

Home / AWS / Guided Lab / How to Encrypt an S3 bucket using AWS KMS and monitor the activities with CloudTrail

How to Encrypt an S3 bucket using AWS KMS and monitor the activities with CloudTrail

Level: Fundamental

Amazon S3 AWS Key Management Service Amazon Web Services AWS CloudTrail



0h 27m 26s left



End Lab

Open Console

Validation

Lab Credentials

User Name ⓘ

Whiz_User_80425.91468665



Password ⓘ

719d2c68-ed4b-4967-ab76-292266aeec1f



Access Key ⓘ

AKIA5T3LYKMHR67WNNKK



Secret Key ⓘ

+Okr1gLitWYcytYO/CDdOnz+Jmw0m4EgsMXh9fXv






Lab Resources

No Lab Resources Found

Support Documents

1. [FAQs and Troubleshooting](#)
2. [Labs - Instructions and Guidelines](#)

Need help?

-  How to use Hands on Lab
-  Troubleshooting Lab
-  FAQs

[Submit Feedback](#)[Share](#)[Lab Overview](#)[Lab Steps](#)[Lab Validation](#) Cloud Architect, Cloud Security Engineer Security, Management & Governance

Lab Steps

Task 1: Sign in to AWS Management Console

1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.

2. On the AWS sign-in page,

- Leave the Account ID as default. Never edit/remove the 12-digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
- Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign in** button

3. Once Signed In to the AWS Management Console, Make the default AWS Region as **US East (N. Virginia) us-east-1**.

Task 2: Create a customer-managed KMS key

In this task, you will create a customer-managed KMS key and use it to encrypt S3 objects.

1. Navigate to Key Management Service by clicking on **Services** in the AWS Management Console, and selecting **Key Management Service** under **Security, Identity and Compliance** section.
2. Click on **Create a Key**
3. Under configure key:
 - Key type : Select **Symmetric**
 - Key usage : Select **Encrypt and Decrypt**
4. Click on **Next**
5. Under **Add labels**:
 - Alias : Enter ***whiz-kms-key***
 - Description : Enter ***KMS key to encrypt S3 Objects***
6. Click on **Next**
7. Under **Define key administrative permissions**:
 - Key administrators: **Select the role that is associated with the account you are working with.** For example: **whizlabs_user-*<RANDOM_NUMBER>***
8. Click on **Next**
9. Under **Define Key usage permissions**:
 - **Select the role that is associated with the account you are working with.** For **whizlabs_user-*<RANDOM_NUMBER>***
10. Click on **Next**
11. Review everything and click on the **Finish** button.
12. You have successfully created the KMS key.



13. Copy the Key ID and paste it in the notepad, we will use this later in the lab.

Task 3: Create an S3 bucket

In this task, you will create an S3 bucket to upload and encrypt an object and also to store events.



1. Navigate to S3 by clicking on **Services** in the AWS Management Console, and selecting **S3** under **Storage** section.
2. Click on **Create Bucket**
3. Under **General configuration**:
 - Note: **Bucket name must be a unique name within the global namespace.**
 - Bucket name : Enter ***whizlabs-cloudtrail-kms***
 - AWS Region : Select **US-East (N. Virginia) us-east-1**
 - Object ownership: Select **ACLs enabled** option and choose **Object writer** as the Object owner

Object Ownership info
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.

☐ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☒ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ 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.

Object Ownership
☐ **Bucket owner preferred**
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☒ **Object writer**
The object writer remains the object owner.

4. Leave the rest as default and click on **Create Bucket**.
5. You have successfully created an S3 bucket.

✔ **Successfully created bucket "whizlabs-cloudtrail-kms"**
To upload files and folders, or to configure additional bucket settings choose **View details**.

Task 4: Create a CloudTrail and configure it to store events in S3

In this task, you will create a CloudTrail and configure it to store KMS activities in S3 bucket.

1. Navigate to CloudTrail by clicking on **Services** in the AWS Management Console, and selecting **CloudTrail** under **Management & Governance** section.
2. Click on the menu section (three lines) on the left side panel and click on **Trails**.
3. Click on **Create Trail**.

Quick trail create

Trail details
Start logging management events by creating a trail with simplified settings. Logs are sent to an S3 bucket we create on your behalf. To choose a different bucket or additional events, go to the full [Create trail](#) workflow.
A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Trail log bucket and folder
aws-cloudtrail-logs-562622705552-a804f3b4
Logs will be stored in aws-cloudtrail-logs-562622705552-a804f3b4/AWSLogs/562622705552

Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs.

