



lab



lab title

Encryption on AWS
V1.00



Course title

BackSpace Academy
AWS Certified Associate



Table of Contents

Contents

Table of Contents.....	1
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.

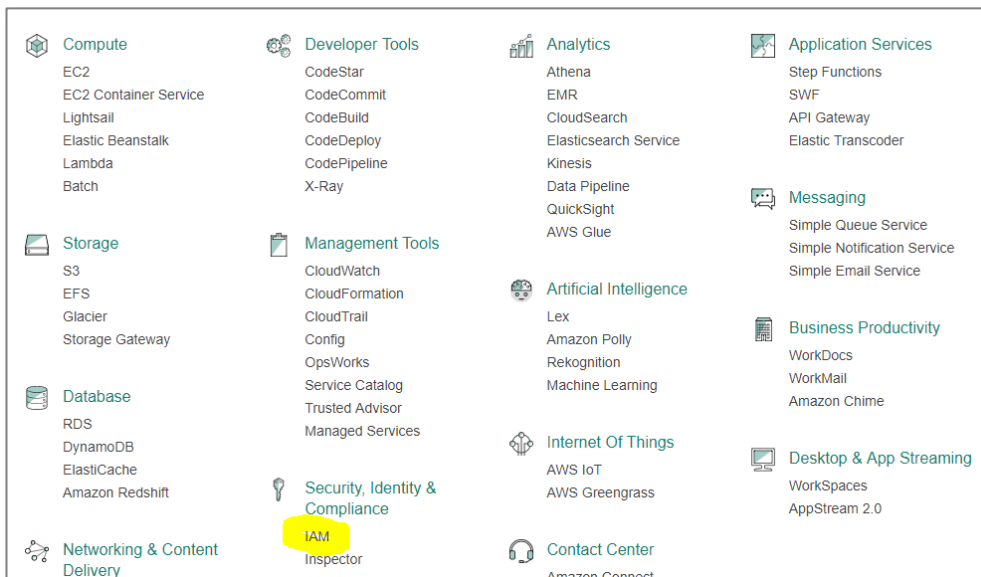
Please note that AWS services change on a weekly basis and it is extremely important you check the version number on this document to ensure you have the latest version with any updates or corrections.

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.

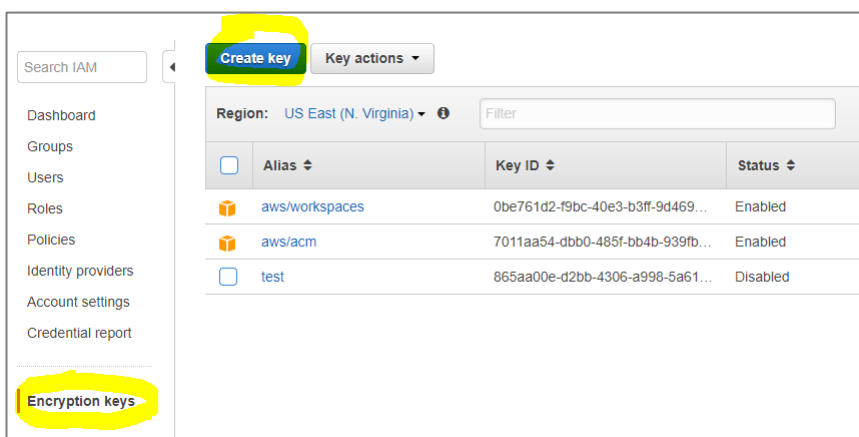
From the AWS console click “Services”

Select “IAM” from the Security, Identity & Compliance services.



Select *Encryption keys*

Click *Create key*



Give your key a name

Click *Next step*

Create Key in US East (N. Virginia)

Step 1 : Create Alias and Description

Step 2 : Add Tags

Step 3 : Define Key Administrative Permissions

Step 4 : Define Key Usage Permissions

Step 5 : Preview Key Policy

Create Alias and Description

Provide an alias and a description for this key. These properties of the key can be changed later. [Learn more.](#)

Alias (required) backspace-lab

Description Description of the key

► Advanced Options

Cancel **Next Step**

Leave Tags as is

Click *Next step*

Select users that will have permission to administer the key.

