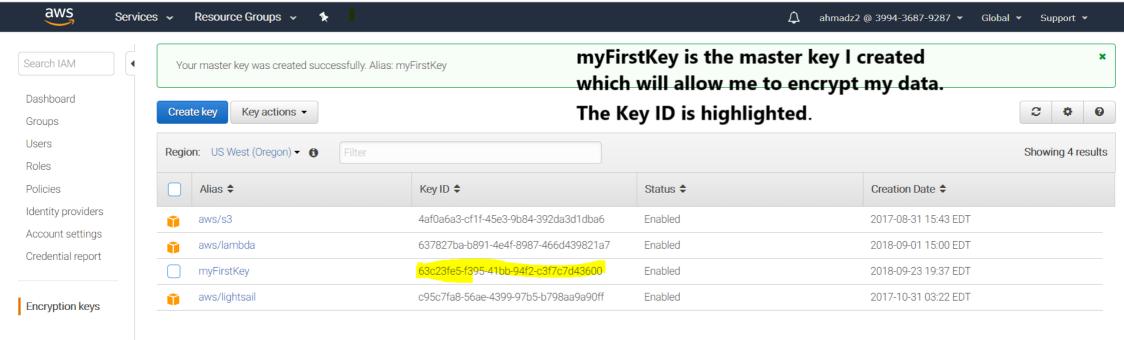# Introduction to AWS Key Management Service

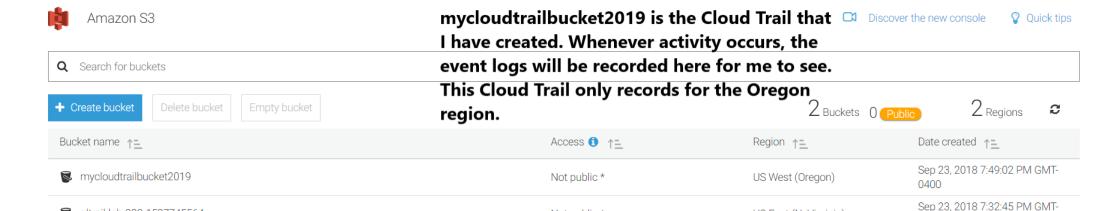In this lab, I will be demonstrating the features of AWS Key Management Service (KMS) including:

- Creating Keys
- Assigning Management and Usage Permissions
- Encrypting Data
- Monitoring Access and Usage of Keys

AWS KMS allows you to have centralized control over all your encryption keys. KMS allows you to create, import, rotate, disable, delete and define usage policies for all encryption keys. AWS KMS also include CloudTrail which allows you the with ability to audit and view logs of all events related to your keys.

Topics Covered:

- Create an Encryption Key
- Create an S3 Bucket with CloudTrail Logging Functions
- Encrypt Data stored in an S3 bucket using Encryption Key
- Monitor encryption key usage via CloudTrail
- Manage Encryption Keys for Users and Roles

Search IAM

Your master key was created successfully. Alias: myFirstKey   ✕

myFirstKey is the master key I created which will allow me to encrypt my data. The Key ID is highlighted.

Dashboard

Groups

Create key   Key actions ▾   🔄 ⚙️ ❓

Users

Roles

	Region: US West (Oregon) ▾ ⓘ	Filter		Showing 4 results

Policies

Identity providers

Account settings

Credential report

☐	Alias ⬍	Key ID ⬍	Status ⬍	Creation Date ⬍
📦	aws/s3	4af0a6a3-cf1f-45e3-9b84-392da3d1dba6	Enabled	2017-08-31 15:43 EDT
📦	aws/lambda	637827ba-b891-4e4f-8987-466d439821a7	Enabled	2018-09-01 15:00 EDT
☐	myFirstKey	63c23fe5-f395-41bb-94f2-c3f7c7d43600	Enabled	2018-09-23 19:37 EDT
📦	aws/lightsail	c95c7fa8-56ae-4399-97b5-b798aa9a90ff	Enabled	2017-10-31 03:22 EDT

Encryption keys

Amazon S3

mycloudtrailbucket2019 is the Cloud Trail that I have created. Whenever activity occurs, the event logs will be recorded here for me to see. This Cloud Trail only records for the Oregon region.

