Introduction to AWS Key Management Service

Lab Overview

This lab introduces you to AWS Key Management Service It will demonstrate the basic steps required to get started with Key Management Service, creating keys, assigning management and usage permissions for the keys, encrypting data and monitoring the access and usage of keys.

Topics covered

By the end of this lab, you will be able to:

- Create an Encryption Key
- Create an S3 bucket with CloudTrail logging functions
- Encrypt data stored in a S3 bucket using an encryption key
- Monitor CloudTrail using CloudWatch

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.

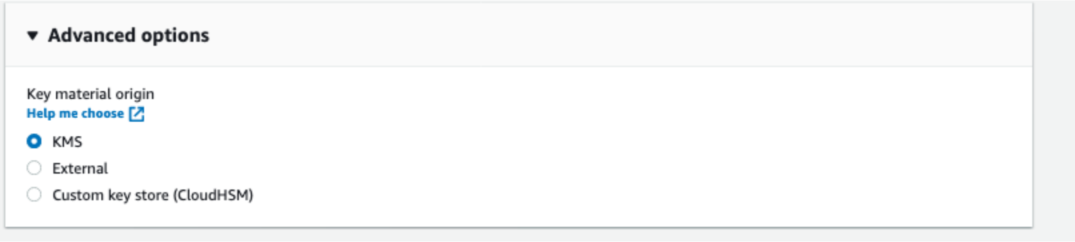
Task 1: Create Your KMS Master Key

In this task you will 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. In the **AWS Management Console**, on the Services menu, click **Key Management Service**.
4. Click Create a key then configure:

- On the **Configure key** page, select *Symmetric*
- Click Advanced Options to explore options. Keep KMS selected as the default option.

In this lab, we will be using KMS for the Key material origin. The AWS KMS service also provides the option to import your own customer master key or use a custom key store



▼ **Advanced options**

Key material origin
Help me choose
● KMS
○ External
○ Custom key store (CloudHSM)

- Click Next

5. On the **Add labels** page configure:

- **Alias:** myFirstKey
- **Description:** KMS Key for S3 data
- Click Next

It is a good practice to describe what services the encryption key will be associated with in the description.

6. On the **Define key administrative permissions**, select the user or role you're signed into the Console with.

This user is displayed at the top of the page, to the left of the region Fo AWS Event Engine Events, the administrative role should be **TeamRole**

7. Click Next

On this page, you can alter the keys description, **Add** or **Remove** Key Administrators and Key Users, allow external users to access the key and place the key into annual rotation.

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

8. On the **Define key usage permissions** page, select the user or role you're signed into the Console with.
9. Click Next

Key Users are the users or roles that will use the key to encrypt and decrypt data.

10. On the **Review and edit key policy** page:

- Review the key policy
- Click Finish

11. Copy the Key ID for **myFirstKey** to a text editor.

You will use the Key ID later when looking at the log activity for this KMS key.

Task 2: Configure CloudTrail to Store Logs in An S3 Bucket

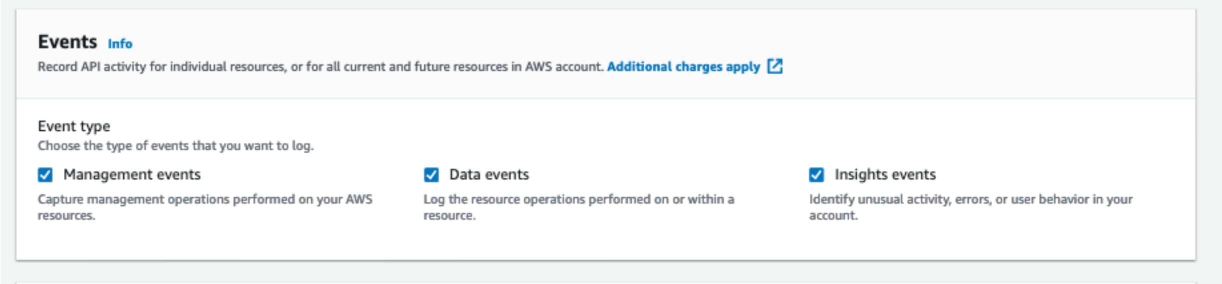
In this task you will configure CloudTrail to store log files in a new S3 bucket.

