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

**Introduction**

**Amazon S3**

1. A lot of companies today need the ability to simply and securely collect, store, and analyze their data at a massive scale.
2. Amazon S3 is an**object storage** built to store and retrieve any amount of data from anywhere be it Websites, Mobile applications, Commercial applications, and data from IoT sensors or devices.
3. It is designed to deliver **99.999999999%** durability and stores data for millions of applications.
4. Amazon S3 provides comprehensive security with Server-Side Encryption, Customer-Side Encryption, Bucket policies and ACLs.

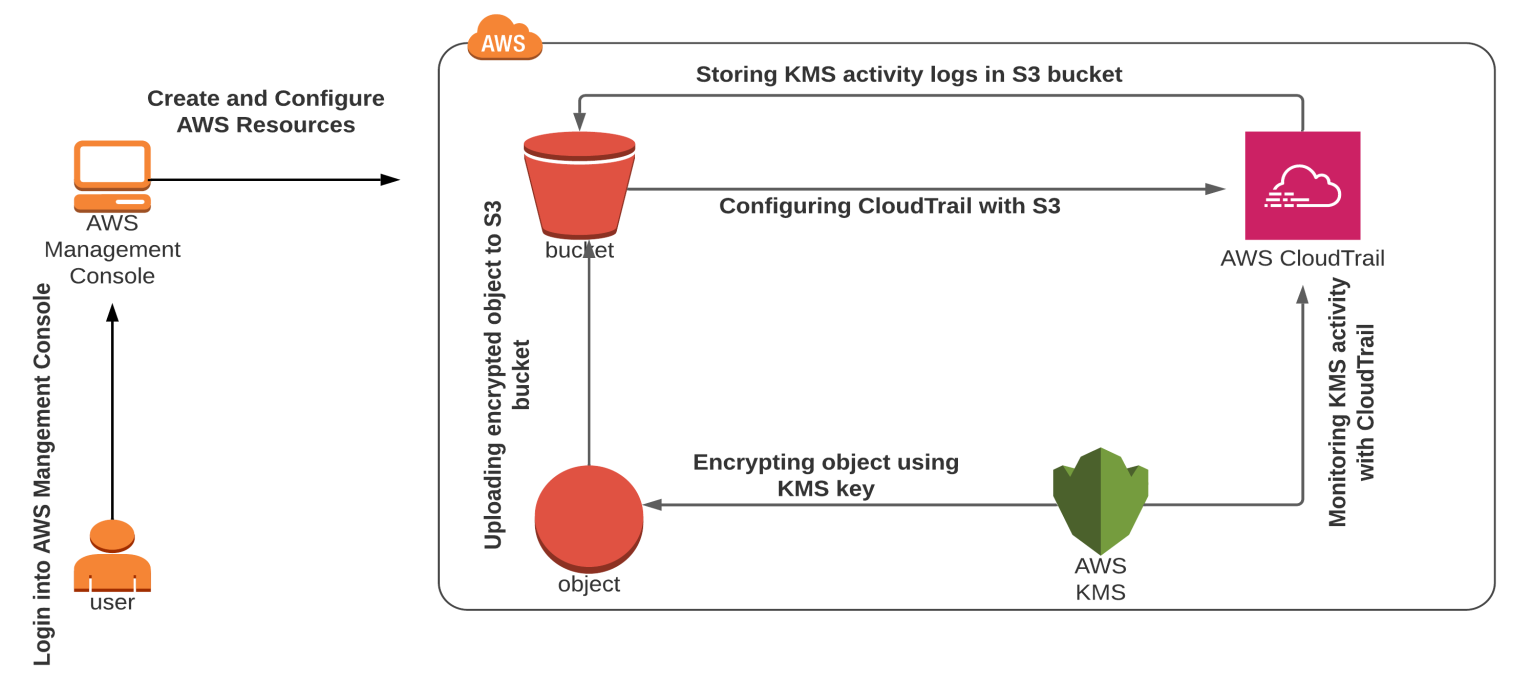
**AWS Key Management Service (KMS)**

1. AWS KMS is a managed service that makes it easy for us to create and control the encryption keys used to encrypt our data, and uses Hardware Security Modules (a hardware used for encryption keys) to protect the security of our keys.
2. AWS KMS is integrated with several other AWS services to help us protect the data we store while working with these services.
3. AWS KMS is also integrated with AWS CloudTrail to provide us with the logs of all key usage to help us meet our regulatory and compliance needs.

**AWS CloudTrail**

1. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.
2. With CloudTrail, we can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.
3. CloudTrail provides a history of all events and API calls made within our AWS account, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
4. This event history helps us with security analysis, resource change tracking, and troubleshooting.
5. Whenever a service or resource has been deleted accidentally, the first place we go and look at is AWS CloudTrail.

**Architecture Diagram**



**Task Details**

1. Sign into the AWS Management Console.
2. Create a customer managed KMS key.
3. Create an S3 bucket.
4. Create a CloudTrail and configure it to store events in S3.
5. Uploading an object and encrypting it.
6. Accessing the encrypted object.
7. Monitoring KMS activity using CloudTrail Logs.
8. Deleting AWS Resources.

