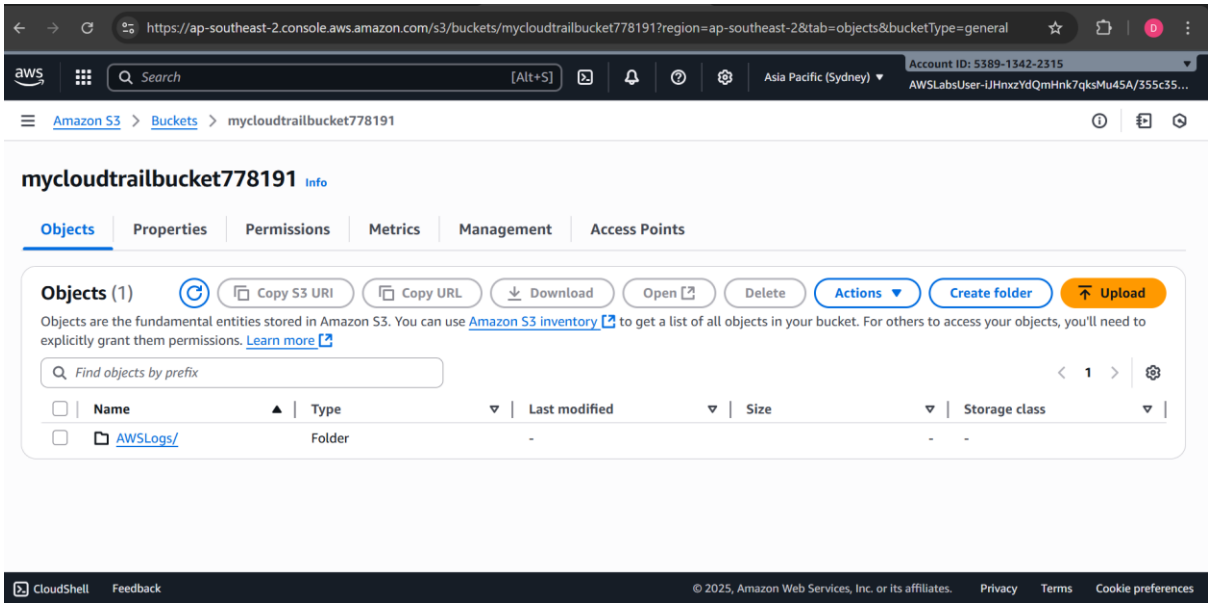
Task 3: Upload an image to your S3 bucket and encrypt it

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

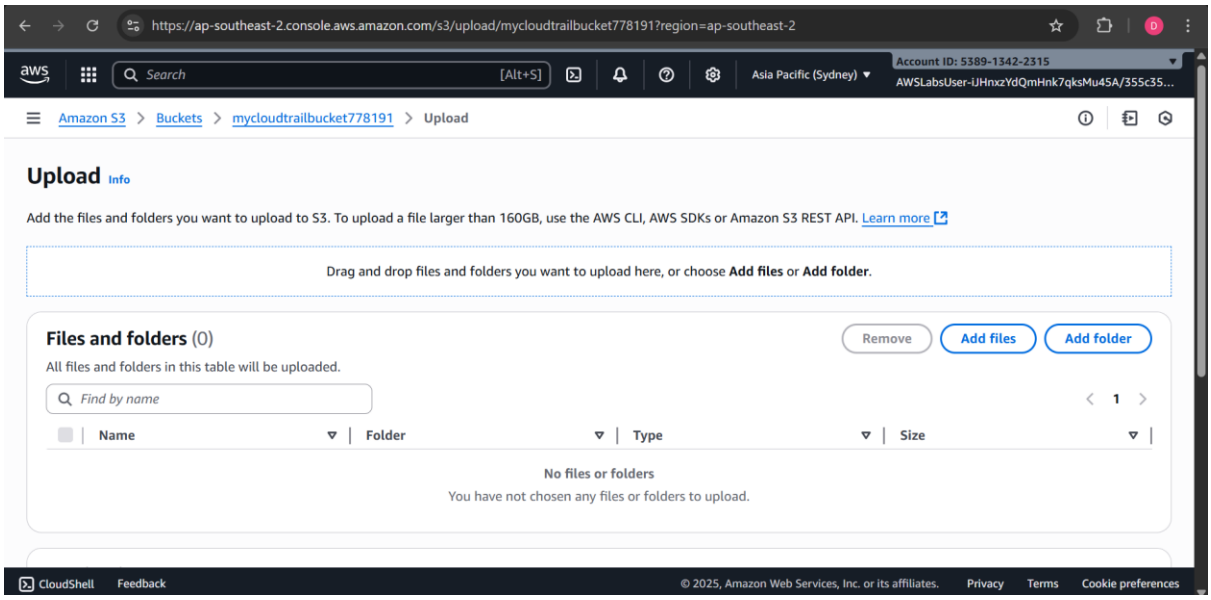
27. At the top of the page, in the unified search bar, search for and choose S3
28. Choose mycloudtrailbucket*.



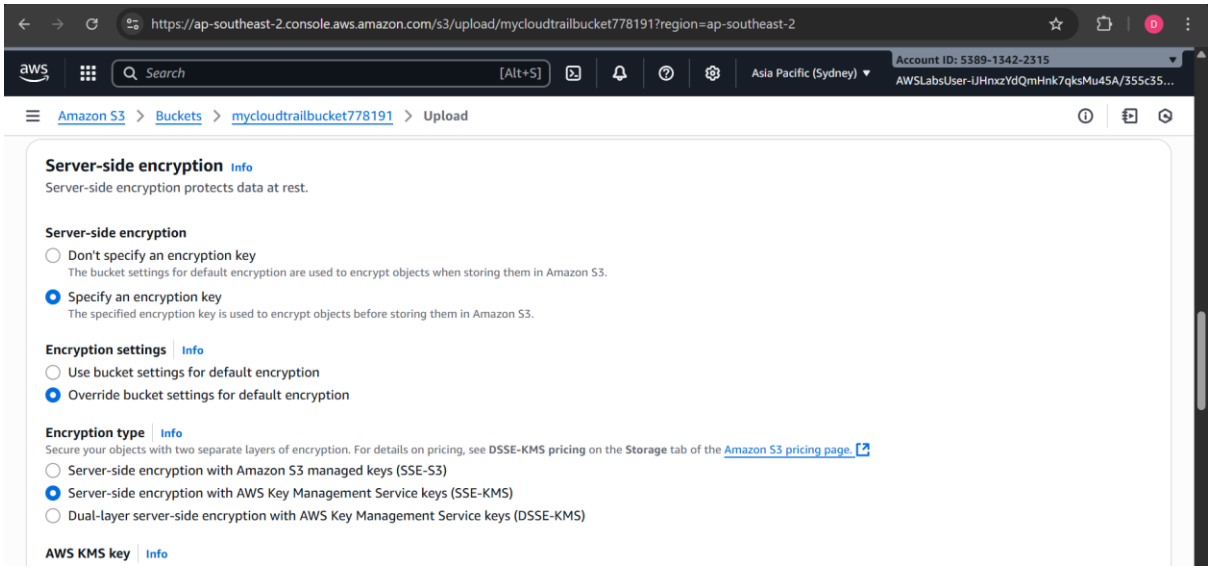
29. From the **Objects** tab, choose **Upload**.

