



## Microsoft Azure Virtual WAN の統合

簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。

**Cisco vManage から Cisco Catalyst SD-WAN Manager への変更、Cisco vAnalytics から Cisco Catalyst SD-WAN Analytics への変更、Cisco vBond から Cisco Catalyst SD-WAN Validator への変更、Cisco vSmart から Cisco Catalyst SD-WAN コントローラへの変更、および Cisco コントローラから Cisco Catalyst SD-WAN 制御コンポーネントへの変更。**すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 1: 機能の履歴

機能名	リリース情報	説明
Azure Virtual WAN と Cisco Catalyst SD-WAN の自動統合	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	<p>この機能は、Cisco Catalyst 8000V Edge ソフトウェア (Cisco Catalyst 8000V) をトランジット VNet 内に展開するのではなく、Azure Virtual WAN ハブ内に展開できるようにすることで、Cloud OnRamp と Microsoft Azure の統合を強化します。また、Cisco Catalyst 8000V を介した Azure Virtual WAN ハブへの Cisco Catalyst SD-WAN ファブリック接続を自動化します。リージョン間の Azure Virtual WAN ハブ間の接続もサポートされます。</p> <p>さらに、Cisco SD-WAN Manager を使用して作成された Azure Virtual WAN ハブを、内部に Azure ファイアウォールを展開することで、セキュリティ保護付きハブに変換することができます。ただし、セキュリティ保護付き仮想ハブは、Microsoft Azure ポータルを使用してのみ設定できます。</p>

機能名	リリース情報	説明
Azure ポータルを使用した Cisco Catalyst SD-WAN と Azure Virtual WAN ハブの統合	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	Cisco Catalyst SD-WAN と Azure Virtual WAN の統合の一環として、Azure ポータルを使用して、Cisco Catalyst 8000V インスタンスのブートストラップ構成ファイルをアップロードすることもできます。これらのインスタンスは、その後、Azure ポータルを使用して仮想 WAN ハブを作成する際に使用できます。
仮想ハブファイアウォールまたはローカルファイアウォールへのトラフィックフローのルーティング	Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能により、Microsoft Azure Virtual WAN ハブのトラフィックをローカルブランチルータのファイアウォールにルーティングしたり、ローカルブランチのトラフィックを Azure のセキュリティ保護付き仮想ハブに転送したりして、Azure Firewall Manager のセキュリティポリシーの対象にすることができます。
ネットワーク仮想アプライアンスの Azure スケーリング、監査、およびセキュリティ	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、SKU スケール値を編集し、ネットワーク仮想アプライアンス (NVA) のセキュリティを強化することができます。監査サービスは、Cisco SD-WAN Manager と Azure クラウドデータベースからの情報を比較し、不一致を特定します。
定期的な監査、Azure のスケーリングと監査の強化、および ExpressRoute 接続。	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	Cisco SD-WAN Manager は、2 時間ごとのオプションの定期監査を提供しています。この自動監査はバックグラウンドで実行され、不一致のレポートが生成されます。自動修正オプションを有効にすると、Cisco SD-WAN Manager は定期監査中に検出された回復可能な問題を自動的に解決します。  オンデマンド監査の開始後に生成された個々の不一致を修正できます。  Cisco SD-WAN Manager は、Cisco Catalyst SD-WAN トンネルを介したブランチオフィスから NVA への ExpressRoute 接続をサポートしています。ExpressRoute 接続は、データ転送のための、信頼性が高く、遅延が少なく、接続が高速なプライベートネットワークです。

機能名	リリース情報	説明
各リージョンの複数の仮想ハブのサポート	Cisco vManage リリース 20.11.1 Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a	1つの Azure リージョンに複数の仮想ハブを作成できます。
Azure インスタスタタイプの追加	Cisco Catalyst SD-WAN Manager リリース 20.12.1 Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a	Azure の米国中西部およびオーストラリア東部リージョン用に、Standard_D16_v5 Azure インスタスタタイプが追加されました。これには、16 個の CPU コアと 64 GB のメモリが含まれています。このタイプのインスタンスは、20、40、60、および 80 の SKU スケール値で展開できます。

- [Azure Virtual WAN 統合に関する情報 \(3 ページ\)](#)
- [Azure Virtual WAN 統合でサポートされるデバイス \(13 ページ\)](#)
- [Azure Virtual WAN 統合の前提条件 \(15 ページ\)](#)
- [Azure Virtual WAN 統合の制約事項 \(16 ページ\)](#)
- [Azure Virtual WAN 統合のユースケース \(17 ページ\)](#)
- [Azure Virtual WAN 統合の設定 \(18 ページ\)](#)
- [Azure Virtual WAN 統合の確認 \(35 ページ\)](#)
- [Cisco SD-WAN Manager を使用した Azure Virtual WAN 統合のモニター \(37 ページ\)](#)

## Azure Virtual WAN 統合に関する情報

### Azure Virtual WAN ハブと Cisco Catalyst SD-WAN の統合

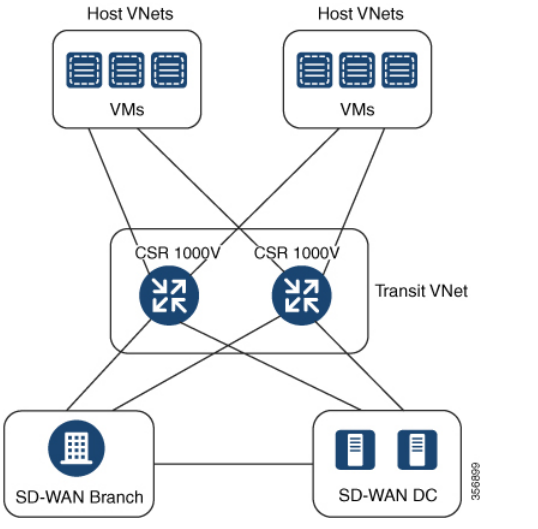
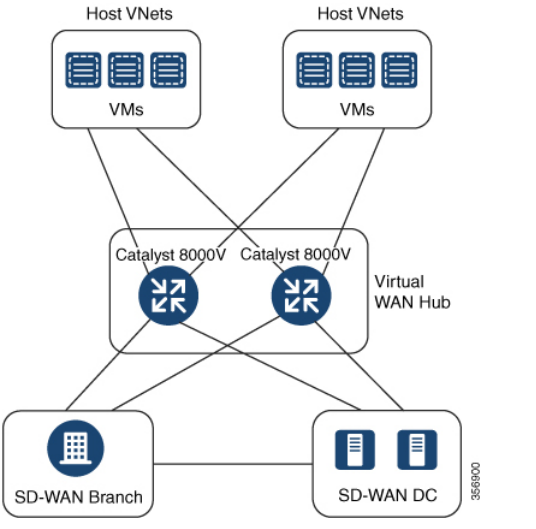
サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a、Cisco vManage リリース 20.4.1

Cisco Catalyst SD-WAN ソリューションと Azure Virtual WAN の統合により、Cloud OnRamp for Multicloud 展開が強化され、Cisco Catalyst 8000V Edge ソフトウェア (Cisco Catalyst 8000V) を Azure Virtual WAN ハブのネットワーク仮想アプライアンス (NVA) として設定できます。

この統合により、トランジット仮想ネットワーク (VNet) を作成する必要がなくなり、Azure 仮想 WAN ハブを介してホスト VNet 接続を直接制御できるため、クラウドサービスの消費モデルが簡素化されます。Azure Virtual WAN は、Microsoft Azure を介して最適化および自動化されたブランチ間の接続を提供するネットワークングサービスです。Azure と通信できるブランチデバイスを接続して設定できます。Azure 仮想ハブ内に Cisco Catalyst 8000V インスタンスを設定すると、より高速で広い帯域幅が提供され、トランジット VNet を使用する場合の速度と帯域幅の制限が克服されます。

## Cloud OnRamp for IaaS と Cloud OnRamp for Multicloud の比較

この表では、Microsoft Azure 統合のコンテキストでの Cloud OnRamp for IaaS と Cloud OnRamp for Multicloud の違いを示しています。

Azure 用の Cloud OnRamp for IaaS	Azure 用の Cloud OnRamp for Multicloud
	
<p>Cisco SD-WAN Manager での Cloud OnRamp for IaaS ワークフローを介したトランジット VNet の自動プロビジョニングを可能にします</p>	<p>Cisco SD-WAN Manager での Cloud OnRamp for Multicloud ワークフローを介した Azure 仮想ハブの自動プロビジョニングを可能にします</p>
<p>Cisco SD-WAN Manager がトランジット VNet 内の 2 つの Cisco Cloud Services Router 1000V シリーズ (Cisco CSR1000V) デバイスを自動的にプロビジョニングします</p>	<p>Cisco SD-WAN Manager が Azure 仮想ハブ内の 2 つの Cisco Catalyst 8000V インスタンスを自動的にプロビジョニングします</p>

Azure を使用した Cloud OnRamp for IaaS に関する情報と、トランジット VNet の設定方法については、「[Configure Cloud OnRamp for IaaS for Azure](#)」を参照してください。

## 仮想 WAN ハブ統合の仕組み

オーバーレイネットワークとパブリック クラウドアプリケーション間の接続は、Azure 用の Cloud OnRamp for Multicloud ワークフローの一環として Azure Virtual WAN ハブ内で設定された冗長 Cisco Catalyst 8000V インスタンスのペアによって提供されます。冗長ルータを使用してトランジットを形成すると、パブリッククラウドに対するパスの復元力が得られます。

