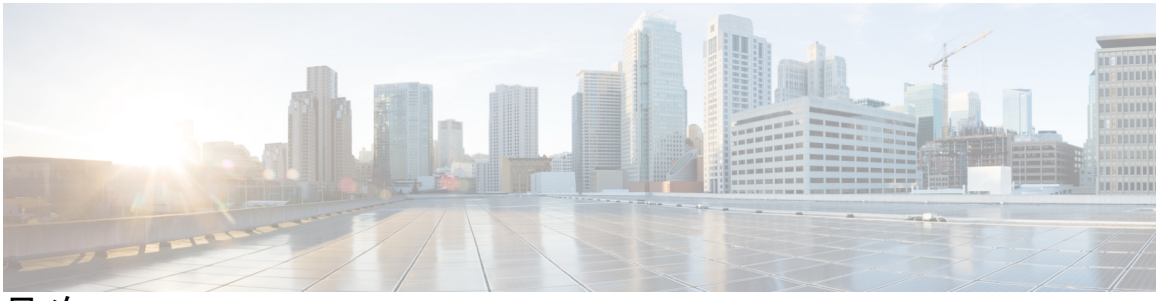
Microsoft Azure での Cisco Catalyst 8000V エッジソフトウェアの展開

初版：2020 年 9 月 25 日

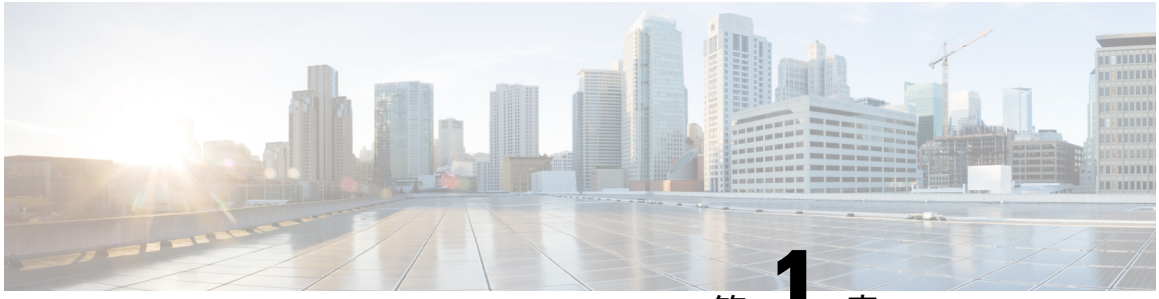
最終更新：2023 年 8 月 22 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



目 次

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



第 1 章

はじめに

ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

対象読者および適用範囲

このドキュメントは、Cisco Enterprise ルータの設定担当者を対象としています。このドキュメントの対象者は、主に次のとおりです。

- ネットワーキングに関する技術的な背景知識と経験を持つお客様。
- ルータベースのインターネットワーキングに関する基本的な知識に精通しているが、Cisco IOS ソフトウェアについては経験の浅いシステム管理者。
- インターネットワーキング装置のインストールと設定を担当しているシステム管理者、および Cisco IOS ソフトウェアに精通しているシステム管理者。

機能の互換性

コンフィギュレーション ガイドで説明されているデバイスで使用可能な機能などの Cisco IOS XE ソフトウェアの詳細については、それぞれのルータのドキュメントセットを参照してください。

特定の機能のサポートを確認するには、Cisco Feature Navigator ツールを使用します。これは、特定のソフトウェアリリース、フィーチャセット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェアイメージを判別できるツールです。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または **Ctrl**	^ および **Ctrl** シンボルは、Ctrl キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、**Ctrl** キーを押しながら **D** キーを押すことを意味します。キーは大文字で表記されていますが、大文字と小文字の区別はありません。
string	ストリングは、イタリックで示される引用符を付けない一組の文字です。たとえば、SNMP コミュニティ ストリングとして public を設定する場合、ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

コマンドシンタックスの説明には、次の表記法を使用しています。

表記法	説明
ボールド	ユーザが入力するコマンドおよびキーワードを示します。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
|	縦棒で区切られている場合、複数の任意または必須のキーワードまたは引数から、1 つを選択します。
[x | y]	角カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、任意の選択肢です。
{x | y}	波カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、必須の選択肢です。

省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。たとえば、次の表を参照してください。

表記法	説明
[x {y | z}]	角カッコ内の波カッコおよび縦棒は、任意の要素内の必須の選択肢です。

例では、次の表記法を使用しています。

表記法	説明
`screen`	画面に表示される情報の例は、Courier フォントで表します。
`bold screen`	ユーザの入力が必要なテキストの例は、太字の Courier フォントで表します。
< >	山カッコで囲まれたテキストは、パスワードなど、画面に出力されないテキストを表します。
!	行の先頭にある感嘆符（!）は、コメント行を表します。また、いくつかのプロセスでも、Cisco IOS XE ソフトウェアにより感嘆符が表示されることがあります。
[ ]	角カッコは、システム プロンプトに対するデフォルトの応答です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。

- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

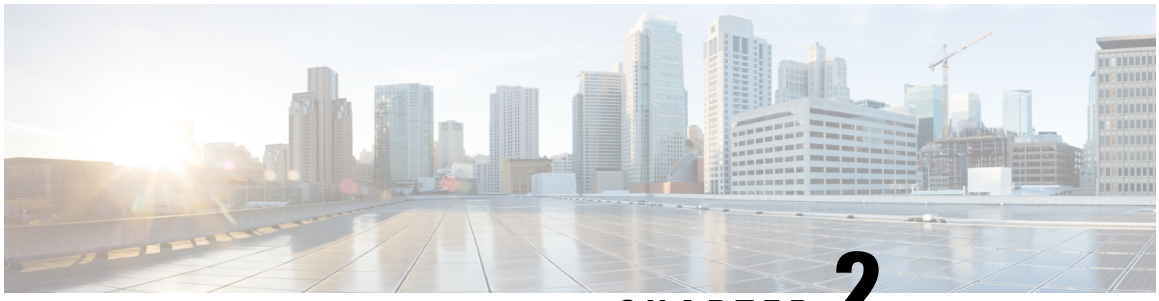
マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

トラブルシューティング

トラブルシューティングの最新の詳細情報については、
https://www.cisco.com/c/ja_jp/support/index.html にある Cisco TAC Web サイトを参照してください。

製品カテゴリに移動し、リストから製品を選択するか、製品の名前を入力します。発生している問題に関する情報を見つけるには、**トラブルシュートおよびアラート**を参照してください。



CHAPTER 2

Microsoft Azure での Cisco Catalyst 8000V エッジソフトウェア の概要

Cisco Catalyst 8000V エッジソフトウェア はフル機能の Cisco IOS XE ルータであり、IT 部門が Microsoft Azure クラウドでエンタープライズクラスのネットワーキングサービスを展開することを可能にします。ほとんどの Cisco IOS XE の機能は、仮想 Cisco Catalyst 8000V でも使用できます。

仮想ネットワークなどの新規または既存のインフラストラクチャに Cisco Catalyst 8000V ソフトウェアを展開することを選択できます。

次の VPN 機能が Cisco Catalyst 8000V でサポートされています。IPsec、DMVPN、FlexVPN、Easy VPN、および SSLVPN。EIGRP、OSPF、BGP などのダイナミック ルーティング プロトコルを使用して、Azure 内に多層アーキテクチャを構築し、企業の拠点や他のクラウドと相互接続できます。

アプリケーション認識型のゾーン ベース ファイアウォールを使用して、ハイブリッド クラウド ネットワーク トラフィックを保護、検査、および監査できます。また、IP SLA およびアプリケーションの可視性と制御（AVC）を使用して、パフォーマンスの問題を確認し、アプリケーションフローを調べ、詳細なフローデータをエクスポートしてリアルタイム分析とネットワーク調査を行います。

Microsoft Azure での Cisco Catalyst 8000V を展開するための前提条件

Cisco Catalyst 8000V を展開するための主な 3 つの前提条件は次のとおりです。

- Microsoft Azure のユーザーアカウントやサブスクリプションが必要です。Microsoft Azure のアカウント作成の詳細については、「Get started with Azure」を参照してください。
- Cisco Catalyst 8000V の展開前または展開中に、いくつかのリソースを展開する必要があります。必要なリソースの説明については、Microsoft Azure のリソース を参照してください。
- BYOL ソフトウェアライセンスを取得するか、Cisco Catalyst 8000V インスタンスのペイアズユーゴーのライセンスモデルを選択する必要があります。詳細については、本ガイドの「ライセンス」セクションを参照してください。

Microsoft Azure のリソース

Microsoft Azure で Cisco Catalyst 8000V を展開するには、次のリソースが必要です。必要なリソースが Azure ネットワークに存在しない場合は、Cisco Catalyst 8000V の展開時に作成する必要があります。

- [Resource group] はリソースのコンテナです。リソースには、仮想マシン、インターフェイス、仮想ネットワーク、ルーティングテーブル、パブリック IP アドレス、セキュリティグループ、ストレージアカウントが含まれます。これらのリソースについては、以下で詳しく説明します。

（注） 既存のリソースグループ内に 1 つのインターフェイスを持つ Cisco Catalyst 8000V を展開する必要があります。リソースグループには、すでに他のリソースが含まれていることがあります。

2 番目のリソースグループ内のオブジェクトに依存するオブジェクトをリソースグループに作成する場合、最初のリソースグループ内のオブジェクトを削除するまで、2 番目のリソースグループを削除することはできません。新しい展開用の新しいリソースグループを作成します。リソースグループの詳細については、「Azure Resource Manager overview」を参照してください。

- [Virtual network] では、2、4、または 8 つのネットワーク インターフェイス カード（NIC）を持つ Cisco Catalyst 8000V には、一連のサブネットが定義された仮想ネットワークが必要です。1 つのインターフェイスを持つ Cisco Catalyst 8000V には、1 つのサブネットを持つ新規または既存の仮想ネットワークが必要です。仮想ネットワークの詳細については、「Azure Virtual Network」を参照してください。
- [Route table] にはサブネットワークのユーザー定義ルート（UDR）が含まれます。
- [Security group] には仮想ネットワークのセキュリティルールが含まれます。
- [Public IP address] は Cisco Catalyst 8000V インスタンスのパブリック IP アドレスです。
- [Storage account] は Cisco Catalyst 8000V イメージ、VM ディスクファイル、および起動診断に必要です。現在サポートされているタイプは、ストレージアカウントのタイプが