[Cancel](#) [Create trail](#)

4. Under **General details**:

- Trail name : Enter ***whiz-kms-trails***
- Storage location : Choose **Use existing S3 bucket**
- Trail log bucket name : Click on **Browse** and choose the S3 bucket that you have created earlier(i.e **whizlabs-cloudtrail-kms**)

5. Log file SSE-KMS encryption : **Uncheck** Enabled

Choose trail attributes

General details
A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

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

Storage location [Info](#)

☐ Create new S3 bucket
Create a bucket to store logs for the trail.

☒ Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket name
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

[Browse](#)

Prefix - optional

Logs will be stored in whizlabs-cloudtrail-kms/AWSLogs/327748403707

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

6. Leave the rest as default and click on **Next**.

7. Choose log events:

- Event type : Check both **Management events** and **Data events**.

Choose log events

Events [Info](#)

Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

Event type
Choose the type of events that you want to log.

☒ **Management events**
Capture management operations performed on your AWS resources.

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

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

8. Management events:

- API activity : Check both **Read** and **Write**

Management events [Info](#)

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

ⓘ Multiple management events trails detected. Charges apply to duplicated logged management events. [Additional charges apply](#)

API activity
Choose the activities you want to log.

☒ **Read** ☒ **Write**

☐ Exclude AWS KMS events

☐ Exclude Amazon RDS Data API events

9. Data events:

- Click on **Switch to basic event selectors** button.
- Click on **Continue** button on pop up.
- All current and future S3 buckets : Uncheck both **Read** and **Write**
- Individual bucket selection : Click on **Browse** and choose the S3 bucket that we have created earlier(i.e **whizlabs-cloudtrail-kms**)
- Make sure you have checked both **Read** and **Write** next to the Browse.

Data events [Info](#)

Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

Basic event selectors are enabled

Switch to advanced data event selectors for fine-grained control over the data events captured by your trail.

[Switch to advanced event selectors](#)

Data event: S3 [Info](#) [Remove](#)

Data event source
Select source of data events to log.

S3

S3 bucket
You can choose to log read and/or write events for all buckets. You can also choose individual buckets.

All current and future S3 buckets ☐ Read ☐ Write

Individual bucket selection
Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

[Browse](#) ☒ Read ☒ Write [X](#)

[Add bucket](#)

[Add data event type](#)

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

10. Click on **Next**.

11. Review everything and click on **Create Trail**.

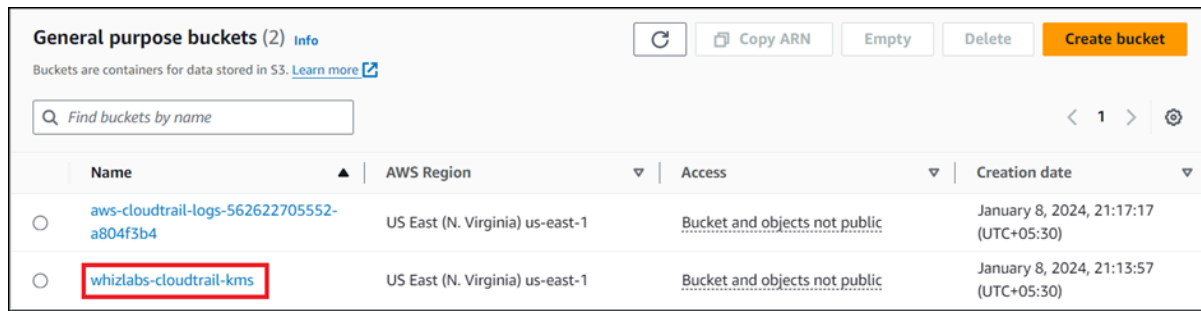
12. You have successfully created a CloudTrail and can find yours under Trails.