Cisco SD-WAN Manager の Cloud OnRamp for Multicloud フローは、地理的なクラウドリージョン内の既存の VNet を検出し、選択した VNet をオーバーレイネットワークに接続できるようにします。このようなシナリオでは、Cloud OnRamp for Multicloud を使用すると、レガシーパブリッククラウド接続と Cisco Catalyst SD-WAN オーバーレイネットワークを簡単に統合できます。

Cisco SD-WAN Manager の構成ウィザードは、パブリック クラウドアカウントに接続するための Azure Virtual WAN ハブの起動を自動化します。また、このウィザードは、パブリック クラウドアプリケーションと、オーバーレイネットワーク内のブランチにいるそれらのアプリケーションのユーザーとの間の接続を自動化します。Cisco SD-WAN Manager では、タグを使用して、ブランチ内のサービス VPN をパブリッククラウドインフラストラクチャ内の特定の VNet にマッピングできます。

### VNet から VPN へのマッピング

Cisco SD-WAN Manager のインテント管理ワークフローは、Cisco SD-WAN VPN (ブランチネットワーク) と VNet 間の接続、および VNet から VNet への接続を可能にします。VNet は、Cloud OnRamp for Multicloud の Discover ワークフローで作成されたタグで表されます。VNet が仮想 WAN ハブに接続するようにマッピングされると、デフォルトルートが割り当てられ、デフォルトトラベルに伝達されます。Azure リージョン内で VNet タグを作成すると、同じタグを共有する他の VNet および VPN に基づいてマッピングが自動的に作成されます。

Cisco SD-WAN Manager が接続のインテントを記録すると、クラウドゲートウェイが存在するリージョンのクラウドでマッピングが実現されます。クラウドゲートウェイが異なるリージョンに存在しなくても、マッピングインテントを入力できます。マッピングインテントは、新しいクラウドゲートウェイまたはマッピングの変更が検出されたときに保持され、実現されます。クラウドゲートウェイが異なるリージョンでインスタンス化または検出されると、マッピングインテントがそれらのリージョンで実現されます。同様に、タグ付け操作はさまざまなリージョンのマッピングにも影響を与える可能性があり、タグごとのマッピングはクラウドで実現されます。



- (注) VNet タグにマッピングされるように選択した VPN は、重複する IP アドレスを持つことはできません。これは、Microsoft Azure Virtual WAN ではセグメンテーションがサポートされていないためです。

リージョン間の Azure ハブ間接続は、VNet タグを作成し、それらを VPN サイトにマッピングすることで有効になります。リージョン間のハブ間接続を有効にするために、追加の設定は必要ありません。VNet は、それぞれのリージョンの仮想 WAN ハブに関連付けられます。異なる Azure リージョン内の VNet が同じ VNet タグを共有している場合、そのような VNet 間の接続は自動的に確立され、VNet が接続されているそれぞれの仮想 WAN ハブを介して実行されます。

### Azure 仮想 WAN 統合ワークフローのコンポーネント

ブランチとデータセンターをパブリック クラウドインフラストラクチャに接続するためのクラウドゲートウェイは、Cisco Catalyst 8000V インスタンスをホストする論理オブジェクトです。Azure リソースグループ、Azure Virtual WAN、および Azure Virtual WAN ハブで構成されます。

### リソース グループ

すべての Azure ネットワーキングリソースはリソースグループに属し、リソースグループは Azure サブスクリプションの下に作成されます。Azure クラウドゲートウェイの場合、Azure 仮想 WAN と Azure 仮想 WAN ハブはリソースグループの下に作成されます。

したがって、Azure クラウドゲートウェイを作成する最初の手順は、リソースグループを作成することです。

リソースグループを作成したら、Azure 仮想 WAN を構成できます。

### Azure 仮想 WAN

Azure 仮想 WAN は、Azure ネットワーキングサービスのバックボーンです。既存の Azure リソースグループの下に作成されます。Azure 仮想 WAN には、各仮想ハブが異なる Azure リージョンに属している限り、複数の Azure 仮想ハブを含めることができます。Azure リージョンごとに 1 つの仮想ハブのみがサポートされます。

リージョン内のリソースグループで仮想 WAN を定義したら、次のステップは Azure 仮想 WAN ハブの作成です。

### Azure 仮想 WAN ハブ

Azure Virtual WAN ハブは、VPN サイトと NVA および VNet 間のコア接続を管理します。仮想ハブが作成されると、Cisco Catalyst 8000V インスタンスを Azure ネットワーキングサービスに統合できます。

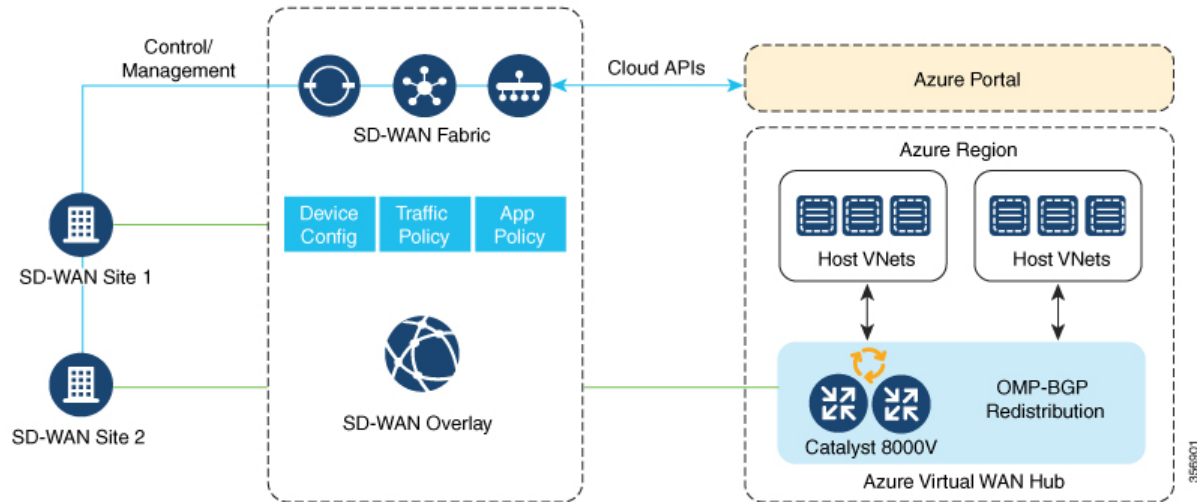
## 接続モデル

Azure Virtual WAN と Cisco Catalyst SD-WAN ソリューションの統合では、次の接続モデルがサポートされています。

- Cisco Catalyst SD-WAN ブランチから同じ Azure リージョン内の Azure ホスト VNet へ
- リージョン間の Azure 仮想ハブから仮想ハブへの接続

## Cisco Catalyst SD-WAN ブランチから Azure ホスト VNet へ（単一リージョン）

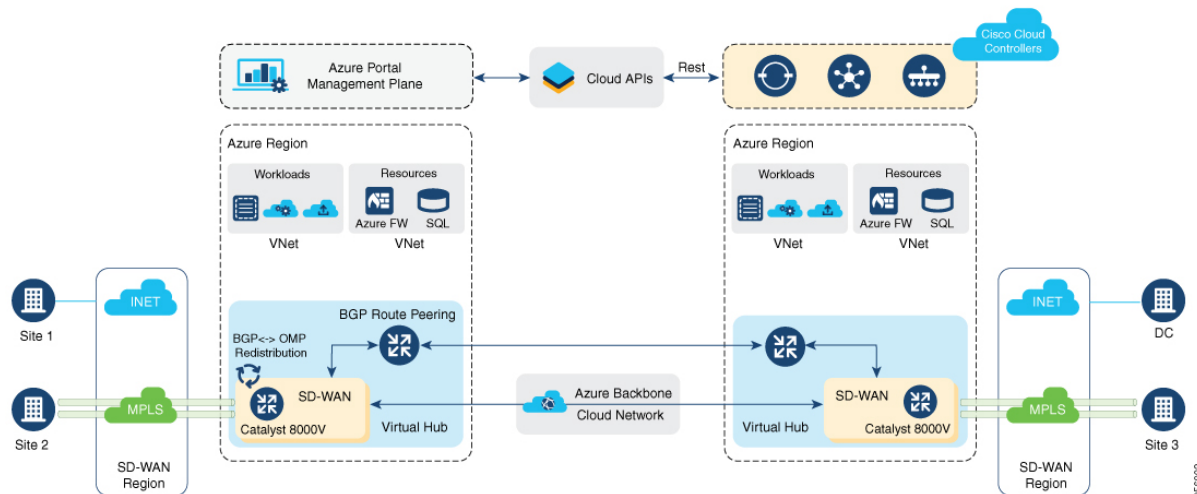
図 1: 同じ Azure リージョン内の VNet から VNet へのマッピング



このシナリオでは、仮想ハブはスタンドアロンであり、他の Azure リージョンの仮想ハブには接続されていません。このような場合、VNet は仮想ハブと同じリージョンに属し、Cisco SD-WAN Manager で定義されている VNet タグを使用してブランチ VPN に接続されます。