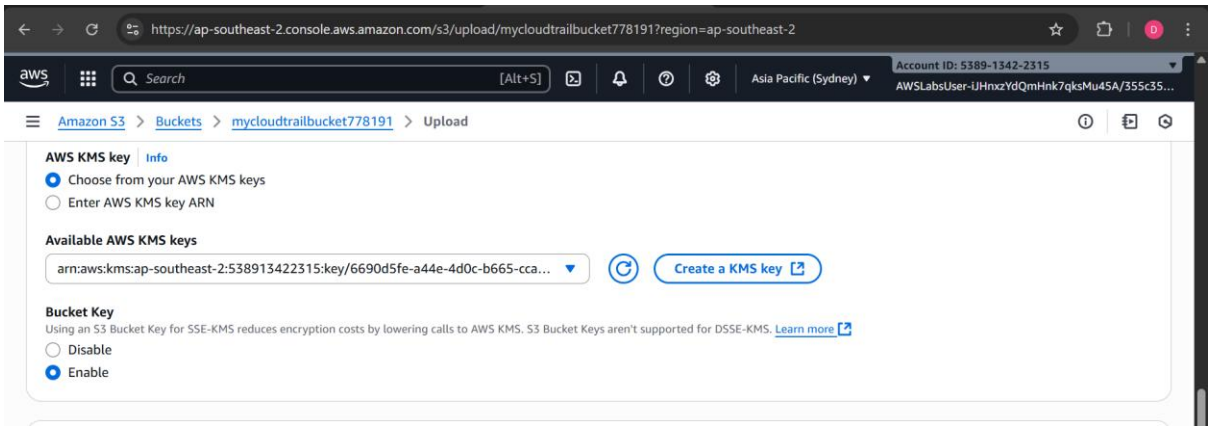


30. Choose **Add files**.



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**.



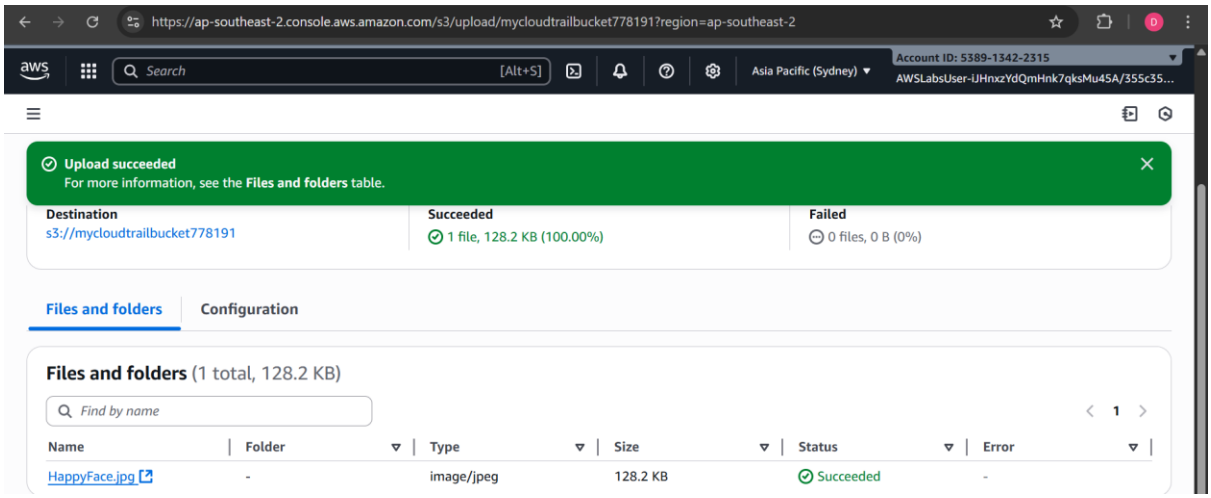


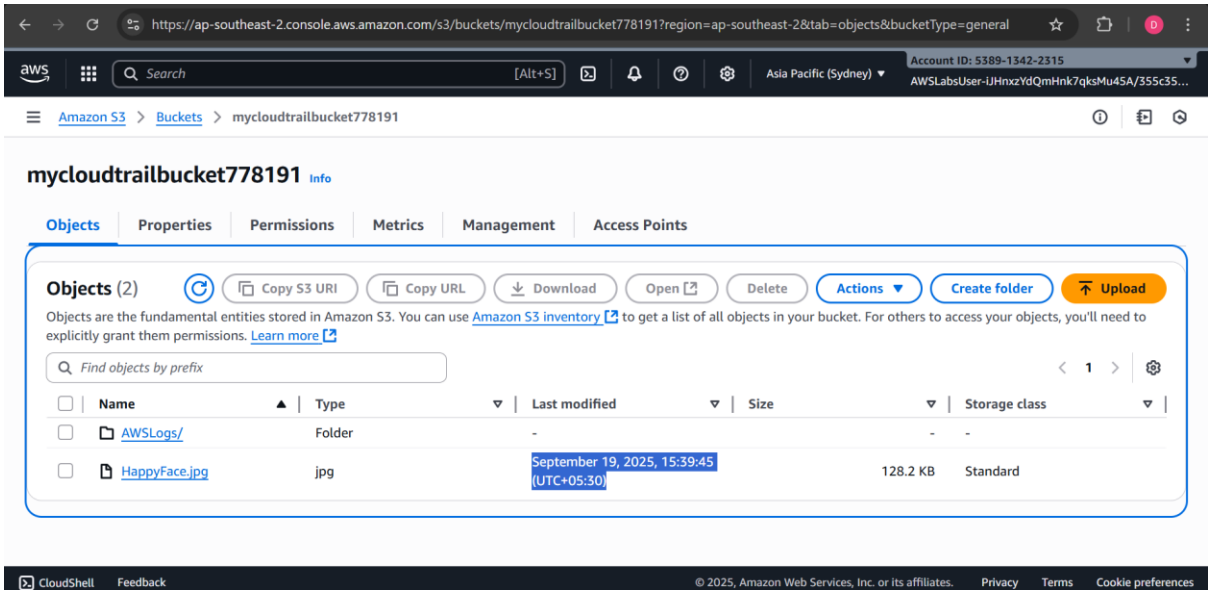
39. In the **Upload: status** page, a message shows the image was succesfully uploaded.

- 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.





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

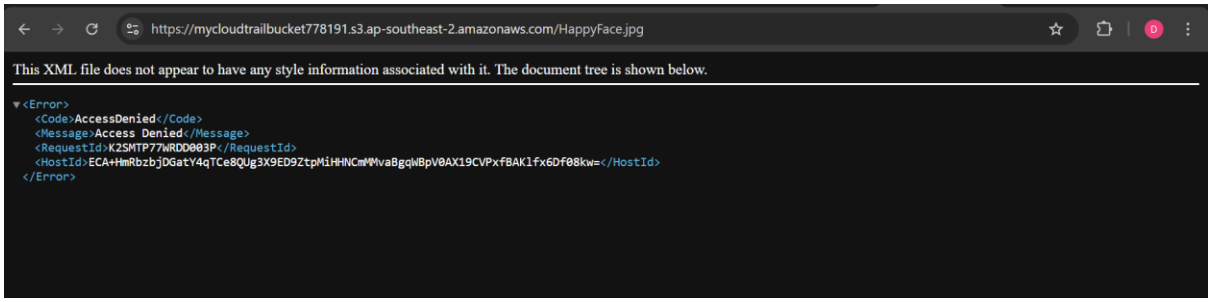
- AWS KMS decrypts the key by using the appropriate master key and sends the plaintext key back to Amazon S3
- Amazon S3 decrypts the ciphertext and removes the plaintext data key from memory as soon as possible

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.

