Multicloud Defense ウィザードを使用したセットアップ

Multicloud Defense Controller は、Multicloud Defense とそのセキュリティポリシーを展開および管理するための、SaaS 型の一元化されたコントロールプレーンを提供します。

[設定（Setup）] では、次の一連の簡単な手順を使用して、Multicloud Defense セキュリティの設定プロセスを案内します。

- [アカウントの接続（Connect your Account）]：このプロセスでは、クラウドサービスプロバイダー アカウントを Multicloud Defense にオンボーディングし、それと同時に、アカウントに関連付けられているリージョンおよび追加のインベントリとアセットを検出します。
- [トラフィックの可視性の有効化（Enable Traffic Visibility）]：簡単セットアップ方法を使用して、トラフィックのフローを把握するためのログの収集を有効化できます。
- [アカウントの保護（Secure Your Account）]：この手順では、（お持ちのクラウドアカウントに応じて）VNET または VPC、および Multicloud Defense Gateway を設定してエクスペリエンスを保護できます。

- クラウドアカウントの接続 （1 ページ）
- トラフィックの可視性の有効化 （9 ページ）
- アカウントを保護 （12 ページ）

クラウドアカウントの接続

最初のステップは、1つ以上のクラウドアカウントのセットをオンボーディングすることです。これにより、Multicloud Defense Controller は、インベントリの検出、トラフィックとログの有効化、セキュリティ展開のオーケストレーション、ポリシーの作成と管理を行うことで、各アカウントと対話できるようになります。

クラウドサービスプロバイダーのアカウントを Multicloud Defense Controller に接続するには、次の手順を実行します。

AWS アカウントの接続

Multicloud Defense の簡単セットアップウィザードから AWS サブスクリプションに接続するには、次の手順を実行します。

始める前に

- アクティブな Amazon Web Services（AWS）アカウントが必要です。
- CDO テナントの管理者またはネットワーク管理者のユーザーロールが必要です。
- Multicloud Defense を CDO テナントに対して有効にしておく必要があります。

（注） Multicloud Defense Gateway バージョン 23.04 以降を使用している場合、Multicloud Defense Controllerバージョン23.10はAWS EC2インスタンスでデフォルトでIMDSv2に設定されます。IMDSv1 と IMDSv2 の違いの詳細については、AWS のドキュメントを参照してください。

手順

ステップ 1 Multicloud Defense Controller ダッシュボードから、ウィンドウの左側にある [設定（Setup）] をクリックします。

ステップ 2 [アカウントの接続（Connect Account）] を選択します。

ステップ 3 AWS アイコンをクリックします。

ステップ 4 モーダルに次の情報を入力します。

a) [スタックの起動（Launch Stack）] をクリックして、CloudFormation テンプレートをダウンロードして展開します。これにより、テンプレートを展開するための別のタブが開きます。AWS へのログインが必要です。

b) CloudFormation スタック出力からコントローラ IAM ロールの ARN をコピーして、CloudFormation テンプレートに貼り付けます。

c) Multicloud Defense Controller 簡単セットアップモーダルで、[AWSアカウント番号（AWS Account Number）] を入力します。この番号は、CloudFormation テンプレートの [現在のアカウント（Current Account）] の出力値で確認できます。

d) Multicloud Defense Controller のアカウントに割り当てる [アカウント名（Account Name）] を入力します。

e) （任意）アカウントの [説明（Description）] を入力します。

f) [外部ID（External ID）]を入力します。これは、IAM ロールの信頼ポリシーのランダムな文字列です。この値は、作成されたコントローラ IAM ロールで使用されます。外部 ID は編集または再生成できます。

g) [コントローラIAMロール（Controller IAM Role）] を入力しますこれは、CloudFormation テンプレート（CFT）の展開中に Multicloud Defense Controller に対して作成された IAM ロールです。CFT スタック

で出力値 MCDControllerRoleArm を探します。次のような値となります： `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`。

h) [インベントリモニターロール（Inventory Monitor Role）] を入力しますこれは、CFT の展開時に Multicloud Defense Inventory 用に作成される IAM ロールです。CFT スタックで出力値 MCDInventoryRoleArn を探します。次のような値となります：`arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`。