## 仮想 WAN ハブから仮想 WAN ハブへ（リージョン間）

図 2: 仮想ハブを介したリージョン間の VNet-VNet マッピング



この画像は、Azure バックボーンでのハブ間接続を表しています。この接続を個別に設定する必要はありません。異なる Azure リージョンの VNet が同じ VNet タグを共有している場合、この接続は自動的に実現されます。



## セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックフローのルーティング

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a、Cisco vManage リリース 20.6.1

Microsoft Azure 環境には、Azure Virtual Network (VNet) ワークロードとローカルブランチデバイス間の接続を可能にする仮想ハブが含まれています。Cisco Catalyst SD-WAN と Azure 環境の統合により、次のファイアウォールオプションが有効になります。

- Azure Virtual WAN ハブの発信インターネットトラフィックを、ローカルブランチルータのファイアウォールにルーティングする
- ローカルブランチルータからの発信インターネットトラフィックを Azure のセキュリティ保護付き仮想ハブにルーティングし、Azure Firewall Manager のセキュリティポリシーを適用する。



(注) Azure のセキュリティ保護付き仮想ハブは、Azure Firewall Manager によって管理されるセキュリティおよびルーティングポリシーを持つ Azure Virtual WAN ハブです。

どちらの場合も、リターントラフィックは発信インターネットトラフィックと同じパスをたどるため、同じファイアウォールポリシーが両方向のトラフィックに適用されます。

## Azure Virtual WAN の監査

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

マルチクラウド監査サービスは、Cisco SD-WAN Manager データベースの情報を Azure クラウドデータベースの情報と比較します。この情報には、Azure Virtual WAN、仮想ハブ、ネットワーク仮想アプライアンス、仮想ネットワーク、および VPN から仮想ネットワークへのマッピングが含まれます。その後、Cloud OnRamp for Multicloud は結果を比較して不一致を特定し、エラーの有無にかかわらず Microsoft Azure オブジェクトのリストを表示します。

Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、監査機能には次の拡張機能が組み込まれています。

- オンデマンド監査を開始すると、Cloud OnRamp for Multicloud の監査サービスが、Cisco SD-WAN Manager データベース内の情報と Azure クラウド内の情報の不一致を特定して一覧表示します。すべての不一致をまとめて修正するか、不一致を選択して個別に修正することができます。個々の不一致の横にあるチェックボックスをオンにすると、問題の簡単な説明が不一致の下に表示されます。

監査の不一致と解決の詳細については、「[Audit Discrepancies and Resolutions](#)」を参照してください。



- 定期監査を有効または無効にできるようになりました。詳細については、「[Enable Periodic Audit](#)」を参照してください。

## 定期監査に関する情報

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a、Cisco vManage リリース 20.8.1

Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、Cisco SD-WAN Manager は 2 時間間隔のオプションの定期監査を提供しています。この自動監査はバックグラウンドで実行され、不一致のレポートが生成されます。自動修正オプションを有効にすると、Cisco SD-WAN Manager は定期監査中に検出された回復可能な問題を自動的に解決します（存在する場合）。定期監査とその解決の詳細については、「[Audit Discrepancies and Resolutions](#)」を参照してください。



- (注) Cisco SD-WAN Manager バージョンをアップグレードした場合、定期監査と自動修正のオプションはデフォルトで無効になっています。[Cloud Global Settings] ウィンドウから有効にできます。詳細については、「[Add and Manage Global Cloud Settings](#)」を参照してください。

## 監査の不一致と解決

次の表に、監査の不一致と解決の詳細を示します。

表 2: 監査の不一致の例

不一致	説明	対処法	
		オンデマンド監査の [Fix Sync Issues] ボタン	定期監査と自動修正
タグ内の VNet が使用できない	Cisco SD-WAN Manager データベースでは VNet がタグ付けされているが、Azure ポータルでは使用できない場合。	Cisco SD-WAN Manager データベースから VNet を削除するには、[Fix Sync Issues] をクリックします。	Cisco SD-WAN Manager データベースから VNet を削除します。 注2を参照してください。
	Azure ポータルから VNet タグが削除された場合、または Cisco SD-WAN Manager と Azure ポータルの間で VNet タグの不一致がある場合。	Cisco SD-WAN Manager データベースから Azure ポータルに VNet タグを適用するには、[Fix Sync Issues] をクリックします。	Cisco SD-WAN Manager データベースから Azure ポータルに VNet タグを追加します。

不一致	説明	対処法	
		オンデマンド監査の[Fix Sync Issues] ボタン	定期監査と自動修正
ストレージアカウント（NVA の設定の保存）が使用できない	Azure ポータルではストレージアカウントが使用できないが、Cisco SD-WAN Manager データベースでは使用できる場合。	Cisco SD-WAN Manager データベースからストレージアカウントを削除するには、[Fix Sync Issues] をクリックします。	Cisco SD-WAN Manager データベースからストレージアカウントを削除します。 注2を参照してください。
仮想 WAN、vHub、および NVA が使用できない	Azure ポータルで仮想 WAN、vHub、または NVA が使用できない場合。	(注) クラウドゲートウェイを手動で削除しないでください。クラウドゲートウェイを削除すると、クラウドプロバイダー間で不一致が発生し、さらにプロビジョニングする機能に影響を与えたり、他の CoR 操作に影響を与えたりする可能性があります。	注2を参照してください。
Azure ポータルでマッピングが使用できない 注1を参照してください。	Cisco SD-WAN Manager データベースにはマッピングがありますが、Azure ポータルにはありません。	マッピングを Azure ポータルに再度追加するには、[Fix Sync Issues] をクリックします。	マッピングを Azure ポータルに再度追加します。

不一致	説明	対処法	
		オンデマンド監査の [Fix Sync Issues] ボタン	定期監査と自動修正
Cisco SD-WAN Manager データベースでマッピングを使用できない  (注) この不一致は Cisco vManage リリース 20.8.1 でのみ表示および修正できません。  。	Azure ポータルにはマッピングがありますが、Cisco SD-WAN Manager データベースにはありません。	マッピングを Cisco SD-WAN Manager データベースに再度追加するには、Cisco SD-WAN Manager ワークフローを使用して VNet を手動でタグ付けし、マッピングする必要があります。  (注) [Fix Sync Issues] をクリックしても、この問題は解決されません。	マッピングを Cisco SD-WAN Manager データベースに再度追加するには、Cisco SD-WAN Manager ワークフローを使用して VNet を手動でタグ付けし、マッピングする必要があります。  (注) 定期監査では、この問題は解決されません。



(注) 1. Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、この不一致を表示して修正することができます。



(注) 2. Cisco vManage リリース 20.9.x 以降では、自動修正オプションは使用できません。代わりに、次のようにクラウドサービス監査を表示します。Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択して、[Intent Management] ペインで [Audit] をクリックします。クラウドプロバイダーを選択します。Cisco SD-WAN Manager が監査レポートを表示します。

## ネットワーク仮想アプライアンスの SKU スケール値

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

Azure で Cisco Catalyst 8000V Edge インスタンスの SKU スケール値を編集できます。Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1 より前のリリースでは、SKU スケール値は編集できません。SKU スケール値を変更する場合は、クラウドゲートウェイを削除してから、新しい SKU スケール値を使用して再作成する必要があります。

より高い SKU スケール値を選択してパフォーマンスを向上させることや、より低い値を選択してコスト効率を高めることができます。

SKU スケール値を更新する方法の詳細については、「[Configure SKU Scale Value](#)」を参照してください。



(注) SKU スケール値を編集した後は、3～4分のネットワークダウンタイムが予想されます。

サポートされる SKU スケールの詳細については、「[Supported Azure Instances for Azure Virtual WAN Integration](#)」を参照してください。

## ネットワーク仮想アプライアンスのセキュリティルールの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

Microsoft Azure には、ネットワーク仮想アプライアンス (NVA) のセキュリティルールを編集するオプションがあります。Cisco SD-WAN Manager は、NVA のこれらのセキュリティルールの設定をサポートしています。

クラウドゲートウェイの作成中に起動される Cisco Catalyst 8000V NVA は、Cisco Catalyst SD-WAN 関連のポートを除くすべてのインバウンドポートの使用を禁止します。NVA 機能のセキュリティルール設定を使用すると、デバッグ目的などで、必要に応じて特定のポートを有効にすることができます。新しい NVA ルールを追加してポートを有効にすると、そのポートは2時間だけアクティブのままになります。同時に、別の NVA ルールを追加するとタイマーが再起動し、すべての有効なポートが2時間アクティブのままになります。



- (注)
- クラウドゲートウェイの操作が進行中の場合、NVA のセキュリティルールは設定できません。
  - Azure の送信元 IP アドレスには、サフィックスとして /30、/31、または /32 のみを使用できます。Azure の送信元 IP アドレスの例には、192.0.2.0/30、192.0.2.0/31、192.0.2.0/32 などがあります。

## NVA への Azure ExpressRoute 接続に関する情報

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a、Cisco vManage リリース 20.8.1

Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、Cisco SD-WAN Manager は、SD-WAN トンネルを介したブランチオフィスから NVA への ExpressRoute 接続をサポートしています。ExpressRoute 接続は、データ転送のための、信頼性が高く、遅延が少なく、接続が高速なプライベートネットワークです。