`Standard_LRS` のみです。ストレージアカウントの作成の詳細については、「About Azure storage accounts」を参照してください。

- [Boot Diagnostics] は Cisco Catalyst 8000V の操作中に見つかった問題のデバッグに役立ちます。
- [Availability Set] には VM のグループが含まれます。VM は論理的に分離され、データセンター内の複数のサーバー、ラック、およびスイッチで実行できます。可用性セットの詳細については、このドキュメントの可用性セットに関する情報を参照してください。Microsoft Azure のドキュメントで可用性セットの検索も行ってください。
- [Managed Disks] では VM ディスクのストレージアカウントを管理します。マネージドディスクを作成するときは、ディスクの種類（Premium または Standard）と必要なディスクのサイズを指定します。Azure の Storage Service Encryption（SSE）は、デフォルトですべてのマネージドディスクに対して使用されます。マネージドディスクの詳細については、「Azure Managed Disks Overview」を参照してください。
- [Interfaces] では 2、4、または 8 つのネットワーク インターフェイスを持つ Cisco Catalyst 8000V VM にパブリック IP アドレスを任意のインターフェイスに割り当てることができます。通常、パブリック IP アドレスは最初のインターフェイスに割り当てられます。すべての Cisco Catalyst 8000V VM インターフェイスはプライベートサブネットにあります。インターフェイス設定の **ip address dhcp** コマンドを使用して各プライベート インターフェイスの IP アドレスを割り当てるか、**ip address** コマンドを使用して静的 IP アドレスを割り当てることができます。たとえば、`ip address 1.1.1.1 255.255.255.0` などです。静的 IP アドレスを使用する場合は、その IP アドレスが Microsoft Azure によって割り当てられた IP アドレスと同じであることを確認してください。Azure Marketplace の VM ネットワーク設定を調べて、インターフェイスの IP アドレスを表示させます。

Microsoft Azure Marketplace で Cisco Catalyst 8000V を展開

シスコは、リソースの作成と管理に役立つ展開のセットを Microsoft Azure マーケットプレイスで公開しています。現在、次のテンプレートがサポートされています。

- Cisco Catalyst 8000V ソリューションテンプレート。このテンプレートを使用すると、他の必要なリソースを使用して、2、4、または 8 つの NIC を持つ Cisco Catalyst 8000V を展開できます。
- Cisco Catalyst 8000V 仮想マシンテンプレート。このテンプレートを使用すると、既存のリソースを使用して、1 つのインターフェイスを持つ Cisco Catalyst 8000V を展開できます。

既存のリソースがない新しいネットワークに Cisco Catalyst 8000V インスタンスを展開する場合は、完全なソリューションテンプレートを使用することをお勧めします。詳細については、「Cisco Catalyst 8000V Public Cloud Deployments」セクションを参照してください。

政府機関のクラウドの展開については、「Cisco Catalyst 8000V Government Cloud Deployments」セクションを参照してください。

2、4、または 8 つの NIC ソリューションテンプレートを持つ Cisco Catalyst 8000V インスタンスを展開すると、多くのリソースが自動的に作成されます。仮想ネットワークに必要なイン

ターフェイスまたはサブネットの数に基づいてソリューションテンプレートを選択してください。インスタンスを展開する方法については、このガイドの「Deploy a Cisco Catalyst 8000V with Multiple Interfaces」を参照してください。

Cisco Catalyst 8000V インスタンスを展開し、Microsoft Azure にすでに存在するリソースを使用するには、1つのインターフェイステンプレートを使用してインスタンスを展開します。詳細については、「Deploy a Cisco Catalyst 8000V with a Single Interface」セクションを参照してください。1つのインターフェイスを持つCisco Catalyst 8000Vインスタンスを展開した後、Powershell または Azure CLI コマンドを使用して、さらにインターフェイスを手動で追加できます。

Cisco Catalyst 8000V パブリッククラウドの展開

次の 2、4、および 8 つの NIC ソリューションテンプレートは、現在、パブリッククラウドの Microsoft Azure マーケットプレイスで提供されています。

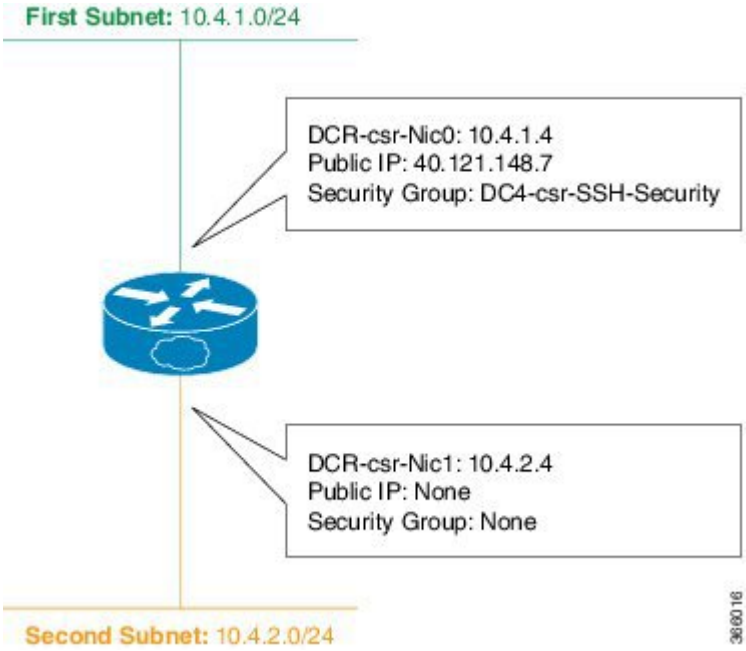
Cisco IOS XE リリース	サポートされるインスタンスタイプおよびサポートされる最大 NIC
Cisco IOS XE 17.4.1 リリース以降	DS2_ v2、D2_v2（2 NIC） DS3_v2、D3_v2（4 NIC） DS4_v2、D4_v2（8 NIC） F16s_v2（4 NIC） F32s_v2（8 NIC）
Cisco IOS XE 17.12.1 リリース以降	DS2_ v2、D2_v2（2 NIC） DS3_v2、D3_v2（4 NIC） DS4_v2、D4_v2（8 NIC） D16_v5（8 NIC） F16s_v2（4 NIC） F32s_v2（8 NIC）

2つのネットワーク インターフェイスを持つCisco Catalyst 8000Vの例

この例は、Azure Marketplace から 2 つのネットワーク インターフェイス ソリューション テンプレートを展開した後の設定を示しています。

Cisco Catalyst 8000V 仮想マシン（2 vCPU、7G RAM）は 2 つのインターフェイスで設定されています。最初のサブネット（NIC0）のインターフェイスにアタッチされたパブリック IP アドレスがあります。最初のサブネット（NIC0）には、インターフェイスのインバウンドルールを持つセキュリティグループがあります。Cisco Catalyst 8000V の Microsoft Azure ハイパーバイザ

のルータには、デフォルトのルーティングテーブルが設定されています。Cisco Catalyst 8000V インスタンスは、新規または既存の仮想ネットワークに展開できます。



サブネット化の制限

Microsoft Azure での Cisco Catalyst 8000V では、/8 と /29（CIDR 定義）の間のサブネットマスクがサポートされています。

サブネット /29 は、8 つの IP ホストアドレスをサポートする Microsoft Azure で使用できる最小のものです。サブネットごとに 4 つの IP ホストアドレスが Microsoft Azure によって予約されています。したがって、/29 サブネットの場合、4 つの IP ホストアドレスを使用できます。

可用性セットに関する情報

Azure Marketplace から 2、4、または 8 つのネットワーク インターフェイス用のソリューションテンプレートを使用して Cisco Catalyst 8000V を展開し、可用性セット機能の使用を選択した場合は、新しい可用性セットを使用する必要があります。

可用性セットは、パブリッククラウドのソリューションテンプレートでのみ使用できます。政府機関のクラウドのソリューションテンプレートでは使用できません。

詳細については、「Azure Managed Disks Overview」を参照してください。

2、4、または 8 つのネットワーク インターフェイスを持つ Cisco Catalyst 8000V の可用性セット

可用性セット内の VM リソースを論理的にグループ化すると、VM のグループを互いに分離した状態に保つことができます。可用性セット内の VM は、複数の物理サーバー、コンピューティングラック、ストレージユニット、およびネットワークスイッチで実行できます。可用性

セットを使用していて、ハードウェアまたはMicrosoft Azureソフトウェアの障害が発生した場合、影響を受けるのはVMのサブセットのみです。2、4、または8つのネットワークインターフェイス用のソリューションテンプレートを使用してCisco Catalyst 8000Vを展開する場合は、新しい可用性セットを使用する必要があります。可用性セットは、Cisco Catalyst 8000Vのパブリッククラウドの展開でのみ使用できます。可用性セットは、Cisco Catalyst 8000Vの政府機関のクラウドの展開には使用できません。

可用性セットの使用を選択し、ソリューションテンプレートを使用して2、4、または8つのネットワーク インターフェイスを持つCisco Catalyst 8000Vを展開する場合、次のパラメータを入力するように求められます。

- [Availability Set Name] は新しい可用性セットの名前です。既存の可用性セットの名前は使用できません。
- [Platform Fault Domain Count] は障害ドメイン数です。同じ障害ドメインにあるVMは、共通のストレージと、共通の電源とネットワークスイッチを共有します。値：1または2（デフォルト値は2）。
- [Platform Update Domain Count] は同時に再起動できるVMおよび基礎となる物理ハードウェアのグループである更新ドメインの数です。値：1 ～ 20（デフォルト値は20）。

1つのインターフェイスを持つ Cisco Catalyst 8000V の可用性セット

既存の可用性セットを使用するには、1つのインターフェイスを持つCisco Catalyst 8000Vを展開する必要があります。

Cisco Catalyst 8000V の展開に関するよくある質問

1. Azure Marketplace で C8000V を検索すると、Cisco Catalyst 8000V ソリューションテンプレートや展開のリストが表示されます。どれを選べばいいですか？

ソリューションテンプレート（2、4、または8つのNIC）を選択するか、個別のCisco Catalyst 8000Vを選択するかを決定するためのベストプラクティスは次のとおりです。