**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,

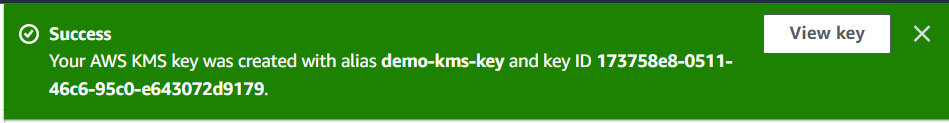
* Leave the Account ID as default. Never edit/remove the 12-digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
* Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign in** button

     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 ***demo-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: demo\_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 demo\_user-<RANDOM\_NUMBER>
10. Click on **Next**
11. Review everything and click on the **Finish**button.
12. You have successfully created the KMS key.

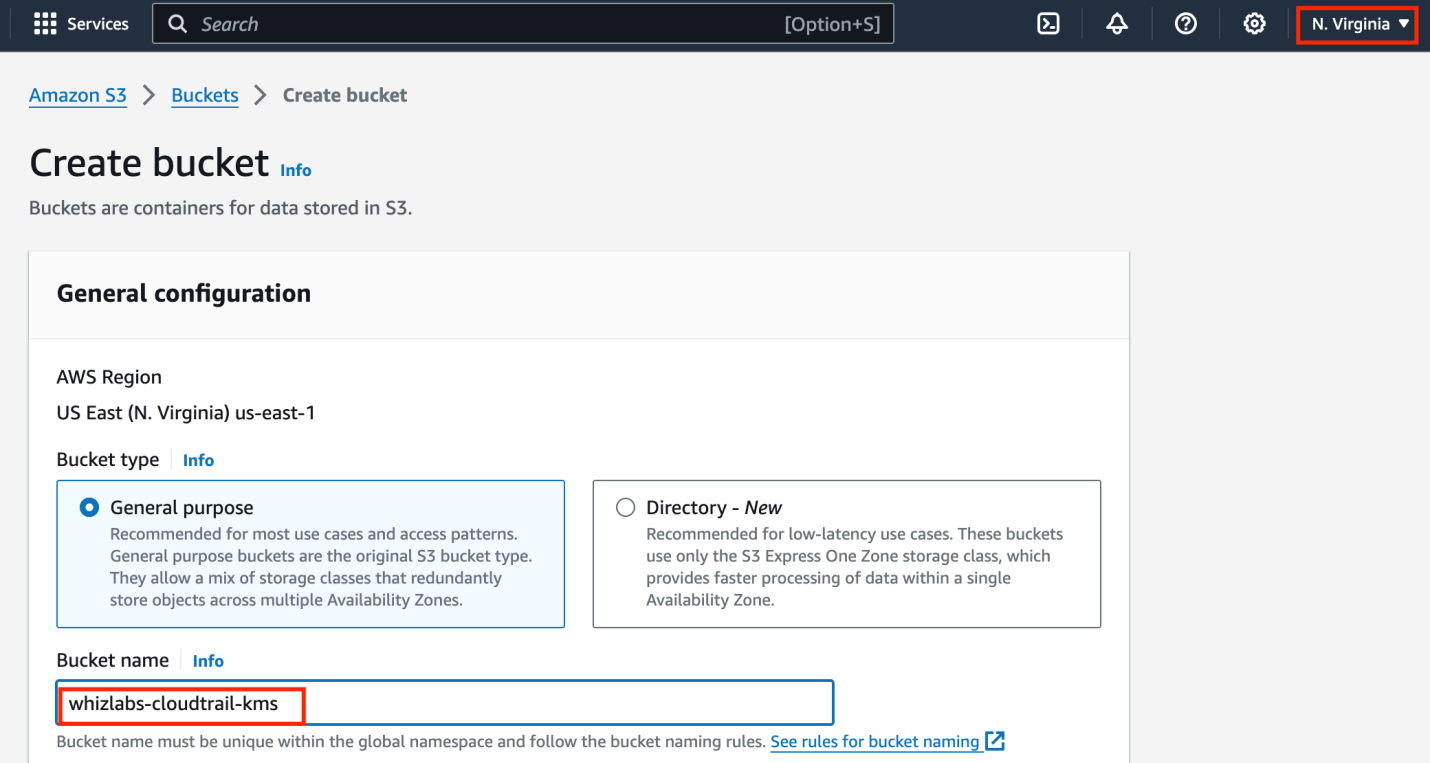


1. Copy the Key ID and paste it in the notepad, we will use this later in the lab.