NVA への Azure ExpressRoute 接続の詳細については、「[Alternative Azure Designs](#)」を参照してください。

## 各リージョンの複数の仮想ハブに関する情報

サポート対象の最小リリース：Cisco vManage リリース 20.11.1



(注) この機能は、Azure クラウドと Azure Government クラウドの両方でサポートされています。

単一のリージョンで Azure に接続されている数千のサイトを持つ組織の場合、Microsoft は複数のクラウドゲートウェイの作成と、単一のリージョンで最大 8 つの仮想ハブの作成をサポートしています。

Cisco vManage リリース 20.10.1 以前のリリースでは、Azure Virtual WAN ソリューションは、1 つのリージョンで単一の仮想ハブのみをサポートしています。Cisco vManage リリース 20.11.1 以降では、このソリューションは各リージョンで複数の仮想ハブをサポートしています。

仮想ネットワークへのクラウドゲートウェイアタッチメントは、ロードバランシングアルゴリズムに基づいています。クラウドゲートウェイアタッチメントにタグを追加する場合は、[Auto] を選択し、これによって、ロードバランシングアルゴリズムに基づいて VNet を配布することができます。新しいクラウドゲートウェイを作成したときは、VNet を再配布して、すべてのクラウドゲートウェイ間で既存の VNet をロードバランスすることができます。[Auto] の VNet タグを選択した場合にのみ、クラウドゲートウェイ間で VNet を再割り当てできます。クラウドゲートウェイにアタッチされている専用 VNet タグを再割り当てすることはできません。

## Azure Virtual WAN 統合でサポートされるデバイス

### サポートされている Azure インスタンス

Azure Virtual WAN 統合は、次の Cisco Catalyst 8000V インスタンスをサポートしています。

表 3: SKU スケール値と Azure インスタンスタイプ

SKU スケール値	Azure インスタンスタイプ	インスタンスリソース	インスタンス数	サポート開始
2	Standard_D2_v2	2 個の CPU コアと 7 GB のメモリ	2	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a

SKU スケール値	Azure インスタンスタイプ	インスタンスリソース	インスタンス数	サポート開始
4	Standard_D3_v2	4 個の CPU コアと 14 GB のメモリ	2	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a
10	Standard_D4_v2	8 個の CPU コアと 28 GB のメモリ	2	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a
20 (Azure の米国中西部およびオーストラリア東部のリージョンでサポートされています)	Standard_D16_v5	16 個の CPU コアと 64 GB のメモリ	2	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a
40 (Azure の米国中西部およびオーストラリア東部のリージョンでサポートされています)	Standard_D16_v5	16 個の CPU コアと 64 GB のメモリ	3	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a
60 (Azure の米国中西部およびオーストラリア東部のリージョンでサポートされています)	Standard_D16_v5	16 個の CPU コアと 64 GB のメモリ	4	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a
80 (Azure の米国中西部およびオーストラリア東部のリージョンでサポートされています)	Standard_D16_v5	16 個の CPU コアと 64 GB のメモリ	5	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a

## Azure Virtual WAN 統合の前提条件

### セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックのルーティングの前提条件



- (注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ** への変更、および **Cisco コントローラ** から **Cisco Catalyst SD-WAN 制御コンポーネント** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a、Cisco vManage リリース 20.6.1

Cisco Cloud OnRamp for Multicloud は、Microsoft Azure 環境と連携して動作するように設定されています。「[Microsoft Azure Virtual WAN Integration](#)」を参照してください。

### ネットワーク仮想アプライアンスの Azure SKU スケーリング、監査、およびセキュリティルールの前提条件

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

- Cisco Cloud OnRamp for Multicloud は、Microsoft Azure 環境と連携して動作するように設定する必要があります。「[Microsoft Azure Virtual WAN Integration](#)」を参照してください。
- Azure クラウドアカウントの詳細。
- Azure マーケットプレイスへのサブスクリプション。
- Cisco SD-WAN Manager はインターネットに接続されている必要があり、Azure アカウントを認証するために Microsoft Azure と通信する必要があります。
- クラウドゲートウェイが動作している必要があります。



# Azure Virtual WAN 統合の制約事項

## Azure Virtual WAN 統合の制約事項

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a、Cisco vManage リリース 20.4.1

- Azure Virtual WAN ハブアーキテクチャは、セグメンテーションをサポートしていません。
- VNet へのマッピング用に選択する VPN には、IP アドレス空間が重複しないようにする必要があります。
- VNet のタグ付けにより、すべての VPN と VNet が他のすべての VPN と VNet で表示されます。
- 各 Azure リージョンおよび各リソースグループに設定できる仮想ハブは 1 つだけです。
- Cisco SD-WAN Manager では、1 つのリソースグループのみが許可されます。
- リージョン間のハブ間接続の場合、すべての仮想ハブが同じ Azure Virtual WAN の一部である必要があります。
- IPv6 はサポートしていません。
- Azure Virtual WAN ハブはトレースルートをサポートしていません。
- 仮想 WAN ハブに接続されているブランチは、仮想 WAN ハブのデフォルトルートテーブルにのみ割り当てることができます。
- Cisco SD-WAN Manager を介して Azure リージョンで仮想 WAN ハブが作成または検出されない場合、そのリージョンの VNet は VNet タグを使用してマッピングされません。
- Azure WAN ハブに Cisco Catalyst 8000V ネットワーク仮想アライアンス (NVA) を展開する場合、1 つのリソースグループと仮想 WAN でサポートされます。異なるリソースグループに Cisco Catalyst 8000V を展開することはできません。Cisco Catalyst 8000V NVA を展開すると、デフォルトでは、後続の展開のためにそのリソースグループと仮想 WAN に関連付けられます。

## セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックのルーティングの制約事項

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a、Cisco vManage リリース 20.6.1

Azure Firewall Manager で動作する Azure のセキュリティ保護付き仮想ハブへのローカルトラフィックのルーティングには、Azure 環境の追加の運用料金がかかる場合があります。Azure サービスの条件を確認してください。

## ネットワーク仮想アプライアンスの Azure SKU スケーリング、監査、およびセキュリティルールの制約事項

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

- クラウドゲートウェイの作成、編集、または削除中は、マルチクラウド監査サービスを実行できません。
- SKU スケール値と監査機能を変更する機能、およびポートを開く機能が、マルチクラウドを使用して Cisco SD-WAN Manager で作成されたクラウドゲートウェイにのみ一時的に適用されます。これらの機能は、Azure ポータルで直接作成されたネットワーク仮想アプライアンスには適用されません。

## リージョンごとの複数の仮想ハブの制約事項

サポート対象の最小リリース：Cisco vManage リリース 20.11.1

リージョンごとに最大 8 つの仮想ハブを作成できます。

## Azure Virtual WAN 統合のユースケース

### セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックフローのルーティングのユースケース

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a、Cisco vManage リリース 20.6.1

- セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックのルーティングは、Azure ベースのファイアウォールまたはローカルファイアウォールのいずれかを使用して、すべての Azure ベースおよびローカルのインターネットトラフィックに同じファイアウォールポリシーを適用することが望ましい場合に役立つ可能性があります。
- ローカルブランチデバイスでファイアウォールを設定しない場合は、ローカルトラフィックをセキュリティ保護付き仮想ハブにルーティングすることが役立つ可能性があります。
- Azure 環境でファイアウォールを設定しない場合は、Azure トラフィックをローカルファイアウォールにルーティングすることが役立つ可能性があります。

### Azure SKU スケーリングのユースケース

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

クラウドゲートウェイサービスのパフォーマンスまたはコスト効率を向上させるために、SKU スケール値を設定できます。CPU 負荷が 75% を超える場合はより高い SKU スケール値を設定でき、CPU 負荷が 25% を下回る場合はより低い SKU スケール値を設定できます。

## Azure 監査のユースケース

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

接続またはネットワークの問題に直面している場合は、監査を開始します。Azure 監査によって提供される情報は、ネットワークの問題のトラブルシューティングに役立ちます。

## NVA のセキュリティルールのユースケース

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

NVA のセキュリティルールを設定すると、特定のポートを有効にできます。

## Azure Virtual WAN 統合の設定

### Azure Virtual WAN ハブの設定

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a、Cisco vManage リリース 20.4.1

Cisco SD-WAN Manager の Cloud OnRamp for Multicloud ワークフローを使用して、Azure Virtual WAN ハブを作成し、Cisco Catalyst SD-WAN ブランチをプライベートネットワークまたはホスト VNet のアプリケーションに接続します。Azure Virtual WAN ハブを設定するには、次のタスクを指定された順序で実行します。

### 設定要件

Cisco SD-WAN Manager を使用して Azure Virtual WAN ハブを設定するには、以下が必要です。

- Azure クラウドアカウントの詳細。
- Azure マーケットプレイスへのサブスクリプション。
- Cisco SD-WAN Manager には、Azure クラウドゲートウェイを作成するために自由に使用できる 2 つの Cisco Catalyst 8000V ライセンスが必要です。
- Cisco SD-WAN Manager はインターネットに接続されている必要があり、Azure アカウントを認証するために Microsoft Azure と通信できる必要があります。

## Azure クラウドアカウントの統合

### Cisco SD-WAN Manager とアカウントの関連付け

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. **[Setup]** で、**[Associate Cloud Account]** をクリックします。
3. **[Cloud Provider]** フィールドで、ドロップダウンリストから **[Microsoft Azure]** を選択します。
4. 必要な情報を入力します。

