デバイスとサービスの導入準備

ライブデバイスとモデルデバイスの両方を CDO に対して導入準備できます。モデルデバイスはアップロードされた構成ファイルであり、CDO を使用して閲覧および編集できます。

ほとんどのライブデバイスおよびサービスでは、Secure Device Connector が CDO をデバイスまたはサービスに接続できるように、オープンな HTTPS 接続が必要となります。

SDC とそのステータスの詳細については、Secure Device Connector（SDC） を参照してください。

この章は、次のセクションで構成されています。

AWS VPC の導入準備

AWS VPC を CDO に対して導入準備するには、以下の手順に従います。

始める前に

（注） CDO は、ピアリングされた AWS VPC をサポートしていません。ピア VPC で定義されたセキュリティグループを参照する、ピアリングされた VPC を導入準備しようとすると、導入準備プロセスは失敗します。

Amazon Web Service（AWS）仮想プライベートクラウド（VPC）を CDO に対して導入準備する前に、以下の前提条件を確認してください。

- CDO を AWS VPC に接続するために必要なネットワーク要件を Cisco Defense Orchestrator の管理対象デバイスへの接続 で確認します。
- AWS VPC を導入準備するには、AWS VPC のアクセスキーとシークレットアクセスキーが必要です。これらはいずれもアイデンティティとアクセス管理（IAM）コンソールを使

用して生成されます。詳細については、「セキュリティログイン情報の理解と取得」（https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html）を参照してください。

- CDO が AWS VPC と通信できるように権限を設定します。詳細は、「IAM ユーザーの権限の変更」（https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_change-permissions.html）を参照してください必要な権限については、以下の例を参照してください。

```
{
            "Version": "2012-10-17",
            "Statement": [
                {
                   "Effect": "Allow",
                   "Action": [
                       "ec2:AuthorizeSecurityGroupEgress",
                       "ec2:AuthorizeSecurityGroupIngress",
                       "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                       "ec2:DescribeInstances",
                       "ec2:DescribeVpnConnections",
                       "ec2:DescribeRegions",
                       "ec2:DescribeSecurityGroups",
                       "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
                       "ec2:RevokeSecurityGroupIngress",
                       "ec2:DescribeVpcs",
                       "ec2:RevokeSecurityGroupEgress",
                       "sts:GetCallerIdentity",
                       "ec2:DescribeSubnets",
                       "ec2:DescribeVpnGateways"
                   ],
                   "Resource": "*"
               }
           ]
       }
```

ステップ 1 CDO のナビゲーションバーで、[デバイスとサービス] をクリックします。

ステップ 2 青いプラスボタンをクリックして、デバイスの導入準備を開始します。

ステップ 3 [AWS VPC] をクリックします。

ステップ 4 AWS アカウントに接続するためのアクセスキー ID とシークレットアクセスキーのログイン情報を入力します。生成された名前のリストは、ログイン情報を入力した AWS VPC から取得されます。

ステップ 5 [接続（Connect）] をクリックします。

ステップ 6 ドロップダウンメニューから [リージョン] を選択します。VPC のローカルであるリージョンを選択する必要があります。

ステップ 7 [選択（Select）] をクリックします。

ステップ 8 ドロップダウンメニューを使用して、正しいAWS名を選択します。生成された名前のリストは、ログイン情報を入力した AWS VPC から取得されます。ドロップダウンメニューから目的の AWS VPC を選択します。AWS VPC ID の名前は一意であり、2 つ以上のインスタンスが同じ ID を持つことはできません。

ステップ 9 [選択（Select）] をクリックします。

ステップ 10 CDO UI で表示する名前を入力します。

ステップ 11 [続行（Continue）] をクリックします。

ステップ 12 （オプション）デバイスのラベルを入力します。AWS VPC のラベルを作成する場合、テーブルはデバイスに自動的に同期されません。AWS コンソールで、ラベルをタグとして手動で再作成する必要があります。詳細については、AWS VPC のラベルとタグを参照してください。

ステップ 13 [続行（Continue）] をクリックします。

ステップ 14 [デバイスとサービス]ページに戻ります。デバイスが正常に導入準備されると、構成ステータスが [同期済み] 、接続状態が [オンライン] と表示されます。

関連情報：

- AWS VPC 接続ログイン情報の更新
- AWS VPC ポリシー
- AWS VPC と CDO のセキュリティグループ
- AWS とその他の管理対象デバイス間でオブジェクトを共有する

CDO からのデバイスの削除

CDO からデバイスを削除するには、次の手順を使用します。

ステップ 1 CDO にログインします。

ステップ 2 [インベントリ] ページに移動します。

ステップ 3 削除するデバイスを見つけ、そのデバイスの行でデバイスをチェックして選択します。

ステップ 4 右側にある [デバイスアクション] パネルで、[削除] を選択します。

ステップ 5 プロンプトが表示されたら、[OK] を選択して、選択したデバイスの削除を確認します。[キャンセル] を選択して、デバイスを導入準備したままにします。