AWS の IAM ロールと権限

AWS の IAM ロールと権限

（注） AWS IAM の役割と権限の詳細については*AWS* ユーザ ガイドの *Cisco Cloud APIC*、次のいずれかのタイプのテナントとして AWS プロバイダを設定する方法などを参照してください。

- 信頼できるテナント
- 信頼できないテナント
- 組織テナント、リリース 4.2(3) 以降でサポートされています。

AWS ユーザ ガイドの *Cisco Cloud APIC* は、次の ＵＲＬ から入手できます。

https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/tsd-products-support-series-home.html

Cisco Cloud APIC のインストールと操作には、特定の AWS IAM の役割と権限が必要です。

CloudFormation テンプレート (CFT) を使用して Cisco Cloud APIC をインストールする場合は、AWS に完全な管理者アクセス権を持つユーザ (たとえば、権限ポリシー ARN **arn:aws:iam::aws:policy/AdministratorAccess**が、直接、ロール ポリシーにより、またはユーザ グループにより接続されているユーザ)によってインストールすることを推奨します。ただし、使用可能な AWS 管理者アクセス権を持つユーザがいない場合は、Cisco Cloud APIC をインストールするユーザに次の最小権限セットが必要です。

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

AWS の IAM ロールと権限

```
   "Effect": "Allow",
   "Action": "ec2:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "cloudformation:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "s3:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "sns:*",
   "Resource": "*"
  }
 ]
}
```

上記の権限セットは、CFT を使用して Cisco Cloud APIC をインストールするユーザに必要です。次に、**[アクション (Action)]**行に示すように、上記の必要な権限の詳細について説明します。

- **iam権限:** Cisco Cloud APICインスタンスは、 **ApicAdmin**という名前の AWS ロールで実行される AWS EC2 インスタンスです。このロールは、CloudFormation スタックによって作成される必要があります。**ApicAdmin**ロールを使用して Cisco Cloud APIC インスタンスを実行すると、Cisco Cloud APIC インスタンスは AWS メタデータ サービスを使用して一時的なクレデンシャルを取得できます。これにより、Cisco Cloud APIC インスタンスは、AWS API コールを行うために、固定のアクセス キー ID と秘密アクセス キーを使用する必要がなくなります。
- **ec2権限:**スタックが必要なVPC、サブネット、セキュリティグループなどを作成できるようにするために必要です。スタックによって、 Cisco Cloud APIC インスタンスが展開されるインフラ VPC が作成されます。
- **cloudformationの権限:** CFT 自体を実行するために必要です。
- **s3権限:** CFT が AWS CloudFormation スタックのニーズに基づいて S3 バケットに保存されるようにするために必要です。
- **sns権限:** CloudFormation スタックを実行するための通知を取得するために必要です。

操作の場合、Cisco Cloud APIC は **ApicAdmin** ロールで実行されます。このロールには 2 つのポリシーが付加されており、CloudFormation テンプレートの起動の一環として作成されます。

- **ApicAdminFullAccessポリシー:** このポリシーにリストされている権限によって、Cisco Cloud APIC は EC2 および VPC リソース、S3 バケット、リソースグループ、アカウント通知、およびログを作成および管理できます。Cisco Cloud APIC は、作成したリソースの管理のみを試行することに注意してください。他のアプリケーションによって作成されたリソースには処理しません。

  このポリシーには、次の権限が必要です。

AWS の IAM ロールと権限

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Action": "organizations:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "ec2:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "s3:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "sqs:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "elasticloadbalancing:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "acm:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "cloudtrail:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "cloudwatch:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "logs:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "resource-groups:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "events:*",
   "Resource": "*",
   "Effect": "Allow",
   "Sid": "CloudWatchEventsFullAccess"
  },
  {
   "Action": "autoscaling:*",
   "Resource": "*",
   "Effect": "Allow"
  }
```

AWS の IAM ロールと権限

```
 ]
}
```

- **ApicTenantsAccessポリシー:**このポリシーにリストされている権限によって、Cisco Cloud APIC は、テナント アカウントのロールと、それらのテナント AWS アカウントのコール AWS API を引き受けることができます。これにより、Cisco Cloud APIC は、テナント アカウントのハード クレデンシャルを使用せずにテナント アカウントにアクセスすることができます。

  このポリシーには、次の権限が必要です。

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

Cisco Cloud APIC 自体は、操作のために IAM 権限を必要としません。これは、インストール後に IAM ポリシーやロールが作成されないためです。

Cisco Cloud APIC は、それによって作成された AWS リソースの管理を試みますが、既存のリソースをインベントリとしてリストするのではなく、他のアプリケーションによって作成されたリソースの管理を試みません。同時に、これらのアカウント (インフラ アカウントと他のテナント アカウントの両方) の IAM ユーザは、Cisco Cloud APIC によって作成されたリソースに干渉しないようにする必要があります。したがって、AWS で Cisco Cloud APIC により作成されたすべてのリソースには、次の 2 つのタグのうち少なくとも 1 つが適用されます。

- **AciDnTag**
- **AciOwnerTag**

したがって、EC2、VPC、およびその他のリソースを作成、削除、または更新する権限を持つ AWS IAM ユーザを作成する場合、これらのユーザが Cisco Cloud APIC によって作成および管理されるリソースへアクセスすることや変更することを防止する必要があります。このような制限は、インフラとその他のユーザのテナントアカウントの両方に適用する必要があります。AWS アカウント管理者は、上記の2つのタグを使用して、ユーザが Cisco Cloud APIC によって作成および管理されるリソースへのアクセスや変更を防止する必要があります。

たとえば、次のようなアクセス ポリシーがある場合、Cisco Cloud APIC によって管理されているリソースへの意図しないアクセスを防止するために、IAM ユーザのアクセス ポリシーを設定することができます。

```
{
 "Effect": "Deny",
 "Action": [
  "ec2:*"
 ],
 "Resource": "*",
 "Condition": {
  "StringLike": {
```

AWS の IAM ロールと権限

```
      "ec2:ResourceTag/AciDnTag": "*"
    }
   }
  }
```

AWS の IAM ロールと権限