フィールド	説明
Cloud Account Name	Azure サブスクリプションの名前を入力します。
[説明 (Description) ] (任意)	アカウントの説明を入力します。このフィールドは任意です。
Use for Cloud Gateway	[Yes] を選択すると、アカウントにクラウドゲートウェイが作成されます。デフォルトでは [No] が選択されています。
テナント ID	Azure Active Directory (AD) の ID を入力します。テナント ID を見つけるには、Azure Active Directory に移動し、 <b>[Properties]</b> をクリックします。
Subscription ID	このワークフローの一部として使用する Azure サブスクリプションの ID を入力します。
Client ID	既存の Azure アプリケーション ID を入力します。Azure AD にアプリケーションを登録する方法、クライアント ID と秘密キーを取得する方法などの詳細については、 <a href="#">Azure のドキュメント</a> を参照してください。
秘密キー (Secret Key)	クライアント ID に関連付けられたパスワードを入力します。

5. **[Add]** をクリックします。



- (注) 複数の Azure サブスクリプションを使用して VNet を検出したり、クラウドゲートウェイを作成したりする場合は、**[Cloud OnRamp for Multicloud Set up] > [Associate Cloud Account]** で、異なる Azure アカウントとして同じテナントの下にあるすべてのサブスクリプションを追加する必要があります。

### グローバルクラウド設定の追加と管理

1. [Cloud OnRamp for Multicloud] ウィンドウで、[Setup] エリアの [Cloud Global Settings] をクリックします。
2. [Cloud Provider] フィールドで、ドロップダウンリストから [Microsoft Azure] を選択します。
3. グローバル設定を編集するには、[Edit] をクリックします。
4. グローバル設定を追加するには、[Add] をクリックします。
5. Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降では、[Enable Configuration Group] オプションを有効にして、設定グループを使用してマルチクラウドワークフローでデバイスを設定します。
6. [Software Image] フィールドで、Azure Virtual Hub で使用する WAN エッジデバイスのソフトウェアイメージを選択します。これは、プリインストールされた Cisco Catalyst 8000V イメージである必要があります。



- (注) Cisco SD-WAN Manager リリースに基づいて、Cisco Catalyst 8000V イメージを選択します。Cisco SD-WAN Manager リリース 20.n の場合は、Cisco IOS XE リリース 17.n 以前の Cisco Catalyst 8000V イメージを選択します。たとえば、Cisco SD-WAN Manager リリース 20.5 の場合、Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a または Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a に対応するイメージを選択できます。Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降に対応するソフトウェアイメージがプリインストールされたイメージから使用可能な場合、Cisco SD-WAN Manager リリースと互換性がないため、そのようなイメージを選択しないでください。

7. [SKU Scale] フィールドで、容量要件に基づいて、ドロップダウンリストからスケールを選択します。
8. [IP Subnet Pool] フィールドで、Azure Virtual WAN ハブに使用する IP サブネットプールを指定します。サブネットプールには、/16 ~ /24 の範囲内のプレフィックスが必要です。

単一の /24 サブネットプールは、1つのクラウドゲートウェイのみをサポートできます。他のクラウドゲートウェイがすでにプールを使用している場合、プールを変更することはできません。サブネットの重複は許可されていません。

IP サブネットプールは、Azure Virtual WAN 内のすべての Azure Virtual WAN ハブを対象としていて、Virtual WAN ハブごとに1つの/24 プレフィックスがあります。Virtual WAN 内に作成する予定のすべての Virtual WAN ハブに、十分な/24 サブネットを割り当てていることを確認してください。Virtual WAN ハブが Microsoft Azure ですすでに作成されている場合は、Cisco SD-WAN Manager を介してそれを検出し、検出されたハブに既存のサブネットプールを使用できます。

9. [Autonomous System Number] フィールドで、仮想ハブとの eBGP ピアリングのためにクラウドゲートウェイが使用する ASN を指定します。



**注目** この値は、クラウドゲートウェイの作成後に変更することはできません。

10. [Push Monitoring Metrics to Azure] フィールドで、[Enabled] または [Disabled] を選択します。[Enabled] を選択すると、Azure サブスクリプションに関連付けられたクラウドゲートウェイメトリックが Microsoft Azure Monitoring Service ポータルに定期的に送信されます。これらのメトリックは、すべての NVA ベンダーに対して Microsoft Azure によって規定された形式で送信されます。



**重要**

- Cisco SD-WAN Manager を介して送信されるデータを処理およびモニタリングするための Azure Monitor サービスの使用に関連するコストが別途発生します。課金と使用条件については、Microsoft Azure のドキュメントを参照してください。
- テレメトリデータの収集と処理に関して、エンドユーザーに通知してエンドユーザーから必要な法的権利と許可を取得することは、マネージドサービスプロバイダーの責任です。

11. Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、[Advertise Default route to Azure Virtual Hub] フィールドを有効または無効にできます。デフォルトでは、このフィールドは [Disabled] になっています。[Enabled] をクリックすると、仮想ネットワークからのインターネットトラフィックが Cisco Catalyst SD-WAN ブランチ経由でリダイレクトされます。
12. Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、[Enabled] または [Disabled] をクリックして、[Enable Periodic Audit] フィールドを有効または無効にできます。
- 定期監査を有効にすると、Cisco SD-WAN Manager は 2 時間ごとに自動監査をトリガーします。この自動監査はバックグラウンドで実行され、不一致レポートが生成されます。
13. Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a および Cisco vManage リリース 20.8.1 以降では、[Enabled] または [Disabled] をクリックして、[Enable Auto Correct] フィールドを有効または無効にできます。自動修正オプションを有効にすると、定期的な監査がトリガーされるたびに、検出されたすべての回復可能な問題が自動修正されます。
14. [Add] または [Update] をクリックします。

## クラウドゲートウェイの作成と管理

クラウドゲートウェイの作成には、Azure Virtual WAN ハブとハブ内の 2 つの Cisco Catalyst 8000V インスタンスのインスタンス化または検出が含まれます。



(注) Azure ポータルを使用して Cisco Catalyst 8000V インスタンスをプロビジョニングしていて、Azure ポータルを使用して Azure Virtual WAN と Azure Virtual WAN ハブを作成した場合は、以下の手順を使用してそれらを検出することもできます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration] > [Cloud OnRamp for Multicloud]** を選択します。
2. **[Manage]** で、**[Create Cloud Gateway]** をクリックします。
3. **[Cloud Provider]** フィールドで、ドロップダウンリストから **[Microsoft Azure]** を選択します。
4. **[Cloud Gateway Name]** フィールドに、クラウドゲートウェイの名前を入力します。



(注) Azure ポータルを使用して Azure Virtual WAN ハブを作成した場合は、このフィールドに正確な仮想ハブ名を入力してください。これにより、ハブに関連付けられたリソースが確実に検出されます。関連付けられた Azure Virtual WAN と Azure Virtual WAN ハブは、**[Virtual WAN]** および **[Virtual Hub]** フィールドから選択できるようになります。関連付けられた NVA も、**[UUID]** フィールドに自動入力されます。

5. (任意) **[Description]** フィールドに、クラウドゲートウェイの説明を入力します。
6. **[Account Name]** フィールドで、ドロップダウンリストから Azure アカウント名を選択します。
7. **[Region]** フィールドで、ドロップダウンリストから **[Azure]** リージョンを選択します。
8. (Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降、クラウドゲートウェイを作成したとき、または Azure クラウドゲートウェイのグローバル設定を構成したときに **[Enable Configuration Group]** オプションを有効にした場合にのみ適用) **[Configuration Group]** ドロップダウンリストから次のいずれかのアクションを実行します。
  - 構成グループを選択します。
  - 新しい設定グループを作成して使用するには、**[Create New]** を選択します。**[Create Configuration Group]** ダイアログボックスで、新しい設定グループの名前を入力し、**[Done]** をクリックします。ドロップダウンリストから新しい設定グループを選択します。

選択した設定グループは、マルチクラウドワークフローでデバイスを設定するために使用されます。





- (注) [Configuration Group] ドロップダウンリストには、この手順の説明に従って作成した設定グループのみが含まれています。Cisco Catalyst SD-WAN で作成された他の設定グループは含まれません。このドロップダウンリストの設定グループには、このプロバイダーに必要なオプションが含まれています。

設定グループの詳細については、『[Cisco Catalyst SD-WAN Configuration Groups](#)』を参照してください。

9. [Resource Group] フィールドで、ドロップダウンリストからリソースグループを選択するか、[Create New] を選択します。



- (注) 新しいリソースグループの作成を選択した場合は、次の2つのフィールドで新しい Azure Virtual WAN と Azure Virtual WAN ハブも作成する必要があります。

10. [Virtual WAN] フィールドで、ドロップダウンリストから Azure Virtual WAN を選択します。または、[Create New] をクリックして、新しい Azure 仮想 WAN を作成します。

11. [Virtual HUB] フィールドで、ドロップダウンリストから Azure 仮想 WAN ハブを選択します。または、[Create New] をクリックして、新しい Azure 仮想 WAN ハブを作成します。

(サポート対象の最小リリース : Cisco vManage リリース 20.11.1) [Region]、[Resource Group]、および [Virtual WAN] を選択すると、[Azure Virtual WAN Hub] フィールドに [Create a new vHub using Cloud Gateway Name] と表示されます。ドロップダウンリストから、検出された仮想ハブを選択します。