Trails									
Copy events to Lake Refresh Delete Create trail									
Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status	
whiz-kms-trail	US East (N. Virginia)	Yes	Disabled	No	aws-cloudtrail-logs-562622705552-a804f3b4	-	-	Logging	
whiz-kms-trails	US East (N. Virginia)	Yes	Disabled	No	whizlabs-cloudtrail-kms	-	-	Logging	

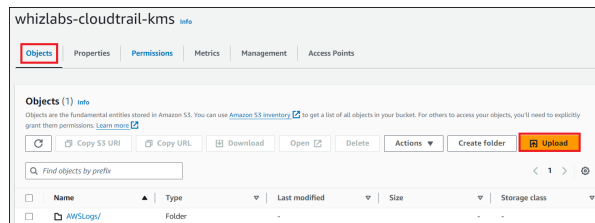
Task 5: Uploading an object and encrypting it

In this task, you will upload an image from our local PC and encrypt it using the KMS key we have created in Task 3.

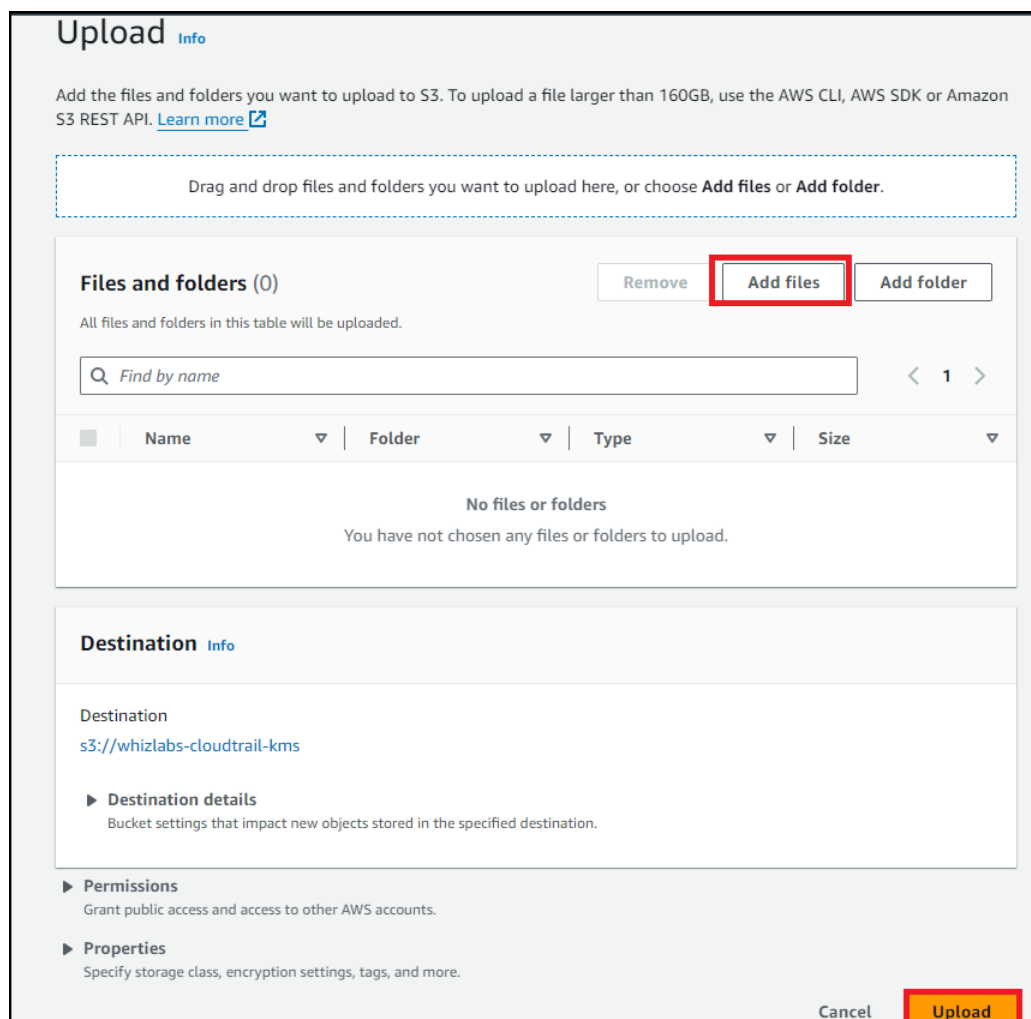
1. Navigate to S3 by clicking on **Services** in the AWS Management Console, and selecting **S3** under the **Storage** section.
2. Click on the S3 bucket (**whizlabs-cloudtrail-kms**) we have created.