ステップ 5 [Next] をクリックします。アカウントは Multicloud Defense Controller にオンボーディングされます。

次のタスク

アカウントを接続すると、Multicloud Defense Controller はクラウド サービス プロバイダー アカウントに関連付けられているアセットとインベントリの検出を自動的に開始します。これはトラフィックの検出とは異なることに注意してください。Multicloud Defense Controller はデフォルトでアカウントのアセットとインベントリを検出するため、このウィザードの次のステップは、Azure アカウントのトラフィックの有効化です。

Azure アカウントの接続

Multicloud Defense Controller の簡単セットアップウィザードから Azure サブスクリプションに接続するには、次の手順を実行します。

始める前に

- アクティブな Azure サブスクリプションが必要です。
- CDO テナントの管理者またはネットワーク管理者のユーザーロールが必要です。
- Multicloud Defense を CDO テナントに対して有効にしておく必要があります。

手順

ステップ 1 CDO ダッシュボードで、左側のナビゲーションペインにある **Multicloud Defense** タブをクリックします。

ステップ 2 右上のウィンドウにある **Multicloud Defense Controller** をクリックします。

ステップ 3 Multicloud Defense Controller ダッシュボードから、ウィンドウの左側にある [設定（Setup）] をクリックします。

ステップ 4 [アカウントの接続（Connect Account）] を選択します。

ステップ 5 Azure アイコンをクリックします。

ステップ 6 モーダルに次の情報を入力します。

a) リンクをクリックすると、Azure Cloud Shell が bash モードで開きます。

b) Azure アカウントモーダルで、[コピー（Copy）] をクリックしてオンボーディングスクリプトをコピーし、ステップ 1 で開いた bash シェルで実行します。

c) Azure アカウントモーダルで、この Azure アカウントの名前を入力します。Azure サブスクリプション名と同じ名前を付けることができます。この名前はMulticloud Defense Controllerアカウントページにのみ表示されます。
d) （任意）サブスクリプションの説明を入力します。
e) [ディレクトリID（Directory ID）]（テナント ID とも呼ばれます）を入力します。
f) オンボーディングするサブスクリプションの [サブスクリプションID（Subscription ID）] を入力します。
g) オンボーディングスクリプトによって作成された [アプリケーションID（Application ID）]（クライアント ID とも呼ばれます）を入力します。
h) [クライアントシークレット（Client Secret）]（シークレット ID とも呼ばれます）を入力します。

ステップ 7 [次へ（Next）] をクリックします。

次のタスク

アカウントを接続すると、Multicloud Defense Controller はクラウド サービス プロバイダー アカウントに関連付けられているアセットとインベントリの検出を自動的に開始します。これはトラフィックの検出とは異なることに注意してください。Multicloud Defense Controller はデフォルトでアカウントのアセットとインベントリを検出するため、このウィザードの次のステップは、Azure アカウントのトラフィックの有効化です。

Google Cloud Platform アカウントの接続

Multicloud Defense Controller の簡単セットアップウィザードを使用して、単一の GCP プロジェクトをアカウントとしてオンボードするには、次の手順を実行します。

始める前に

- アクティブな Google Cloud Platform（GCP）プロジェクトが必要です。
- GCP プロジェクト内で VPC、サブネット、およびサービスアカウントを作成するために必要な権限を持っている必要があります。詳細については、GCPのドキュメントを参照してください。
- CDO テナントの管理者またはネットワーク管理者のユーザーロールが必要です。
- Multicloud Defense を CDO テナントに対して有効にしておく必要があります。