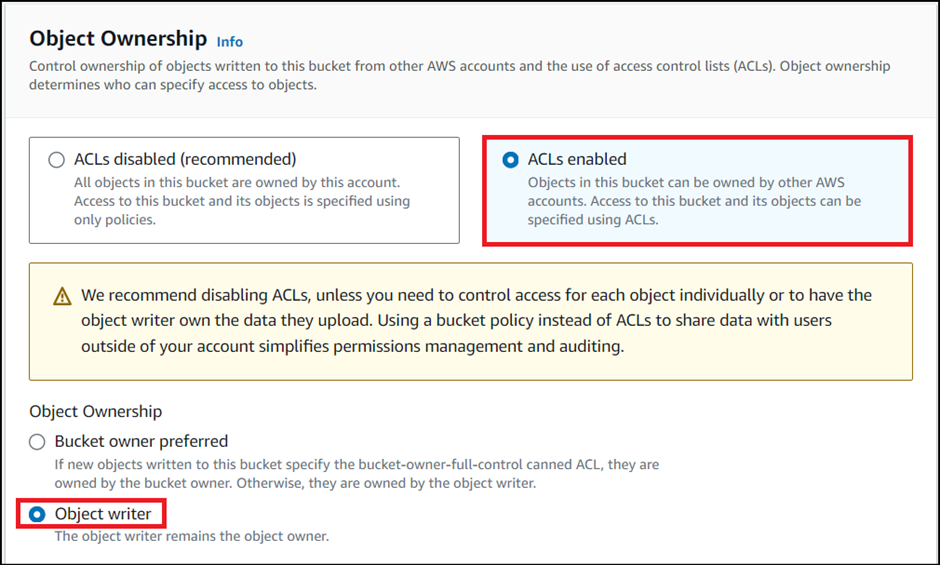
**Task 3: Create an S3 bucket**

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

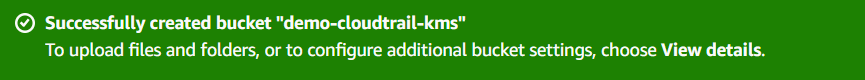
1. Navigate to S3 by clicking on **Services** in the AWS Management Console, and selecting **S3** under **Storage**section.
2. Click on **Create Bucket**
3. Under **General configuration:**
   * Note: **Bucket name must be a unique name within the global namespace.**
   * Bucket type : **General purpose**
   * Bucket name : Enter ***demo-cloudtrail-kms***



Object ownership: Select **ACLs enabled** option and choose **Object writer** as the Object owner



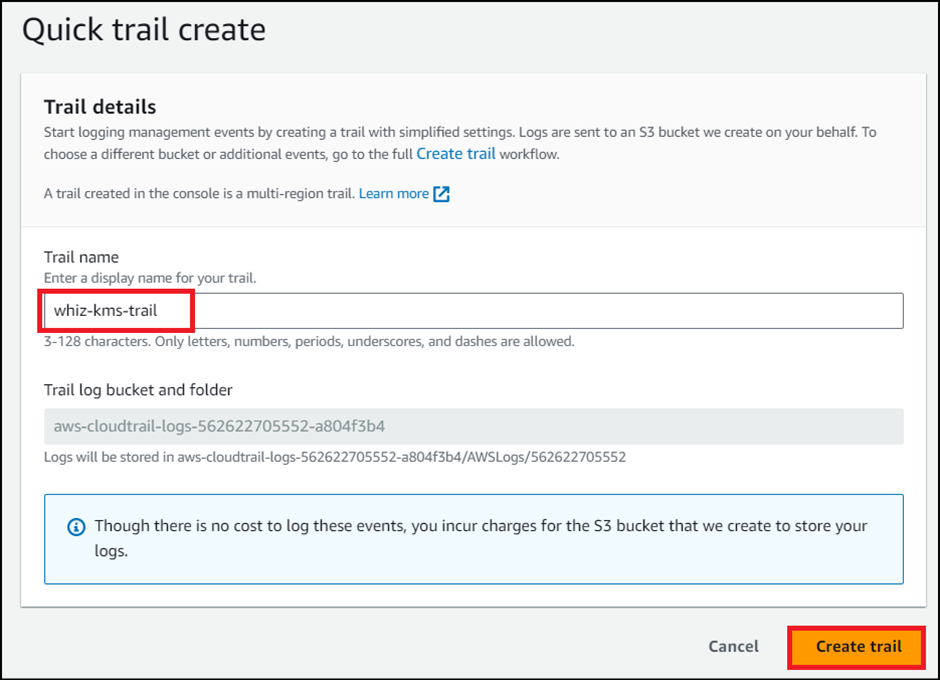
1. Leave the rest as default and click on **Create Bucket.**
2. You have successfully created an S3 bucket.



