AWS環境でセキュリティトークンサービス(STS)を有効にする方法

内容

[概要](#)
[AWS環境でセキュリティトークンサービス(STS)を有効にする方法](#)
[CCOを開始したロールのポリシー作成手順](#)
[ジョブの起動を承認する他のアカウントのロールを作成する手順](#)

概要

このドキュメントでは、Cloud Center - Amazon Cloud統合で使用されるAWS環境でセキュリティトークンサービス(STS)を有効にする方法について説明します。

AWS環境でセキュリティトークンサービス(STS)を有効にする方法

CCOを開始したロールのポリシー作成手順

ステップ1:AWSにログインし、IAMダッシュボードに移動します。

ステップ2:[ポリシーの作成]を選択し、[独自のポリシーの作成]に移動します。

ステップ3：ポリシー名を指定します（ポリシー名を入力します）。

ステップ4：ポリシードキュメントで、このデータを挿入して保存します。

```
{
「バージョン」:「2012-10-17」
「ステートメント」:{
「効果」:"許可",
「アクション」:"sts:AssumeRole",
「リソース」:"*"
}
}
```

ステップ5:CCOを起動したロールを選択し、[Attach Policy]を選択します。

ステップ6：上で作成したポリシー名を選択しますか。ステップ3. AmazonEC2FullAccessポリシ

ーが既にこの**ロールに割**り当てられていることを確認します。

ジョブの起動を承認する他のアカウントのロールを作成する手順

ステップ1:AWSにログインし、IAMに移動します。

ステップ2：新しいロールを作成し、ロール名を入力して、[next]を選択します。

ステップ3:[Role Type]を[**Role for Cross-Account Access]に選択します**。

ステップ4:[Provide access between **AWS accounts you owned**(所有するAWSアカウント間のアクセスを提供**する)]オプションを選択します**。

ステップ5:IAMロールでCCOを起動したユーザのアカウントIDを入力します。

手順 6： AmazonEC2FullAccessポリシーをロールにアタッチします。

ステップ7：ロールを確認して保存します。

ステップ8:UIで設定されている既存のAmazon Cloudと新しいAmazonクラウドの両方に対して、CCM UIでこのロールを使用します。[Add Cloud Account]オプションを使用します。