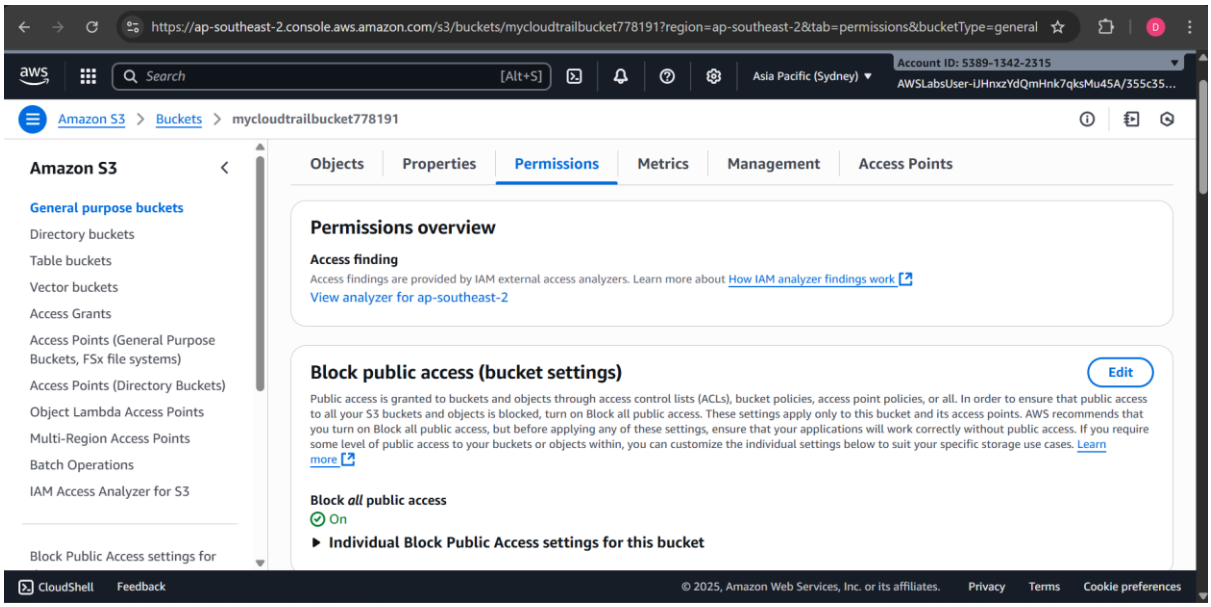
The URL should look similar to *https://mycloudtrailbucket10619.s3-us-west-2.amazonaws.com/Eiffel.jpg*

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.



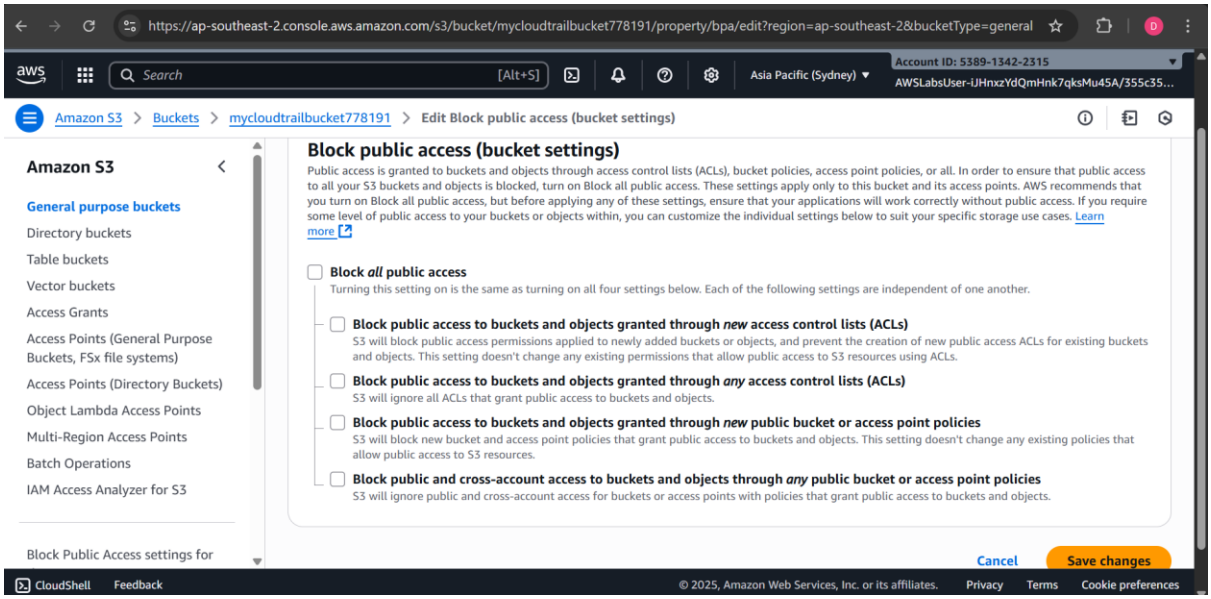
48. Return to the AWS Management Console.
49. In the **mycloudtrailbucket*** page, choose the **Permissions** tab.
50. In the **Block public access (bucket settings)** section, choose **Edit**.

