OCI

OCI アカウントの準備

Multicloud Defense に OCI テナントをオンボーディングする前に、OCI アカウントを適切にセットアップする必要があります。テナントを準備するために必要な一般的な手順は次のとおりです。

（注） Multicloud Defense は、OCI の入力と出力/East-West の保護の両方をサポートします。インベントリおよびトラフィック検出はサポートされていません。

OCI テナントをオンボーディングするには、米国西部（サンノゼ）リージョンに登録する必要があります。このリージョンに登録しないと、OCI テナントのオンボーディングでエラーが発生します。

Multicloud Defense Gateway を OCI に展開するには、Multicloud Defense コンピューティングイメージの利用規約に各 OCI コンパートメントで同意する**必要があります**。そうしないと、不正なエラーによって展開は失敗します。

次の手順は、Multicloud Defense に正常に接続するために OCI 環境を準備する方法を示しています。これらの要件を達成する方法に関する OCI 固有のドキュメントについては、OCI のマニュアルを参照してください。

自動化手順の概要

Multicloud Defense では、OCI アカウントの準備を自動化するスクリプトを提供しています。この自動化には、後で説明する手動手順に含まれる、必要なグループ、ポリシー、権限、およびユーザーが含まれます。

1. Oracle Cloud Shell または Linux ベースのシェルプロンプトを開きます。

2. 次のコマンドを入力して実行します。

```
bash <(curl -sSL
https://raw.githubusercontent.com/valtix-security/cli-oci-setup/main/oci_onboarding.sh)
```

3. 正常に完了したら、Multicloud Defense ダッシュボードから Multicloud Defense Controller に Oracle OCI テナントを接続します。 （3 ページ） に進みます。

手動手順の概要

OCI アカウントを手動で準備するには、次の手順を実行します。

1. グループを作成します。
2. ポリシーを作成します。ポリシーには `root` コンパートメントが選択されている必要があり、次の権限が含まれていることに注意してください。

```
Allow group <group_name> to inspect instance-images in compartment <compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to use volume-family in compartment <compartment_name>
Allow group <group_name> to use virtual-network-family in compartment
<compartment_name>
Allow group <group_name> to manage volume-attachments in compartment <compartment_name>
Allow group <group_name> to manage instances in compartment <compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment <compartment_name>
Allow group <group_name> to manage load-balancers in compartment <compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to manage app-catalog-listing in compartment
<compartment_name>
Allow group <group_name> to read virtual-network-family in tenancy
Allow group <group_name> to read instance-family in tenancy
Allow group <group_name> to read load-balancers in tenancy
Allow group <controller-group> to manage cloudevents-rules in tenancy
Allow group <controller-group> to manage ons-family in tenancy
```

3. ユーザーを作成します。
4. ユーザーをグループに追加します。
5. ユーザーの API キーを作成します。
6. ユーザーとテナントの OCID を記録します。
7. 利用規約に同意します。

次に行う作業：

Multicloud Defense ダッシュボードから Multicloud Defense Controller に Oracle OCI テナントを接続します。 （3 ページ） を実行して、OCI アカウントを Multicloud Defense に接続します。

Multicloud Defense ダッシュボードから Multicloud Defense Controller に Oracle OCI テナントを接続します。

始める前に

OCI アカウントの準備 （1 ページ）で要件を確認してください。

手順

ステップ 1 [クラウドアカウント（Cloud Accounts）] ペインで、[アカウントの追加（Add Account）] をクリックします。.

ステップ 2 [一般情報（General Information）] ページで、[アカウントタイプ（Account Type）] リストボックスから [OCI] を選択します。

ステップ 3 [Oracle Cloud Shell] をクリックして、ネイティブシェルプロンプトを起動します。

ステップ 4 Multicloud Defense セットアップウィザードで提供されるコマンドをコピーし、Cloud Shell に貼り付けます。コマンドを実行します。

このコマンドは、IAM ポリシー、OCI グループ、および OCI ユーザーを作成するプロセスを自動化し、OCI アカウントと Multicloud Defense 間の通信を容易します。

ステップ 5 次のフィールドを入力します。

- [OCIアカウント名（OCI Account Name）]：Multicloud Defense Controller 内でこの OCI テナントを識別するために使用されます。
- [テナントOCID（Tenancy OCID）]：OCI ユーザーから取得したテナントの Oracle Cloud 識別子です。
- [ユーザーOCID（User OCID）]：OCI ユーザーから取得したユーザー OCID。
- [秘密キー（Private Key）]：OCI ユーザーに割り当てられた API 秘密キー。

次のタスク

トラフィックの可視性を有効化します。

Multicloud Defense ダッシュボードから **Multicloud Defense Controller** に **Oracle OCI** テナントを接続します。

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。