Search for buckets

+ Create bucket | Delete bucket | Empty bucket

2 Buckets 0 Public 2 Regions ⟳

Bucket name ↑=	Access 🛈 ↑=	Region ↑=	Date created ↑=
🪣 mycloudtrailbucket2019	Not public *	US West (Oregon)	Sep 23, 2018 7:49:02 PM GMT-0400
🪣 qltrail-lab-220-1537745564	Not public *	US East (N. Virginia)	Sep 23, 2018 7:32:45 PM GMT-0400

* Objects might still be publicly accessible due to object ACLs. Learn more

Picture1.png   Latest version ▼

This is the image I uploaded to my cloud trail bucket. This image is encrypted using the Master Key I created before. It also gives me timestamp for when the image is last modified and a link to decrypt and view the image.

Overview	Properties	Permissions	Select from

Open   Download   Download as   Make public   Copy path

Owner
aws08193

Last modified
Sep 23, 2018 7:51:33 PM GMT-0400

Etag
5b9eabb786d15938ba928b734c8691e7

Storage class
Standard

Server-side encryption
AWS-KMS

KMS key ID
arn:aws:kms:us-west-2:399436879287:key/63c23fe5-f395-41bb-94f2-c3f7c7d43600

Size
208229

Link
https://s3-us-west-2.amazonaws.com/mycloudtrailbucket2019/Picture1.png

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

```xml
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>F10B33B68925B618</RequestId>
 ▼<HostId>
     2r8PnezqPLYdgIL/Qd4Z8DT07yErWMIqxJVWLn/Lr835xHUzQK/6f45YQhM5C65itY89zeVDchY=
   </HostId>
 </Error>
```

I am receiving an Access Denied error because I am trying to access my encrypted image using a public link. In order to access, my image I need to use AWS Signature Version 4.