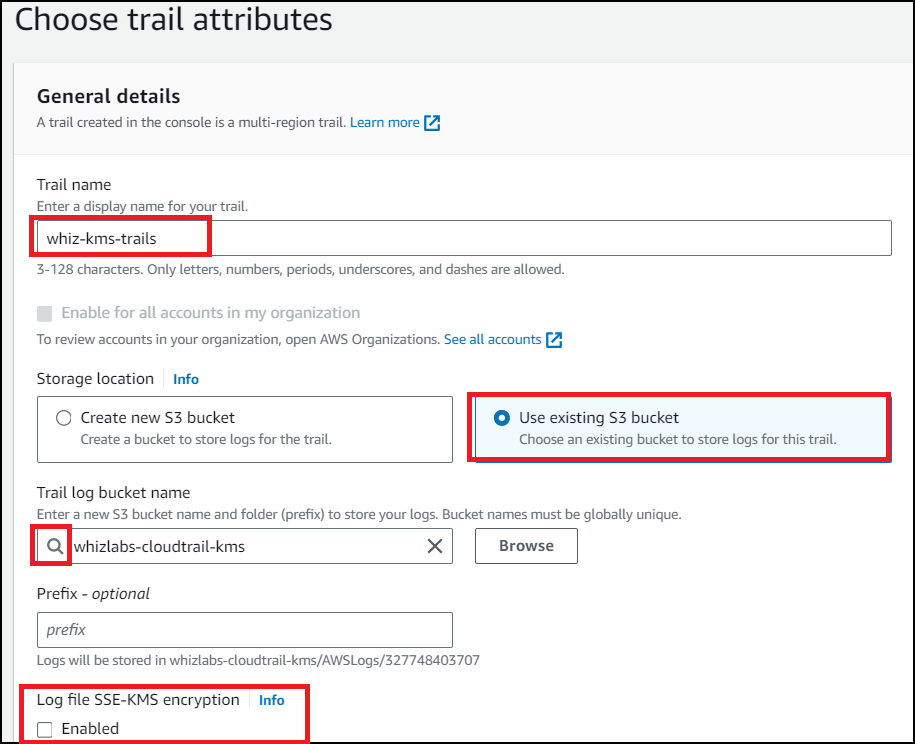
**Task 4: Create a CloudTrail and configure it to store events in S3**

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

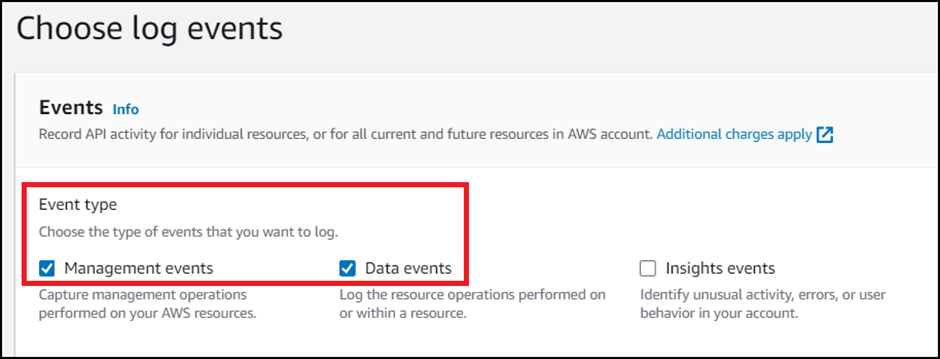
1. Navigate to CloudTrail by clicking on **Services** in the AWS Management Console, and selecting **CloudTrail**under **Management & Governance** section.
2. Click on the menu section (three lines) on the left side panel and click on **Trails**.
3. Click on **Create Trail.**



1. 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**)
2. Log file SSE-KMS encryption : **Uncheck**Enabled

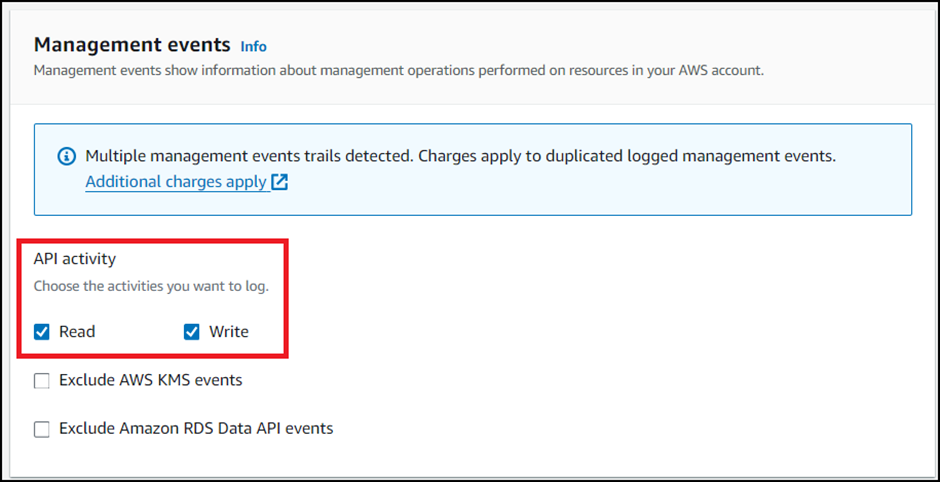


1. Leave the rest as default and click on **Next.**
2. **Choose log events:**
   * Event type : Check both **Management events** and **Data events**.