仮想ハブは、Cisco SD-WAN Manager で次の2つの方法で検出されます。

- Azure ポータルで作成された、ネットワーク仮想アプライアンス (NVA) を備えた仮想ハブ。
- Azure ポータルで作成され、Cisco SD-WAN Manager によって検出された仮想ハブ。その後、Cisco SD-WAN Manager で仮想ハブに NVA を追加できます。

12. (最小リリース : Cisco vManage リリース 20.10.1) [Site Name] ドロップダウンリストから、クラウドゲートウェイを作成するサイトを選択します。

13. [Settings] フィールドで、次のいずれかを選択します。

- [Default] : IP サブネットプール、イメージバージョン、および SKU スケールサイズのデフォルト値が、グローバル設定から取得されます。
- [Customized] : このオプションを使用してグローバル設定を上書きできます。このオプションは、新しく作成されたクラウドゲートウェイにのみ適用されます。

(サポート対象の最小リリース : Cisco vManage リリース 20.10.1)

Azure ポータルで作成された Cisco Catalyst 8000V を使用した仮想ハブを Cisco SD-WAN Manager にオンボードした場合にのみ、[Instance Setting] エリアの次のフィールドにグローバル設定の設定が自動入力されます。

- ソフトウェア イメージ
- SKU Scale
- IP Subnet Pool
- UUID (specify 2)



- (注) Cisco SD-WAN Manager でクラウドゲートウェイがオンボードされると、NVA なしで、[IP Subnet Pool] フィールドと [UUID (specify 2)] フィールドが自動入力されます。

ドロップダウンリストでオプションを選択することで、グローバル設定を上書きできません。

14. Cisco Catalyst SD-WAN Manager リリース 20.13.1 以降、クラウドゲートウェイを作成したとき、または Azure クラウドゲートウェイのグローバル設定を構成したときに [Enable Configuration Group] オプションを有効にした場合にのみ適用) [Configuration Group] で、クラウドゲートウェイの作成に使用される設定グループの名前を選択するか、新しい設定グループを作成します。

(

15. [UUID (specify 2)] フィールドで、ドロップダウンリストから 2 つの Cisco Catalyst 8000V ライセンスを選択します。



- (注) Cisco vManage リリース 20.10.1 以降では、[Site Name] ドロップダウンリストからサイトを選択すると、UUID が自動的に入力されます。

16. (最小リリース : Cisco vManage リリース 20.10.1) [Multi-Region Fabric Settings] エリアの [MRF Role] で、[Border] または [Edge] を選択します。

このオプションは、マルチリージョンファブリックが有効になっている場合にのみ使用できます。

17. [Add] をクリックします。



- (注) Azure Virtual WAN ハブが作成され、Cisco Catalyst 8000V インスタンスが仮想ハブ内にプロビジョニングされるまでに、最大 40 分かかることがあります。



- (注) Azure Virtual WAN ハブの作成が完了したら、それをセキュリティで保護された Azure Virtual WAN ハブに変換するオプションを使用できます。ただし、この設定は Microsoft Azure ポータルからのみ実行できます。詳細については、Microsoft Azure のドキュメントを参照してください。



- (注) 異なるリージョンに Azure クラウドゲートウェイを同時に作成できます。
- 異なるリージョンに複数のクラウドゲートウェイを作成する前に、最初のクラウドゲートウェイのリソースグループ、仮想 WAN、およびストレージアカウントを作成します。
  - 同じリージョンに複数のクラウドゲートウェイを作成する前に、リージョン内の最初のクラウドゲートウェイの仮想ハブを作成します。
  - Cloud OnRamp for Multicloud 用に Azure でストレージアカウントを作成するには、BLOB アクセスが必要です。Cisco Catalyst 8000V デバイスでクラウドゲートウェイを作成する際、およびスケール操作を変更する際には、BLOB アクセスが必要です。



- (注) Cloud OnRamp for Multicloud ワークフローは、各 Azure リージョンで最大 8 つの仮想ハブをサポートしています。各仮想ハブに 2 つのクラウドゲートウェイ ネットワーク仮想アプライアンス (NVA) を展開できます。

## ホスト VNet の検出とタグの作成

Azure 仮想ハブを作成したら、仮想ハブのリージョンでホスト VNet を検出できます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。

2. **[Discover]** ワークフローで、**[Host Private Networks]** をクリックします。

3. **[Cloud Provider]** フィールドで、**[Microsoft Azure]** を選択します。

ホスト VNet のリストがテーブルに表示され、**[Cloud Region]**、**[Account Name]**、**[VNET Tag]**、**[Cloud Gateway Attachment]**、**[Account ID]**、**[Resource Group]**、および **[VNet Name]** 列が表示されます。

4. **[Tag Actions]** ドロップダウンリストをクリックして、次のいずれかを選択します。

- **[Add Tag]** : VNet または VNet のグループのタグを作成します。

(サポート対象の最小リリース : Cisco vManage リリース 20.11.1) **[Cloud Gateway Attachment]** に **[Auto]** を選択するか、既存のクラウドゲートウェイにマッピングすることができます。

- [Edit Tag] : 選択した VNet の既存のタグを変更します。

(サポート対象の最小リリース : Cisco vManage リリース 20.11.1) [Edit Tag] から [Cloud Gateway Attachment] を選択できます。選択しない場合、またはクラウドゲートウェイがそのリージョンでまだ作成されていない場合は、[Auto] オプションが自動的に選択されます。[Auto] オプションは、ロードバランシングアルゴリズムに基づいています。[Auto] オプションが選択された VNet では、クラウドゲートウェイアタッチメントは、タグの作成時ではなく、マッピング時に選択されます。

- [Delete Tag] : 選択した VNet のタグを削除します。

## VNet タグとブランチネットワーク VPN のマッピング

VNet から VPN へのマッピングを有効にするには、1 つまたは複数の Azure リージョンで VNet のセットを選択し、タグを定義します。次に、同じタグを使用して VNet をマッピングするサービス VPN を選択します。1 セットのブランチオフィスには 1 セットの VNet のみをマッピングできます。選択したすべての VNet は、選択したすべての VPN に対して表示され、その逆も同様です。1 つのサービス VPN は、1 つまたは複数のタグにマッピングできます。複数の VNet が同じタグを持つことができます。クラウドゲートウェイが同じリージョンに存在する場合、またはタグ付け操作が行われる場合、マッピングは自動的に実現されます。



- (注) VNet タグにマッピングされるように選択した VPN は、重複する IP アドレスを持つことはできません。これは、Microsoft Azure Virtual WAN ではセグメンテーションがサポートされていないためです。

Cisco Catalyst SD-WAN ネットワークの VNet-VPN マッピングを編集するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。
2. [Intent Management] で、[Connectivity] をクリックします。
3. インテントを定義するには、[Edit] をクリックします。
4. VPN、およびそれに関連付けられている VNet タグに対応するセルを選択し、[Save] をクリックします。

[Intent Management - Connectivity] ウィンドウには、ブランチ VPN とそれらがマッピングされている VNet タグ間の接続ステータスが表示されます。画面の上部には、さまざまなステータスを理解するのに役立つ凡例が表示されます。表示されたマトリックス内のセルのいずれかをクリックすると、[Mapped]、[Unmapped]、[Outstanding] マッピングなど、詳細なステータス情報が表示されます。

## VNet の再調整

サポート対象の最小リリース : Cisco vManage リリース 20.11.1

VNet を再配布して、特定のタグのリージョン内のすべてのクラウドゲートウェイ間で既存の VNet をいつでもロードバランスすることができます。クラウドゲートウェイ全体で [Auto] オプションが選択されている VNet のみを再割り当てできます。VNet の割り当ては、ロードバランシングアルゴリズムに基づいています。再バランシングにはクラウドゲートウェイへの VNET のデタッチと再アタッチが含まれるため、トラフィックの中断が発生する可能性があります。VNet の再バランシング後、[tagging] ページで、VNET からクラウドゲートウェイへの修正済みマッピングを表示できます。



(注) 次の場合は、VNet を再バランシングできません。

- クラウドゲートウェイの作成、編集、または削除が進行中の場合。
- VNet のマッピングが進行中の場合。
- 監査が進行中の場合。

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。
2. [Intent Management] ワークフローで、[Rebalance VNETS (Azure/GovCloud)] をクリックします
3. [Cloud Provider] フィールドで、[Microsoft Azure] を選択します。
4. [Region] フィールドで、ドロップダウンリストから [Azure] リージョンを選択します。
5. [Tag Name] フィールドで、ドロップダウンリストからタグを選択します。
6. [再調整 (Rebalance) ] をクリックします。

## Azure ポータルからの Azure Virtual WAN ハブの設定

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a、Cisco vManage リリース 20.4.1



(注) Azure Virtual WAN ハブのエンドツーエンド設定は、Cisco SD-WAN Manager を使用して行うことができます。または、Azure ポータルを使用してリソースグループ、仮想 WAN、および仮想 WAN ハブを作成してから、Cisco SD-WAN Manager に戻って Azure ポータルを使用して作成したインフラストラクチャを検出し、VNet タグを作成してそれらをサービス VPN にマッピングすることもできます。

