LOGICLABS TECHNOLOGIES

www.logiclabstech.com

Amazon Web Services

Encryption

ankitnarula1991@gmail.com

Encryption

- With an increasing number of enterprises using public and hybrid cloud deployments, and while more sensitive data is stored in cloud service provider (CSP) environments, organizations are aggressively seeking better ways to protect their information in the cloud. Naturally, one of the most prevalent controls that organizations are evaluating is one they are already comfortable using: encryption.

- Types of Encryption

- SSE-S3
- SSE-KMS (Key management service)

Encryption

- **SSE-S3**

- Encryption using keys handled & Managed by Amazon S3
- It encrypts the key itself with a root key that it regularly rotates

- **SSE-KMS**

- AWS KMS keys (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.
- There are separate permissions for the use of a KMS key that provides added protection against unauthorized access of your objects in Amazon SE.
- KMS uses customer master keys (CMKs) to encrypt the S3 objects.

Encryption

- **Level of Encryption**

- Bucket Level
- Object Level

- Create bucket

- Select ACLs Enabled

- Unblock all public access

- Click on create bucket

Encryption - Object Level

- Upload the object in the bucket
- Go to properties
- Go to Server side encryption settings
- Select specify an encryption key
- Select the key type as per our requirement
- Click on upload

Encryption - Bucket level

- Open Bucket
- Go to Properties tab
- Click on edit for Default Encryption
- Select enable
- Select the key type as per our requirement
- Click on save changes

ankitnarula1991@gmail.com