Azure

Azure アカウントの準備

Multicloud Defense Controller に接続してオンボーディングする前に、次の手順で Azure アカウントとサブスクリプションを準備します。

- Microsoft Entra ID へのアプリケーションの登録サブスクリプションが Microsoft Entra ID に関連付けられていることを確認します。Azure ポータルで**アプリケーション登録**のリストを確認し、サブスクリプションが Multicloud Defense に正しくリンクされているかどうかを確認します。
- Azure サブスクリプションのアプリケーションに割り当てるカスタムロールの作成します。
- Multicloud Defense ダッシュボードから Multicloud Defense Controller に Azure サブスクリプションを接続する （4 ページ）

自動スクリプトを使用できない場合は、アカウントを手動でオンボーディングする別の手順を参照してください（こちら）。

（注） Multicloud Defense で構成するサブスクリプションが複数ある場合は、1 つのサブスクリプションで Multicloud Defense ダッシュボードから Multicloud Defense Controller に Azure サブスクリプションを接続する （4 ページ） の手順を実行してから、Azure ポータルでポリシーを変更して他のサブスクリプションを追加します。これらのサブスクリプションは個別にオンボーディングする必要がありますが、Multicloud Defense に一括で関連付けることができます。

Microsoft Entra ID へのアプリケーションの登録

Multicloud Defense アプリケーションを Entra ID に登録するには、次の手順を実行します。

手順

ステップ 1 Azure ポータルから [Microsoft Entra ID] に移動します。

ステップ 2 [アプリケーションの登録（App Registration）] を選択します。

ステップ 3 [新規登録（New Registration）] をクリックします。

ステップ 4 新規登録するアプリケーションを示す名前を入力します（例：Multicloud Defense Controller）。 [サポートされているアカウントタイプ（Supported Account Types）] で、2 番目のオプションである [任意の組織ディレクトリのアカウント（Accounts in any organizational directory）] を選択します。

ステップ 5 組織に適したオプションを選択します。[リダイレクトURI（Redirect URI）] は、アプリケーション登録の作成時には必要ないことに注意してください。

ステップ 6 [登録（Register）] をクリックします。

ステップ 7 新しく作成したアプリケーションの下にある左側のナビゲーションバーで、[証明書およびシークレット（Certificates & secrets）] をクリックします。

ステップ 8 [+新しいクライアントシークレット（+ New Client Secret）] をクリックし、[クライアントシークレットの追加（Add a client secret）] ダイアログに必要な情報を入力します。

- [説明（Description）]：説明を追加します（例：Multicloud Defense-controller-secret1）
- [有効期限（Expires）]：[なし（Never）] を選択します。この選択はいつでも行うことができます。現在のシークレットが期限切れになったら、新しいシークレットを作成する必要があります）

ステップ 9 [追加（Add）] をクリックします。クライアントシークレットが [値（Value）] 列の下に入力されます。

ステップ 10 クライアントシークレットをメモ帳にコピーします。これは 1 回だけ表示され、再度表示されることはありません。

ステップ 11 左側のナビゲーションバーで、[概要（Overview）] をクリックします。

ステップ 12 アプリケーション（クライアント）ID とディレクトリ（テナント）ID をメモ帳にコピーします。

アプリケーションに割り当てるカスタムロールの作成

CloudFormation テンプレートによって次のロールが作成されます。

- [カスタムロール（Custom Role）]：カスタムロールは、インベントリ情報を読み取り、リソース（VM、ロードバランサなど）を作成する権限をアプリケーションに付与します。カスタムロールは複数の方法で作成できます。

Multicloud Defense Controller 用に作成されたアプリケーションに割り当てられる**カスタムロール**を作成します。カスタムロールは、インベントリ情報を読み取り、リソース（VM、ロード

バランサなど）を作成する権限をアプリケーションに付与します。カスタムロールは複数の方法で作成できます。

手順

ステップ 1 [サブスクリプション（Subscriptions）] に移動し、[アクセス制御（IAM）（Access Control (IAM)）] をクリックします。

ステップ 2 [ロール（Roles）] をクリックし、上部のメニューバーで**[+追加（+Add）]**>**[カスタムロールの追加（Add Custom Role）]**をクリックします。

ステップ 3 カスタムロールに名前を付けます（例：`Multicloud Defense-controller-role`）。

ステップ 4 JSON 編集画面が表示されるまで、[次へ（Next）] をクリックし続けます。

ステップ 5 画面で [編集（Edit）] をクリックし、JSON テキストの [権限>アクション（permissions > actions）] セクションで、角カッコの間に次のコンテンツをコピーして貼り付けます（インデントを維持する必要はありません）。