3. Click on the **Upload** button.

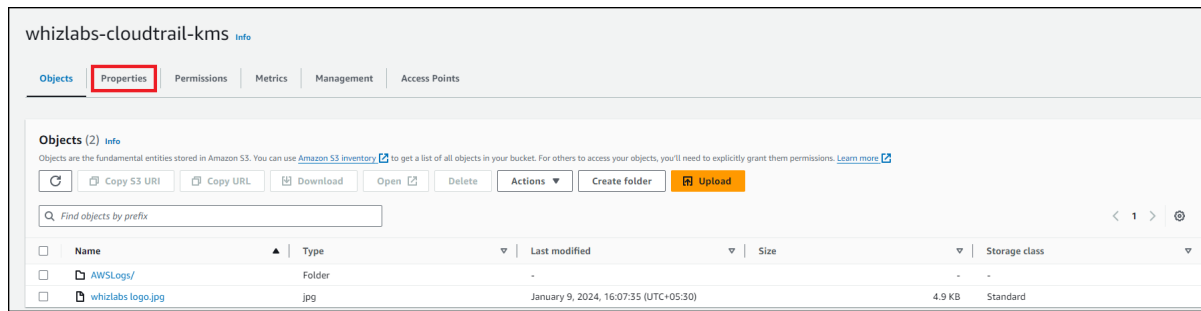


4. Click on **Add files** and choose a picture from your local PC and Click on the **Upload** button.



5. Click on the **object** which we have created.

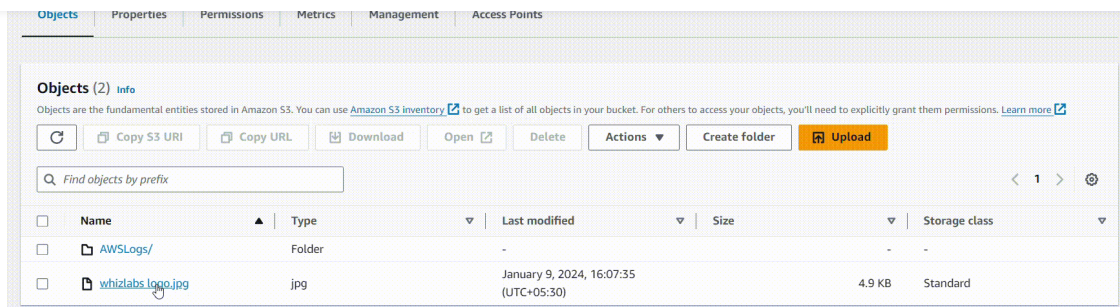
6. Scroll down to **Properties** and click on it to expand.



7. Scroll down to **Server-side encryption settings**:

- Encryption settings : **Override bucket settings for default encryption**
- Encryption key type : Select **Server Side Encryption with AWS Key Management Service key(SSE-KMS)**
- AWS KMS key : Select **Choose from your AWS KMS keys** and from the drop-down

you can select the KMS key you have created in this step. You



8. Click on the **Save Changes** button.

9. Click on close and you will see your uploaded picture under the objects section.

10. Note the Last Modified time in the notepad.

Task 6: Accessing the encrypted object

In this task, you will try to access the encrypted object through both S3 console and Object URL.

1. Click on the picture you have uploaded and click on **Open** on the top right side of your screen.



2. The picture opens in a new tab/window.

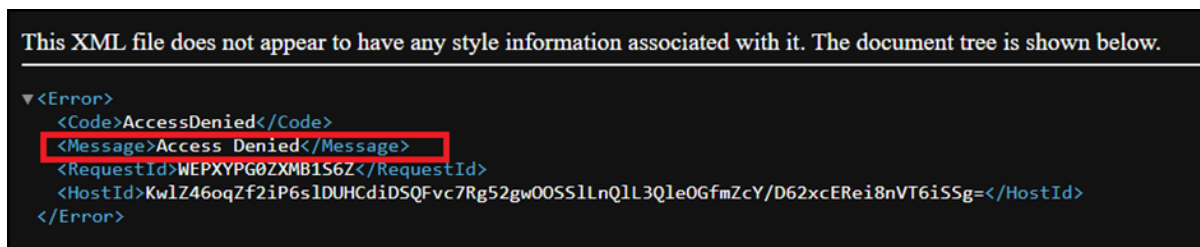
3. What happens behind the scenes

- 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 cypher text and removes the plaintext data key from memory as soon as possible.

