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

Required Points	10
Lab Duration	00:50:00
Average Start time	Less than a minute

Start Lab →

Need help?

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

Submit Feedback | Share

Lab Overview

Cloud Architect, Cloud Security Engineer

Security, Management & Governance

Lab Details

1. This lab walks you through the AWS KMS, AWS S3 and AWS CloudTrail. You will create a custom encryption key using KMS and use it to encrypt objects S3 Bucket and configure CloudTrail to watch S3 events.
2. Duration: **50 minutes**
3. AWS Region: **US East (N. Virginia) us-east-1**

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

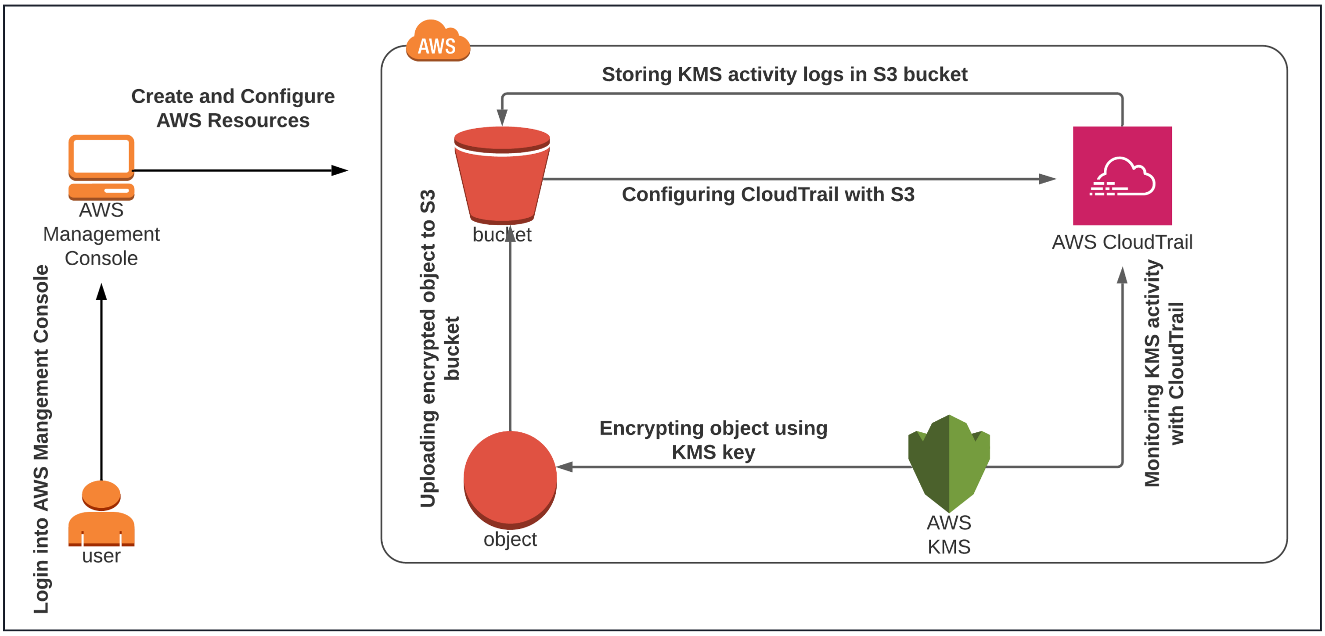
1. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.
2. With CloudTrail, we can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.
3. CloudTrail provides a history of all 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


AWS
Create and Configure AWS Resources
AWS Management Console
Login into AWS Mangement Console
user
Storing KMS activity logs in S3 bucket
Configuring CloudTrail with S3
bucket
AWS CloudTrail
Uploading encrypted object to S3 bucket
Monitoring KMS activity with CloudTrail
Encrypting object using KMS key
object
AWS KMS

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.

Launching Lab Environment

1. To launch the lab environment, Click on the **Start Lab** button.

2. Please wait until the cloud environment is provisioned. It will take less than a minute to provision.
3. Once the Lab is started, you will be provided with **IAM user name**, **Password**, **Access Key**, and **Secret Access Key**.

Note : You can only start one lab at any given time.