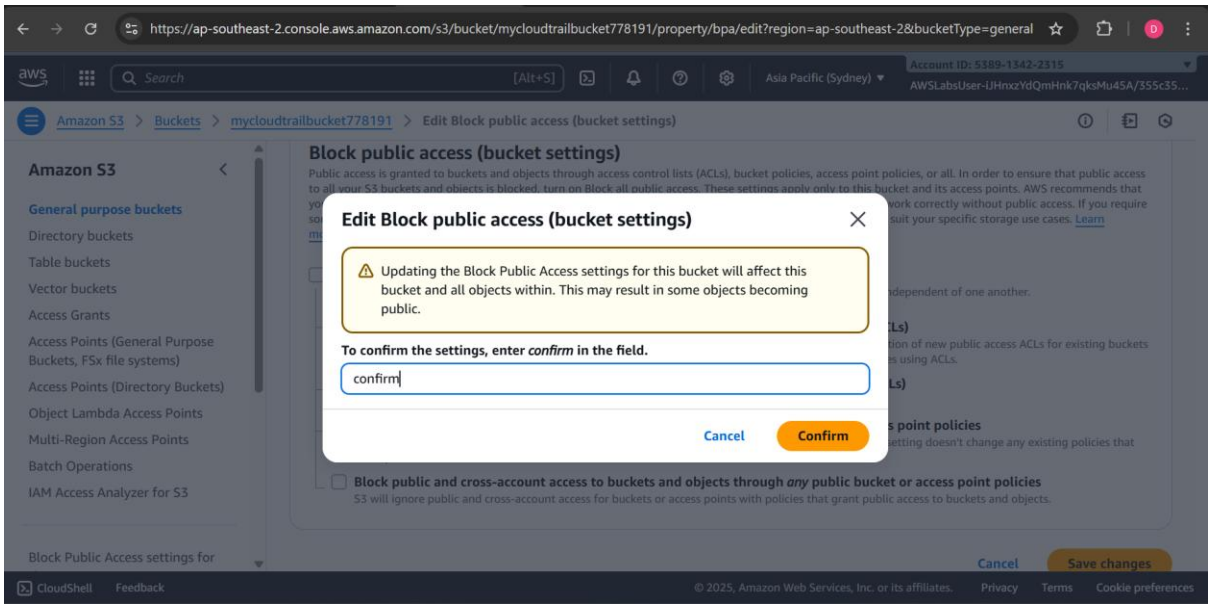


51. De-select **Block all public access**.

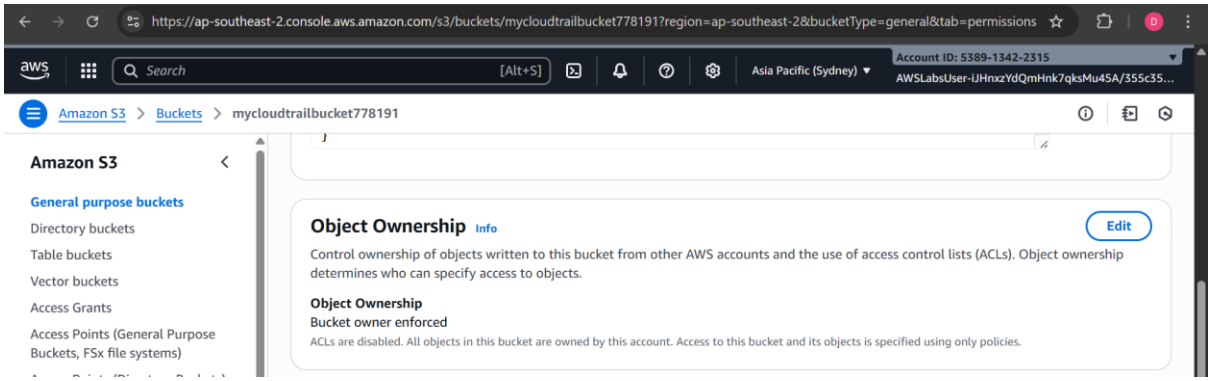
52. Choose **Save changes** then:

- Enter confirm
- Choose **Confirm**.

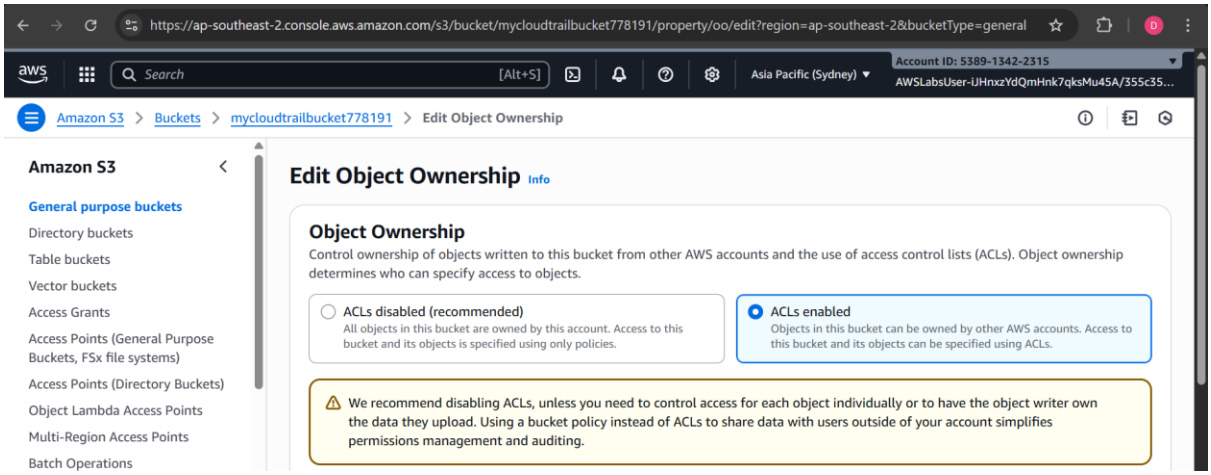




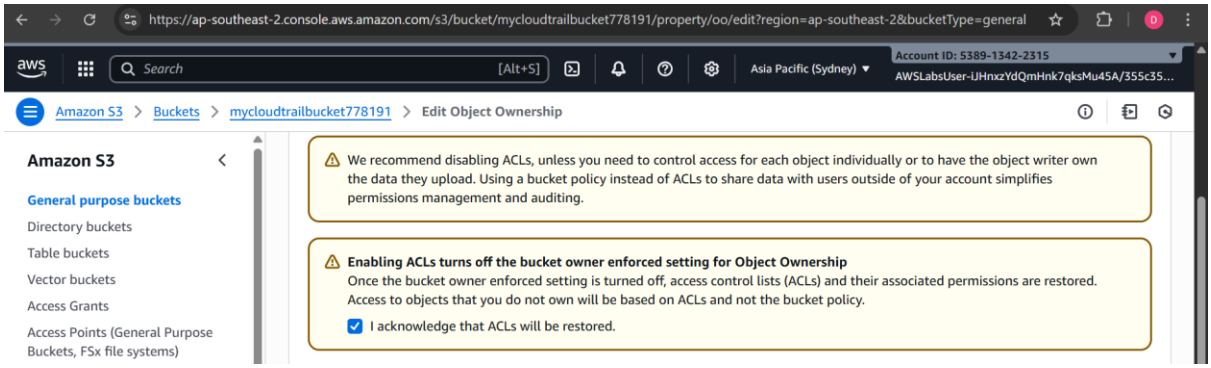
53. Scroll to the **Object Ownership** section, choose **Edit**.