新しい仮想ネットワークを作成する場合は、ソリューションテンプレート（2、4、または8つのNIC）の1つを使用します。これにより、すべてのリソースを手動で作成する時間と労力を節約できます。

次のいずれかの条件が当てはまる場合は、個別のCisco Catalyst 8000Vを使用します。

- Cisco Catalyst 8000Vが含まれていない既存のリソースグループがあり、そのリソースグループにCisco Catalyst 8000Vを展開する場合。
- Cisco Catalyst 8000Vがすでに含まれている既存のリソースグループがあり、同じ可用性セットに別のリソースグループを展開する場合。

2. サブスクリプションに複数の Cisco Catalyst 8000V インスタンスを作成し、それらをすべて 1 つの可用性セットに展開したい。どうすればいですか？

次の操作を行ってください。

1. 2、4、または 8 つの NIC ソリューションテンプレートを使用して最初の Cisco Catalyst 8000V を展開します。この Cisco Catalyst 8000V インスタンスの新しい可用性セットを作成します。
2. 個別の Cisco Catalyst 8000V を展開します。手順 1 で作成したものと同じ可用性セットを選択します。この所有ライセンス持ち込みを使用すると、個別の Cisco Catalyst 8000V では既存の空でないリソースグループで既存のリソースを再利用できます。
3. 残りのすべての Cisco Catalyst 8000V インスタンスについて、手順 2 を繰り返します。

ライセンス

Cisco Catalyst 8000V は、次のライセンスモデルをサポートしています。

所有ライセンス持ち込みモデル

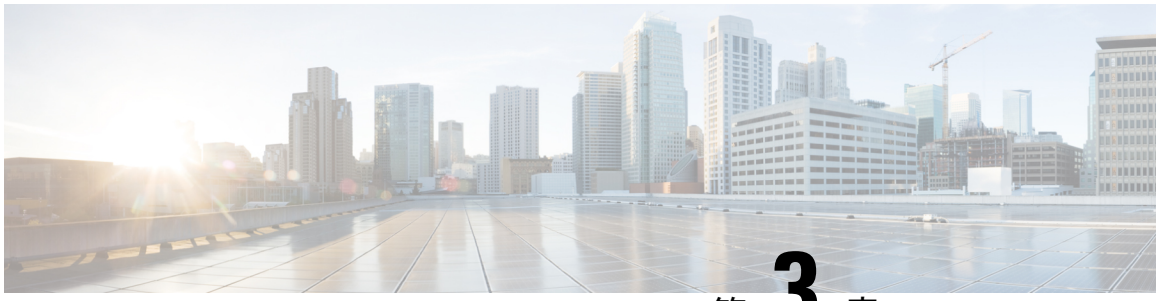
Microsoft Azure での Cisco Catalyst 8000V の所有ライセンス持ち込み（BYOL）のライセンスモデルは、シスコ スマート ライセンシングの使用ポリシーによってサポートされています。このライセンスモデルでは、ライセンスを Cisco Catalyst 8000V インスタンスに動的に割り当てることができます。各ライセンスを特定の Cisco Catalyst 8000V UDI シリアル番号にロックすることなく、異なる Cisco Catalyst 8000V インスタンス間でライセンスを管理できます。

（注） Cisco Catalyst 8000V のライセンスの支払いに加えて、Microsoft VM インスタンスの支払いも必要です。

ペイアズユーゴーライセンス

ペイアズユーゴー（PAYG）は、Microsoft Azure で実行する Cisco Catalyst 8000V によってサポートされるライセンスモデルです。このライセンスモデルでは、Azure Marketplace から時間単位の Cisco Catalyst 8000V インスタンスを起動し、必要に応じて設定した期間、インスタンスを使用できます。これにより、年次または複数年の請求ではなく、インスタンスを使用した時間に対してのみ支払うことができます。Cisco Catalyst 8000V PAYG インスタンスは、BYOL ライセンスモデルで使用できる既存のすべての展開モデルをサポートしています。

（注） スループットライセンスのパフォーマンスを有効にするには、高速ネットワーク機能を有効にする必要があります。



第 3 章

Microsoft Azure での Cisco Catalyst 8000V の展開

Microsoft Azure ポータルのカスタマイズ

仮想マシンや仮想ネットワークなどの頻繁に使用されるオブジェクトを左側のパネルに追加することで、Microsoft Azure ポータルの GUI をカスタマイズできます。

（注） これらのオプションの手順を実行する必要があるのは、リソースを手動で追加する必要がある 1 つのインターフェイスを使用している Cisco Catalyst 8000V インスタンスを展開する場合のみです。ソリューションテンプレートを使用して 2、4、または 8 つのインターフェイスを持つ Cisco Catalyst 8000V インスタンスを展開する場合、これらのリソースを手動で作成する必要はありません。

始める前に

ポータルをカスタマイズするには、Microsoft Azure サブスクリプションが必要です。

ステップ 1 Microsoft Azure ポータルにサインインします。

ステップ 2 [Browse] をクリックし、左側のパネルに追加するオブジェクトを選択します。

ステップ 3 ドロップダウンメニューで、選択したオブジェクトの星印をクリックします。
このオブジェクトの詳細は、将来的な使用のために保存されます。手順 2 と 3 を繰り返して、一連のオブジェクトを左側のサイドパネルに追加します。

1 つのインターフェイスを持つ Cisco Catalyst 8000V を展開する

1 つのインターフェイスを持つ Cisco Catalyst 8000V を展開するには、次の手順を実行します。

（注） 2、4、または 8 つの NIC のソリューションテンプレートを持つ Cisco Catalyst 8000V を展開する場合、次の手順は必要ありません。代わりに、Microsoft Azure ポータルにアクセスして、Cisco Catalyst 8000V のパブリック IP アドレスを決定してください。次に、「Access the Cisco Catalyst 8000V CLI」セクションの説明に従って Cisco Catalyst 8000V に [ssh] で接続します。

ステップ 1 左側のパネルで [Virtual machines] を選択します。

ステップ 2 [Add]をクリックします。

ステップ 3 `c8000v` と入力します。検索が開始され、Azure Marketplace で Cisco Catalyst 8000V VM の展開が見つかります。

ステップ 4 [Deployments] を選択します。

ステップ 5 [Create] をクリックします。

[Basics] サブメニューが強調表示されます。

ステップ 6 [Name] に仮想ネットワークの名前を入力します。

仮想ネットワークは、プライベートネットワークを表すために Microsoft Azure が使用するクラウドベースのネットワークです。

ステップ 7 [VM disk type] で VM ディスクの種類を選択します。

VM ディスクの種類は SSD または HDD のいずれかです。

ステップ 8 **ユーザー名**

Cisco Catalyst 8000V 仮想マシンのユーザー名。これは、Cisco Catalyst 8000V インスタンスへのログインに使用するユーザー名です。

ステップ 9 [Authentication type] でパスワード（デフォルト）または SSH 公開キーを入力します。

ステップ 10 [Subscription] でサブスクリプションの名前を選択します。

仮想マシンの名前に基づくデフォルト名が提供されます。このデフォルト名は変更できます。

ステップ 11 [Resource Group] で [Create new] を選択して新しいグループを作成するか、[Use existing] を選択して既存のグループを選択します。

[Size] サブメニューが強調表示されます。

新規の、または既存のリソースグループの名前を指定します。

ステップ 12 [OK] をクリックします。

ステップ 13 [Virtual machine size] をクリックします

仮想マシンのサイズの詳細については、「Sizes for Windows virtual machines in Azure」を参照してください。

ステップ 14 [OK] をクリックします。

[Settings] サブメニューが強調表示されます。

ステップ 15 [High Availability] で既存の可用性セットを選択するか、新しい可用性セットを作成します。

高可用性を使用するには、既存の可用性セットを選択するか、新しい可用性セットを作成します。

ステップ 16 [Storage] でストレージアカウント名を入力します。

マネージドディスクを使用して VM ディスクのストレージアカウントを管理している場合は、ストレージアカウント名を入力します。

ステップ 17 [Virtual network] で仮想ネットワークアドレスを入力します。

Classless Inter-Domain Routing（CIDR）表記を使用して、仮想ネットワークのアドレスを入力します。例：`10.4.1.0/16`

ステップ 18 [Subnet] でサブネットの IP アドレスを入力します。

ステップ 19 [Public IP address] でパブリック IP アドレス名を入力します。

IP アドレスは Azure によって提供されます。

ステップ 20 [Network Security groups] でネットワーク セキュリティ グループの名前を入力します。

ステップ 21 [Auto-shutdown]

自動シャットダウンを有効にするには、[Enable] を [On] に設定します。自動シャットダウンを無効にするには、[Enable] を [Off] に設定します。自動シャットダウンの詳細については、Microsoft Azure のマニュアルで自動シャットダウンを検索してください。

ステップ 22 （任意）[Monitoring] で [Monitoring] を選択してモニタリングを有効にします。

起動診断を使用して、Cisco Catalyst 8000V のモニタリングを有効にします。モニタリングを有効にする場合は、起動診断のアカウント名も入力する必要があります。

ステップ 23 [OK] をクリックします。

[4 Summary] サブメニューが強調表示されます。展開しようとしている VM の概要の詳細がシステムに表示されます。

ステップ 24 [Create] をクリックします。

VM が作成され、購入が確定されます。

ステップ 25 左側のパネルで [Virtual machines] をクリックします。

VM ステータスを確認します。数分後、VM のステータスが [Creating] から [Running] に変わります。パブリック IP アドレス名をメモします。

次のタスク

Cisco Catalyst 8000V へ [ssh] で接続する方法が説明されている「Access the Cisco Catalyst 8000V CLI」セクションに移動します。