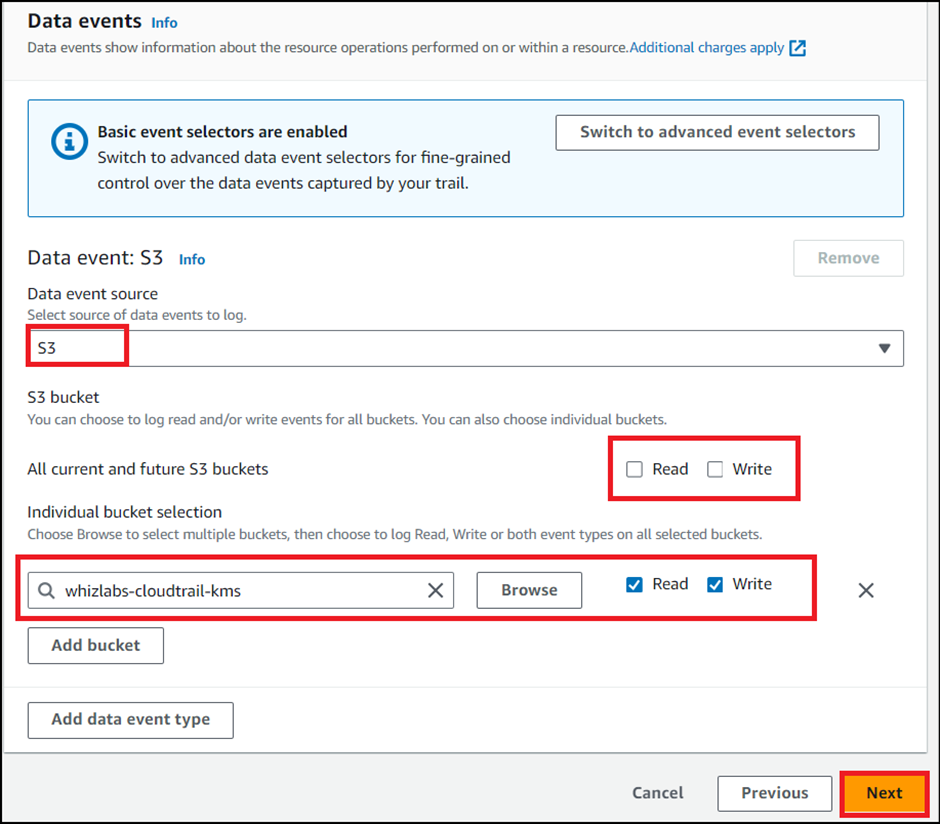
**Management events:**

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

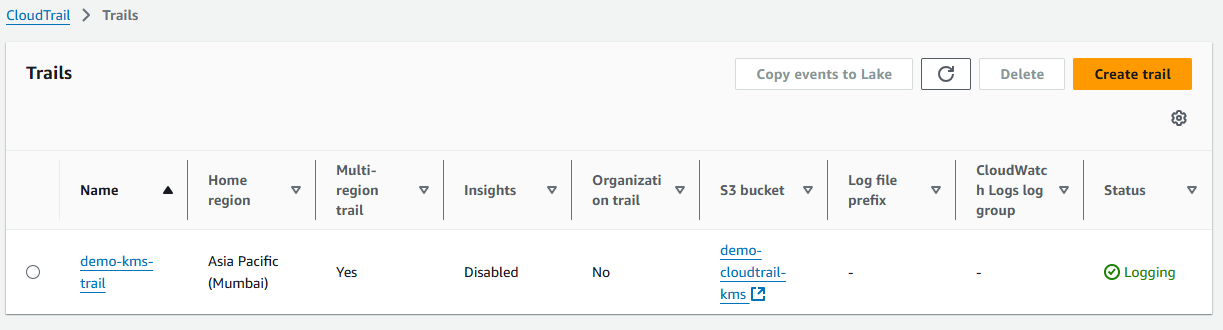


**Data events:**

* 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.



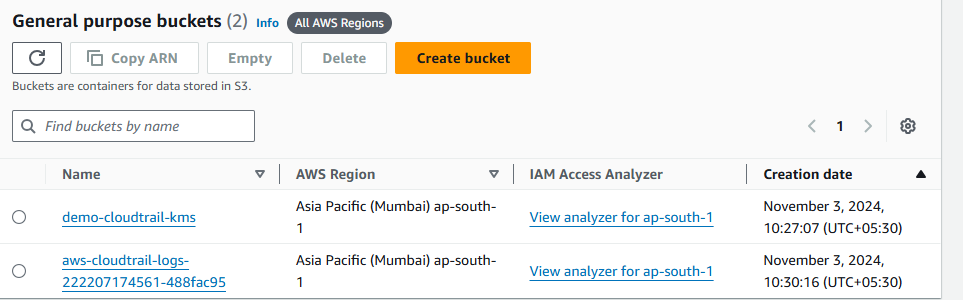
1. Click on **Next.**
2. Review everything and click on **Create Trail.**
3. You have successfully created a CloudTrail and can find yours under Trails.



