S3 Encryption

Encryption

A CLOUD GURU

- In Transit:
  - SSL/TLS
- At Rest:
  - Server Side Encryption:
    - S3 Managed Keys - **SSE-S3**
    - AWS Key Management Service, Managed Keys, **SSE-KMS**
    - Server Side Encryption with Customer Provided Keys - **SSE-C**
- Client Side Encryption

S3 Encryption

Enforcing Encryption on S3 Buckets

A CLOUD GURU

- Every time a file is uploaded to S3, a PUT request is initiated.
- This is what a PUT request looks like:

```
PUT /myFile HTTP/1.1
Host: myBucket.s3.amazonaws.com
Date: Wed, 25 Apr 2018 09:50:00 GMT
Authorization: authorization string
Content-Type: text/plain
Content-Length: 27364
x-amz-meta-author: Faye
Expect: 100-continue
[27364 bytes of object data]
```

Enforcing Encryption on S3 Buckets

A CLOUD GURU

- If the file is to be encrypted at upload time, the x-amz-server-side-encryption parameter will be included in the request header
- Two options are currently available:
  x-amz-server-side-encryption: AES256 (SSE-S3 - S3 managed keys)
  x-amz-server-side-encryption: ams:kms (SSE-KMS - KMS managed keys)
- When this parameter is included in the header of the PUT request, it tells S3 to encrypt the object at the time of upload, using the specified encryption method.
- You can enforce the use of Server Side Encryption by using a Bucket Policy which denies any S3 PUT request which doesn't include the x-amz-server-side-encryption parameter in the request header.

S3 Encryption

Enforcing Encryption on S3 Buckets

A CLOUD GURU

The following request tells S3 to encrypt the file using SSE-S3 (AES 256) at the time of upload:

```
PUT /myFile HTTP/1.1
Host: myBucket.s3.amazonaws.com
Date: Wed, 25 Apr 2018 09:50:00 GMT
Authorization: authorization string
Content-Type: text/plain
Content-Length: 27364
x-amz-meta-author: Faye
Expect: 100-continue
x-amz-server-side-encryption: AES256
[27364 bytes of object data]
```

S3 Encryption Exam Tips

A CLOUD GURU

- Encryption In-Transit
  - SSL/TLS (HTTPS)
- Encryption At Rest
  - Server Side Encryption
    - SSE-S3
    - SSE-KMS
    - SSE-C
  - Client Side Encryption
- If you want to enforce the use of encryption for your files stored in S3, use an S3 Bucket Policy to deny all PUT requests that don't include the x-amz-server-side-encryption parameter in the request header.