複数のインターフェイスを持つ Cisco Catalyst 8000V を展開する

複数のインターフェイスを持つCisco Catalyst 8000V を展開するには、次の手順を実行します。

ステップ 1 左側のパネルで [Virtual machines] を選択します。

ステップ 2 [Add]をクリックします。

ステップ 3 「C8000V」と入力します。

Azure Marketplace で Cisco Catalyst 8000V VM の展開を検索します。

ステップ 4 2、4、または 8 つの NIC を持つ展開を選択します。

ステップ 5 [Create] をクリックします。

ステップ 6 [Virtual Machine Name] で [Basics] サブメニューを選択し、仮想マシン名を入力します。

プライベートネットワークを表すために Microsoft Azure が使用するクラウドベースのネットワークの名前です。

ステップ 7 [Username] でユーザー名を選択します。

Cisco Catalyst 8000V インスタンスへのログインに使用できる Cisco Catalyst 8000V 仮想マシンのユーザー名です。

ステップ 8 [Authentication type] でパスワード（デフォルト）または SSH 公開キーを入力します。

ステップ 9 [Cisco IOS XE Image Version] で Cisco IOS XE バージョンを選択します。

ステップ 10 [Subscription] でサブスクリプション名を変更（任意）します。

仮想マシンの名前に基づいて、デフォルトのサブスクリプション名が提供されます。このデフォルトのサブスクリプション名は変更できます。

ステップ 11 [Resource Group] で [Create new] または [Use existing] を選択します。

Cisco Catalyst 8000V は、新しいリソースグループ（または完全に空の既存のリソースグループ）にのみ作成できます。リソースグループを削除するには、Cisco Catalyst 8000V VM を削除してから、リソースグループを削除します。

ステップ 12 [OK] をクリックします。

ステップ 13 [Cisco C8000V Settings] サブメニューを選択してから、[Number of Network Interfaces in C8000V] を選択します。

ステップ 14 インターフェイスの数を 2、4、または 8 から選択します。

ステップ 15 [License Type] でライセンスタイプとして [BYOL] または [PAYG] を選択します。

ステップ 16 [Managed Disk] で [Enabled] を選択します。

ステップ 17 [Storage Account] でストレージアカウントの名前を入力します。

ストレージアカウントの詳細については、このガイドの「Microsoft Azure Resources」セクションを参照してください。

ステップ 18 [Virtual machine size] で適切な仮想マシンのサイズを選択します。

使用しているインターフェイスの数に基づいて、適切な仮想マシンのサイズを選択します。Microsoft Azureは、期待されるパフォーマンスが異なるさまざまなイメージタイプをサポートしています。サポートされているインスタンスタイプと仮想マシンサイズを表示するには、次のリンクを参照してください。

- 「Dv2 and DSv2 series」
- 「Fsv2 series」

ステップ 19 [Custom Data] で、ブートストラップ設定ファイルを提供する場合は、[Yes] を選択します。

Cisco Catalyst 8000V インスタンスにブートストラップ設定ファイルを提供する方法の詳細については、「Deploying a Cisco Catalyst 8000V VM Using a Day 0 Bootstrap File」セクションおよび「Customdata-examples」セクションを参照してください。

ステップ 20 [Availability Set] で [Yes] を選択します。

ステップ 21 [Availability Set name] で可用性セットの名前を入力します。

ステップ 22 [Availability Set fault domain count] で可用性セットの障害ドメイン数を入力します。

障害ドメインは、共通の電源とネットワークスイッチを共有する VM のグループを定義します。可用性セットは、障害ドメイン全体に仮想マシンを配置します。

ステップ 23 [Availability Set update domain count] で可用性セットの更新ドメイン数を入力します。

更新ドメインは、同時に再起動できる VM と基礎となる物理ハードウェアのグループです。

ステップ 24 [Boot diagnostics] で起動診断を入力します。

起動診断の詳細については、「Information About Deploying Cisco Catalyst 8000V in Microsoft Azure」セクションを参照してください。

ステップ 25 [Diagnostics Storage account] でストレージアカウント名を入力します。

ステップ 26 [Public IP Address] でパブリック IP アドレス名を入力します。

パブリック IP アドレスの詳細については、「Microsoft Azure Resources」セクションを参照してください。

ステップ 27 [DNS label] で DNS ラベルの名前を変更（任意）します。

DNS ラベルは、Cisco Catalyst 8000Vに割り当てられるパブリック IP アドレスの名前です。DNS ラベルのデフォルト値がテキストボックスに表示されます。これは、VM 名の後に「-dns」が続きます。

ステップ 28 [Virtual network] で [Create New] または [Use existing] のいずれかを選択します。

新しい仮想ネットワークの場合、名前と IP アドレスを入力します。

ステップ 29 [Subnets] をクリックし、サブネット名と IP アドレスを入力します。

ステップ 30 すべての Cisco Catalyst 8000V 設定が許容範囲であることを確認し、[OK] をクリックします。

[3 Summary] サブメニューが強調表示されます。

ステップ 31 [OK] をクリックします。

[4 Buy] サブメニューが強調表示されます。

ステップ 32 [Create] をクリックします。

VM が作成され、購入が確定されます。

ステップ 33 左側のパネルで [Virtual machines] をクリックします。

数分後、最近作成された VM のステータスが [Creating] から [Running] に変わります。パブリック IP アドレス名をメモします。

Cisco Catalyst 8000V CLI へのアクセス

ターミナルサーバーを介して Cisco Catalyst 8000V VM の CLI にアクセスします。

始める前に

CLI にアクセスする前に、前述の展開手順のいずれかの手順を実行します。1 つのインターフェイスを持つ Cisco Catalyst 8000V を展開するか、複数のインターフェイスを持つ Cisco Catalyst 8000V を展開します。

以下の 2 つのサブステップのいずれかのコマンドシンタックスを使用して、**ssh** コマンドを入力します。

選択したターミナルサーバーで **ssh** コマンドを入力して、CLI にアクセスします。

- 以前に SSH 公開キーを使用していない場合（「azureuser」というユーザー名を指定しなかった場合）、次のコマンドを使用して Cisco Catalyst 8000V CLI にアクセスできます。**ssh –o ServerAliveInterval=**60 *username @ c8000v_ip_address*
- 以前に SSH 公開キーを使用していた場合（「azureuser」というユーザー名を指定した場合）、次のコマンドを使用して Cisco Catalyst 8000V CLI にアクセスできます。**ssh –i***key***-o ServerAliveInterval=**60 azureuser*@c8000v_ip_address*

例

次の例では、ユーザー名は「azureuser」、パブリック IP アドレスは「40.121.148.7」、パスワードは「xxx」が **ssh** コマンドのパラメータとして **show ip route** のような他のコマンドの前に使用されています。（以前に ssh 公開キーを指定していません。）

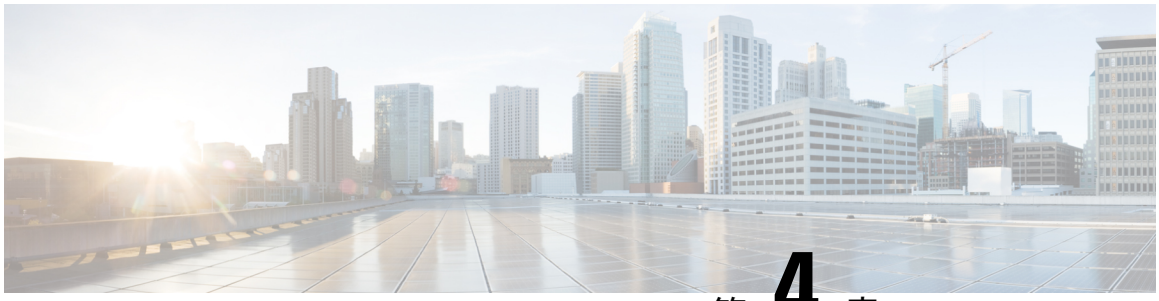
```
$ ssh -o ServerAliveInterval=60  azureuser@40.121.148.7
                The authenticity of host '40.121.148.7 (40.121.148.7)' can't be
established.
                RSA key fingerprint is 94:79:e9:d2:2e:85:93:d6:52:41:cc:a3:d9:14:7f:5f.
                Are you sure you want to continue connecting (yes/no)? yes
                Warning: Permanently added '40.121.148.7' (RSA) to the list of known
hosts.
                Password: mypassword

# show ip int br
                Interface              IP-Address      OK? Method Status
     Protocol
                GigabitEthernet1       10.4.1.4        YES DHCP   up
     up
                GigabitEthernet2  unassigned     YES unset  administratively down
down


# configure terminal
                Enter configuration commands, one per line.  End with CNTL/Z.
                # interface g2
                # ip address dh
                # ip address dhcp
                # no shutdown
                # end
                # show run interface g2
                Building configuration...
                Current configuration : 69 bytes
                !
                interface GigabitEthernet2
                ip address dhcp
                negotiation auto
                end
                # show ip interface brief
                Interface              IP-Address      OK? Method Status
 Protocol
                GigabitEthernet1       10.4.0.4        YES DHCP   up
 up
                GigabitEthernet2       10.4.1.4        YES DHCP   up
 up

                # show ip route
                <output snipped for brevity>
                Gateway of last resort is 10.4.1.1 to network 0.0.0.0

                S*    0.0.0.0/0 [1/0] via 10.4.1.1
                10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
                C        10.4.1.0/24 is directly connected, GigabitEthernet1
                L        10.4.1.4/32 is directly connected, GigabitEthernet1
                C        10.4.2.0/24 is directly connected, GigabitEthernet2
                L        10.4.2.4/32 is directly connected, GigabitEthernet2
                168.63.0.0/32 is subnetted, 1 subnets
                S        168.63.129.16 [254/0] via 10.4.1.1
```



第 4 章

Microsoft Azure の Cisco Catalyst 8000V の設定

次の章では、Microsoft Azure 用に Cisco Catalyst 8000V インスタンスを設定する方法について説明します。

ルートテーブルの更新

Microsoft Azure では、すべての VM がハイパーバイザのルータにパケットを送信し、ハイパーバイザはそのサブネットに関連付けられたルーティングテーブルに基づいてパケットを転送します。

Cisco Catalyst 8000V VM が作成されると、サブネットごとにルートテーブルが作成されます。2 つの vNIC を持つ Cisco Catalyst 8000V VM の場合、Cisco Catalyst 8000V を指す 2 番目の（内部に面した）サブネットに対してデフォルトルートが作成されます。このサブネット上に作成されたすべての VM は、デフォルトゲートウェイとして Cisco Catalyst 8000V を使用します。3 つ以上の vNIC を持つ Cisco Catalyst 8000V VM の場合、デフォルトルートを定義してサブネットに適用する必要があります。