54. Select **ACLs enabled**.



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

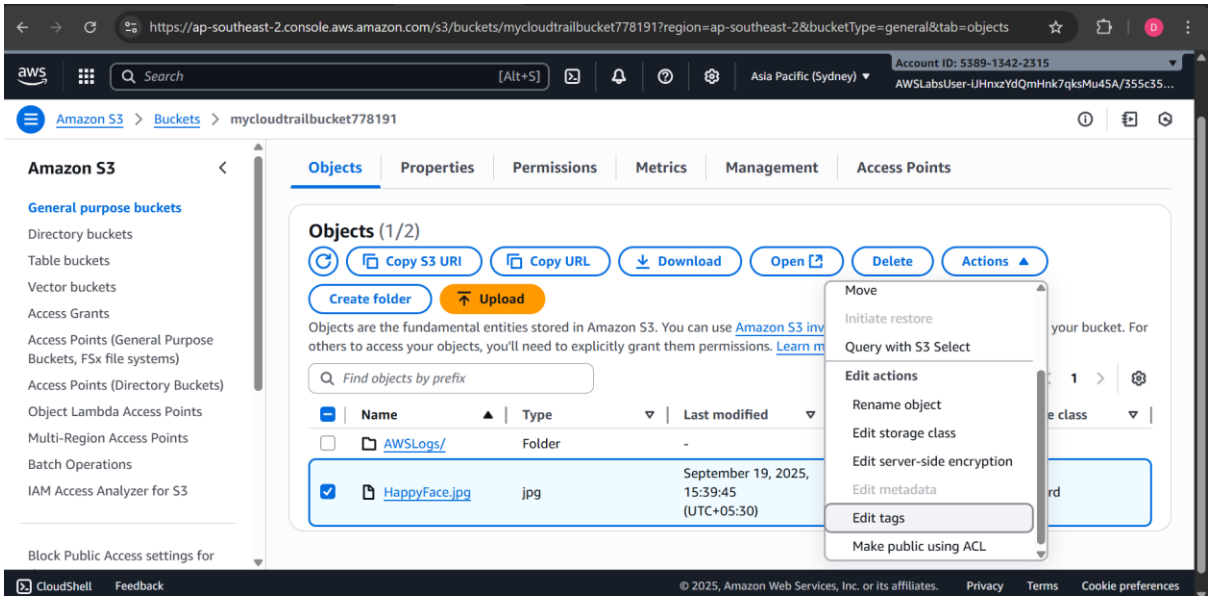


56. Choose **Save changes**.

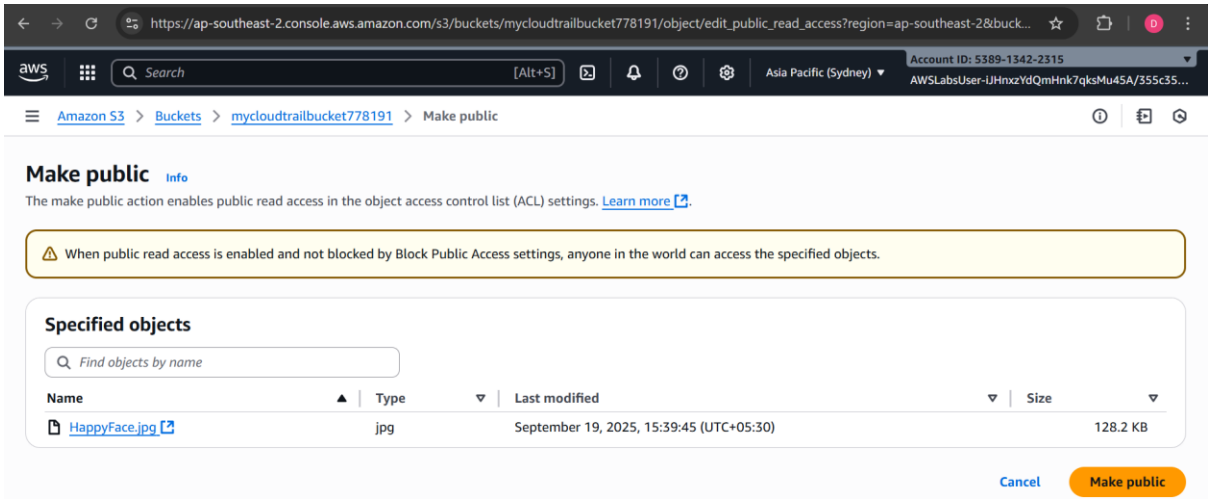
57. In the **Object** tab, select your image.

58. Choose **Actions**

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

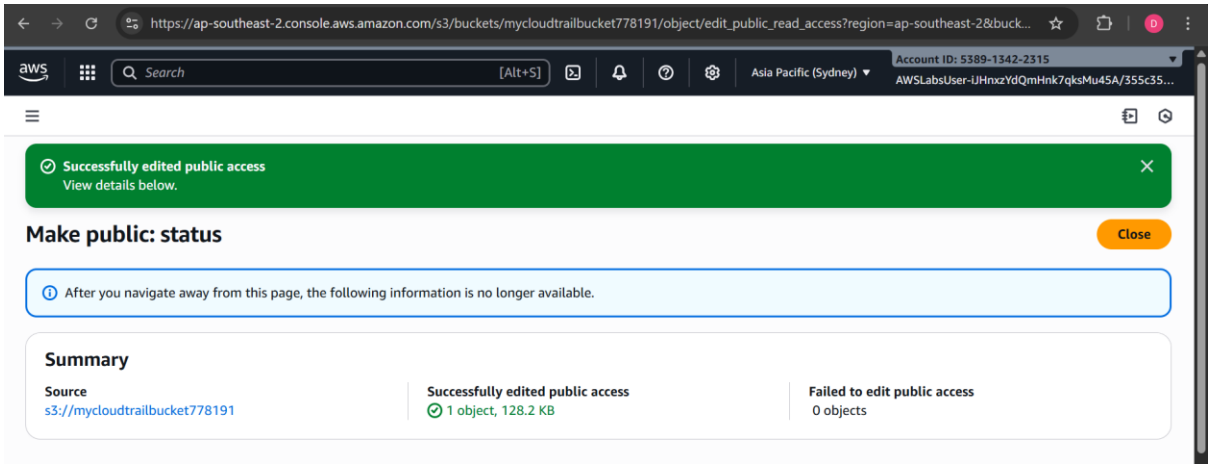


59. Choose **Make public**.



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

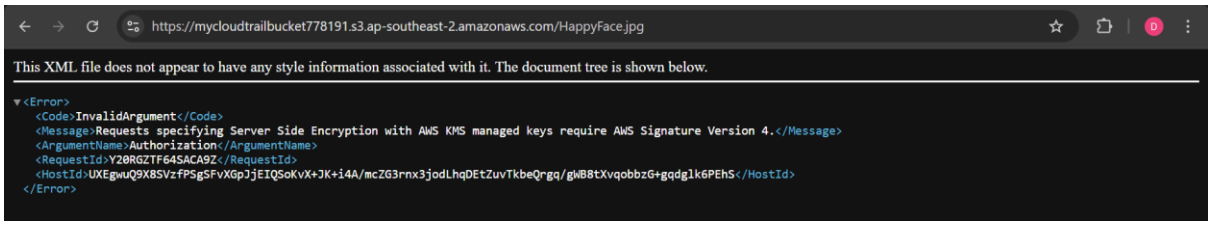
- Choose **Close**.



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.*



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]

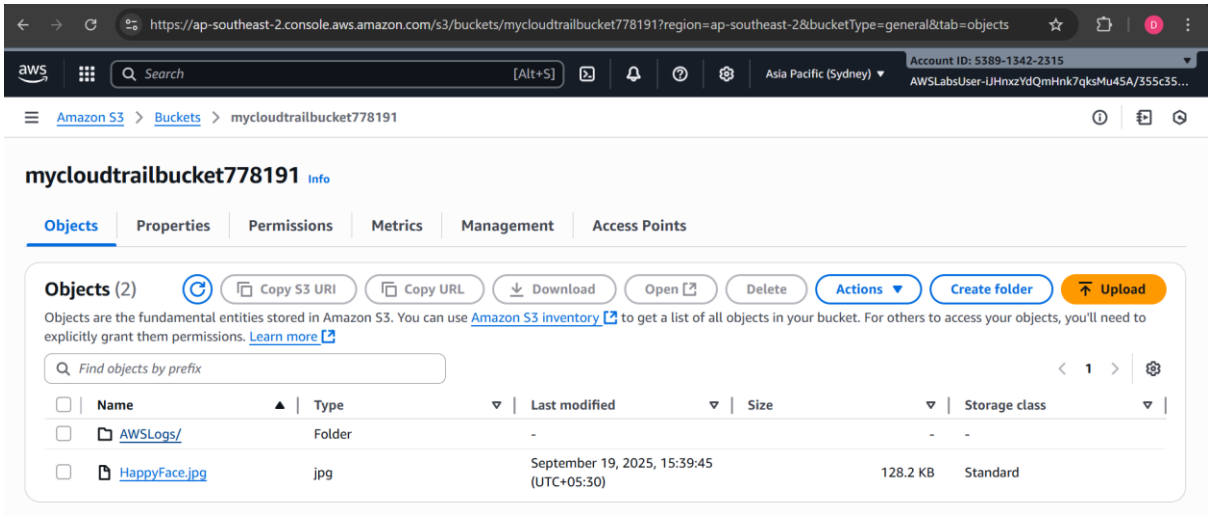
64. Close the **S3 Object URL** tab/window.