**Task 5: Uploading an object and encrypting it**

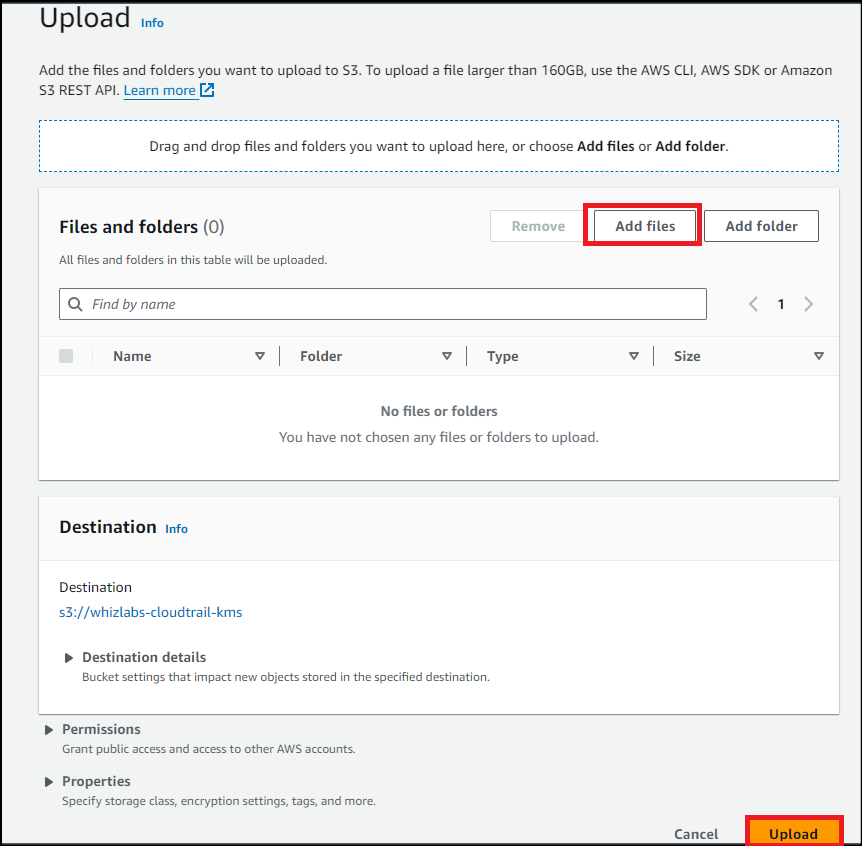
In this task, you will upload an image from our local PC and encrypt it using the KMS key we have created in Task 3.

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 **(demo-cloudtrail-kms)** we have created.

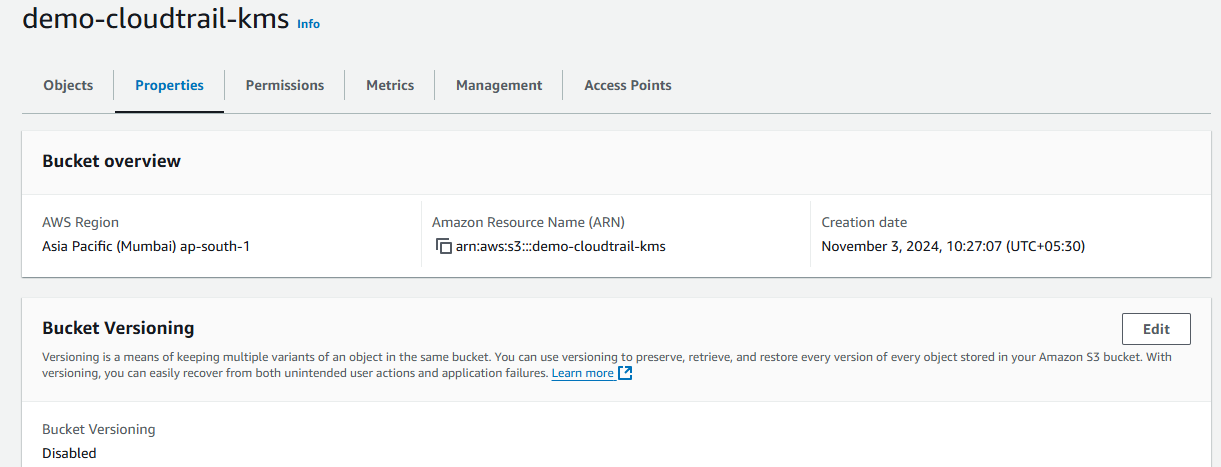
****

Click on the **Upload**button.