ステップ 1 [Route Tables] をクリックします。
[Settings] ペインを展開します。

ステップ 2 [Route Tables] ペインに移動し、ターゲットのルートテーブルを選択します。

ステップ 3 [All Settings] をクリックします。

ステップ 4 [Settings] ペインで [Routes] をクリックします。

ルートを追加または変更します。

セキュリティグループの更新

セキュリティグループは、特定のインターフェイスに対してどのポート/宛先をハイパーバイザが許可または拒否するかを制御するものです。Cisco Catalyst 8000V を作成すると、デフォルトで最初のサブネットのインバウンドインターフェイスに新しいセキュリティグループが作成されます。この展開を通じてデプロイされた Cisco Catalyst 8000V 仮想マシンの場合、インバウンド インターネット トラフィック用に次のポートが追加されます。TCP 22、UDP 500、および UDP 4500。他のポートの使用は拒否されます。

ステップ 1 左側のパネルで [Network security groups] をクリックします。

[Network security groups] ペインが表示され、セキュリティグループのリストが表示されます。

ステップ 2 ターゲットのネットワーク セキュリティ グループをクリックします。

セキュリティグループの詳細を示すペインが表示されます。

ステップ 3 [All Settings] をクリックします。

ステップ 4 [Settings] ペインで、[Inbound Security Rules] をクリックします。

ステップ 5 [Network Security Rules] で、[Add] をクリックしてルールを追加します。

IPsec VPN の設定

次の例は、Microsoft Azure で実行されている Cisco Catalyst 8000V インスタンス用に設定された IPsec VPN を示しています。

```
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 0.0.0.0
crypto ipsec transform-set T1 esp-3des esp-md5-hmac
 mode transport
crypto ipsec profile P1
 set transform-set T1
interface Tunnel0
 ip address 3.3.3.1 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 104.45.154.184
 tunnel protection ipsec profile P1
end
```

```
!!!! To test, create loop back interface and static route!!!!!
interface Loopback1
 ip address 5.5.5.5 255.255.255.255
end
ip route 6.6.6.6 255.255.255.255 Tunnel0
```

ベストプラクティスと注意事項

1. リソースはリソースグループに保持することを推奨します。グループ内のすべてのリソースをクリーンアップするには、関連するリソースグループを削除します。
2. Cisco Catalyst 8000V VM が削除されても、VM のすべてのリソース（ルートテーブル、セキュリティグループ、パブリック IP、ネットワーク インターフェイス）が削除されるわけではありません。その後、以前と同じ名前で新たに Cisco Catalyst 8000V を作成すると、以前のリソースが再利用される可能性があります。これらのリソースを再利用したくない場合は、次のいずれかのアクションを選択します。
   - 各リソースを手動で削除します。
   - 個々のリソースを含むリソースグループを削除します。
   - 別の名前で新しいCisco Catalyst 8000V VM を作成します。
3. 展開テンプレートを使用して Cisco Catalyst 8000V インスタンスを作成する場合は、パブリック IP アドレスが Microsoft Azure で静的として設定されていることを確認してください。これを行うには、Microsoft Azure でパブリック IP アドレスに移動します。設定で、アドレスが動的または静的として表示されているかどうかを確認します。[Static] オプションを選択します。デフォルトのオプションは動的であることに注意してください。

SSH 接続の問題

Cisco Catalyst 8000V を最初にデプロイした後、または Cisco Catalyst 8000V をリロードまたは再起動した後に、Microsoft Azure での Cisco Catalyst 8000V への SSH 接続を確立できない場合があります。Azure ポータルでは、Cisco Catalyst 8000V インスタンスは実行状態です。次の 3 つのシナリオでは、SSH を使用した接続に失敗した場合の回避策を提案します。

シナリオ 1Cisco Catalyst 8000V の起動直後に SSH アクセスを試みた

起動直後に Cisco Catalyst 8000V にアクセスしようとすると、SSH 接続の確立に失敗する場合があります。インスタンスの展開を開始してから、SSH 接続が利用可能になるまで約 5 分かかります。

シナリオ 2 Microsoft Azure インフラストラクチャのバインドの問題

Microsoft Azure サポートでは、次の手順を実行することを推奨します。

1. パブリック IP アドレスを持つ Cisco Catalyst 8000V インターフェイスで、プライベート IP アドレスをサブネット内の新しい静的 IP アドレスに再割り当てします。

2. Azure ポータルで PowerShell を開きます。
3. ARM VM を更新します。

   次の Azure のドキュメントを参照してください。https://docs.microsoft.com/en-us/powershell/module/azurerm.compute/update-azurermvm?view=azurermps-5.6.0
4. PowerShell で次のコマンドを実行してください。

   $vm = Get-AzureRmVM -Name "reload-lnx" **-ResourceGroupName** "reload-rg"

   Update-AzureRmVM -VM $vm -ResourceGroupName "reload-rg"
5. パブリック IP アドレスがアタッチされているネットワーク インターフェイスをリセットします。

   ネットワーク インターフェイスのリセットの詳細については、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/reset-network-interface を参照してください。
6. [VM] > [Networking] を選択し、ネットワーク インターフェイスを選択します。
7. [IP configurations] に移動し、IP 名を選択します。
8. インターフェイスに割り当てられているプライベート IP アドレスが静的に設定されている場合は、手順 **13** で使用するためにアドレスを書き留めます。
9. [Assignment] で、[Static] をクリックします。
10. [IP Address] フィールドで、使用可能な IP アドレスを使用します。ネットワーク インターフェイスが接続されているサブネット内で使用可能な IP アドレスを選択します。
11. [Save] をクリックして、保存が完了するまで待ちます。
12. SSH を使用してルータへの接続を再試行します。
13. 静的 IP アドレスを追加（または変更）して VM にアクセスした後、このインターフェイスに最初に割り当てた IP アドレス（手順 **8** を参照）が静的に設定されている場合は、IP アドレスを静的から動的に変更できます。または、IP アドレスを元のアドレス（手順 **8** で書き留めたアドレス）に再設定できます。

シナリオ 3 アイドル端末のタイムアウトの設定不備

Cisco Catalyst 8000V への SSH セッションを開始するときは、次のように端末の VTY タイムアウトを無限に設定しないでください。`exec-timeout 0 0` タイムアウトにはゼロ以外の値を使用します。たとえば、`exec-timeout 4 0` などです。このコマンドは、4 分 0 秒のタイムアウトを指定します。

`exec-timeout 0 0` コマンドが問題を引き起こす理由は次のとおりです。

Azure では、コンソールのアイドル期間に 4 分から 30 分のタイムアウトが適用されます。アイドルタイマーが期限切れになると、Azure は SSH セッションを切断します。しかし、`exec-timeout 0 0` コンフィギュレーション コマンドによってタイムアウトが無限に設定されていると、セッションは Cisco Catalyst 8000V からはクリアされません。切断により、端末セッションが孤立します。Cisco Catalyst 8000V のセッションは無期限に開いたままになります。新しい SSH セッ

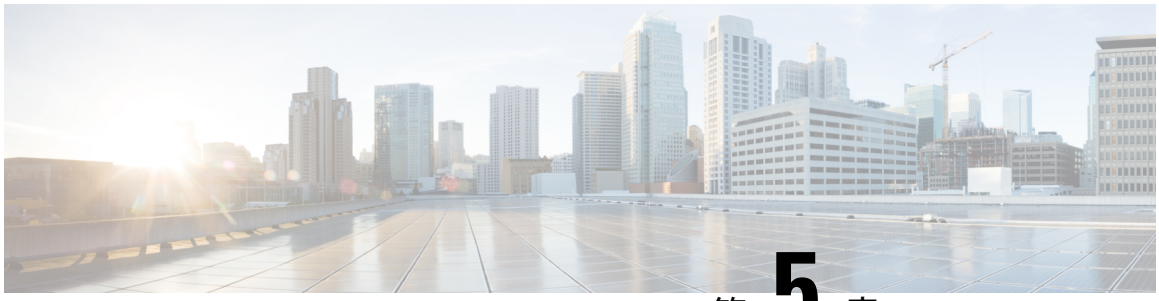
ションを確立しようとすると、新しい仮想端末セッションが使用されます。このパターンが引き続き発生すると、許可されている同時端末セッションの数に達し、新しいセッションを確立できなくなります。

`exec-timeout` コマンドを正しく設定することに加えて、次の例に示すコマンドを使用して、アイドル状態の仮想端末セッションを削除することもお勧めします。

```
Router# show users
Line User Host(s) Idle Location
2 vty 0 cisco idle 00:07:40 128.107.241.177
* 3 vty 1 cisco idle 00:00:00 128.107.241.177

Router# clear line 2
```

上記のシナリオの回避策が効果がない場合は、最後の手段として、Azure ポータルから Cisco Catalyst 8000V インスタンスを再起動できます。



第 5 章

ユーザー定義ルートの使用上のガイドライン

Cisco Catalyst 8000V ルートテーブルの概要

このセクションでは、ユーザー定義ルートを決定してルートテーブルに追加するのに役立つガイドラインを提供します。Microsoft Azure Marketplace テンプレートを使用して仮想ネットワークに Cisco Catalyst 8000V を展開すると、Cisco Catalyst 8000V がネットワーク接続を持つサブネットごとにルートテーブルが作成されます。たとえば、Microsoft Azure Marketplace から Cisco Catalyst 8000V の 4 つの NIC バージョンを展開すると、4 つのサブネットが作成されます。各サブネットには、関連付けられたルートテーブルがあります。ルートはルートテーブルに自動的にインストールされません。

ユーザー定義ルートの定義の詳細については、次の Microsoft Azure のドキュメントの「User Defined Routes」セクションを参照してください。https://docs.microsoft.com/en-us/azure/

- 同じ仮想ネットワーク内のユーザー定義ルート （27 ページ）
- 仮想ネットワークまたはオンプレミスネットワーク間のルーティング （28 ページ）
- 高可用性のためのユーザー定義ルート （28 ページ）