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/natGateways/*",
"Microsoft.Network/networkinterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read"
```

ステップ 6 **任意**：Multicloud Defense で複数のサブスクリプションを使用する場合は、`assignableScopes` で JSON を編集して別のサブスクリプション品目を追加か、またはすべてのサブスクリプションでカスタムロールを使用できるように *****（星印）に変更する必要があります。

ステップ 7 テキストボックスの上部にある [保存（Save）] をクリックします。

ステップ 8 [確認して作成（Review + Create）] をクリックして、ロールを作成します。

ステップ 9 カスタムロールが作成されたら、[アクセス制御（IAM）（Access Control (IAM)）] に戻ります。

ステップ 10 上部のメニューバーで、**[追加（Add）]** > **[ロール割り当ての追加（Add role assignment）]**をクリックします。

ステップ 11 [ロール（Role）] ドロップダウンで、上で作成したカスタムロールを選択します。

ステップ 12 [アクセス権の割り当て先（Assign Access To）] ドロップダウンリストはデフォルト値のままとします（Azure AD ユーザー、グループ、またはサービスプリンシパル）。

ステップ 13 [選択（Select）] テキストボックスに、先ほど作成したアプリケーションの名前（例：`Multicloud Defensecontrollerapp`）を入力し、[保存（Save）] をクリックします。

ステップ 14 [サブスクリプション（Subscription）] ページで、左側のメニューバーの [概要（Overview）] をクリックし、サブスクリプション ID をメモ帳にコピーします。

Multicloud Defense ダッシュボードから Multicloud Defense Controller に Azure サブスクリプションを接続する

前のセクションの説明に従ってAzureアカウントとサブスクリプションを準備したら、Multicloud Defense Controller にリンクできます。

手順

ステップ 1 Multicloud Defense Controller ダッシュボードで、[クラウドアカウント（Cloud Accounts）] ペインの [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 [Azure] を選択します。

ステップ 3 ステップ 1 で、リンクをクリックすると、Azure Cloud Shell が bash モードで開きます。

ステップ 4 ステップ 2 で、[コピー（Copy）] ボタンをクリックします。

ステップ 5 bash シェルでオンボーディングスクリプトを実行します。

（注）
- Multicloud Defense にすでに接続されている別の Azure サブスクリプションがある場合、同じ既存の名前で IAM ロールを作成すると、このスクリプトが失敗する可能性があります。複数の IAM ロールを設定することはできません。回避策として、`-p`プレフィックスを付けてBashスクリプトを実行します。
- サブスクリプション全体でスポーク VNet 保護をサポートするには、Active Directory アプリケーション登録を使用してサブスクリプションをオンボーディングします。

ステップ 6 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。

ステップ 7 （任意）サブスクリプションの説明を入力します。

ステップ 8 [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。

ステップ 9 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。

ステップ 10 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。

ステップ 11 [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 12 [保存して続行（Save & Continue）] をクリックします。

Azure サブスクリプションがオンボーディングされ、ダッシュボードに戻ると、新しいデバイスが追加されたことを確認できます。

次のタスク

- Azure ポータルでポリシーを作成します。
- Azure サブスクリプションの VNet ルートテーブル （5 ページ）
- オンボーディング後の手順 （6 ページ）。
- トラフィックの可視性を有効にします。

Azure サブスクリプションの VNet ルートテーブル

出力展開の場合、ユーザー定義ルーティング（UDR）テーブルを作成して、スポークネットワークの宛先を手動で指定する必要があります。ピア間で秘密情報が交換されるため、デフォルトで、Azure との両方に、ルーティング値を自動的に識別する機能があります。これはイングレスゲートウェイには最適ですが、エグレスゲートウェイには適していません。

出力展開用にこれらの値またはサブネット ルーティング テーブル全体をオーバーライドするには、Azure ポータルで値を再割り当てする必要があります。詳細については、Azure のドキュメントを参照してください。

ゲートウェイが使用しているルーティングテーブルの種類

ルーティングテーブルがピアデバイスの VNet に基づいているかどうかを判断するには、**[管理（Manage）]** > **[ゲートウェイ（Gateways）]** でサブスクリプションに割り当てられているゲートウェイを表示し、[詳細の表示（View Details）] をクリックします。このウィンドウから、**[トラブルシューティング（Troubleshooting）]** > **[データパスサブネット（Datapath Subnet）]** タブに移動します。ルーティングテーブルが表示されない場合、サブスクリプションはピアデバイスからプルされたデフォルトのルーティングテーブルを使用しています。

Multicloud Defense によって作成されるロール

提供されたスクリプトを使用してクラウドサービスアカウントを Multicloud Defense Controller にオンボーディングすると、サービス間の通信を確実に保護するために、クラウド サービス プロバイダーのパラメータ内でユーザーロールが作成されます。クラウド サービス プロバイダーに応じて、さまざまなロールと権限が作成されます。

アカウントをオンボーディングすると、次のロールが作成されます。

Azure IAM ロール

Multicloud Defense Controller 用に作成されたアプリケーションに割り当てるカスタムロールを作成する必要があります。カスタムロールは、インベントリ情報を読み取り、VM、ロードバランサなどのリソースを作成する権限をアプリケーションに付与します。カスタムロールは複数の方法で作成できます。最も簡単な方法の 1 つは、サブスクリプションに移動し、[アクセス制御（IAM）（Access Control (IAM)）] をクリックすることです。

カスタムロールを追加する場合は、ロールに名前を付け、JSON ファイルを編集する必要があります。このファイルは、サブスクリプションと Multicloud Defense Controller 間の通信とデータ転送を許可するために必要なすべての権限に対応します。次のリストは、このために必要なすべての権限を示します。

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/natGateways/*",
"Microsoft.Network/networkinterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read"
```