## 設定ワークフロー

タスク	説明
タスク 1	Cisco SD-WAN Manager のメニューから、Azure Virtual WAN ハブに自由に使用できる 2 つの Cisco Catalyst 8000V インスタンスを選択します。次に、これらのインスタンスのブートストラップ構成ファイルを生成してダウンロードします。
タスク 2	Azure ポータルで、仮想 WAN ハブを作成し、作成した仮想 WAN ハブに Cisco Catalyst 8000V インスタンスを関連付けます。
タスク 3	Azure ポータルで、Cisco SD-WAN Manager で生成されたブートストラップ構成ファイルを使用して、Cisco Catalyst 8000V の NVA を作成します。
タスク 4	Cisco SD-WAN Manager で、Azure ポータルで作成したインフラストラクチャを検出します。  この検出の一環として、Azure Virtual WAN ハブで作成された NVA が起動します。
タスク 5	Cisco SD-WAN Manager で、VNet タグをマッピングして、ホスト VNet とサービス VPN 間の接続を設定します。



(注) Azure ポータルを使用して行う設定は、このドキュメントの範囲外です。ただし、[Azure ポータル](#)を使用して設定を完了するために役立つ Azure ドキュメントへのリンクが用意されています。

## タスク 1. Cisco Catalyst 8000V のブートストラップ設定の生成

前提条件：次の手順に進む前に、2 つの Cisco Catalyst 8000V インスタンスの Cisco SD-WAN Manager で使用可能なライセンスが必要です。

1. Cisco SD-WAN Manager のメニューから、**[Configuration] > [Templates]** の順に選択します。
2. **[Device Template]** をクリックします。



(注) Cisco vManage リリース 20.7.1 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[Template Type]** ドロップダウンリストから **[Default]** を選択します。  
デフォルトテンプレートのリストが表示されます。

4. [Default\_Azure\_vWAN\_C8000V\_Template\_V01] の目的の行について、[...] をクリックし、[Attach Devices] を選択します。
5. [Available Devices] のリストから 2 つの Cisco Catalyst 8000V インスタンスを選択し、[Attach] をクリックします。  
次の画面に、デバイステンプレートにアタッチしたデバイスが表示されます。
6. [Device Templates] 画面で、デバイスの行ごとに [...] をクリックし、[Update Device Template] を選択します。
7. デバイスごとに、要求された情報（ホスト名、システム IP、およびサイト ID）を入力します。Update をクリックします。
8. [Next] をクリックします。[Configure Devices] ダイアログボックスで、チェックボックスをオンにして [OK] をクリックします。  
[Task View] 画面が開きます。デバイス情報が更新されるまで数分かかります。ステータス列にステータスが [Done - Complete] と表示されている場合は、デバイス情報が更新されたことを示しています。
9. Cisco SD-WAN Manager のメニューから、[Configuration] > [Devices] の順に選択します。
10. 更新したデバイスを見つけて、デバイスごとに [...] をクリックします。オプションから [Generate Bootstrap Configuration] を選択します。
11. [Generate Bootstrap Configuration] ダイアログボックスで、[Include Default Root Certificate] の選択を解除し、[OK] をクリックします。
12. ダイアログボックスで、[Download] をクリックします。

## タスク 2. Azure Virtual WAN ハブの作成

この項の手順は、Azure ポータルで実行します。これらの手順を実行するための Azure ドキュメントへのリンクが用意されています。この項の手順を実行するには、Azure のサブスクリプションとログイン情報が必要です。

Azure ポータルで、次の手順を実行します。

1. リソースグループを作成します。
2. 仮想 WAN を作成します。
3. 仮想 WAN ハブを作成します。

次のステップ：仮想ハブで、Cisco Catalyst 8000V インスタンスのネットワーク仮想アプライアンス (NVA) を作成します。NVA を作成する手順は、NVA パートナーによって異なる場合があります。そのため、次の項では Cisco Catalyst 8000V に固有の情報を提供しています。



### タスク 3. Cisco Catalyst 8000V の NVA の作成

1. Azure ポータルの検索ボックスで **Cisco Cloud vWAN Application** を検索し、[Marketplace] の下にある結果をクリックします。
2. [Cisco Cloud vWAN Application] ページが開きます。[Create] をクリックします。  
必要な詳細を入力し、[Next: Cisco SD-WAN Cloud Gateway] をクリックします。
3. 要求された詳細を入力します。この画面で入力する詳細は、Cisco SD-WAN Manager の [Cloud Global Settings] 画面に似ています。
  1. [Virtual WAN] : ドロップダウンリストから作成した仮想 WAN を選択します。
  2. [Virtual WAN Hubs] : 仮想 WAN を選択すると、その WAN 内のすべての仮想ハブがこのドロップダウンリストに表示されます。この手順で使用する仮想 WAN ハブを選択します。
  3. [Scale Unit] :
  4. [Cisco Version] : Cisco Catalyst 8000V インスタンスのソフトウェアバージョンを入力します。
  5. [BGP ASN to peer with Azure Router Service] : これは、NVA が使用する番号です。
  6. [Cisco SDWAN Cloud Gateway Name] : クラウドゲートウェイの名前を入力します。
  7. [Upload the Bootstrap configuration File that was generated] : このフィールドを使用して、Cisco Catalyst 8000V から Cisco SD-WAN Manager 用にダウンロードしたブートストラップ構成ファイルに移動します。



(注) この手順では、必ず両方のブートストラップ構成ファイルを選択してください。

4. [Next] をクリックし、デフォルト値を維持します。
5. チェックボックスをオンにして利用規約に同意します。[Create] をクリックします。  
展開が完了すると、2 つの Cisco Catalyst 8000V インスタンスが仮想ハブ内にプロビジョニングされます。これらが起動すると、Cisco SD-WAN Manager にも接続されます。

Cisco SD-WAN Manager のメインダッシュボードで、[Devices] の横にある上向き矢印をクリックします。Azure ポータルを介した展開が成功すると、2 つの Cisco Catalyst 8000V インスタンスが到達可能として表示されます。

### タスク 4. Cisco SD-WAN Manager での NVA の検出

**前提条件** : Cisco SD-WAN Manager で NVA を検出するには、Cisco SD-WAN Manager に Azure アカウントを追加する必要があります。Azure アカウントを Cisco SD-WAN Manager にまだ関連付けていない場合は、[Azure クラウドアカウントの統合 \(19 ページ\)](#) を参照してください。

Azure ポータルを使用して設定した NVA または Cisco Catalyst 8000V を検出するには、[クラウドゲートウェイの作成と管理 \(22 ページ\)](#) に記載されている手順に従います。

#### タスク 5. VNet と VPN 間の接続の設定

VNet から VPN へのタグ付けを設定するには、まず [Azure リージョン内のホスト VNet を検出してタグを作成してから、VNet タグとブランチネットワーク VPN のマッピング](#) して VNet とブランチネットワークまたは VPN を接続する必要があります。

## セキュリティ保護付き仮想ハブまたはローカルファイアウォールへのトラフィックフローのルーティングの設定

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a、Cisco vManage リリース 20.6.1

### Azure のセキュリティ保護付き仮想ハブへのローカル発信トラフィックフローのルーティング

はじめる前に

- Cisco Catalyst SD-WAN を使用して Azure Virtual WAN ハブの統合を設定します。詳細については、「[Azure Virtual WAN Hub Integration with Cisco SD-WAN](#)」を参照してください。
- Azure 環境でファイアウォールを設定します (必要なファイアウォールポリシーを含む)。

#### Azure のセキュリティ保護付き仮想ハブへのローカル発信トラフィックフローのルーティング

発信インターネットトラフィックを Azure のセキュリティ保護付き仮想ハブにルーティングするようにブランチルータを設定するには、次の手順を実行します。

1. ローカルブランチルータで、ブランチルータに、ブランチからのダイレクトインターネットアクセス (DIA) 用に設定されたスタティックデフォルトルートがないことを確認します。

ローカルブランチルータで、`show ip route vrf vrf-number` コマンドを使用して、スタティックデフォルトルートがサービス側 VPN に設定されていないことを確認します。

2. ローカルブランチルータで、`show ip route vrf vrf-number` コマンドを使用して、ローカルブランチルータと Azure 間の通信用に設定した VRF を使用して、ローカルブランチルータからのインターネットトラフィックが Azure ファイアウォールにルーティングされていることを確認します。コマンド出力で、0.0.0.0 と表されるデフォルトルートに関連付けられている IP アドレスを探します。この IP アドレスが、Azure ファイアウォールが有効になっている Azure ハブで動作しているクラウドゲートウェイに対応している必要があります。

次の例では、VRF 100 を使用しています。この例では、コマンド出力の一部のみが表示されています。Azure ハブで動作しているクラウドゲートウェイに対応する IP アドレスは、209.165.201.1 と 209.165.201.2 です。

```
Device# show ip route vrf 100
...
m* 0.0.0.0/0 [251/0] via 209.165.201.1, 21:06:00, Sdwan-system-intf
    [251/0] via 209.165.201.2, 21:06:00, Sdwan-system-intf
...
```

3. Azure 環境で、Azure ファイアウォールを介してルーティングされるようにインターネットトラフィックを設定します。

## ローカルブランチルータへの Azure 発信トラフィックフローのルーティング

### はじめる前に

- Cisco Catalyst SD-WAN を使用して Azure Virtual WAN ハブの統合を設定します。詳細については、「[Azure Virtual WAN Hub Integration with Cisco SD-WAN](#)」を参照してください。
- ローカルブランチルータでファイアウォールを設定します（必要なファイアウォールポリシーを含む）。

