



lab



lab title

Encryption on AWS

V1.01



Course title

BackSpace Academy
AWS Certified Associate



Table of Contents

Contents

Table of Contents1

About the Lab.....2

Creating an Encryption Key.....3

Using Encryption Keys with Amazon S3.....6

 Clean Up.....8

About the Lab

Please note that not all AWS services are supported in all regions. Please use the US-East-1 (North Virginia) region for this lab.

These lab notes are to support the hands on instructional videos of the Key Management Service (KMS) section of the AWS Certified Associate Course.

Please note that AWS services change on a weekly basis and it is extremely important you check the version number on this document to ensure you have the latest version with any updates or corrections.

Creating an Encryption Key

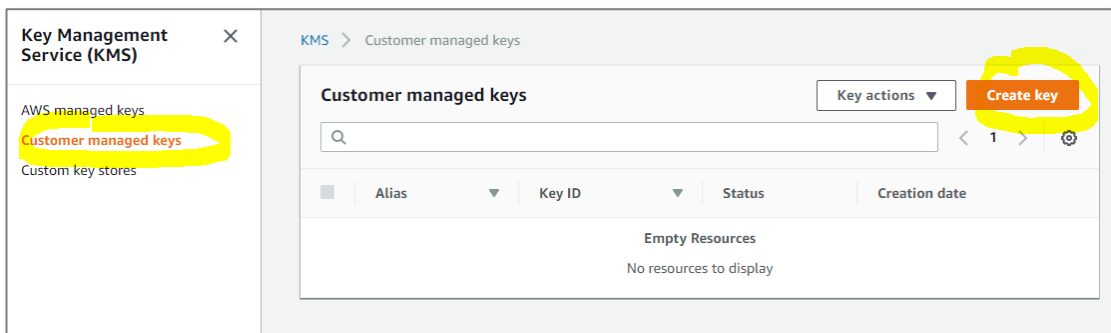
In this section, we will use the Key Management Service (KMS) to create an encryption key to use with AWS services.

From the AWS console click 'Services'

Select 'Key Management Service'

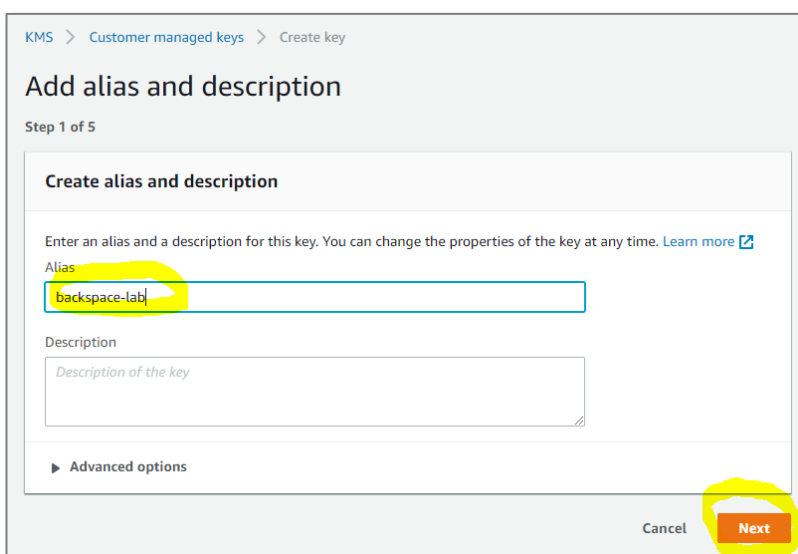
Select *Customer managed keys*

Click *Create key*



Give your key a name

Click *Next*



Leave Tags as is

Click *Next step*

Select users that will have permission to administer the key.

Click *Next*

Define key administrative permissions

Step 3 of 5

Key administrators

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

< 1 2 3 >

<input type="checkbox"/>	Name	Path	Type
<input checked="" type="checkbox"/>	pcoady	/	User

Select users that will have permission to use the key.

Click *Next step*

Define key usage permissions

Step 4 of 5

This account

Select the IAM users and roles that can use the CMK to encrypt and decrypt data with the AWS KMS API. [Learn more](#)

< 1 2 3 >

<input type="checkbox"/>	Name	Path	Type
<input checked="" type="checkbox"/>	pcoady	/	User

Click *Finish*

Review and edit key policy

Step 5 of 5

```
1 {
2   "Id": "key-consolepolicy-3",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Enable IAM User Permissions",
7       "Effect": "Allow",
8       "Principal": {
9         "AWS": "arn:aws:iam::361919435810:root"
10      },
11      "Action": "kms:*",
12      "Resource": "*"
13    },
14    {
15      "Sid": "Allow access for Key Administrators",
```

Cancel Previous **Finish**

Your key has been created

Success

Your customer master key was created with alias [backspace-lab](#) and key ID [b37f025b-f0b5-4826-abf0-6ce4c031ff2c](#).