手順

ステップ 1 Multicloud Defense Controller ダッシュボードから、ウィンドウの左側にある [設定（Setup）] をクリックします。

ステップ 2 [アカウントの接続（Connect Account）] を選択します。

ステップ 3 GCP アイコンをクリックします。

ステップ 4 [Cloud Platform Cloud Shell] をクリックして、Cloud Shell を起動します。または、GCP アカウントにログし、Multicloud Defense に接続するプロジェクトから Cloud Shell を起動します。スクリプトにより、プロジェクト名は Cloud Shell を起動するプロジェクトの名前に自動的に変更されることに注意してください。

a) Multicloud Defense Controller 簡単セットアップモーダルで生成されたコマンドをコピーし、そのコマンドを Cloud Shell に貼り付けます。コマンドを実行して、オンボーディングプロセスを開始します。このスクリプトは、Multicloud Defense Controller のユーザーアカウントを自動的に作成し、GCP プロジェクトと直接通信します。

b) 複数の GCP プロジェクトがある場合は、番号付きリストからプロジェクトを選択するように求められます。接続および送信するプロジェクトの値を選択します。

c) `Continue configuring this project? [y/n]` というプロンプトが表示された場合、「y」または「n」のいずれかのみを入力する必要があることに注意してください。選択内容を送信するために **Enter** を押さないでください。

Multicloud Defense に接続しようとしている GCP プロジェクトが過去にオンボーディングされている場合、GCP クラウドストレージバケットがすでに存在する可能性があるというエラーが表示される場合があることに注意してください。それが受け入れられない場合は、 Multicloud Defenseへの接続後に、このプロジェクトのフローログを処理するための新しいストレージバケットを GCP アカウントに作成します。

ステップ 5 セットアップモーダルで次の情報を入力します。

a) [GCPアカウント名（GCP Account Name）] を入力します。この名前は Multicloud Defense にのみ表示されます。

b) （任意）[説明（Description）] に説明を入力します。

c) GCP プロジェクトの [プロジェクトID（Project ID）] を入力します。これは、ステップ 1 のスクリプトによって生成された秘密キーの上部にあります。

d) オンボーディングプロセスの一部として作成されたサービスアカウントの [クライアント電子メール（Client Email）] を入力します。これは、ステップ 1 のスクリプトによって生成された秘密キーに含まれています。

e) スクリプトの出力からサービスアカウントの [秘密キー（Private key）] をコピーして貼り付けます。

ステップ 6 [Next] をクリックします。

次のタスク

GCP では、プロジェクトが設定されているリージョンは自動では設定に含まれません。プロジェクトが Multicloud Defense に接続されたら、**[管理（Manage）]**>**[インベントリ（Inventory）]** に移動して、該当するすべてのリージョンを手動で変更および追加することを**強く**お勧めします。

アカウントを接続すると、Multicloud Defense Controller はクラウド サービス プロバイダー アカウントに関連付けられているアセットとインベントリの検出を自動的に開始します。これはトラフィックの検出とは異なることに注意してください。Multicloud Defense Controller はデフォルトでアカウントのアセットとインベントリを検出するため、このウィザードの次のステップは、Azure アカウントのトラフィックの有効化です。

OCI アカウントへの接続

Multicloud Defense に接続する前に、次の手順をよく読み、OCI アカウントを準備してください。

OCI アカウントの準備

この手順を実行すると、Multicloud Defense と OCI アカウント間の接続が自動化されます。また、正しい権限を持つポリシーを作成するように指示されます。手順の一部としてリストされているすべての権限がないと、一部の機能が使用できなくなります。

Multicloud Defense のセットアップウィザードを使用して Oracle Cloud（OCI）アカウントに接続するには、次の手順を実行します。

手順

ステップ 1 OCI テナントにログインします。

ステップ 2 **[アイデンティティとセキュリティ（Identity and Security）]** > **[グループ（Groups）]**に移動します。

ステップ 3 [グループの作成（Create Group）] をクリックします。

ステップ 4 次を入力します。

- [名前（Name）]：Multicloud Defense-controller-group
- [説明（Description）]：Multicloud Defense グループ

ステップ 5 [作成（Create）] をクリックします。

ステップ 6 OCI でネットワーク ファイアウォール ポリシーを作成します。詳細については、OCI のドキュメントを参照してください。ただし、ポリシーの作成時には次の情報を含めてください。

- [名前（Name）]：Multicloud Defense-controller-policy。
- [説明（Description）]：Multicloud Defense ポリシー。
- [コンパートメント（Compartment）]：（「root」コンパートメントである必要があります）。

a) [手動エディタの表示（Show Manual Editor）] タブで次の権限を追加します。

```
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
```

