Amazon S3 - How to Set Up Data Encryption

Last Modified on 01/19/2021 12:43 pm EST

Server Side Encryption

There are two types of server side encryption that can be set in Amazon s3 - AES256 or AWS:KMS.

AES256 setup instructions

Option 1 - To set AES256 as your default Server Side Encryption, simply define it as your algorithm in your call to PUT /encryption:

```
{
"encryptionAlgorithm": "AES256"
}
```

`Note` : AWS won't save your encryption key (private key)

Option 2 - AES256 encryption can be set per data resource. This can be done by setting "x-amz-server-side-encryption" and "x-amz-server-side-encryption-customer-key" in the header of your request. The key is an arbitrary, user-specified string.

```
"x-amz-server-side-encryption": "AES256"
"x-amz-server-side-encryption-customer-key": "xxxxxxxxxxxxxxxxxxxxxxx"
```

`Note` : The `x-amz-server-side-encryption-customer-key` should be 32 digits in length

AWS:KMS setup instructions

Option 1 - To set AWS:KMS as your default Server Side Encryption, set the type of algorithm and your AWS key in your call to PUT /encryption:

```
{
"encryptionAlgorithm": "aws:kms",
      "kmsKey": "xxxxxxxxxxxxxxxxxxxxxxx"
}
```

Option 2 - Similar to option 1, you can set the default encryption without generating a new key. AWS will retrieve the default key configured in your s3 policy via IAM. Call PUT /encryption and pass just the algorithm:

```
{
 "encryptionAlgorithm": "aws:kms"
}
```

Option 3 - AWS:KMS can be set on the data resource level. To do this, pass "x-amz-server-side-encryption" and "x-amz-server-side-encryption-aws-kms-key-id" in the header of your request.

```
  "x-amz-server-side-encryption": "aws:kms"
"x-amz-server-side-encryption-aws-kms-key-id": "xxxxxxxxxxxxxxxxxxxxxx"
```

`Note` : The kmsKey is generated in the AWS console of your account. See documentation on how to generate a new key: https://aws.amazon.com/blogs/aws/new-key-management-service/

Client Side Encryption

The Amazon S3 connector now also supports client side encryption. Follow the steps provided in Amazon S3 Documentation to learn how to **use a master key stored within your application** to enable client side encryption.

To enable client side encryption on the UI:

- The **Enable Client Side Encryption** field or in config `clientside.encryption.enabled` should be set to **true**.
- The **Client Side Encryption Key** or in config `clientside.encryption.key` should be of lengths of **16** or **24** or **32** characters.

> **Note:** Both the `clientside.encryption.enabled` and `clientside.encryption.key` are mandatory to enable client side encryption. To disable it, pass `clientside.encryption.enabled` : **false.**