Experiment 5 - Introduction to AWS Key Management Service(KMS)

In this lab, you will learn how to:

- Create an Encryption Key
- Create an S3 bucket with CloudTrail logging functions
- Encrypt data stored in an S3 bucket using an encryption key
- Monitor encryption key usage using CloudTrail
- Manage encryption keys for users and roles

What is KMS?

Identity and access management (IAM) is a framework of business processes, policies and technologies AWS Key Management Service (AWS KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
AWS KMS page
AWS KMS Talk

What is AWS Cloudtrail?

AWS CloudTrail is a service that helps us to monitor, survey, and perform operation auditing along with risk monitoring of the AWS account the user uses. With AWS CloudTrail, the user will be able to log, ceaselessly monitor, and retain account activity associated with actions across the AWS infrastructure.

CloudTrail provides the complete account activity of the Amazon Web Services. CloudTrail also manages the functions performed with the help of the AWS Management Console, program line tools, AWS SDKs, and various AWS services.

This event history simplifies security analysis, resource amendment trailing, and troubleshooting.
AWS Cloudtrail page

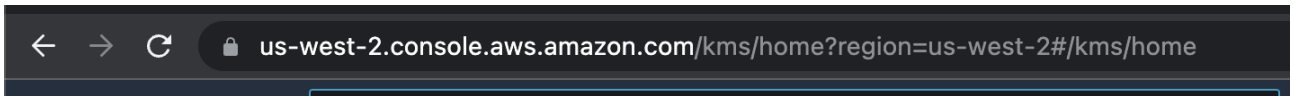
Introduction to Qwiklabs:

Qwiklabs is an online platform that provides end-to-end training in Cloud Services. This is a platform where you can learn in a live environment anywhere, anytime, and on any device. Qwiklabs offers training through various Labs which are specially designed to get you trained in Google Cloud Platform (GCP) as well as Amazon Web Services (AWS). In this course, we will be working with labs that familiarize you with AWS.

Points to note:

1. Qwiklabs will create a temporary AWS account with all the required permissions and access to complete the lab. Do NOT use your personal AWS account**.** To prevent conflicts with any AWS account that you have already signed into on your browser, use Incognito/Private mode.
2. When using the Qwiklabs created AWS account, DO NOT change the default region/ VPC or any other settings that are automatically created by Qwiklabs.
3. The Qwiklabs lab session is timed. After the time limit is reached/ timer runs out, the AWS account will be removed and you'll have to restart the lab from scratch.
4. All code and configuration for the Qwiklabs lab have already been given. The lab experiments do not need you to code anything from scratch or deviate from this. However, in some instances, you may have to name the resources you avail of differently, as instructed.
5. DO NOT try to access or avail of any other resources and services that have not been described in the lab session or your account will be blocked.
6. Ensure that you have signed into Qwiklabs from your Google account.

Note down your region when you start the experiment and open AWS. It'll be useful in the experiment later. In the below image, the region is us-west-2.



Deliverables:

The following screenshots are to be submitted:

a. 1a.png: Showing KMS key created. The name of the alias should be: `<Your SRN>` Eg: `pes1201900001`.
b. 2a.png: Showing the configured CloudTrail named `<Your SRN>-trail`.
c. 3a.png: Showing the configured bucket named `mycloudtrailbucketXXXX`. where XXXX are the last 4 digits of your SRN. You can pad it with 0s if you have less than 4 digits.
d. 4a.png: Showing the "Access Denied" page when you open the link to the image stored in the bucket.
e. 4b.png: Showing the "Requests specifying Server Side Encryption with AWS KMS managed keys require AWS Signature Version 4" page when you open the link to the image stored in the bucket.
f. 5a.png: Showing the key-id being present in the json we get from .gzip'ed cloud trail logs.
g. 6a.png: Showing the state of key users after the user has been removed.
h. 6b.png: Showing the state of key users after the user has been added.

For evaluation:

The submission has 2 parts:

1. Word doc - add all screenshots, file name: your-srn.doc/docx
2. Zip file - The zip file contains only the screenshots, no word document. There should be no subfolders within the zip file. No other file extension other than .zip will be considered. file name: your-srn.zip

Click on the following link to go to the Qwiklabs lab: Introduction to Amazon Key Management Service

Read and follow the instructions carefully to complete the lab.