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

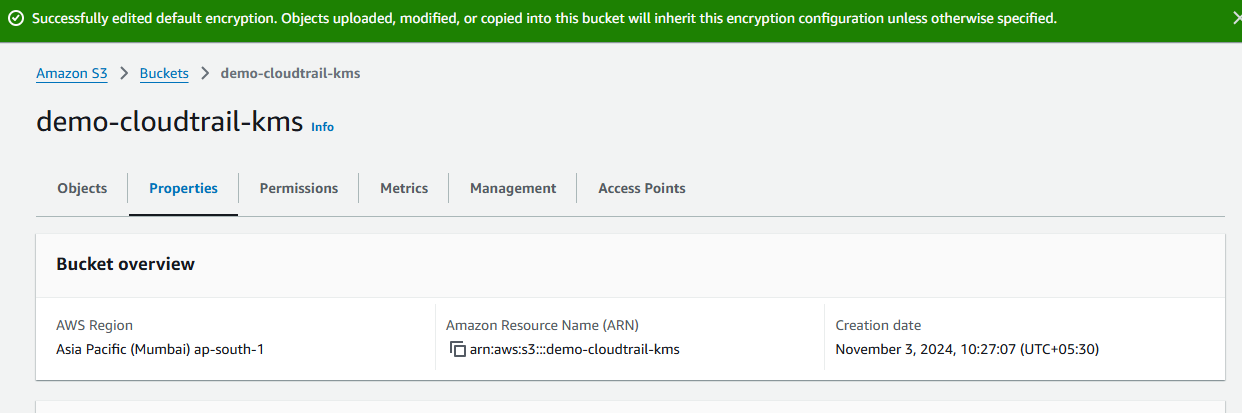


1. Click on the **object** which we have created.
2. Scroll down to **Properties** and click on it to expand.

****

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 menu select the KMS key we have created i.e **demo-kms-key**

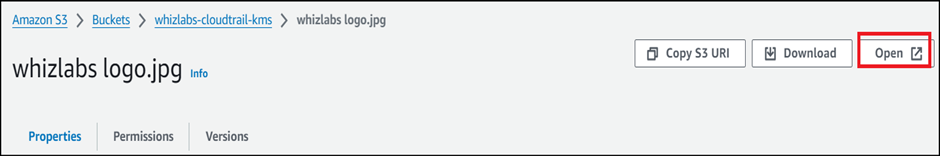
****

1. Click on the **Save Changes** button.
2. Click on close and you will see your uploaded picture under the objects section.
3. Note the Last Modified time in the notepad.

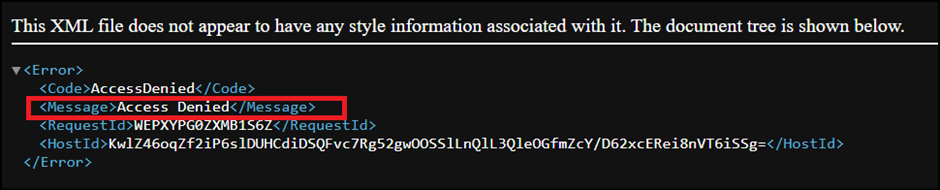
**Task 6: Accessing the encrypted object**

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

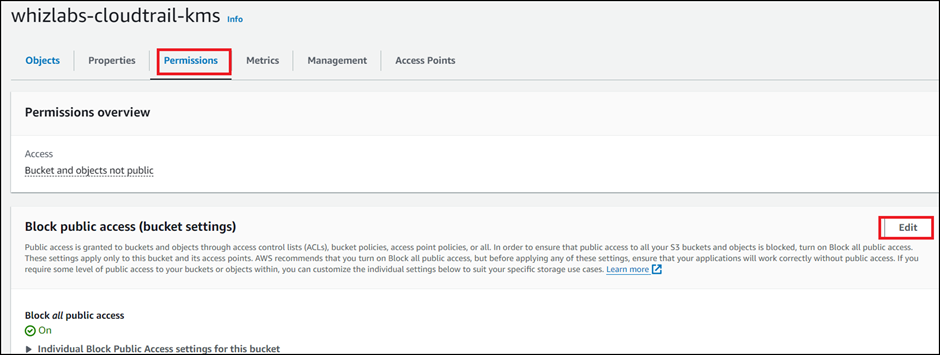
1. Click on the picture you have uploaded and click on **Open** on the top right side of your screen



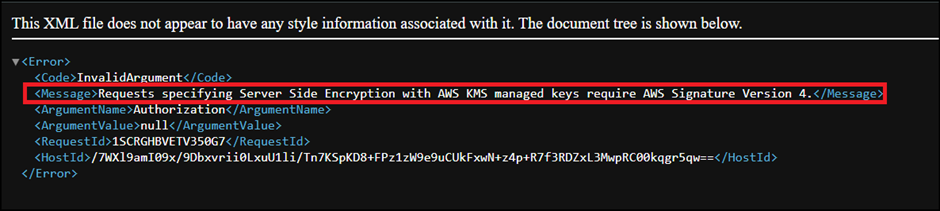
1. The picture opens in a new tab/window.
2. What happens behind the scenes
   * Amazon S3 sends the encrypted data key to AWS KMS.
   * AWS KMS decrypts the key by using the appropriate master key and sends the plaintext key back to Amazon S3.
   * Amazon S3 decrypts the cypher text and removes the plaintext data key from memory as soon as possible.
3. Close the tab/window that displayed your picture.
4. Now copy the **Object URL** and paste it into a new tab of your browser and hit Enter. [In my case : **https://demo-cloudtrail-kms.s3.amazonaws.com/elb.png**]
5. You will see a page with the message “**Access denied**.” And that is because by default, the public access is blocked.