- group_name：Multicloud Defense-controller-group。
- compartment_name：（Multicloud Defense が展開されるコンパートメント）。

（注）
<compartment_name> をポリシーが適用されるコンパートメントの名前に置き換える際に、コンパートメントがサブコンパートメントである場合は、名前形式は **compartment:sub-compartment**（例：Prod:App1）となります。

<compartment_name> がルートコンパートメントとして指定されている場合（例：multicloud (root)）、OCI はポリシーを受け入れず、無効なパラメータのエラーが生成されます。ポリシーは特定のコンパートメントに対して定義する必要があり、そのコンパートメントをルートコンパートメントにすることはできません。

b) [作成（Create）] をクリックします。

ステップ 7 OCI でユーザーを作成します。詳細については、OCI のドキュメントを参照してください。ただし、ユーザーの作成時には次の設定情報を指定してください。

- [名前（Name）]：Multicloud Defense-controller-user
- [説明（Description）]：Multicloud Defense ユーザー

ステップ 8 API キーを作成します。詳細については、OCI のドキュメントを参照してください。

API キーを追加する前に、秘密キーと公開キーの両方をダウンロードしてください。

ステップ 9 OCI アカウントの**利用規約**に同意します。詳細については、OCI のドキュメントを参照してください。また、UI の [イメージの変更（Change image）] セクションにアクセスして、Multicloud Defenseに固有の次の「コミュニティイメージ」情報を追加してください。

a) Multicloud Defense のチェックボックスをオンにします。
b) 「パブリッシャの利用規約、Oracle の利用規約、および Oracle の一般的なプライバシーポリシーを確認し、同意しました」のチェックボックスをオンにします。
c) アカウントを Multicloud Defenseに接続する前に、イメージを展開せずに [終了（Exit）] をクリックすることを**強く**お勧めします。

Multicloud Defense Gateway を展開する予定のコンパートメントごとにこれらの手順を繰り返す必要がある場合があります。

Oracle アカウントの接続

Multicloud Defense Controller の簡単セットアップウィザードから OCI アカウントに接続するには、次の手順を実行します。

始める前に

- 既存の Oracle Cloud（OCI）アカウントが必要です。
- オンボーディングの前に、OCIアカウントの前提条件を満たしておく必要があります。詳細については、OCI アカウントの準備 （6 ページ）を参照してください。
- CDO テナントの管理者またはネットワーク管理者のユーザーロールが必要です。
- Multicloud Defense を CDO テナントに対して有効にしておく必要があります。

手順

ステップ 1 Multicloud Defense Controller ダッシュボードから、ウィンドウの左側にある [設定（Setup）] をクリックします。

ステップ 2 [アカウントの接続（Connect Account）] を選択します。

ステップ 3 OCI アイコンを選択します。

ステップ 4 [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 5 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 6 セットアップモーダルで次の情報を入力します。

a) [OCIアカウント名（OCI Account Name）] を入力します。この名前は識別用に Multicloud Defense Controller 内でのみ使用されます。

b) （任意）[説明（Description）] にアカウントの説明を入力します。

c) [テナントOCID（Tenancy OCID）] を入力します。これは、OCI ユーザーから取得したテナントの Oracle Cloud 識別子です。

d) OCI ユーザーに割り当てられている [秘密キー（Private Key）] を入力します。

ステップ 7 [次へ（Next）] をクリックします。

次のタスク

アカウントを接続すると、Multicloud Defense Controller はクラウド サービス プロバイダー アカウントに関連付けられているアセットとインベントリの検出を自動的に開始します。これはトラフィックの検出とは異なることに注意してください。Multicloud Defense Controller はデフォルトでアカウントのアセットとインベントリを検出するため、このウィザードの次のステップは、Azure アカウントのトラフィックの有効化です。