### ローカルブランチルータへの Azure 発信トラフィックフローのルーティング

発信インターネットトラフィックをローカルブランチルータのファイアウォールにルーティングするように Azure を設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager で、ローカルブランチルータの CLI テンプレートを使用して、次のコマンドを設定に追加します。これにより、ローカルルータが Azure 環境のデフォルトルートとしてアドバタイズされ、Azure Virtual Network が発信インターネットトラフィックをブランチルータにルーティングするようになります。0.0.0.0 はデフォルトルートを表すことに注意してください。

```
address-family ipv4 vrf branch-router-vpn-id
  advertise connected
  advertise static
  advertise network 0.0.0.0/0
```

指定された VPN 内のトラフィックのみがブランチルータに転送されます。VPN が Cisco Catalyst SD-WAN と Azure の間の接続をマッピングする方法については、「[How Virtual WAN Hub Integration Works](#)」を参照してください。

次の例では、VPN 100 の Azure トラフィックをブランチルータに転送しています。

```
address-family ipv4 vrf 100
  advertise connected
  advertise static
  advertise network 0.0.0.0/0
```

2. Azure 環境で、トラフィックがローカルブランチルータにルーティングされていることを確認します。ルーティングテーブルを表示し、次のように表示されていることを確認します。

```
プレフィックス : 0.0.0.0/0
ネクストホップタイプ : VPN_S2S_GATEWAY
```

## SKU スケール値の設定

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

SKU スケール値を設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. **[Manage]** の下の **[Gateway Management]** をクリックします。  
**[Cloud Gateways]** と、クラウドアカウント名、ID、クラウドタイプ、およびその他の情報を含むクラウドゲートウェイのリストを表示するテーブルが表示されます。
3. 対応するクラウドゲートウェイの隣にある [...] をクリックし、**[Edit]** を選択します。
4. **[SKU Scale]** ドロップダウンリストから値を選択します。



---

(注) [2]、[4]、および [10] の SKU スケール値のみがサポートされています。

---

5. **[Update]** をクリックします。

## オンデマンド監査の開始

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

これは、ユーザーが起動する監査です。オンデマンド監査を開始するには、次の手順に従います。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. **[Intent Management]** の下の **[Audit]** をクリックします。
3. **[Cloud Provider]** ドロップダウンリストで、**[Microsoft Azure]** を選択します。  
このウィンドウには、さまざまな Microsoft Azure オブジェクトのステータスが表示されます。いずれかのオブジェクトのステータスが **[In Sync]** の場合は、そのオブジェクトにエラーがないことを意味します。オブジェクトのステータスが **[Out of Sync]** の場合は、Cisco SD-WAN Manager で利用できるオブジェクトの詳細と Azure データベースで利用できる詳細との間に不一致があることを意味します。
4. いずれかのオブジェクトのステータスが **[Out of Sync]** の場合は、**[Fix Sync issues]** をクリックします。このオプションにより、回復可能なエラーがあればそれが解決され、ステータスアクティビティログを表示するウィンドウが開きます。

オブジェクトのステータスが引き続き [Out of Sync] と表示される場合は、手動による介入が必要なエラーであることを意味します。



(注) マルチクラウド監査サービスは、他のクラウド操作の進行中は実行されません。

## 定期監査の有効化

次の手順では、定期監査を有効にする手順について説明します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Setup] エリアで、[Cloud Global Settings] をクリックします。
3. [Enable Periodic Audit] フィールドを有効または無効にするには、[Enabled] または [Disabled] をクリックします。

[Enabled] をクリックすると、Cisco SD-WAN Manager は 2 時間ごとに自動監査をトリガーします。この自動監査はバックグラウンドで実行され、不一致レポートが生成されます。

監査の不一致と解決の例については、「[監査の不一致の例](#)」を参照してください。

4. [Update] をクリックします。

## NVA のセキュリティルールの設定

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

NVA のセキュリティルールを設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. [Manage] の下の [Gateway Management] をクリックします。

[Create Cloud Gateways] ウィンドウと、クラウドアカウント名、ID、クラウドタイプ、およびその他の情報を含むクラウドゲートウェイのリストを表示するテーブルが表示されます。

3. 対応するクラウドゲートウェイの隣にある [...] をクリックし、[Add/Edit Security Rules] を選択します。

[Add/Edit Security Rules] ウィンドウが表示されます。

1. 新しいセキュリティルールを追加するには、[Add Security Rule] をクリックし、次の詳細を入力します。

表 4:パラメータの表

パラメータ	説明
ポート番号	ポート範囲を指定します。
IPv4 送信元アドレス	IP アドレスを指定します。

2. [Add] をクリックします。
  3. (オプション) セキュリティルールを編集するには、鉛筆アイコンをクリックします。
  4. (オプション) セキュリティルールを削除するには、削除アイコンをクリックします。
4. [Update] をクリックします。



(注) セキュリティルールはすべて 2 時間のみアクティブになります。

## Azure Virtual WAN 統合の確認

### クラウドゲートウェイの表示、編集、または削除

1. Cisco SD-WAN Manager のメニューから、[Configuration] > [Cloud OnRamp for Multicloud] を選択します。
2. [Cloud] をクリックします。
3. [Manage] の下の [Gateway Management] をクリックします。  
既存のクラウドゲートウェイの詳細がテーブルにまとめられています。
4. このテーブルで、目的のクラウドゲートウェイの [...] をクリックします。
  - クラウドゲートウェイの詳細を表示するには、[View] をクリックします。
  - クラウドゲートウェイの説明を編集するには、[Edit] をクリックします。
  - クラウドゲートウェイを削除するには、[Delete] をクリックして、ゲートウェイを削除することを確定します。

(サポート対象の最小リリース : Cisco vManage リリース 20.11.1) クラウドゲートウェイを削除すると、アタッチされた VNet はロード バランシング アルゴリズムに基づいて同じリージョン内の他の選択されたクラウドゲートウェイに移動し、VNet は [Auto] としてマークされます。

## Azure SKU スケール値の更新の確認

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

Azure SKU スケール値の更新を確認するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. **[Manage]** の下の **[Gateway Management]** をクリックします。

**[Create Cloud Gateways]** ウィンドウが表示されます。テーブルには、クラウドアカウント名、ID、クラウドタイプ、およびその他の情報とともにクラウドゲートウェイのリストが表示されます。

3. 対応するクラウドゲートウェイの隣にある [...] をクリックし、**[View]** を選択します。  
変更された SKU 値が **[View Cloud Gateway]** ウィンドウに表示されます。

## ネットワーク仮想アプライアンスのセキュリティルールの確認

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a、Cisco vManage リリース 20.7.1

NVA 用に作成されたセキュリティルールを確認するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Cloud OnRamp for Multicloud]** を選択します。
2. **[Manage]** の下の **[Gateway Management]** をクリックします。

**[Create Cloud Gateways]** ウィンドウと、クラウドアカウント名、ID、クラウドタイプ、およびその他の情報を含むクラウドゲートウェイのリストを表示するテーブルが表示されます。

3. 目的のクラウドゲートウェイで、[...] をクリックし、**[Add/Edit Security Rules]** を選択します。

**[Add/Edit Security Rules]** ウィンドウが表示され、更新されたセキュリティの次のいずれかのステータスが示されます。

- **[Successful]**
- **[In-progress: Check the status after sometime.]**
- **[Failed: Recreate the security rule.]**



# Cisco SD-WAN Manager を使用した Azure Virtual WAN 統合のモニター

## Azure Virtual WAN 統合のモニター

サポートされている最小リリース : Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a、Cisco vManage リリース 20.4.1

### NVA 接続

新しいクラウドゲートウェイを作成するときに、Azure Virtual WAN ハブ内でプロビジョニングされた Cisco Catalyst 8000V インスタンスの作成と到達可能性を確認できます。これらのインスタンスが正常に設定されていて到達可能かどうかを表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから **[Monitor]** > **[Overview]** の順に選択します。  
Cisco SD-WAN Manager リリース 20.6.x 以前 : Cisco SD-WAN Manager のメニューから、**[Dashboard]** > **[Main Dashboard]** を選択します。
2. **[WAN Edge]** で、表示された数字の横にある上向き矢印をクリックします。この数字は、使用可能な WAN エッジデバイスを表しています。
3. ポップアップウィンドウに表示されたテーブルで、クラウドゲートウェイの作成時に選択した Cisco Catalyst 8000V インスタンスを探します。クラウドゲートウェイの設定が成功すると、インスタンスがテーブルに表示され、到達可能として表示されます。

### Microsoft Azure Monitor サービスを使用した NVA データのモニター

Cisco SD-WAN Manager では、**[Cloud OnRamp for Multicloud]** > **[Cloud Global Settings]** ウィンドウを使用して、Azure ポータルへのメトリックの送信を有効にできます。

**[Push Monitoring Metrics to Azure]** オプションを有効にすると、Cisco SD-WAN Manager と統合した Azure アカウントに関連付けられているすべてのクラウドゲートウェイに関するデータが Azure Monitor サービスに送信されます。

Azure Monitoring サービスの詳細については、[Azure のドキュメント](#)を参照してください。



#### 重要

- Cisco SD-WAN Manager を介して送信されるデータを処理およびモニタリングするための Azure Monitor サービスの使用に関連するコストが別途発生します。課金と使用条件については、Microsoft Azure のドキュメントを参照してください。
- テレメトリデータの収集と処理に関して、エンドユーザーに通知してエンドユーザーから必要な法的権利と許可を取得することは、マネージドサービスプロバイダーの責任です。



## 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。