KMS > Customer managed keys

Customer managed keys

Key actions

Create key

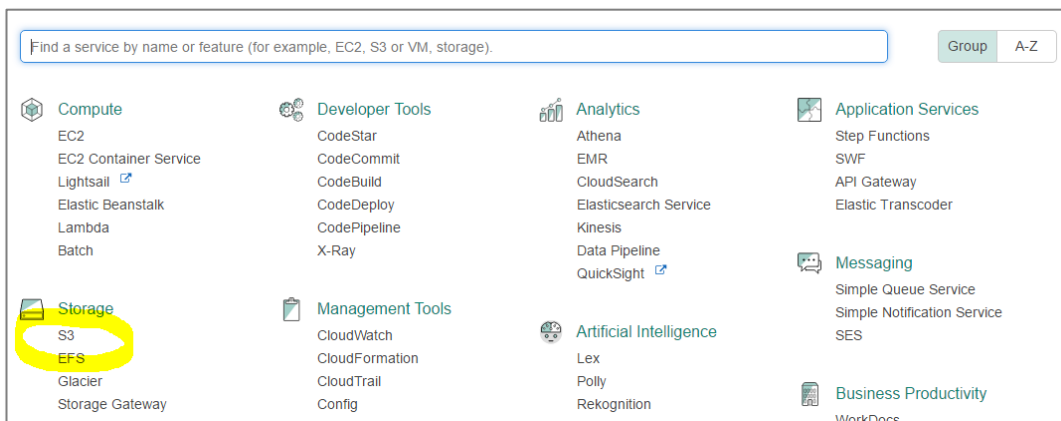
< 1 >

	Alias <div></div>	Key ID <div></div>	Status	Creation date
<input type="checkbox"/>	backspace-lab	b37f025b-f0b5-4826-abf0-6ce4c031ff2c	Enabled	Oct 22, 2019 03:41 GMT+11

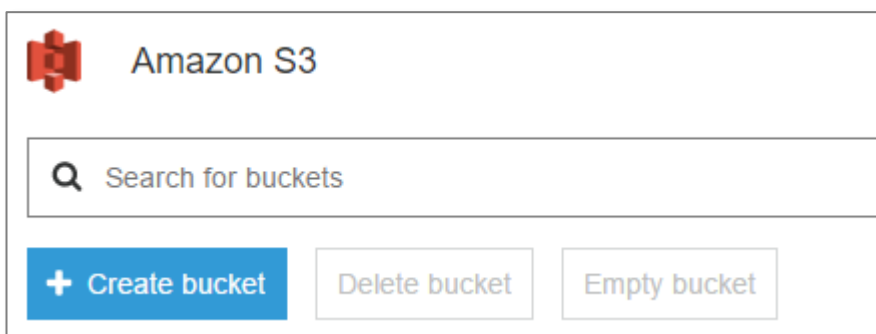
Using Encryption Keys with Amazon S3

In this section, we will use the key we created to automatically encrypt objects in a bucket.

Click on the services menu and select S3.



Click on Create Bucket



The create bucket dialog box will appear.

Enter a unique name for your bucket (it will need to be different from the one below)

Click 'Next'

Create bucket

1 Name and region 2 Set properties 3 Set permissions 4 Review

Name and region

Bucket name ⓘ
test-encryption-tutorial

Region
US East (N. Virginia) ▼

Copy settings from an existing bucket

Select bucket (optional) 1 Buckets ▼

Create Cancel **Next**

Scroll down and click on *Default encryption*

Select **AWS-KMS**

Select the key you created from the drop down list

Click *Save*

Default encryption

☐ None

☐ AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

☒ **AWS-KMS**
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Select a key ▼

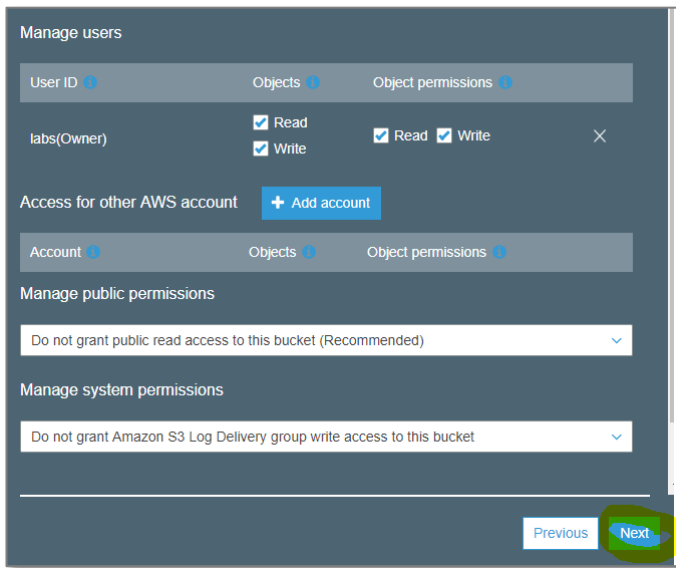
Type to search 🔍

aws/s3
backspace-lab

Click *Next*

Leave permissions as private

Click *Next*

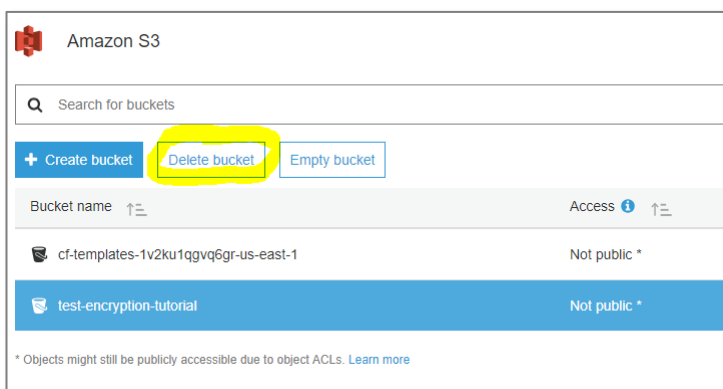


Click *Create bucket*

Now any objects uploaded to this bucket will automatically be encrypted. Any objects downloaded from S3 will be automatically decrypted.

Clean Up

Delete the bucket from the S3 management console



Schedule key deletion from the IAM console