トラフィックの可視性の有効化

トラフィックの可視性を有効にすると、次のログを収集することで、クラウドアカウント内のトラフィックフローに関する認識が深まります。

- NSG フローログ
- （**AWS のみ**）VPC フローログ
- DNS ログ
- Route53 クエリロギング

Multicloud Defense はフローログと DNS クエリログを使用してトラフィックフローを理解し、脅威インテリジェンスのフィードと関連付け、Multicloud Defense を使用して保護できる既存の脅威に関するインサイトを提供します。

トラフィックの可視性を有効にするプロセスは、クラウドアカウントのタイプごとに異なりますが、一般的に、クラウドアカウントのリージョン、モニターする VPC/Vnet、ネットワークセキュリティ グループ、ログ用のクラウド ストレージ アカウントなど、アカウントの特徴を特定する必要があります。

（注） Multicloud Defense は、現時点では OCI のトラフィックの可視性をサポートしていません。この手順の代替アクションとして、アセット検出を有効にすることを強くお勧めします。つまり、Multicloud Defense が外部環境からアセットのメタデータを識別および収集し、収集して得られたデータによって、移行の支援に使用できるインベントリが作成されます。詳細については、アセット検出とインベントリの有効化を参照してください。

AWS アカウントのトラフィックの有効化

セットアップウィザードで AWS アカウントのトラフィックの可視性を有効にするには、次の手順を実行します。

手順

ステップ 1 Multicloud Defense Controller ポータルで、左側のナビゲーションバーの [設定（Setup）] をクリックします。

ステップ 2 セットアップウィザードで、[トラフィックの可視性の有効化（Enable Traffic Visibility）] をクリックします。

ステップ 3 モーダルに次の情報を入力します。

a) [CSPアカウント（CSP Account）]：ドロップダウンメニューを使用して、Multicloud Defense Controller がサービス VPC/VNet を展開するクラウド サービス プロバイダー アカウントを選択します。

b) [リージョン（Region）]：ドロップダウンメニューを使用して、選択したクラウド サービス プロバイダーの所在地があるリージョンを選択します。
c) [VPC]：選択したクラウド サービス プロバイダーのタイプに適用される、使用可能な VPC のテーブルをスクロールし、適切な VPC にチェックを入れます。VPC がすぐに表示されない場合は、[更新（Refresh）] アイコンをクリックして現在のリストを更新します。
d) [S3バケット（S3 Bucket）]：ドロップダウンメニューを使用して、アカウントから既存の S3 バケットを選択します。これは DNS クエリと VPC/VNet フローログが保存される場所です。この S3 バケットは、前のステップで作成されたものです。

ステップ 4 [Next] をクリックします。

次のタスク

アカウントを保護します。

Azure アカウントのトラフィックの有効化

セットアップウィザードから Azure アカウントのトラフィックの可視性を有効にするには、次の手順を実行します。

手順

ステップ 1 Multicloud Defense Controller ポータルで、左側のナビゲーションバーの [設定（Setup）] をクリックします。
ステップ 2 セットアップウィザードで、[トラフィックの可視性の有効化（Enable Traffic Visibility）] をクリックします。
ステップ 3 モーダルに次の情報を入力します。

a) [CSPアカウント（CSP Account）]：ドロップダウンメニューを使用して、Multicloud Defense Controller がサービス VPC/VNet を展開するクラウド サービス プロバイダー アカウントを選択します。
b) [リージョン（Region）]：ドロップダウンメニューを使用して、選択したクラウド サービス プロバイダーの所在地があるリージョンを選択します。
c) スクリプトをコピーして実行します。Azure アカウントを再オンボーディングし、クラウドストレージバケットを再利用しようとしている場合、このスクリプトでは新しいストレージバケットは自動的に作成されないことに注意してください。デフォルトまたは既存のストレージバケットを使用できますが、それ以外の場合は、Azure ダッシュボードで新しいストレージバケットを作成するか、実行前にこのスクリプトコマンドを手動で編集して、アカウントのフローログを保存するストレージバケットの名前を含める必要があります。
d) [NSG]：トラフィックを表示するネットワーク セキュリティ グループ（NSG）を少なくとも 1 つ選択します。選択したクラウド サービス プロバイダーのタイプに適用される、使用可能な NSG のテーブルをスクロールし、適切な NSG にチェックを入れます。NSG がすぐに表示されない場合は、[更新（Refresh）] アイコンをクリックして現在のリストを更新します。
e) [ストレージアカウント（Storage Account）]：上記で選択したリージョンに完全なリソース ID を入力します。