同じ仮想ネットワーク内のユーザー定義ルート

既定では、Microsoft Azure のネットワーク インフラストラクチャは、仮想ネットワーク内のすべてのサブネットを相互接続する基本的なルーティングサービスを提供します。 Cisco Catalyst 8000V インスタンスの助けを借りずに、同じ仮想ネットワーク内の任意の仮想マシン間でパケットを通過させることができます。

ただし、サブネット間のパケットを Cisco Catalyst 8000V に（フィルタリングや QoS などの高度なサービスを実装するために）配信する必要がある場合は、Cisco Catalyst 8000V インスタンスをネクストホップルータとして指定するサブネットのルーティングテーブルにユーザー定義ルートをインストールする必要があります。

仮想ネットワークまたはオンプレミスネットワーク間のルーティング

Microsoft Azure のネットワーク インフラストラクチャは、既定では、異なる仮想ネットワークを相互接続したり、仮想ネットワークをオンプレミスネットワークに接続したりしません。これらのネットワークに接続するには、各ルートテーブルにユーザー定義ルートを作成して、Cisco Catalyst 8000V を各リモートネットワークへのネクストホップルータとして指定する必要があります。ユーザー定義ルートは、デフォルトルートまたは特定の宛先へのルートのいずれかです。Cisco Catalyst 8000V にトラフィックを強制的に通過させるには、デフォルトルートまたは特定の宛先ルートを Cisco Catalyst 8000V を指すルートテーブルにインストールします。

（注） デフォルトルートがルートテーブルにインストールされている場合、すべてのトラフィックは指定されたネクストホップに転送されます。これにより、割り当てられたパブリック IP アドレス（VM への管理アクセスに使用される）を持つ仮想マシンがある場合は問題が発生します。サブネットに関連付けられたルートテーブルにデフォルトルートがある場合、そのパブリック IP アドレスを介して仮想マシンに到達することはできません。

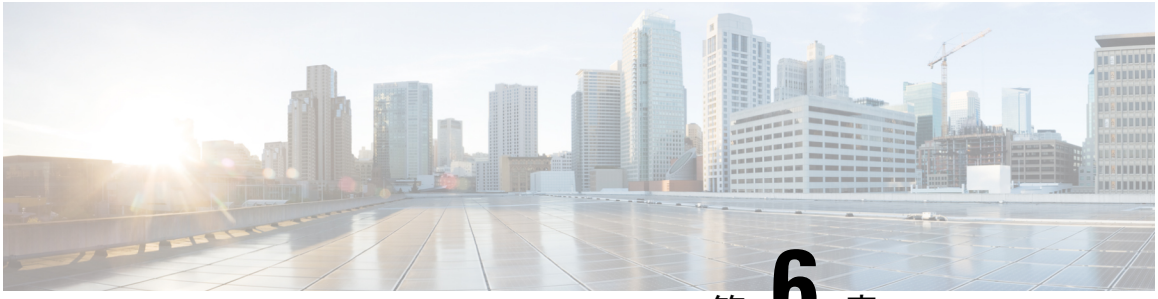
（注） Microsoft Azure は、同じリージョンでホストされている限り仮想ネットワークを相互接続できる VNET ピアリングと呼ばれる機能をサポートしています。Cisco Catalyst 8000V 内で VNET ピアリングを使用してサービスを利用するには、Cisco Catalyst 8000V にトラフィックを強制的に通過させるユーザー定義ルートを追加する必要があります。

高可用性のためのユーザー定義ルート

同じ仮想ネットワークに 2 つの Cisco Catalyst 8000V インスタンスを展開して、高可用性のために 1:1 冗長性を提供できます。Cisco Catalyst 8000V インスタンスを高可用性で設定すると、ピアルータの到達可能性が監視されます。Cisco Catalyst 8000V がピアルータがダウンしたと判断した場合、ルートテーブルに自身の IP アドレスをインストールします。これにより、トラフィックは「動作中」の Cisco Catalyst 8000V インスタンスを介してルーティングされます。

ユーザー定義ルートを設定するときは、Cisco Catalyst 8000V のピアルータの 1 つに障害が発生したときにルートテーブルのエントリを更新するかどうかを決定する必要があります。高可用性機能がトラフィックを「動作中」の Cisco Catalyst 8000V にリダイレクトする必要があるルートテーブルの場合は、各ユーザー定義ルートテーブルに冗長ノードを設定する必要があります。

Cisco Catalyst 8000V のピアに障害が発生した場合、冗長ノードによって指定されたルートテーブルのすべてのルートが更新されます。



第 6 章

高速ネットワークの設定

高速ネットワークとは

高速ネットワークは、Cisco Catalyst 8000V VM などの VM で single root I/O virtualization（SR-IOV）を有効にします。高速ネットワークのパスは仮想スイッチをバイパスし、ネットワークトラフィックの速度を上げ、ネットワークのパフォーマンスを向上させ、ネットワークの遅延とジッターを減らします。

通常、VM に出入りするすべてのネットワークトラフィックは、ホストと仮想スイッチを通過します。ただし、高速ネットワークでは、ネットワークトラフィックは仮想マシンのネットワーク インターフェイス（NIC）に到着し、VM に転送されます。したがって、仮想スイッチが適用するすべてのネットワークポリシーがオフロードされ、ハードウェアに適用されます。

Microsoft Azure で使用できる高速ネットワーク機能の詳細については、「Create a Linux VM With Accelerated Networking Using Azure CLI」を参照してください。

高速ネットワークは、Cisco Catalyst 8000V のパブリッククラウドの展開および政府機関のクラウドの展開で使用できます。

Azure-PMD のサポート

Azure の Azure-PMD（ポーリングモードドライバ）機能は、パフォーマンスを重視するアプリケーション向けに、より高速なユーザー空間のパケット処理フレームワークを提供します。このフレームワークは、仮想マシンのカーネルのネットワークスタックをバイパスします。カーネルのネットワークスタックを使用する一般的なパケット処理では、プロセスは割り込み駆動型です。ネットワーク インターフェイスが着信パケットを受信すると、パケットを処理するためのカーネルへの割り込みと、カーネル空間からユーザー空間へのコンテキストの切り替えが発生します。Azure-PMD は、コンテキストの切り替えと割り込み駆動方式を排除し、高速なパケット処理のためにポーリングモードドライバを使用するユーザー空間の実装を採用しています。

Microsoft Azure で Cisco Catalyst 8000V を実行するために Azure-PMD 機能を有効にすることができます。この機能により、高速ネットワークを使用する以前のバージョンと比較して、Cisco Catalyst 8000V インスタンスのパフォーマンスが向上します。

サポートされている VM インスタンスタイプ

次の VM インスタンスタイプは、高速ネットワーク機能をサポートしています。

IOS XE バージョン	サポートされている VM インスタンスタイプ
17.4.x 以降	DS2_v2、D2_v2 DS3_v2、D3_v2 DS4_v2、D4_v2 F16s_v2 F32s_v2

Mellanox ハードウェアのサポート

Microsoft Azure クラウドには、高速ネットワーク機能をサポートする 2 種類のハードウェアがあります。次の表は、高速ネットワーク機能でサポートされている Mellanox のバージョンを示しています。

表 *1 : IOS* バージョンと高速ネットワークの互換性マトリックス

IOS XE バージョン	高速ネットワークのサポート	MLX4 のサポート	MLX5 のサポート	Azure-PMD のサポート
17.4.x 以降	対応	対応	対応	対応

（注） 現在、Mellanox ConnectX-3（CX3）vNIC は MLX4 ドライバを使用し、ConnectX-4 vNIC（CX4）は MLX5 ドライバを使用しています。VM の展開に Azure が使用する必要のある NIC（MLX4 または MLX5）は指定できません。

Cisco IOS XE 17.4.1 リリースでは、CX3 ドライバと CX4 ドライバの両方に Azure DPDK のフェールセーフ、TAP、MLX IOD モデルのサポートが追加されました。Cisco IOS XE 17.8.1 リリースから、DPDK のフェールセーフ、TAP、MLX I/O モデルは、DPDK NETVSC PMD I/O モデルに置き換えられました。この更新により、高速化されたネットワーク機能を使用する際のオーバーヘッドが軽減されます。

（注） スループットライセンスのパフォーマンスを有効にするには、高速ネットワーク機能を有効にする必要があります。

- 高速ネットワークの有効化 （31 ページ）
- 高速ネットワークの無効化 （32 ページ）
- 高速ネットワークの確認 （33 ページ）

高速ネットワークの有効化

Cisco Catalyst 8000V インスタンスで高速ネットワークを有効にするには、`router# show platform software system hypervisor` コマンドを実行します。

```
Router#show platform software system hypervisor
Hypervisor: AZURE
Manufacturer: Microsoft Corporation
Product Name: Virtual Machine
Serial Number: 0000-0016-9163-0690-4834-7207-16
UUID: 80cbc2ea-29e6-cc43-93e9-f541876836f2
Image Variant: None

Cloud Metadata
-------------------
Region: eastus
Zone:
Instance ID: eac2cb80-e629-43cc-93e9-f541876836f2
Instance Type: Standard_DS4_v2
Version:
Image ID:
Publisher:
Offer:
SKU:

Interface Info
-------------------
Interface Number : 0
IPv4 Public IP: 192.168.61.135
IPv4 Private IP: 10.0.0.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.0.3
IPv4 Gateway: 10.0.0.1
MAC Address: 000D3A103B48

Interface Number : 1
IPv4 Public IP:
IPv4 Private IP: 10.0.1.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.1.3
IPv4 Gateway: 10.0.0.1
MAC Address: 000D3A103348

Interface Number : 2
IPv4 Public IP:
IPv4 Private IP: 10.0.4.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.2.3
IPv4 Gateway: 10.0.0.1
MAC Address: 00224827BA0F

Interface Number : 3
IPv4 Public IP:
IPv4 Private IP: 10.0.3.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.3.3
IPv4 Gateway: 10.0.0.1
MAC Address: 00224827B2A6

Interface Number : 4
IPv4 Public IP:
```

```
IPv4 Private IP: 10.0.4.4
IPv4 Subnet Mask: 255.255.0.0
IPv4 Network: 192.168.4.3
IPv4 Gateway: 10.0.0.1
MAC Address: 00224827B5CB
```