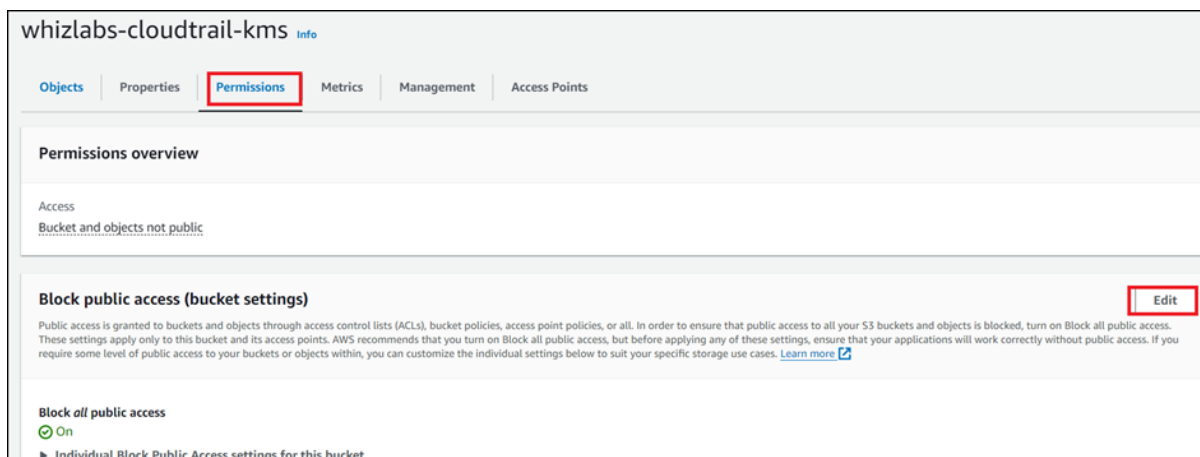
4. Close the tab/window that displayed your picture.

5. Now copy the **Object URL** and paste it into a new tab of your browser and hit Enter. [In my case : <https://whizlabs-cloudtrail-kms.s3.amazonaws.com/Sharingan.png>]

6. You will see a page with the message “**Access denied.**” And that is because by default, the public access is blocked.



7. Go back to the bucket, click on the **Permissions** section.



8. Under Block public access, click on **Edit** and uncheck **Block all public access** and click on **Save changes**.

9. In the next screen, Type **confirm** and click on **Confirm** button.

10. You have successfully edited Block Public Access settings.

11. Now go to the Objects tab and click on your object.

12. On the top right corner, select **Make public** from the **Object actions** drop-down menu and click on **Make public using ACL**.

13. Click on **Make public** button.
14. Now refresh the tab where you have pasted the **Object URL** earlier.
15. You should see a message something like this.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

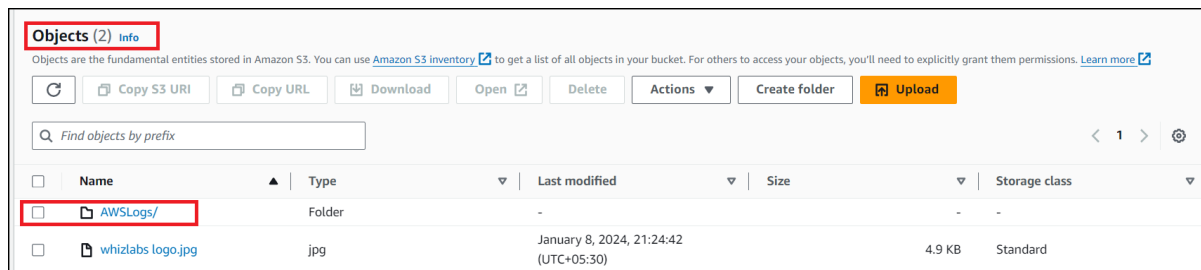
```
<?xml version="1.0" encoding="UTF-8"?>
<Error>
  <Code>InvalidArgument</Code>
  <Message>Requests specifying Server Side Encryption with AWS KMS managed keys require AWS Signature Version 4.</Message>
  <ArgumentName>Authorization</ArgumentName>
  <ArgumentValue>null</ArgumentValue>
  <RequestId>1SCRGHbVETV350G7</RequestId>
  <HostId>/7WX19amI09x/9Dbxvrii0LxuU1li/Tn7KSpKD8+FPz1zW9e9uCUkFwN+z4p+R7f3RDZxL3MwpRC00kqgr5qw==</HostId>
</Error>
```

16. This is because the picture is encrypted and you are not able to view it using the public link. If you are uploading or accessing objects encrypted by SSE-KMS, you need to use AWS Signature Version 4 for added security.