ステップ 4 [Next] をクリックします。

次のタスク

アカウントを保護します。

GCP プロジェクトのトラフィックの有効化

セットアップウィザードで GCP アカウントのトラフィックの可視性を有効にするには、次の手順を実行します。

手順

ステップ 1 Multicloud Defense Controller ポータルで、左側のナビゲーションバーの [設定（Setup）] をクリックします。

ステップ 2 セットアップウィザードで、[トラフィックの可視性の有効化（Enable Traffic Visibility）] をクリックします。

ステップ 3 モーダルに次の情報を入力します。

a) [CSPアカウント（CSP Account）]：ドロップダウンメニューを使用して、Multicloud Defense Controller がサービス VPC/VNet を展開するクラウド サービス プロバイダー アカウントを選択します。

b) [クラウドストレージ（Cloud Storage）]：選択した GCP プロジェクトにすでに割り当てられている、使用可能なクラウドストレージバケットを選択します。

c) [VPCの選択（Select VPC(s)）]：トラフィックを表示する VPC を少なくとも 1 つ選択します。選択したクラウドサービスプロバイダーのタイプに適用される、使用可能な VPC のテーブルをスクロールし、適切な VPC にチェックを入れます。VPC がすぐに表示されない場合は、[更新（Refresh）] アイコンをクリックして現在のリストを更新します。

d) スクリプトをコピーして実行します。GCP プロジェクトを再オンボーディングし、クラウドストレージバケットを再利用しようとしている場合、このスクリプトでは新しいストレージバケットは自動的に作成されないことに注意してください。デフォルトまたは既存のストレージバケットを使用できますが、それ以外の場合は、GCP ダッシュボードで新しいストレージバケットを作成するか、実行前にこのスクリプトコマンドを手動で編集して、GCP プロジェクトのフローログを保存するストレージバケットの名前を含める必要があります。

ステップ 4 [Next] をクリックします。

次のタスク

アカウントを保護します。

アカウントを保護

集中型モデルまたは分散モデルで展開されたゲートウェイを使用してアカウントを保護します。

集中型モデルでは、Multicloud Defense はゲートウェイを含めるように VPC または VNet をオーケストレーションして展開します。これは、VPC または VNet、および必要なすべての追加コンポーネントがオーケストレーションされ、さらにこの構造内でゲートウェイが展開されることを意味します。

分散モデルでは、Multicloud Defense は、ネットワークですでに使用可能な既存のインフラストラクチャ内にゲートウェイを構築して展開します。

次のいずれかの手順に進み、アカウントを保護します。

集中型モデル：VPC または VNet の追加

ゲートウェイを格納し、アカウントを保護するために VPC または VNet を作成して追加するには、次の手順を実行します。

始める前に

このウィザードを開始する前に、少なくとも 1 つのクラウドサービスプロバイダーが Multicloud Defense Controller に接続されている必要があります。一部のプロバイダーでは、必要なパラメータに応じてこの手順が変わる場合があることに注意してください。

手順

ステップ 1 Multicloud Defense Controller ポータルで、左側のナビゲーションバーの [設定（Setup）] をクリックします。

ステップ 2 セットアップウィザードで、[アカウントを保護（Secure Account）] をクリックします。

ステップ 3 [集中型（Centralized）] を選択して強調表示します。

ステップ 4 [Next] をクリックします。

ステップ 5 サービス VPC/VNet を追加します。

a) [名前（Name）]：サービス VPC/VNet の名前を入力します。作成されると、この名前は **[管理（Manage）] > [ゲートウェイ（Gateways）] > [サービスVPC/VNet（Service VPC/VNets）]**ページに表示されます。

b) （AWS のみ）[CSPアカウント（CSP Account）]：ドロップダウンメニューを使用して、Multicloud Defense Controller にすでに接続されているクラウド サービス プロバイダーのアカウントを選択します。サービス VPC/VNet が選択したアカウントに展開されます。