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.

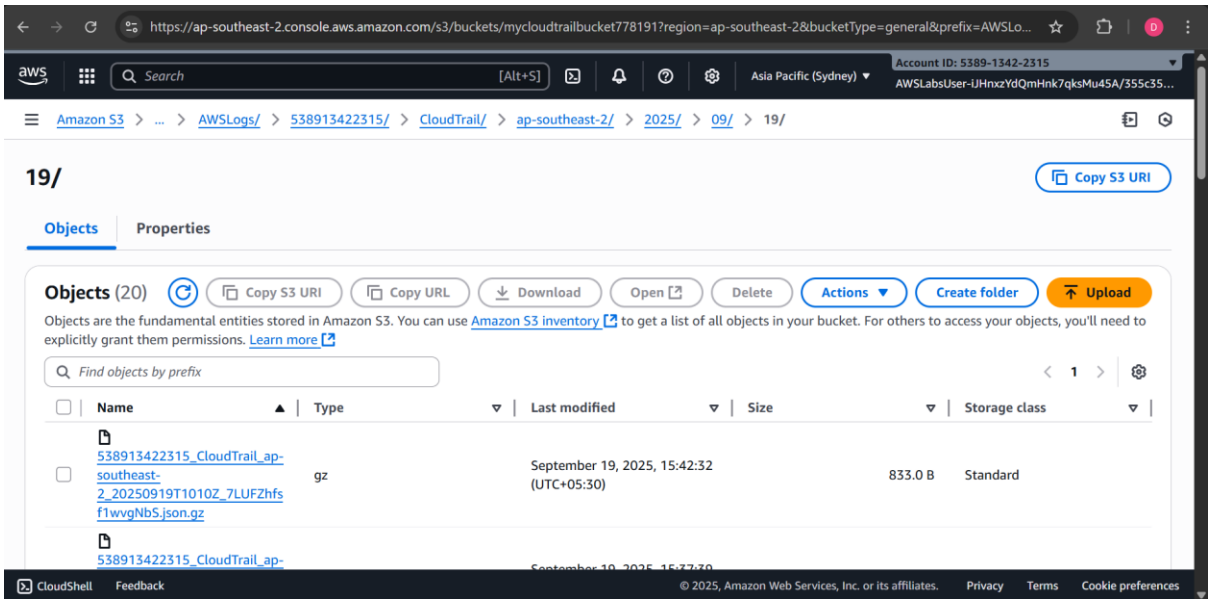
65. In the **mycloudtrailbucket*** page, choose the **Objects** tab.
66. Drill-down through the AWSLogs/ folders till you get to a folder that contains log file(s).



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.

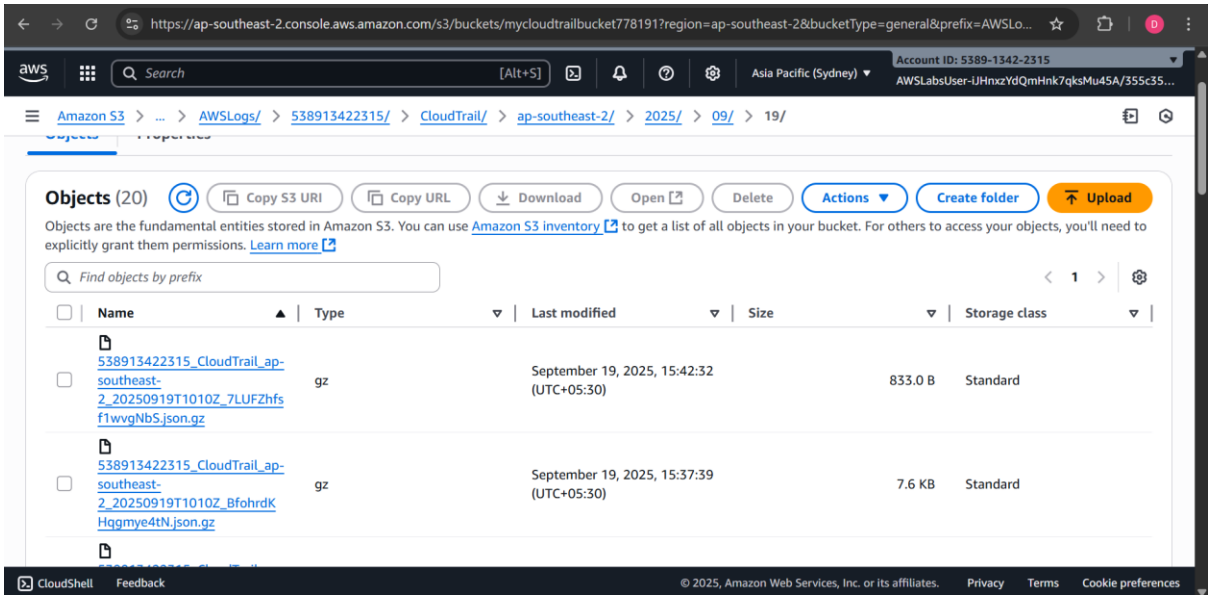
If you don't see any log files, choose the **refresh** button every few seconds till you see a log file.



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.



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** .