12. On the Services menu, click **CloudTrail**.
13. If you see the *New Event history features available in the new CloudTrail console* with **Try out the new console** , click **Try out the new console**, otherwise you can ignore this warning.
14. If you see a warning saying *The option to create an organization trail is not available for this AWS account.*, you can ignore this warning.
15. If you see *You do not have permissions to perform this action. An administrator for your account might need to add permissions to the policy that grants you access to CloudTrail*, you can ignore this warning.
16. In the navigation pane on the left, click **Trails**.
17. Click Create trail then configure:

- **Trail name:** myTrail
- **Trail log bucket and folder:** mycloudtrailbucketNUMBER
- Replace **NUMBER** with a random number
- De-select **Log file SSE-KMS encryption**
- Select the Enabled check box for Cloudwatch Logs
    - For log group, select New
    - Log group name: aws-cloudtrail-logs-ACCOUNTNUMBER-myfirsttrail
    - Create a new IAM role named: Cloudtrail_CloudwatchLogs_role

18. Click Next
19. On the **Choose log events** page, configure:

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



Events Info

Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply

Event type

Choose the type of events that you want to log.

☑ Management events
Capture management operations performed on your AWS resources.

☑ Data events
Log the resource operations performed on or within a resource.

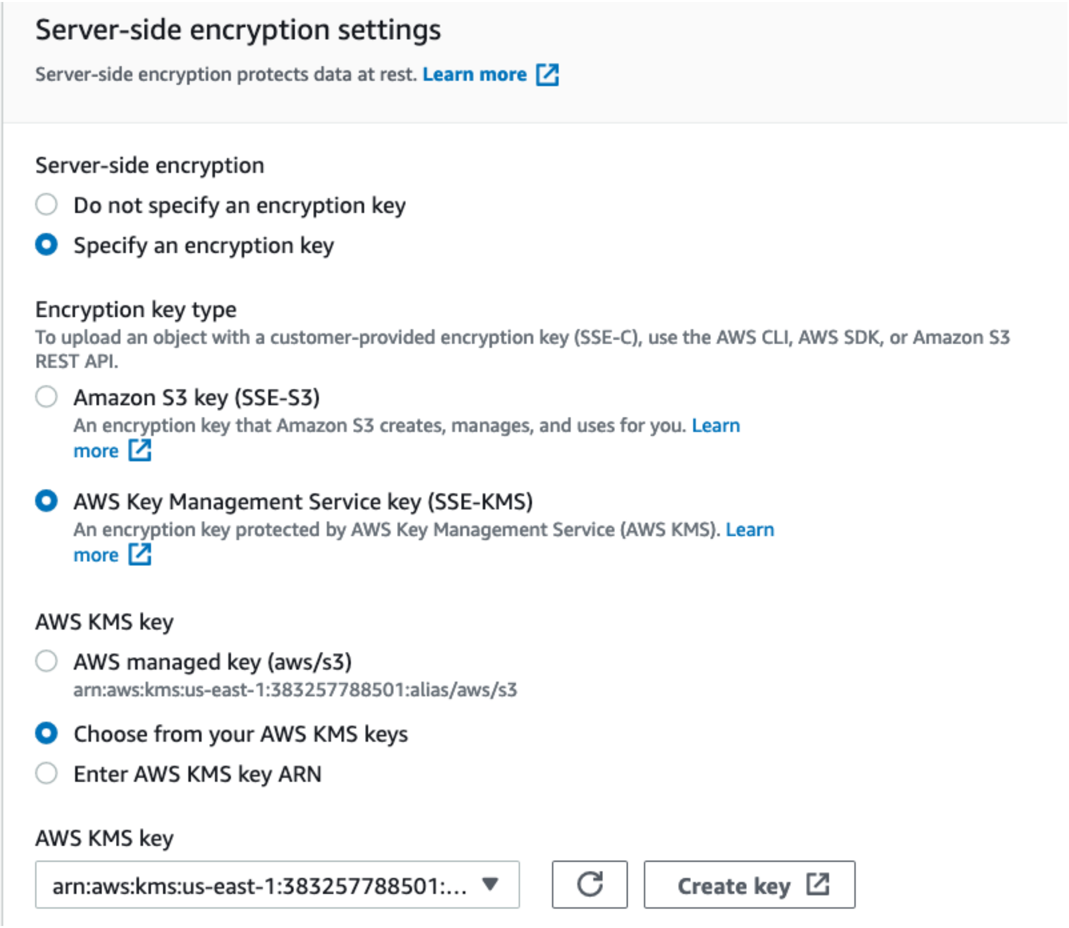
☑ Insights events
Identify unusual activity, errors, or user behavior in your account.