c) [リージョン（Region）]：ドロップダウンメニューを使用して、選択したクラウド サービス プロバイダーの所在地があるリージョンを選択します。

d) [CIDRブロック（CIDR Block）]：サービス VPC/VNet がアタッチされているトランジットゲートウェイの一意の値を入力します。

e) （GCP のみ）[データパスCIDRブロック（Datapath CIDR Block）]：スポーク VPC と重複してはならない、データパス VPC の有効な CIDR ブロックを入力します。

f) （GCP のみ）[管理CIDRブロック（Management CIDR Block）]：管理 VPC の有効な CIDR ブロックを入力します。

g) [可用性ゾーン（Availability Zones）]：生成されたリストから、少なくとも 1 つの可用性ゾーンを選択します。最適な結果を得るには、2 つのゾーンを選択することを**強く**お勧めします。

h) （Azure のみ）[リソースグループ（Resource Group）]：ドロップダウンメニューを使用して、ゲートウェイを関連付けるリソースグループを選択します。現在リソースグループが一覧表示されていない場合は、この画面から [リソースグループの作成（Create Resource Group）] を実行できます。

i) （AWS のみ）[トランジットゲートウェイ（Transit Gateway）]：ドロップダウンメニューを使用して、関連付けする VPC で利用可能なトランジットゲートウェイを選択します。利用可能なものがない場合は、[新規作成（create_new）] をクリックして、このウィンドウからトランジットゲートウェイを作成します。

j) （AWS および Azure のみ）[NATゲートウェイを使用（Use NAT Gateway）]：すべての出力トラフィックを NAT ゲートウェイ経由で送信する場合は、このオプションをオンにします。Multicloud Defense は、選択された可用性ゾーンごとに NAT ゲートウェイを自動的に作成します。

ステップ 6 [Next] をクリックします。

次のタスク

ゲートウェイを追加します。

分散モデル

分散ゲートウェイモデルの場合は、使用しているクラウド サービス プロバイダーに従って、次の手順を実行します。

Azure 分散モデル：ゲートウェイの作成

分散モデルで Azure アカウントのゲートウェイを作成するには、次の手順を実行します。

手順

ステップ 1 Multicloud Defense Controller ポータルで、左側のナビゲーションバーの [設定（Setup）] をクリックします。

ステップ 2 セットアップウィザードで、[アカウントを保護（Secure Account）] をクリックします。

ステップ 3 [分散（Distributed）] を選択して強調表示します。

ステップ 4 [Next] をクリックします。

ステップ 5 次のゲートウェイ情報を入力します。

a) [アカウント（Account）]：ドロップダウンメニューを使用して、ゲートウェイを展開する Azure アカウントを選択します。

b) [名前（Name）]：ゲートウェイの名前を入力します。この名前は、**[管理（Manage）]**>**[ゲートウェイ（Gateways）]**ページに表示されます。

c) （任意）[説明（Description）]：他のゲートウェイと区別するのに役立つようなゲートウェイの説明を入力します。

d) [インスタンスタイプ（Instance Type）]：ドロップダウンメニューを使用して、ゲートウェイを展開するインスタンスタイプを選択します。

e) [インスタンスの最小数（Minimum Instances）]：可用性ゾーンごとに自動スケーリンググループに展開されるインスタンスの最小数を選択します。

f) [インスタンスの最大数（Minimum Instances）]：可用性ゾーンごとに自動スケーリンググループに展開されるインスタンスの最大数を選択します。

g) [ヘルスチェックポート（HealthCheck Port）]：ヘルスチェックのポート番号を入力します。Multicloud Defense Controller はデフォルト値として `65534` を使用します。

h) [ユーザー名（User Name）]：作成したゲートウェイへのアクセスに使用するユーザー名を入力します。

i) [パケットキャプチャプロファイル（Packet Capture Profile）]：ドロップダウンメニューを使用して、クラウドストレージバケットでパケットを保存する場所を選択します。オプションが一覧表示されていない場合は、[パケットキャプチャプロファイルの作成（Create Packet Capture Profile）] をクリックして、このウィンドウから作成します。

