S3-Link for Amazon IAM Users

Introduction

This guide is used to link your Salesforce organization with Amazon S3 using the AWS IAM user.

Prerequisite

Before we start configuration for the IAM user, you need to confirm that you are up-to-date with below items.

- **Sign Up for Amazon S3**

  To start with S3-Link, you must have AWS Key Id and Secret Access Key. For that you need to Sign Up for Amazon. If you already have an Amazon S3 account just ignore it. Otherwise follow the S3-Link Amazon Sign up Guide document.

Create IAM User

You need to create an IAM user and give them full access for Amazon S3. Here are the configuration steps.

- **Get IAM User access keys**
  1. Login in AWS Management Console.
  2. Go to Services > IAM > Users
  3. Click “Add User”. Create individual IAM users (if not created).
  4. Open your IAM User from the list.
  5. Open “Security Credentials” section. Click “Create Access key”
  6. Download csv file for access keys
- **Create IAM User Policy to grant access for Single Bucket**

  If you want to give access to specific buckets then create this policy for IAM users.

  1. Login in AWS Management Console.
  2. Go to Services > IAM > Policies > Create Policy
  3. Go to JSON and add below JSON in the textarea. Here "testversioningsf" is the bucket name. You have to replace it with your bucket name.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
```

```
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:RestoreObject",
                "s3:PutObjectAcl",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::testversioningsf/*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketVersioning",
                "s3:GetBucketLocation",
                "s3:PutBucketVersioning"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:PutBucketCORS"
            ],
            "Resource": "arn:aws:s3:::testversioningsf"
        }
    ]
}
```

4. Click "Review Policy"
5. Give name "S3LinkAccessForSingleBucket"
6. Click "Create Policy"

- **Assign User Policies to IAM User**

  Follow the below steps to grant access of single bucket or all buckets to IAM user

  1. Login in AWS Management Console.
  2. Go to Services > IAM > Users
  3. Click “Add User”. Create individual IAM users (if not created).
  4. Open IAM User detail
  5. Click “Add Permissions”
  6. Add "AmazonS3FullAccess" permissions to that user if you want to give full access of Amazon S3

7. If you want to give access for specified buckets add "S3LinkAccessForSingleBucket" permission to that user.

Enable KMS Encryption(optional)

You want to enable KMS encryption, you will need a KMS Master Key. Here are the configuration steps to get KMS Master Keys.

1. Open service Key Management Service > Customer managed keys
2. Select region from the top drop down
3. Click “Create key”
4. Provide required information
5. Copy "Key Id"
6. Go to S3-Link Administration > System Configuration
7. Paste “Key Id” in "KMS Master Key"
8. Click “Save”