20. Click Next
21. Click Create trail

Task 3: Upload an Image to Your S3 Bucket and Encrypt It

In this task, you will upload an image file to your S3 bucket and encrypt it using the encryption key you created earlier. You'll use the S3 bucket you created in the previous task to store the image file.

22. On the Services menu, click **S3.**
23. Click **mycloudtrailbucket***.
24. From the **Objects** tab, click Upload
25. Click Add files
26. Browse to and select an image file on your computer
27. At the bottom of the screen, expand **Properties**.
28. In the **Server-side encryption settings** section, select *Specify an encryption key*
29. For **Encryption key type**, select **AWS Key Management Service key (SSE-KMS)**
30. For **AWS KMS key** Select **Choose from your AWS KMS keys**
31. From the drop down of the KMS master key, select *myFirstKey*



Server-side encryption settings

Server-side encryption protects data at rest. Learn more

Server-side encryption

○ Do not specify an encryption key

● Specify an encryption key

Encryption key type

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

○ Amazon S3 key (SSE-S3)
An encryption key that Amazon S3 creates, manages, and uses for you. Learn more

● AWS Key Management Service key (SSE-KMS)
An encryption key protected by AWS Key Management Service (AWS KMS). Learn more

AWS KMS key

○ AWS managed key (aws/s3)
arn:aws:kms:us-east-1:383257788501:alias/aws/s3

● Choose from your AWS KMS keys

○ Enter AWS KMS key ARN

AWS KMS key

arn:aws:kms:us-east-1:383257788501:... ▼

32. Scroll to the bottom of the screen, then click Upload
33. Click Close from the right corner of the **Upload: status** page.
34. Return to the bucket details by clicking the bucket name (as seen on the upper left)
35. Record the **Last modified** time to your text editor.
36. Return to the bucket details by clicking the bucket name (as seen on the upper left)

Task 4: Access the Encrypted Image

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

37. In the **Objects** tab, select image name and then click 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

38. Close the window/tab that shows your image.
39. Click the image name and copy the S3 **Object URL** to your text editor.

The S3 Object URL should look similar to *https://mycloudtrailbucket10619.s3-us-west-2.amazonaws.com/Eiffel.jpg*

40. Paste the S3 Object URL that you copied earlier into a new browser/window.
41. Press **Enter**.
42. What does the page show?

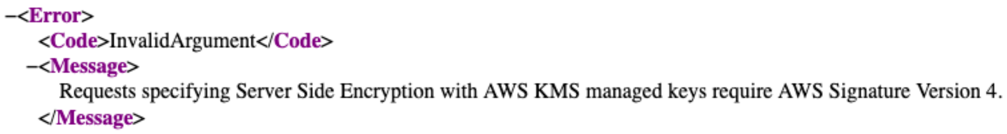
It should show *Access Denied*. This is because, by default public access is not allowed.

43. In the AWS Management Console, at the top of your screen, click the name of your bucket.
44. Click the **Permissions** tab.
45. For **Block public access (bucket settings)**, click Edit
46. De-select **Block all public access**.
47. Click Save changes then:

- Type
- Click Confirm

48. In the **Object** tab, select your image.
49. Click Actions > **Make public**.
50. Click Make public
51. Refresh the screen for the new tab/window that you opened earlier.
52. 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>
```

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

53. Close the new/tab window.

Task 5: Querying CloudTrail Logs in Logs Insights

CloudWatch Logs Insights enables you to interactively search and analyze your log data in Amazon CloudWatch Logs. You can perform queries to help you more efficiently and effectively respond to operational issues. If an issue occurs, you can use CloudWatch Logs Insights to identify potential causes and validate deployed fixes.

CloudWatch Logs Insights automatically discovers fields in logs from AWS services such as Amazon Route 53, AWS Lambda, AWS CloudTrail, and Amazon VPC, and any application or custom log that emits log events as JSON. In this lab exercise, we will query CloudTrail events CloudWatch Logs data with Insights

54. Go to CloudWatch > Logs > Insights
55. Select the CloudWatch Log Group created during the setup from the dropdown.
56. In the query pane, enter the following sample queries

    Find the 25 most recently added log events.

    fields @timestamp, @message | sort @timestamp desc | limit 25

    Find the number of log entries for each service, event type, and AWS Region.

    stats count(*) by eventSource, eventName, awsRegion

Conclusion

Congratulations! You now know how to:

- Create an Encryption Key
- Create an S3 bucket with CloudTrail logging functions
- Encrypt an image and store it in your S3 bucket
- View the encrypted image using the AWS Management Console
- Create CloudTrail logs to continuously monitor account activity related to actions across your AWS infrastructure