Amazon Web Services

Encryption

Dr.U.Seshadri, Assoc Professor, VCE-HYD

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

Amazon Web Services

Metadata and Tags

Dr.U.Seshadri, Assoc Professor, VCE-HYD

METADATA

- It is used to provide more information about the object upload in the bucket

- Types of Metadata

- System define object metadata
- User define object metadata

METADATA - SYSTEM DEFINE OBJECT

- Every object in a bucket has a set of system metadata which is processed by S3.
- System metadata has 2 categories:
- **Metadata**: like object creation date which is controlled by the system and solely Amazon S3 has the ability to update its value.
- **Other system metadata**: like the storage class configured for an object and objects of enabled server- side encryption, are system metadata with values controlled by us.

METADATA - USER DEFINE OBJECT

- When uploading an object, we can also assign metadata to the object. We provide this optional information as a name-value (key-value) pair when you send a PUT or POST request to create the object.
- Create a bucket
- Select ACLs Enabled
- Provide public access
- Upload one object in the bucket
- Give public access to the object

METADATA

- Go to Properties tab of the object
- System has already created one metadata.
- Click on edit for metadata
- Select system defined
- Select the key as per our requirement & enter the value
- Select user defined
- Enter the key & Value as per our requirement

TAGS

- We use object tagging to categorize storage. It will show in the billing where we can easily track for which purpose we are getting the bill.

- Click on Edit for tags

- Enter the Key & Value as per our requirement

- Click on save changes

Amazon Web Services

Access Control List

Dr.U.Seshadri, Assoc Professor, VCE-HYD

ACCESS CONTROL LIST

- Access Control List are used to grant basic read/write permissions on resources to other AWS accounts.

- **Key Features:**

- Each bucket and object has an Access Control List associated with it.
- An ACL is a list of grants identifying grantee and permission granted
- It is Recommended to use Canonical user ID as email address would not be supported

ACCESS CONTROL LIST

- **We can apply ACL at Two levels**

- Object Level
- Bucket Level (Bucket Policy)

- Create Bucket

- Select ACLs Enabled

- Give public access

- Upload the Object

- Give the Public access of the object

- Click on upload

ACCESS CONTROL LIST - OBJECT LEVEL

- Go to Your object
- Go to Permissions tab
- Click on edit
- Click on Add Grantee
- Enter the user canonical ID
- Click on save changes

Amazon Web Services

Bucket Policy

Dr.U.Seshadri, Assoc Professor, VCE-HYD

ACCESS CONTROL LIST - BUCKET POLICY

- We can create and configure bucket policies to grant permission to your Amazon S3 resources. Bucket policies use JSON-based access policy language. It is only apply at the bucket level.
- **Note**: It's the job of AWS administrator.
- Create the Bucket
- Select ACLs Enabled
- Give Public Access
- Upload the Object

ACCESS CONTROL LIST - BUCKET POLICY

- Note: Don't Give Public Access to object
- Click on upload
- Try to Access the object
- Open our bucket & go to permission tab
- To enter the code click on Edit
- Copy the Bucket ARN (Amazon Resource Names)

ACCESS CONTROL LIST - BUCKET POLICY

- Click on Policy generator
- Select type of policy is S3 Bucket Policy
- Select effect as Allow
- Enter principal as * (It means to all the objects)
- Select actions as All Actions
- Enter the bucket ARN with forward slash & star
- Example : arn:aws:s3:::<policy_name>/*

ACCESS CONTROL LIST - BUCKET POLICY

- Click on Add Statement
- Click on Generate policy
- Copy the code & paste in the Policy
- Code: **Click Here**
- Click Save changes
- Check our bucket