



AWS の IAM ロールと権限

- [AWS の IAM ロールと権限 \(1 ページ\)](#)

AWS の IAM ロールと権限



(注) AWS IAM のロール役割と権限の詳細については、[Cisco Cloud Network Controller AWS User Guide](#) を参照してください。次のいずれかのタイプのテナントとして AWS プロバイダを構成する方法などが含まれています。

- 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。

Cisco Cloud Network Controller のインストールと操作には、特定の AWS IAM のロールと権限が必要です。

CloudFormation テンプレート (CFT) を使用して Cisco Cloud Network Controller 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ー (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、またはユーザーグループによりアタッチされているユーザー) によってインストールすることを推奨します。ただし、AWS 管理者アクセス権を持つユーザーがいない場合は、Cisco Cloud Network Controller をインストールするユーザー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": "*"
  }],
  {
    "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 Network Controller をインストールするユーザーに必要です。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 Network Controller 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 Network Controller インスタンスを実行すると、Cisco Cloud Network Controller 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ログイン情報を取得できます。これにより、Cisco Cloud Network Controller インスタンスは、AWS API の呼び出しを行うために、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 Network Controller 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 Network Controller 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 Network Controller 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 Network Controller は、作成した Azure リソースの管理を試みます。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。

```
{
  "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"
  }
]
```

```
    ]
  }
}
```

- **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 Network Controller 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 AWS API の呼び出しを引き受けることができます。これにより、Cisco Cloud Network Controller は、テナントアカウントの固定ログイン情報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 Network Controller 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 Network Controller は、自身が作成した AWS リソースの管理を試みますが、インベントリとしてリストとされている既存のリソースを除き、他のアプリケーションが作成したリソースは管理を試みません。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 AWS IAM ユーザーは、Cisco Cloud Network Controller が作成し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 Network Controller が作成し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 ユーザーを作成する場合、これらのユーザーが、Cisco Cloud Network Controller が作成し、管理するリソースへアクセスしたり、それらを変更したり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、ユーザーが、Cisco Cloud Network Controller が作成し、管理するリソースへアクセスし、それらを変更すること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によって、IAM ユーザーが、Cisco Cloud Network Controller が管理しているリソースに意図せずアクセスするのを防止することができるでしょう。

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

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


翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。