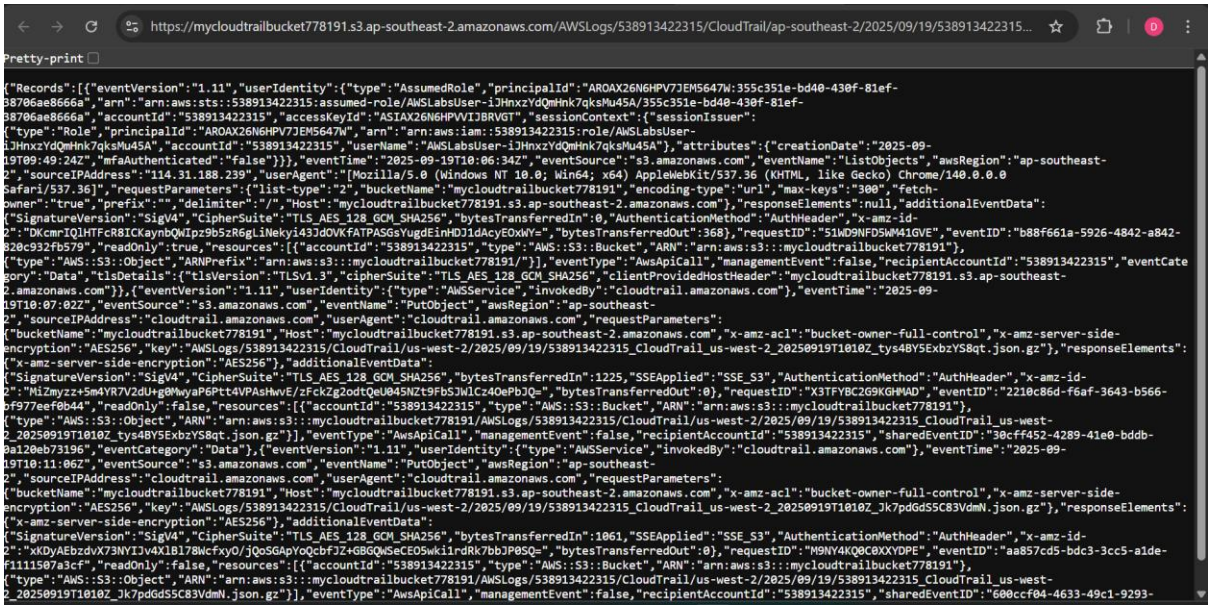
This opens a log file in a new browser tab.

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.



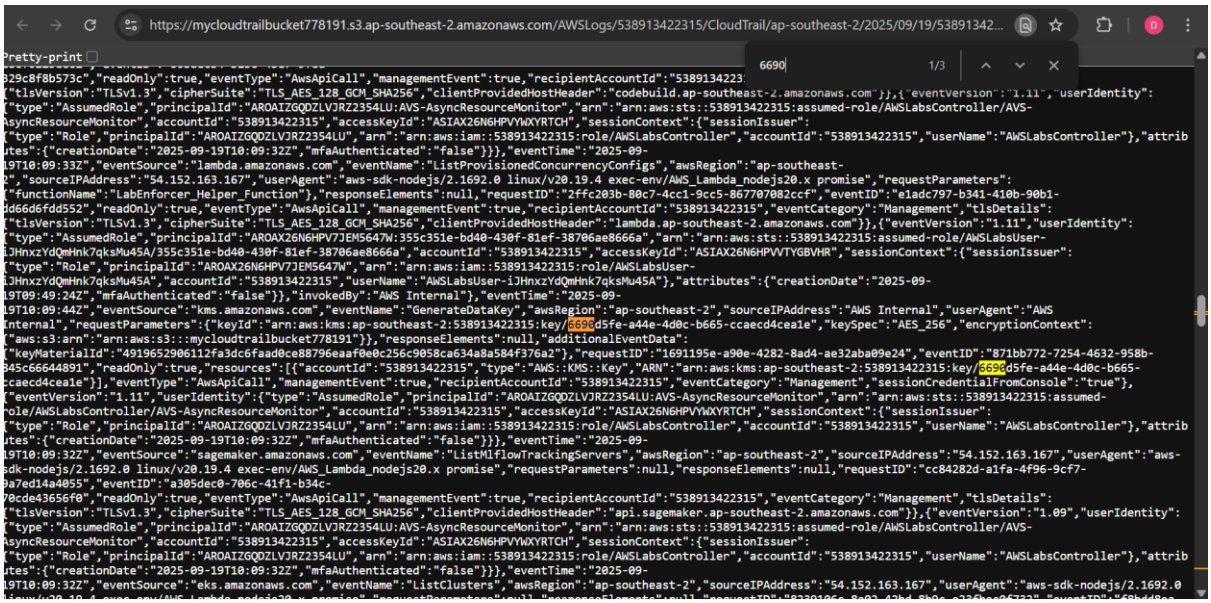
71. Search for the following in your log file:

- 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.

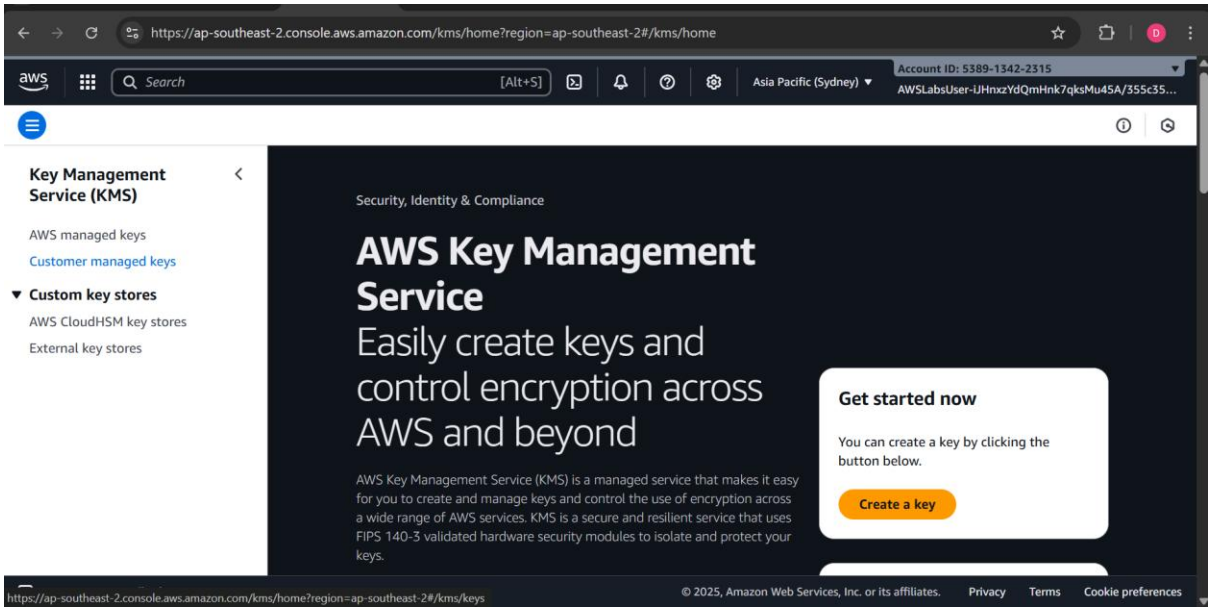


Task complete: You have monitored KMS activity using CloudTrail logs.