注意 Microsoft Azure の制限により、Cisco Catalyst 8000V ルータのすべてのインターフェイスで高速ネットワークを有効にすると、1500 バイトを超えるパケットが Azure インフラストラクチャ全体で送信された場合、パフォーマンスが大幅に低下する可能性があります。Azure は 1438 バイトでパケットのフラグメント化を開始しシーケンスのパケットがドロップするため、パフォーマンスの低下が発生します。これは既知の問題であり、現在 Microsoft でサポートケースが開かれています。

高速ネットワークを有効にするには、**az network nic** コマンドと `--accelerated-networking` オプションを使用して vNIC を作成または変更します。az network nic コマンドに関する Microsoft Azure のドキュメントを参照し、次の例も参照してください。

（注） Cisco Catalyst 8000V インスタンスの作成方法によっては、Cisco Catalyst 8000V NIC で高速ネットワークが最初に無効になっている場合があります。NIC で高速ネットワークが無効になっていて、インターフェイスで高速ネットワークを有効にする場合は、次の例に示すコマンドのいずれかを使用します。

例 1

この例は、**az network nic create** コマンドと `--accelerated-networking true` オプションを使用して vNIC の「mynic1」を作成し高速ネットワークを有効にする方法を示しています。

```
az network nic create -n mynic1 -g "RG1" --accelerated-networking true -l "east us"
--vnet-name "vnetname" --subnet "subnet1"
```

例 2

この例は、**az network nic create** コマンドと `--accelerated-networking true` オプションを使用して vNIC の「mynic2」を作成し高速ネットワークを有効にする方法を示しています。

```
az network nic create -n "mynic2" -g "RG1" --accelerated-networking true -l "east us"
--vnet-name "vnetname" --subnet "subnet1"
```

例 3

この例は、**az network nic update** コマンドと `--accelerated-networking true` オプションを使用して vNIC の「mynic3」を変更し高速ネットワークを有効にする方法を示しています。

```
az network nic update -n mynic3 -g rg1 --accelerated-networking true
```

高速ネットワークの無効化

Cisco Catalyst 8000V の高速ネットワークを無効にするには、**az network nic** コマンドと `--accelerated-networking` オプションを使用して vNIC を作成または変更します。

コマンドの詳細については、az network nic コマンドに関する Microsoft Azure のドキュメントを参照してください。

例

この例は、**az network nic update** コマンドと `--accelerated-networking false` オプションを使用して、vNIC の 「mynic1」 を変更して高速ネットワークを無効にする方法を示しています。

```
az network nic update -n "mynic1" -g rg1 --accelerated-networking false
```

高速ネットワークの確認

NIC で高速ネットワークを有効にした後、次の IOS コマンドを使用して、NIC で高速ネットワークが有効になっているかどうかを確認します。Azure インフラストラクチャは、Mellanox NIC を使用して SR-IOV または高速ネットワークを実現します。

次のコマンドを使用して、パケットを処理するための NIC の I/O ドライバとして Mellanox カーネルドライバを使用することにより、Cisco Catalyst 8000V NIC を確認できます。さらに、Azure インフラストラクチャの HyperV サーバーにある Mellanox NIC は、結合インターフェイスを Cisco Catalyst 8000V のゲスト VM に提供します。この VM は高速ネットワークに使用され、高速ネットワークが有効になっているときは常に結合された状態になっています。

Cisco Catalyst 8000V 17.4.x の高速ネットワークの確認（Azure-PMD を使用）

NIC で高速ネットワークを有効にした後、次の IOS コマンドを使用して、Azure-PMD を使用した高速ネットワークが NIC で有効になっているかどうかを確認します。Azure インフラストラクチャは、Mellanox NIC を使用して SR-IOV または高速ネットワークを実現します。

次のコマンドを使用して、パケットを処理するための NIC の I/O ドライバとして Mellanox Azure-PMD ドライバを使用することで、Cisco Catalyst 8000V NIC を確認します。さらに、Azure インフラストラクチャの HyperV サーバーにある Mellanox NIC は、結合インターフェイスを Cisco Catalyst 8000V のゲスト VM に提供します。この VM は高速ネットワークに使用され、高速ネットワークが有効になっている間、VM は結合された状態になります。結合インターフェイスは同じ MAC アドレスを共有することに注意してください。集約カウンタは Gi インターフェイスに表示され、非高速パケットカウンタは net_tap インターフェイスに表示されます。高速パケットカウンタは、net_mlx インターフェイスに表示されます。

次の例では、インターフェイス Gi2 が、パケットの大部分が net_mlx インターフェイス上を流れていることを示しています。

```
Router#show platform hard qfp act dat pmd controllers | inc NIC|good_packets
NIC extended stats for port 0  (Gi1) net_failsafe 000d.3a8f.1bf1 xstats count 13
  rx_good_packets: 411
  tx_good_packets: 326
NIC extended stats for port 1  (Bonded) net_mlx5 000d.3a8f.1bf1 xstats count 35
  rx_good_packets: 389
  tx_good_packets: 326
NIC extended stats for port 2  (Bonded) net_tap 000d.3a8f.1bf1 xstats count 13
  rx_good_packets: 22
  tx_good_packets: 0
NIC extended stats for port 3  (Gi2) net_failsafe 000d.3a8f.1040 xstats count 13
  rx_good_packets: 10638289
  tx_good_packets: 3634525
```

```
NIC extended stats for port 4  (Bonded) net_mlx5 000d.3a8f.1040 xstats count 35
  rx_good_packets: 10639534.  ==>>> This verifies Accelerated Networking is working
properly for RX
  tx_good_packets: 3636099     ==>>> This verifies Accelerated Networking is working
properly for TX
NIC extended stats for port 5  (Bonded) net_tap 000d.3a8f.1040 xstats count 13
  rx_good_packets: 291
  tx_good_packets: 0
NIC extended stats for port 6  (Gi3) net_failsafe 000d.3a8f.1a90 xstats count 13
  rx_good_packets: 3637187
  tx_good_packets: 10522981
NIC extended stats for port 7  (Bonded) net_mlx5 000d.3a8f.1a90 xstats count 35
  rx_good_packets: 3638631
  tx_good_packets: 10524554
NIC extended stats for port 8  (Bonded) net_tap 000d.3a8f.1a90 xstats count 13
  rx_good_packets: 28
  tx_good_packets: 0
```

Cisco Catalyst 8000V 17.8.x の高速ネットワークの確認（Azure PMD を使用）

Cisco IOS XE 17.8.1 リリースから、以前の DPDK のフェールセーフ、TAP、MLX I/O モデルは、DPDK NETVSC PMD I/O モデルに置き換えられました。次のコマンドを使用して、Cisco IOS XE リリース 17.8.x で実行されている Cisco Catalyst 8000V で高速ネットワーク機能を確認します。

show platform hardware qfp act dat pmd controllers コマンドは、net_netvsc ポートに結合されたデバイスを表示します。

```
Router#show platform hardware qfp active datapath pmd controllers | inc NIC |good_packets
NIC extended stats for port 0 (Gi2) net_netvsc 000d.3a10.3348 xstats count 56
rx_good_packets: 411
tx_good_packets: 350
tx_q0_good_packets: 311
rx_q0_good_packets: 100
vf_rx_good_packets: 487
vf_tx_good_packets: 350
NIC extended stats for port 1 (Gi1) net_netvsc 000d.3a10.3b48 xstats count 56
rx_good_packets: 60359
tx_good_packets: 55464
tx_q0_good_packets: 6579
rx_q0_good_packets: 5633
vf_rx_good_packets: 53780  ==>>> This verifies Accelerated Networking is working properly
 for RX
vf_tx_good_packets: 49831  ==>>> This verifies Accelerated Networking is working properly
 for TX
NIC extended stats for port 2 (Gi4) net_netvsc 0022.4827.b2a6 xstats count 56
rx_good_packets: 0
tx_good_packets: 0
tx_q0_good_packets: 0
rx_q0_good_packets: 0
vf_rx_good_packets: 0
vf_tx_good_packets: 0
NIC extended stats for port 3 (Gi5) net_netvsc 0022.4827.b5cb xstats count 56
rx_good_packets: 0
tx_good_packets: 0
tx_q0_good_packets: 0
rx_q0_good_packets: 0
vf_rx_good_packets: 0
vf_tx_good_packets: 0
NIC extended stats for port 4 (Gi3) net_netvsc 0022.4827.ba0f xstats count 56
rx_good_packets: 0
tx_good_packets: 0
```

```
tx_q0_good_packets: 0
rx_q0_good_packets: 0
vf_rx_good_packets: 0
vf_tx_good_packets: 0
NIC extended stats for port 5 (Bonded) net_mlx4 0022.4827.b2a6 xstats count 13
rx_good_packets: 0
tx_good_packets: 0
NIC extended stats for port 6 (Bonded) net_mlx4 0022.4827.b5cb xstats count 13
rx_good_packets: 0
tx_good_packets: 0
NIC extended stats for port 7 (Bonded) net_mlx4 000d.3a10.3b48 xstats count 13
rx_good_packets: 54726
tx_good_packets: 65464
NIC extended stats for port 8 (Bonded) net_mlx4 0022.4827.ba0f xstats count 13
rx_good_packets: 363863
tx_good_packets: 105245
NIC extended stats for port 9 (Bonded) net_mlx4 000d.3a10.3348 xstats count 13
rx_good_packets: 0
tx_good_packets: 0
```