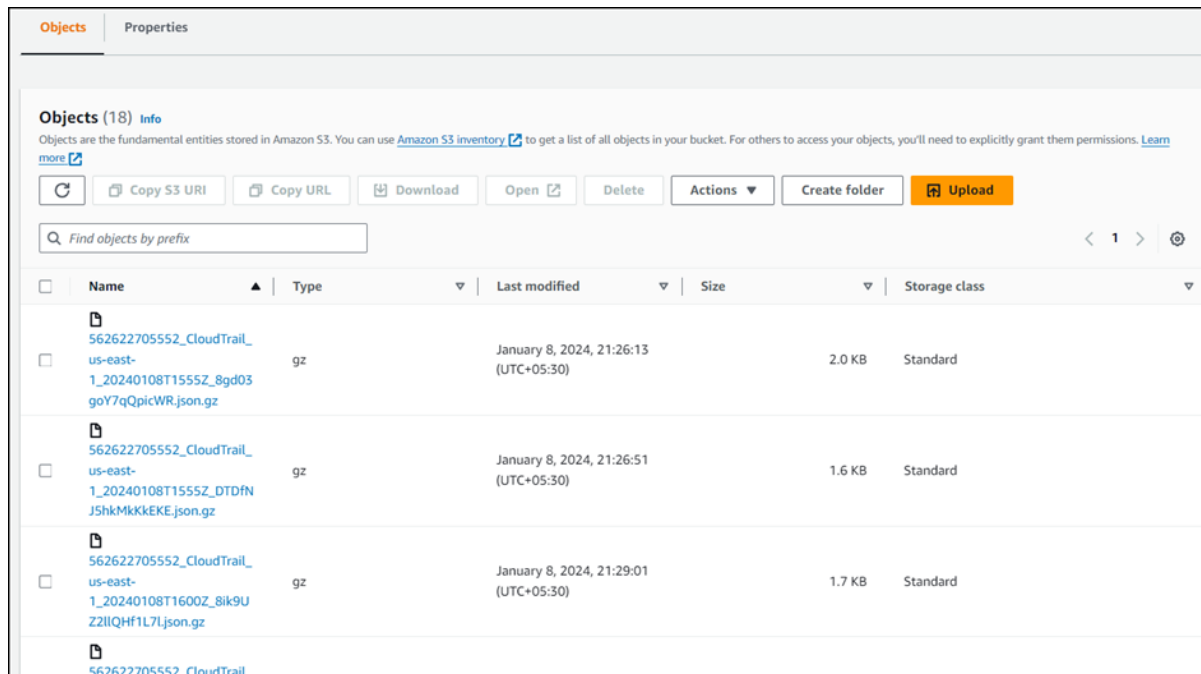
Task 7: Monitoring KMS activity using CloudTrail Logs

In this task, you will access and view our CloudTrail log files in the S3 bucket related to KMS encryption operations.

1. Go back to the S3 bucket we have created and you will be able to find one more object with the name **AWSLogs/**.



2. Click on it and click on the next directory too representing your account number.
3. Now click on the **CloudTrail/** directory and click on **us-east-1/**.
4. In case if you do not see any objects under **CloudTrail/**, please wait for 5 minutes and **refresh** the objects.
5. Now click on the **<year>**, **<month>** and **<date>** one after the other.
6. You will be able to see CloudTrail logs.



