How to Enable Security Token Service (STS) for AWS Envionment?

Contents

Introduction

This document describes how to enable Security Token Service (STS) in AWS environment which is used in Cloud Center - Amazon Cloud integration.

How to Enable Security Token Service (STS) in AWS Environment?

Procedure to Create Policy for the Role who has Launched the CCO

Step 1. Log in to the AWS and navigate to IAM dashboard.

Step 2. Select **Create Policy** and then navigate to **Create your own policy**.

Step 3. Give a policy name .

Step 4. In Policy Document, insert this data and save it.

```
{
"Version": "2012-10-17",
"Statement": {
"Effect": "Allow",
"Action": "sts:AssumeRole",
"Resource": "*"
}
}
```

Step 5. Select the Role who has launched the CCO and select **Attach Policy**.

Step 6. Select the policy name created above in step 3. ensure that **AmazonEC2FullAccess** Policy is already assigned to this Role.

Procedure to Create the Role for the other Account whom you want to Authorize for Launching the Job

Step1. Login to AWS and navigate to IAM.

Step 2. Create a new Role and provide the Role Name and select next.

Step 3. Select the Role Type as **Role for Cross-Account Access**.

Step 4. Select the option **Provide access between AWS accounts you own**.

Step 5. Provide the account ID of the user who has launched the CCO with IAM role.

Step 6. Attach the AmazonEC2FullAccess policy to the Role.

Step 7. Review the Role and Save it.

Step 8. Use this Role in the CCM UI for both the existing configured Amazon Cloud in UI and new Amazon cloud using the option of Add Cloud Account.