j) [ログプロファイル（Log Profile）]：ドロップダウンメニューを使用して、ログの転送先として使用するクラウド サービス プロバイダーを選択します。

k) [メトリックプロファイル（Metrics Profile）]：ドロップダウンメニューを使用して、メトリックを転送するエンティティを選択します。オプションが一覧表示されていない場合は、[メトリック転送プロファイルの作成（Create Metrics Forward Profile）] をクリックして、このウィンドウから作成します。

l) [NTPプロファイル（NTP Profile）]：ドロップダウンメニューを使用して、ゲートウェイに関連付けられている NTP プロファイルを選択します。オプションが一覧表示されていない場合は、[作成（Create）] をクリックして、このウィンドウから作成します。

m) [セキュリティ（Security）]：ゲートウェイが処理する想定のトラフィックフローのタイプを選択します。入力セキュリティは、パブリックインターネットからプライベートネットワークに流れるトラフィックを対象としています。 East-West および出力セキュリティは、プライベートネットワークからのアウトバウンドトラフィックと、データセンター間を移動するトラフィックを対象としています。

n) [ゲートウェイイメージ（Gateway Image）]：ドロップダウンメニューを使用して、ゲートウェイに展開するゲートウェイイメージを選択します。

o) [ポリシールールセット（Policy Ruleset）]：ドロップダウンメニューを使用して、展開するポリシールールセットを選択し、トラフィックの処理を開始します。ルールセットがリストされていない場合は、[新規作成（Create new）] をクリックして、このウィンドウからポリシールールセットを作成します。

p) [リージョン（Region）]：ドロップダウンメニューを使用して、ゲートウェイが展開されているリージョンを選択します。

q) [VPC/VNet ID]：ドロップダウンメニューを使用して、ゲートウェイが展開されている VPC を選択します。

r) [キーの選択（Key Selection）]：SSH 公開キーまたは SSH キーペアのいずれかを選択します。次のテキストフィールドに、ゲートウェイに適用する値を入力します。

s) [リソースグループ（Resource Group）]：ドロップダウンメニューを使用して、ゲートウェイに適用される既存のリソースグループを選択します。

t) [ユーザー割り当てアイデンティティID（User Assigned Identity ID）]：有効な値を入力します。

u) [管理セキュリティグループ（Mgmt. Security Group）]：ドロップダウンメニューを使用して、ゲートウェイ管理インターフェイスに使用するセキュリティグループを選択します。Multicloud Defense で作成されたサービス VPC を選択すると、管理専用のセキュリティグループが作成されることに注意してください。

v) [データパスセキュリティグループ（Datapath Security Group）]：ドロップダウンメニューを使用して、ゲートウェイ データパス インターフェイスに使用するセキュリティグループを選択します。Multicloud Defense で作成されたサービス VPC を選択すると、データパス専用のセキュリティグループが作成されます。

w) [ディスク暗号化（Disc Encryption）]：Azure マネージド暗号化またはカスタマーマネージド暗号化キーを使用してディスク暗号化を有効にします。カスタマーマネージド暗号化キーを選択した場合、展開を成功させるには、IAMポリシーを作成して展開する必要があります。

x) [可用性ゾーン（Availability Zone）]：ドロップダウンメニューを使用して可用性ゾーンを選択します。

y) [管理サブネット（Mgmt. Subnet）]：ドロップダウンメニューを使用して、管理インターフェイスの管理サブネットを選択します。

z) [データパスサブネット（Datapth Subnet）]：ドロップダウンメニューを使用して、データパスインターフェイスのデータパスサブネットを選択します。

インスタンスタイプをさらに追加するには、[+]アイコンをクリックします。その後、[-]アイコンを使用して追加のインスタンスタイプを削除できます。

ステップ 6 [Next] をクリックします。

ステップ 7 次の [詳細設定（Advanced Settings）] に入力します。

a)

ステップ 8 [Next] をクリックします。

ステップ 9 レビュー

次のタスク

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。