{"Records":[{"eventVersion":"1.05","userIdentity":{"type":"FederatedUser","principalId":"399436879287:ahmadz2","arn":"arn:aws:sts::399436879287:federated-user/ahmadz2","accountId":"399436879287","accessKeyId":"ASIAIT4DWICAYWJEIHVQ","sessionContext":{"attributes":{"mfaAuthenticated":"false","creationDate":"2018-09-23T23:32:54Z"},"sessionIssuer":{"type":"IAMUser","principalId":"AIDAJ2T325DHXLNUFVO7K","arn":"arn:aws:iam::399436879287:user/awsstudent","accountId":"399436879287","userName":"awsstudent"}},"invokedBy":"AWS Internal"},"eventTime":"2018-09-23T23:51:32Z","eventSource":"kms.amazonaws.com","eventName":"GenerateDataKey","awsRegion":"us-west-2","sourceIPAddress":"AWS Internal","userAgent":"AWS Internal","requestParameters":{"keyId":"63c23fe5-f395-41bb-94f2-c3f7c7d43600","keySpec":"AES_256","encryptionContext":{"aws:s3:arn":"arn:aws:s3:::mycloudtrailbucket2019/Picture1.png"}},"responseElements":null,"requestID":"0cc8c041-7ac2-43ad-a8bc-dd2fc0e8154a","eventID":"a62e141a-c591-42a8-8279-142e9b963051","readOnly":true,"resources":[{"ARN":"arn:aws:kms:us-west-2:399436879287:key/63c23fe5-f395-41bb-94f2-c3f7c7d43600","accountId":"399436879287","type":"AWS::KMS::Key"}],"eventType":"AwsApiCall","recipientAccountId":"399436879287"},{"eventVersion":"1.05","userIdentity":{"type":"FederatedUser","principalId":"399436879287:ahmadz2","arn":"arn:aws:sts::399436879287:federated-user/ahmadz2","accountId":"399436879287","accessKeyId":"ASIAV2ACLCW32UVILDX7","sessionContext":{"attributes":{"mfaAuthenticated":"false","creationDate":"2018-09-23T23:32:54Z"},"sessionIssuer":{"type":"IAMUser","principalId":"AIDAJ2T325DHXLNUFVO7K","arn":"arn:aws:iam::399436879287:user/awsstudent","accountId":"399436879287","userName":"awsstudent"}}},"eventTime":"2018-09-23T23:48:19Z","eventSource":"kms.amazonaws.com","eventName":"ListKeys","awsRegion":"us-west-2","sourceIPAddress":"75.75.49.81","userAgent":"AWSCloudTrail, aws-internal/3 aws-sdk-java/1.11.408 Linux/4.9.119-0.1.ac.277.71.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.181-b13 java/1.8.0_181","requestParameters":null,"responseElements":null,"requestID":"b64e79d1-4f08-45fb-b023-0c3e5a462f92","eventID":"a7dec089-5d73-478f-8249-b841081eda8a","readOnly":true,"resources":[],"eventType":"AwsApiCall","recipientAccountId":"399436879287"},{"eventVersion":"1.05","userIdentity":{"type":"FederatedUser","principalId":"399436879287:ahmadz2","arn":"arn:aws:sts::399436879287:federated-user/ahmadz2","accountId":"399436879287","accessKeyId":"ASIAV2ACLCW32UVILDX7","sessionContext":{"attributes":{"mfaAuthenticated":"false","creationDate":"2018-09-23T23:32:54Z"},"sessionIssuer":{"type":"IAMUser","principalId":"AIDAJ2T325DHXLNUFVO7K","arn":"arn:aws:iam::399436879287:user/awsstudent","accountId":"399436879287","userName":"awsstudent"}}},"eventTime":"2018-09-23T23:48:18Z","eventSource":"kms.amazonaws.com","eventName":"ListAliases","awsRegion":"us-west-2","sourceIPAddress":"75.75.49.81","userAgent":"AWSCloudTrail, aws-internal/3 aws-sdk-java/1.11.408 Linux/4.9.119-0.1.ac.277.71.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.181-b13 java/1.8.0_181","requestParameters":null,"responseElements":null,"requestID":"c34997e9-e66d-4eaa-8f27-2ccd9c58628a","eventID":"74787f75-8a12-4357-b5be-effab9418761","readOnly":true,"resources":[],"eventType":"AwsApiCall","recipientAccountId":"399436879287"},{"eventVersion":"1.05","userIdentity":{"type":"FederatedUser","principalId":"399436879287:ahmadz2","arn":"arn:aws:sts::399436879287:federated-user/ahmadz2","accountId":"399436879287","accessKeyId":"ASIAV2ACLCW3QYGGDTXJ","sessionContext":{"attributes":{"mfaAuthenticated":"false","creationDate":"2018-09-23T23:32:54Z"},"sessionIssuer":{"type":"IAMUser","principalId":"AIDAJ2T325DHXLNUFVO7K","arn":"arn:aws:iam::399436879287:user/awsstuden