Click *Next step*

Create Key in US East (N. Virginia)

[Step 1 : Create Alias and Description](#)

[Step 2 : Add Tags](#)

Step 3 : Define Key Administrative Permissions

Step 4 : Define Key Usage Permissions

Step 5 : Preview Key Policy

Define Key Administrative Permissions

▼ Key Administrators

Choose the IAM users and roles that 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.](#)

Filter Showing 6 results

<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*

Create Key in US East (N. Virginia)

Step 1: Create Alias and Description

Step 2: Add Tags

Step 3: Define Key Administrative Permissions

Step 4: Define Key Usage Permissions

Step 5: Preview Key Policy

Define Key Usage Permissions

▼ This Account

Choose the IAM users and roles that can use this key to encrypt and decrypt data from within applications and when using AWS services integrated with KMS. [Learn more.](#)

Showing 6 results

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

Click *Finish*

Create Key in US East (N. Virginia)

Step 1: Create Alias and Description

Step 2: Add Tags

Step 3: Define Key Administrative Permissions

Step 4: Define Key Usage Permissions

Step 5: Preview Key Policy

Preview Key Policy

This is a preview of your key policy

```
{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::361919435810:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access for Key Administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::361919435810:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}
```

Cancel
Previous
Finish

You key has been created

Your master key was created successfully. Alias: backspace-lab

Create key Key actions

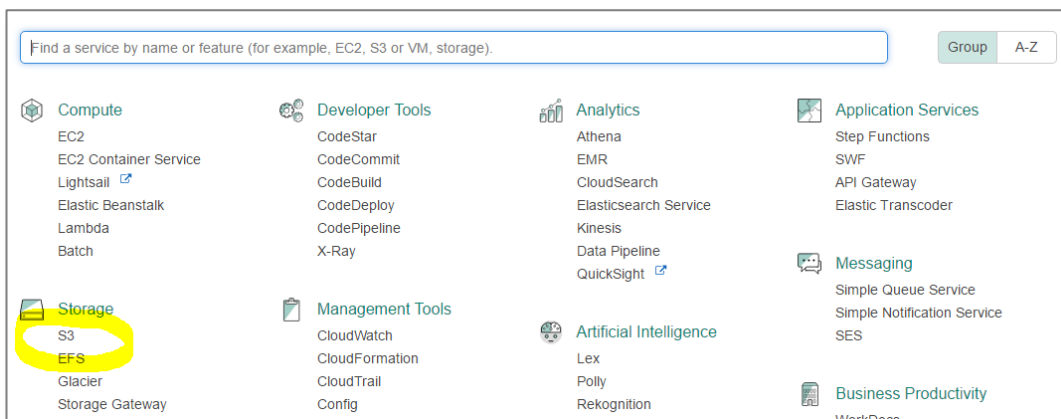
Region: US East (N. Virginia) Filter Showing 4 results

<input type="checkbox"/>	Alias ↕	Key ID ↕	Status ↕	Creation Date ↕
<input checked="" type="checkbox"/>	aws/workspaces	0be761d2-f9bc-40e3-b3ff-9d469...	Enabled	2018-06-22 16:00 UTC+1000
<input checked="" type="checkbox"/>	aws/acm	7011aa54-dbb0-485f-bb4b-939fb...	Enabled	2018-06-11 03:09 UTC+1000
<input checked="" type="checkbox"/>	backspace-lab	84954f73-8f6f-4b2b-baf0-20b1bb...	Enabled	2018-06-27 16:57 UTC+1000