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



1. Under Block public access, click on **Edit**and uncheck **Block all public access** and click on **Save changes**.
2. In the next screen, Type **confirm** and click on **Confirm** button.
3. You have successfully edited Block Public Access settings.
4. Now go to the Objects tab and click on your object.
5. On the top right corner, select **Make public** from the **Object actions** drop-down menu and click on **Make public** **using ACL.**
6. Click on **Make public**button.
7. Now refresh the tab where you have pasted the **Object URL** earlier.
8. You should see a message something like this.

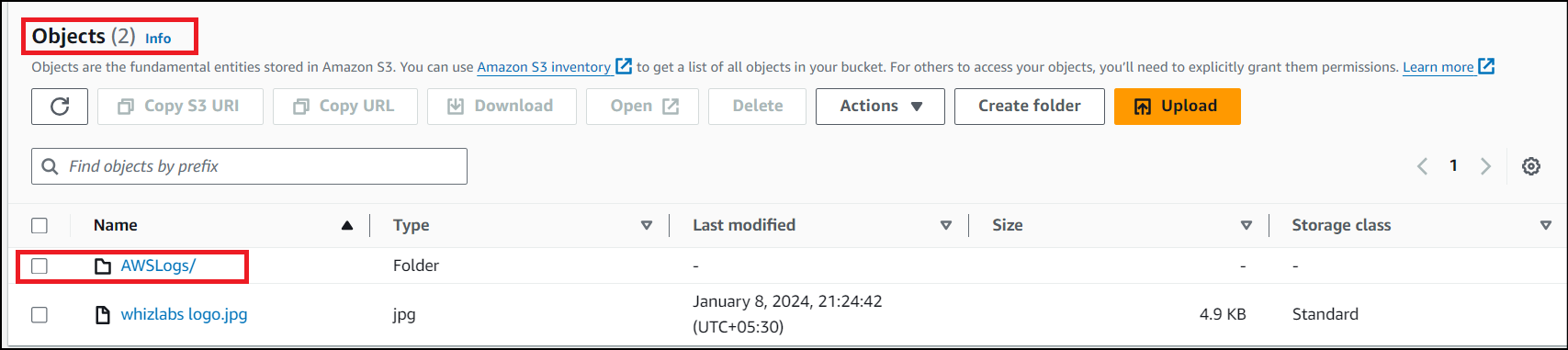


1. This is because the picture is encrypted and you are not able to view it using the public link. If you are uploading or accessing objects encrypted by SSE-KMS, you need to use AWS Signature Version 4 for added security.

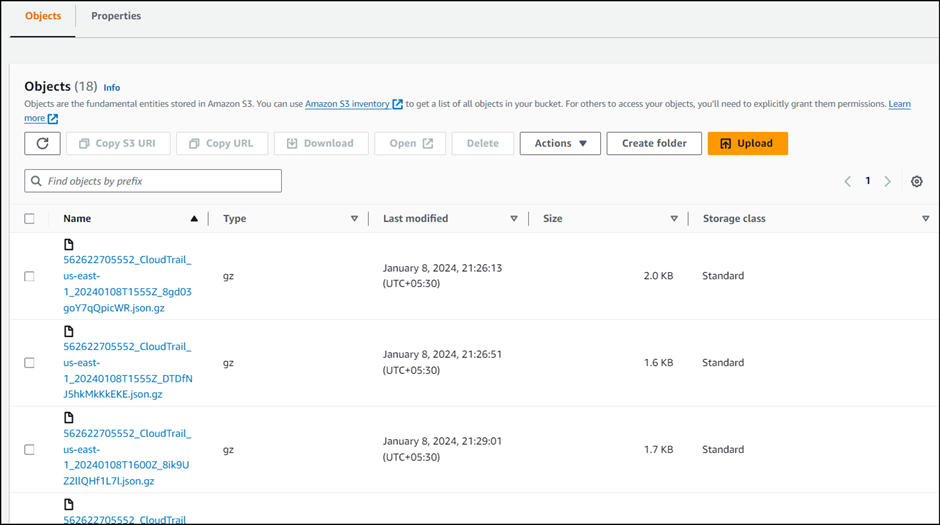
**Task 7: Monitoring KMS activity using CloudTrail Logs**

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/**.



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



1. Click on the log file whose Last modified time is greater than the timestamp of the picture when it is uploaded.(Refer your notepad)
2. 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.
3. Click on the latest log file from the list.
4. Click on **Open**.
5. Press **Ctrl+F** and search for the Key Id you have saved in the notepad and the picture name you have created.
6. 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.
7. Wait for some time and now search for the logs whose time is greater than that of what you just noted down.
8. 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 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.