オンボーディング後の手順

Multicloud Defense で Azure アカウントをまとめて保護するには、次の手順を実行します。

Azure VNet のセットアップ

このドキュメントでは、VNet で Multicloud Defense Gateway を作成できるように、VNet で作成するリソース（サブネット、セキュリティグループ）と要件について説明します。

サブネット

ゲートウェイの展開を設定するときに、Multicloud Defense Controller は、[管理（management）] および [データパス（datapath）] サブネット情報の入力を求めます。

[管理（management）] サブネットは、インターネットへのデフォルトルートを持つルートテーブルに関連付ける必要があるパブリックサブネットです。Multicloud Defense Gateway インスタ

ンスには、Multicloud Defense Controller との通信に使用する、このサブネットにアタッチされたインターフェイスがあります。このインターフェイスは、Multicloud Defense Controller と Multicloud Defense Gateway インスタンス間のポリシーのプッシュやその他の管理およびテレメトリアクティビティに使用されます。お客様のアプリケーションのトラフィックは、このインターフェイスとサブネットを**通過しません**。インターフェイスは、以下の 「セキュリティグループ」セクションで説明されている [管理（management）] セキュリティグループに関連付けられます。

[データパス（datapath）] サブネットは、インターネットへのデフォルトルートを持つルートテーブルに関連付ける必要があるパブリックサブネットです。Multicloud Defense Controller は、このサブネットにネットワーク ロード バランサ（NLB）を作成します。さらに、Multicloud Defense Gateway インスタンスには、このサブネットにアタッチされたインターフェイスがあります。お客様のアプリケーションのトラフィックは、このインターフェイスを**通過します**。セキュリティポリシーは、このインターフェイスを介して入力されるトラフィックに適用されます。インターフェイスは、「セキュリティグループ」セクションで説明されている [データパス（datapath）] セキュリティグループに関連付けられます。

セキュリティ グループ

管理セキュリティグループとデータパスセキュリティグループは、上記のサブネットセクションで説明されているように、Multicloud Defense Gateway インスタンスのそれぞれのインターフェイスに関連付けられます。

[管理（management）]セキュリティグループは、ゲートウェイインスタンスがコントローラと通信できるように、アウトバウンドトラフィックを許可する必要があります。必要に応じて、インバウンドルールでは、ポート 22（SSH）を有効にしてゲートウェイインスタンスへの SSH アクセスを許可します。Multicloud Defense Gateway が正常に機能するのに SSH は必須ではありません。

[データパス（datapath）] セキュリティグループはデータパスインターフェイスにアタッチされ、インターネットから Multicloud Defense Gateway へのトラフィックを許可します。現在、Multicloud Defense Controller はこのセキュリティグループを管理していません。アウトバウンドルールが存在し、トラフィックがこのインターフェイスから出力されることを許可する必要があります。Multicloud Defense Controller のセキュリティポリシーで設定され、Multicloud Defense Gateway によって使用されるポートごとに、インバウンドポートを開く必要があります。

たとえば、アプリケーションがポート 3000 で実行されていて、Multicloud Defense Gateway によってポート 443 でプロキシ接続されている場合、ポート 443 はデータパス セキュリティ グループで開く必要があります。この例は、アプリケーションにアタッチされているセキュリティグループでポート 3000 が開いていることも示しています。

ARM テンプレートの起動

を使用して、このページで説明されているすべてのリソースを作成します。

このテンプレートにより新しい VNet が作成されます。これは、既存の実稼働環境に手を加えることなく Multicloud Defense を開始する場合に非常に役立ちます。

テンプレートでは次のリソースが作成されます。

- VNet。
- 管理サブネット。
- データパスサブネット。
- アウトバウンドルールを持つ管理セキュリティグループ。
- ポート 443 のアウトバウンドルールとインバウンドルールを持つデータパス セキュリティグループ。

必要に応じて、追加のサブネットを作成してアプリケーションを実行し、アプリケーション固有のセキュリティグループを作成できます。

ARM テンプレートを起動するには、次の手順を実行します。

手順

ステップ 1 Azure アカウントにログインし、カスタムテンプレートを展開します。

ステップ 2 [エディタで独自のテンプレートを構築する（Build your own template in the editor）] をクリックします。

ステップ 3 ARM テンプレートから内容をコピーし、エディタに貼り付けます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [サブスクリプション（Subscription）]、[リソースグループ（Resource group）]、および[リージョン（Region）] を選択します。

ステップ 6 [確認して作成（Review + create）] をクリックします。

ステップ 7 すべてのリソースが作成されるまで数分待ちます。

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。