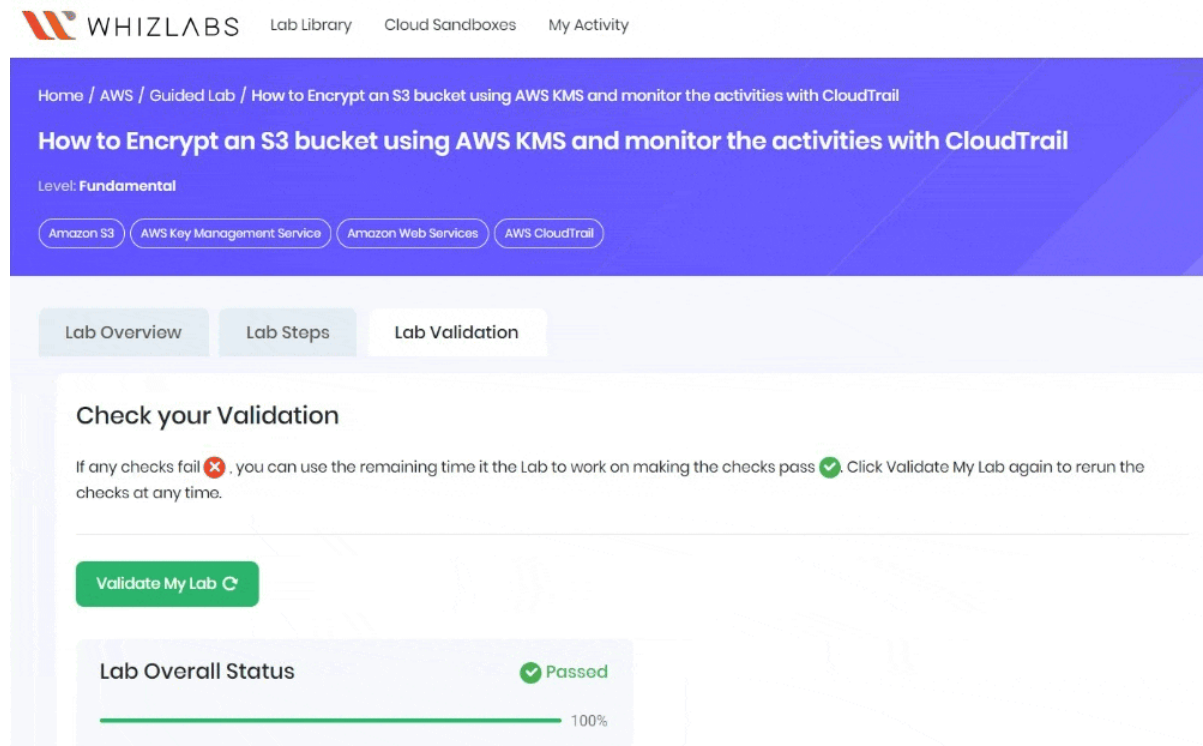
7. Click on the log file whose Last modified time is greater than the timestamp of the picture when it is uploaded.(Refer your notepad)
8. If there is no log file whose Last modified time is greater than the timestamp of the picture when it is uploaded, wait for 5 more minutes.
9. Click on the latest log file from the list.
10. Click on **Open**.
11. Press **Ctrl+F** and search for the Key Id you have saved in the notepad and the picture name you have created.
12. If you are unable to find them, copy the object URL of the picture you have uploaded again and paste it in the browser and note down the time.
13. Wait for some time and now search for the logs whose time is greater than that of what you just noted down.
14. Now you will be able to find the Key ID in the log record.

Do you know?

Encrypting an S3 bucket using AWS Key Management Service (KMS) and monitoring the activities with CloudTrail is a secure way to protect your data and track any changes or access to the bucket. Here are some points to consider for each heading:

Task 8: Validation Test

1. Once the lab steps are completed, please click on the **Validate** button on the left side panel.
2. This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
3. Sample output :



Task 9: Delete AWS Resources

Deleting KMS key

1. Navigate to Key Management Service by clicking on **Services** in the AWS Management Console, and selecting **Key Management Service** under **Security, Identity and Compliance** section.
2. On the left side panel, click on the Customer **managed key**.
3. Select the KMS key we have created and select Disable from the drop down menu.
4. Check **Confirm that you want to disable this key** click on Disable key.

5. Now select the KMS key again and select **Schedule key deletion** from the drop down menu.
6. Waiting period : Enter **7**
7. Check **Confirm that you want to schedule these keys for deletion after a 7-day waiting period** and click on Schedule deletion.

Completion and Conclusion

1. You have successfully created a KMS key and an S3 bucket.
2. You have successfully created a CloudTrail and configured it to store events in S3.
3. You have successfully monitored KMS activity using CloudTrail Logs in S3 bucket.

End Lab

1. Sign out of the AWS Account.
2. You have successfully completed the lab.
3. Once you have completed the steps, click on **End Lab** from your whizlabs dashboard.

[About Us](#) [Subscription](#) [Instructions and Guidelines](#) [FAQ's](#) [Contact Us](#)



© 2024, Whizlabs Software Pvt. Ltd.