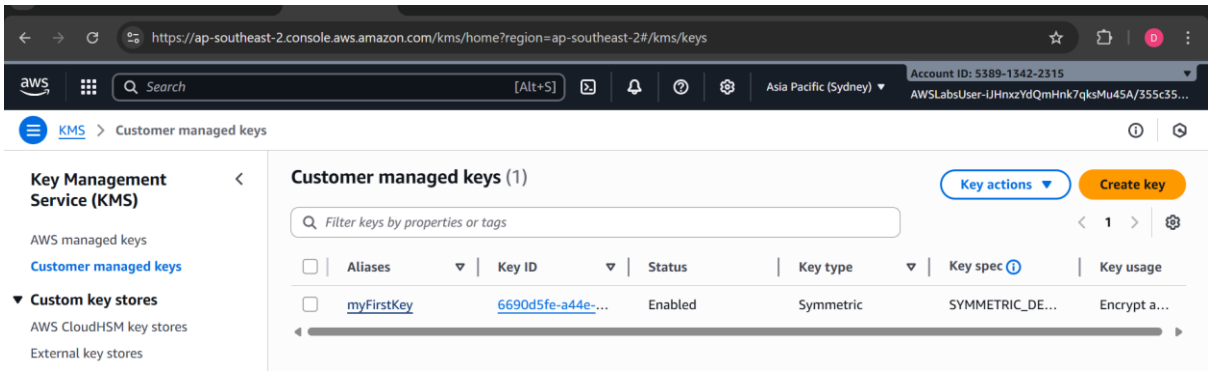
Task 6: Manage encryption keys

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

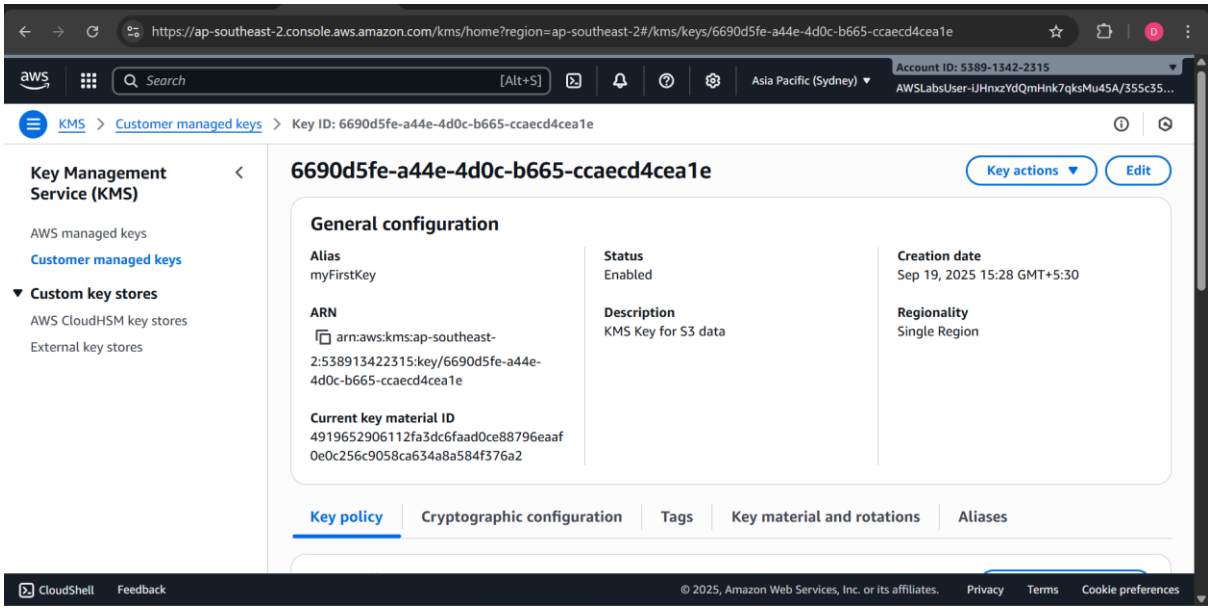
72. Navigate to the browser tab/window S3 service.
73. At the top of the page, in the unified search bar, search for and choose Key Management Service
74. In the left navigation panel, choose **Customer managed keys**.



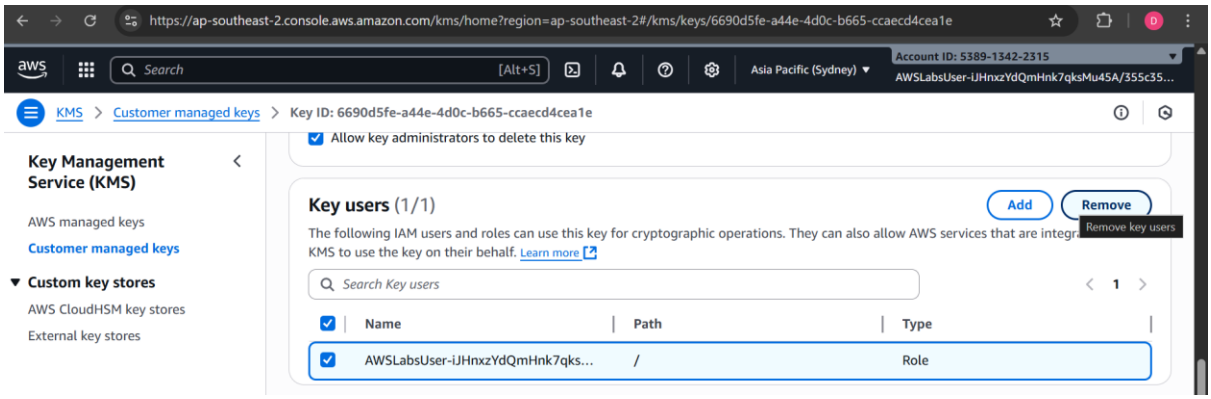
77. Choose myFirstKey.



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.



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



77. Choose **Remove**.

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

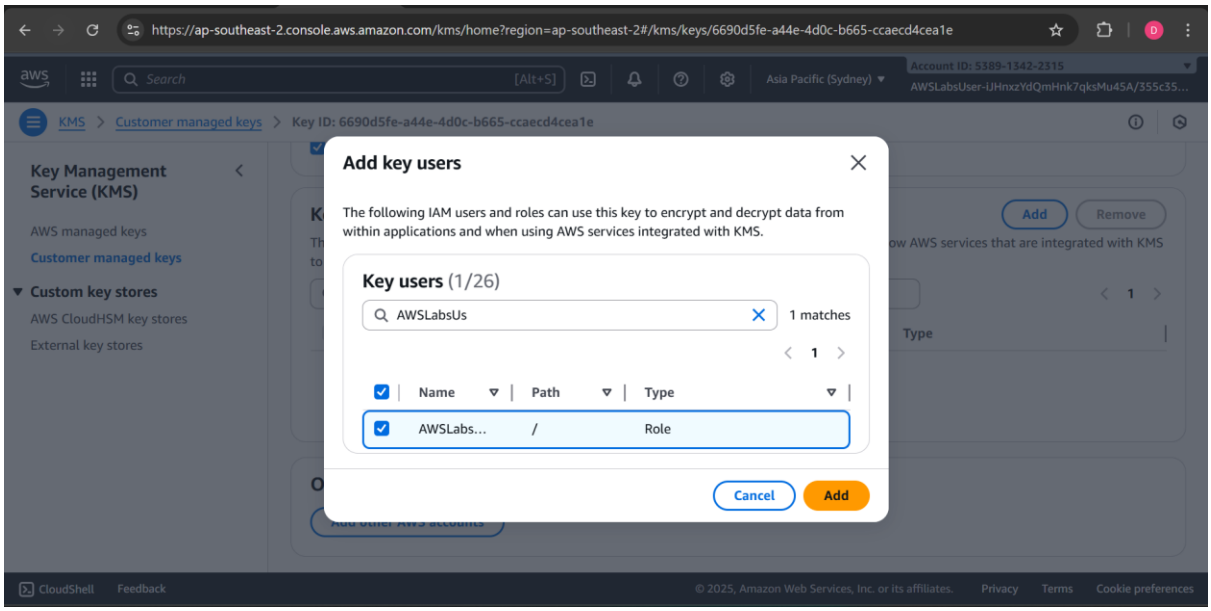
78. In the **Key users** section, choose **Add** then:

- 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.



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