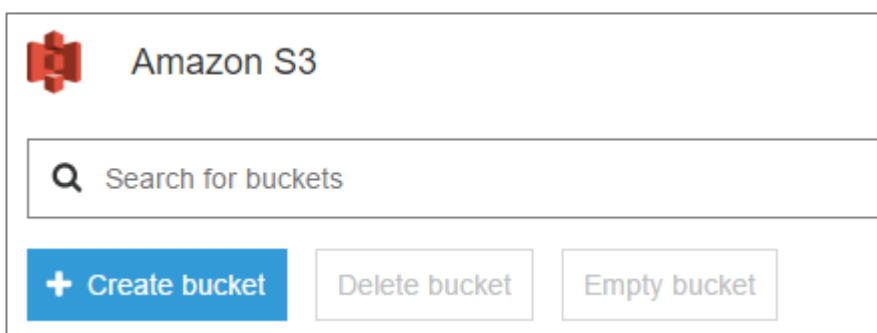
Using Encryption Keys with Amazon S3

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 ⁱ

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 🔍

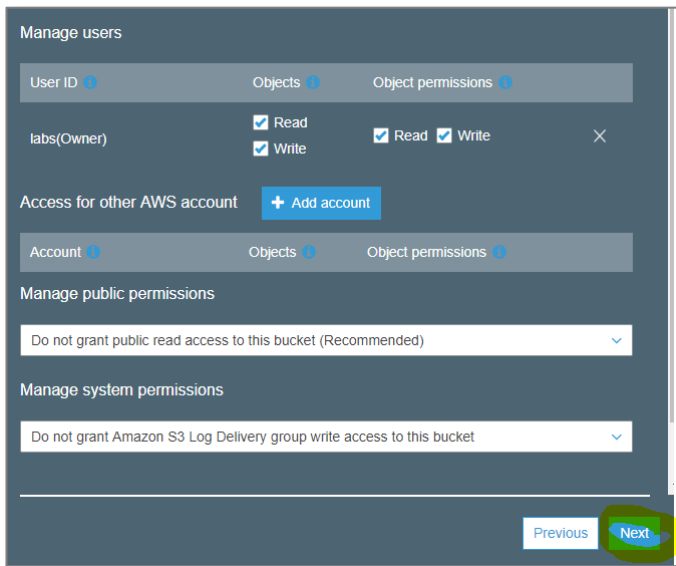
aws/s3

backspace-lab

Click *Next*

Leave permissions as private

Click *Next*

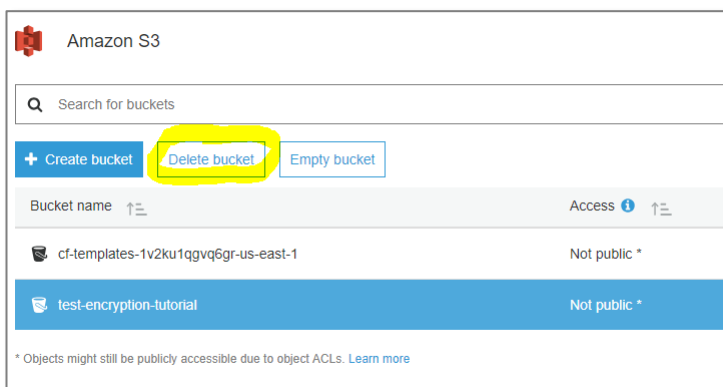


Click *Create bucket*

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

Search IAM

Your master key was created successfully. Alias: backspace-lab

Create key Key actions

Region: US

Alias

aws/wo

aws/acn

backspa

Enable

Disable

Schedule key deletion

Cancel key deletion

Delete key material

Add or edit tags

Filter

Key ID

0be761d2-f9bc-40e3-b3ff-9c

7011aa54-dbb0-485f-bb4b-9

84954f73-8f6f-4b2b-baf0-20

Schedule key deletion

Deleting a key makes all data encrypted under that key unrecoverable. AWS KMS enforces a minimum waiting period of 7 days to give you time to verify whether the key(s) are still needed to decrypt data. You can set up an Amazon CloudWatch alarm on any attempts to use the key(s) during the waiting period. [Learn More](#).

You can cancel deletion any time before the waiting period ends. After the waiting period ends, AWS KMS deletes the key(s).

Enter a waiting period between 7 and 30 days.

Waiting period (in days) 7

Alias	Key ID
backspace-lab	84954f73-8f6f-4b2b-baf0-20b1bb8218f3

Confirm you want to schedule this key for deletion in 7 days.

Cancel Schedule deletion