23T23:51:31Z","eventSource":"s3.amazonaws.com","eventName":"GetBucketEncryption","awsRegion":"us-west-
Linux/3.2.45-0.6.wd.971.49.326.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.181-b13 java/1.8.0_181]","err
configuration was not found","requestParameters":{"encryption":[""],"bucketName":"mycloudtrailbucket201
2049b349"},"requestID":"758AAC4D13330688","eventID":"c0af73c8-7ed2-45c3-a552-d13e860aa830","eventType
23T23:51:09Z","eventSource":"ec2.amazonaws.com","eventName":"DescribeInstances","awsRegion":"us-west-2
linux","requestParameters":{"instancesSet":{},"filterSet":{"items":[{"name":"instance-state-name","val
"value":"stopped"}]}}]}},"responseElements":null,"requestID":"7ceabfb3-7bde-46d2-ab8e-474ae9bb7811","
a5798598864e","eventType":"AwsApiCall","recipientAccountId":"399436879287"},{"eventVersion":"1.05","us
{"type":"FederatedUser","principalId":"399436879287:ahmadz2","arn":"arn:aws:sts::399436879287:federate
{"attributes":{"mfaAuthenticated":"false","creationDate":"2018-09-23T23:32:54Z"},"sessionIssuer":
{"type":"IAMUser","principalId":"AIDAJ2T325DHXLNUFVO7K","arn":"arn:aws:iam::399436879287:user/awsstudent","accountId":"399436879287","userName":"awsstudent"}}},"eventTime":"2018-09-23T23:49:12Z","eventSource":"s3.amazonaws.com","eventName":"GetBucketVersioning","awsRegion":"us-west-2","sourceIPAddress":"75.75.49.81","userAgent":"[S3Console/0.4, aws-internal/3 aws-sdk-java/1.11.408 Linux/3.2.45-0.6.wd.971.49.326.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.181-b13 java/1.8.0_181]","requestParameters":{"bucketName":"mycloudtrailbucket2019","versioning":[""]},"responseElements":null,"additionalEventData":{"vpcEndpointId":"vpce-2049b349"},"requestID":"2B74C0D42E8BF280","eventID":"6f370be1-22ce-4ecd-8356-532d954eda2c","eventType":"AwsApiCall","recipientAccountId":"399436879287","vpcEndpointId":"vpce-2049b349"},{"eventVersion":"1.05","userIdentity":{"type":"FederatedUser","principalId":"399436879287:ahmadz2","arn":"arn:aws:sts::399436879287:federated-user/ahmadz2","accountId":"399436879287","accessKeyId":"ASIAV2ACLCW32UVILDX7","sessionContext":{"attributes":{"mfaAuthenticated":"false","creationDate":"2018-09-23T23:32:54Z"},"sessionIssuer":{"type":"IAMUser","principalId":"AIDAJ2T325DHXLNUFVO7K","arn":"arn:aws:iam::399436879287:user/awsstudent","accountId":"399436879287","userName":"awsstudent"}}},"eventTime":"2018-09-23T23:48:51Z","eventSource":"kms.amazonaws.com","eventName":"ListAliases","awsRegion":"us-west-2","sourceIPAddress":"75.75.49.81","userAgent":"AWSCloudTrail, aws-internal/3 aws-sdk-java/1.11.408 Linux/4.9.119-0.1.ac.277.71.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.181-b13 java/1.8.0_181","requestParameters":null,"responseElements":null,"requestID":"e26eb416-7496-40cf-8ec0-696c41ae5d69","eventID":"3f0c8ef5-2623-4dc8-933c-6c2ee2c5fc5d","readOnly":true,"resources":[],"eventType":"AwsApiCall","recipientAccountId":"399436879287"},{"eventVersion":"1.05","userIdentity":{"type":"FederatedUser","principalId":"399436879287:ahmadz2","arn":"arn:aws:sts::399436879287:federated-user/ahmadz2","accountId":"399436879287","accessKeyId":"ASIAV2ACLCW32UVILDX7","sessionContext":{"attributes":{"mfaAuthenticated":"false","creationDate":"2018-09-23T23:32:54Z"},"sessionIssuer":{"type":"IAMUser","principalId":"AIDAJ2T325DHXLNUFVO7K","arn":"arn:aws:iam::399436879287:user/awsstudent","accountId":"399436879287","userName":"awsstudent"}}},"eventTime":"2018-09-

Because I created a Cloud Trail Bucket earlier which logged all events, this is one of the log files that was created in that bucket. This was the latest log file. This log shows a request by S3 -- I have highlighted the image name (this is what is being encrypted) -- I have also highlighted the KeyID (this is encryption key being used to encrypt the image).