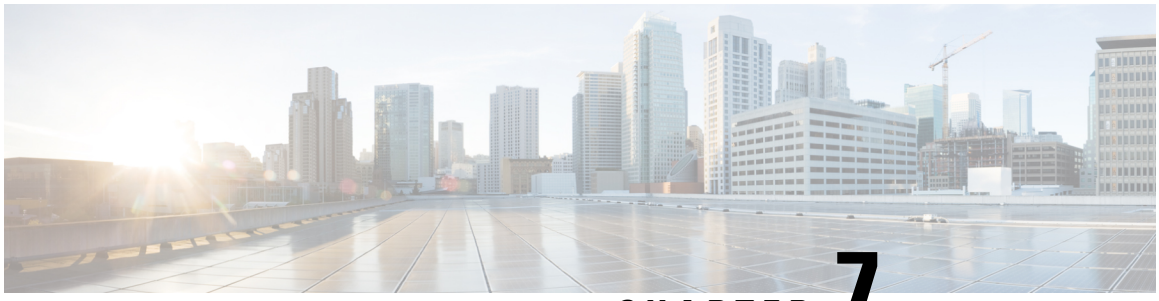
show platform software vnic-if interface-mapping コマンドは、net_netvsc ドライバが Cisco IOS XE 17.8.1 リリースから使用されていることを示します。

```
show platform software vnic-if interface-mapping
------------------------------------------------------------
 Interface Name        Driver Name         Mac Addr
------------------------------------------------------------
 GigabitEthernet3       net_netvsc         000d.3a4e.7542
 GigabitEthernet2       net_netvsc         000d.3a4e.7163
 GigabitEthernet1       net_netvsc         000d.3a4e.757d
------------------------------------------------------------
```

show platform software vnic database コマンドは、MLX4 または MLX5 が存在するかどうかを示し、使用されている PMD も示します。

```
show platform software vnic-if database
vNIC Database
  eth00_1572882209232255500
    Device Name : eth0
    Driver Name : mlx5_pci
    MAC Address : 000d.3a4e.757d
    PCI DBDF    : b421:00:02.0
    Server      : IFDEV_SERVER_KERN
    Management  : no
    Status      : bonded
  eth01_1572882212261074300
    Device Name : eth1
    Driver Name : mlx5_pci
    MAC Address : 000d.3a4e.7542
    PCI DBDF    : 83e2:00:02.0
    Server      : IFDEV_SERVER_KERN
    Management  : no
    Status      : bonded
  eth02_1572882215293497600
    Device Name : eth2
    Driver Name : mlx5_pci
    MAC Address : 000d.3a4e.7163
    PCI DBDF    : be1d:00:02.0
    Server      : IFDEV_SERVER_KERN
    Management  : no
    Status      : bonded
  eth_15__1572882218326526600
    Device Name : Gi1
    Driver Name : hv_netvsc
```

```
  MAC Address : 000d.3a4e.757d
  PCI DBDF    : 000d3a1f-26f8-000d-3a1f-26f8000d3a1f
  Server      : IFDEV_SERVER_UIO
  Management  : no
  Status      : supported
eth_16__1572882223436559900
  Device Name : Gi2
  Driver Name : hv_netvsc
  MAC Address : 000d.3a4e.7163
  PCI DBDF    : 000d3a1f-26f8-000d-3a1f-26f8000d3a1f
  Server      : IFDEV_SERVER_UIO
  Management  : no
  Status      : supported
eth_17__1572882228553741500
  Device Name : Gi3
  Driver Name : hv_netvsc
  MAC Address : 000d.3a4e.7542
  PCI DBDF    : 000d3a1f-26f8-000d-3a1f-26f8000d3a1f
  Server      : IFDEV_SERVER_UIO
  Management  : no
  Status      : supported
```



CHAPTER 7

Azure トランジット VNET DMVPN ソリューションの展開

トランジット VNet ソリューションを展開するための前提条件

- Cisco Catalyst 8000V インスタンスの Azure アカウントが必要です。
- ライセンスが登録され、有効であることを確認してください。
- スポークを設定する前に、ハブが稼働していることを確認してください。

トランジット VNet ソリューションの展開に関する制約事項

- スポーク VNet を別のクラウド サービス プロバイダーに展開することはできません。
- すべての場所にトランジット VNet ソリューションを設定することはできません。サポートされている場所のリストを表示するには、インスタンスを作成した後、[Configure Basic Settings] ページの [Location] フィールドのすべてのオプションを確認します。

Azure トランジット VNET DMVPN を展開する方法

トランジット VNet ハブの作成

この手順は、トランジット VNet ソリューションを設定する最初の手順です。これは、トランジット VNet の設定を行う必要がある展開において、非常に重要な部分です。これらの設定は、アクセスキーを使用してトランジット VNet ストレージのアカウントにメタデータとして保存される DMVPN IPsec パラメータに対応しています。スポークのテンプレートを設定するときは、TVNET ストレージのアカウントとアクセスキーのみを設定する必要があります。スポークに必要な関連する DMVPN IPsec パラメータは、デバイスから自動的に選択されます。

ステップ 1 Microsoft Azure ポータルにサインインします。

ステップ 2 [Create a Resource] をクリックし、Cisco Catalyst 8000V の展開を検索して、[Enter] を押します。システムは、DMVPN のトランジット VNET テンプレートを検索して表示します。

ステップ 3 [Transit VNET DMVPN] > [Create] を選択します。

ステップ 4 [Basics] 画面で、仮想マシンの名前、トランジット VNet ハブの名前、およびユーザー名を入力します。

Note [Transit VNet Name] には小文字のみを使用してください。

ステップ 5 [Authentication Type] ドロップダウンリストから、[SSH Public Key] を選択します。

ステップ 6 パスワードを指定し、確認用にパスワードを再入力します。

ステップ 7 [SKU] ドロップダウンリストから、適切なイメージバージョンを選択します。

ステップ 8 [Location] ドロップダウンリストから、TVNET ハブを展開できるリージョンの 1 つを選択します。

ステップ 9 Cisco C8000V の設定ページで、設定を行います。Cisco Catalyst 8000V の設定の詳細については、「*Deploying the Cisco Catalyst 8000V on Microsoft Azure*」セクションを参照してください。

ステップ 10 トランジット VNet の設定で、次の設定を行います。

a) [TVNET Storage Account] はキーワード「strg」が追加されたトランジット VNet 名に由来するストレージアカウント名です。スポークの作成時にこの値が必要です。このフィールドの値は自動入力されます。ただし、このフィールドの値は編集できます。

b) [Private TVNET Storage Account] でキーの保存に必要なストレージアカウントを選択します。このフィールドは、オートスケーラーの展開に必要です。

c) [DMVPN Tunnel ID] はすべての Cisco Catalyst 8000V デバイス（ハブとスポークの両方）でトンネルを設定するために使用されるトンネルの ID です。

d) [DMVPN Tunnel Key] は 6 ～ 8 桁の数値のトンネルキーです。

e) [IPSEC Tunnel Authentication]

f) **[IPSEC Tunnel Cipher]**

g) [IPSEC Shared Key] はトンネルを認証するためのキーワードです。

h) [DMVPN Tunnel Network] は DMVPN のオーバーレイに使用されるトンネルネットワークです。

Note デフォルトのオプションは、ハブ用に作成された VNet とクラッシュする可能性があります。この値が既存の仮想ネットワーク（VNet）と重複しないようにしてください。

この時点では、[Configure Subnets] セクションでサブネットを設定する必要はありません。

ステップ 11 [Summary] 画面でパラメータを確認し、[OK] をクリックします。

ステップ 12 [Buy] セクションで [Create] をクリックして、トランジット VNet ハブソリューションを展開します。この手順により、次のリソースが作成されます。

- 1 つの可用性セットに展開された 2 つの Cisco Catalyst 8000V インスタンス（C8000V1 および C8000V2）仮想マシン
- 2 つのストレージディスク（Cisco Catalyst 8000V ごとに 1 つ）
- 4 つの NIC（Cisco Catalyst 8000V インスタンスごとに 2 つの NIC）
- トランジット VNET 全体に 1 つのセキュリティグループ（インバウンド用に SSH のみを開きます）
- 2 つのパブリック IP（インスタンスごとに 1 つの PIP）
- 2 つのルートテーブル（インスタンスのサブネットごとに 1 つの RT）
- 2 つのストレージアカウント（Cisco Catalyst 8000V 診断用の 1 つのストレージとトランジット VNET メタデータ用の 1 つのストレージ）
- 1 つの VNET /16 CIDR
- 1 つの Resource-Manager グループを使用して展開された上記すべて（この RG を削除すると、上記のすべてのコンポーネントが削除されます）

展開が完了し、リソースが作成されるまでに数分かかります。[All Resources] をクリックし、[Group By Type] オプションを選択することで、展開をモニタリングできます。展開が完了すると、[notification] パネルに「Deployment Succeeded」というメッセージが表示されます。

Azure DMVPN スポーク VNET の作成

Before you begin

トランジット VNet ソリューションのスポークを作成する前に、ハブが正常に作成されていることを確認してください。

ステップ 1 Microsoft Azure Marketplace から、[Cisco CSR 1000V DMVPN Transit VNet] テンプレートを検索して選択します。

ステップ 2 テンプレートをクリックし、ドロップダウンリストから必要となる適切なスポークオプションを選択します。

ステップ 3 [Create] をクリックします。

ステップ 4 [Basics settings] 画面で、次の設定の詳細を指定していることを確認します。

a) [Filename] でこのフィールドにトランジット VNet の名前を指定します。
b) [Transit VNet Storage Name] は、ハブ構成の TVNET ストレージアカウントの値と同じです。この名前は、キーワード「strg」が追加されたトランジット VNet 名に由来します。
c) [Storage Key] にアクセスするには、[public Hub] を検索してクリックし、[Access Key] オプションをクリックします。

ステップ 5 [Basics Settings] 画面で他の値を設定し、[OK] をクリックします。

ステップ 6 Cisco Catalyst 8000V の設定画面で、フィールドを設定するか、そのままにするか（デフォルト値）を選択できます。

パラメータの詳細については、「*How to Deploy a Cisco Catalyst 8000V on Microsoft Azure*」を参照してください。

Note 可用性ゾーンは、Microsoft Azure のすべてのリージョンでまだ完全にはサポートされていません。したがって、ソリューションテンプレートには可用性ゾーンのオプションはありませんが、「Availability-Sets」を使用して復元力が考慮されています。詳細については、Microsoft Azure のドキュメント（https://docs.microsoft.com/en-us/azure/availability-zones/az-overview）を参照してください。

ステップ 7 [Virtual Network] の横にある矢印をクリックして仮想ネットワークの値を指定し、[OK] をクリックします。

ステップ 8 [Address Space] フィールドに、Classless Inter-Domain Routing（CIDR）表記を使用して、仮想ネットワークのアドレスを入力します。

Note VNET CIDR は、TVNET-HUB の Cisco Catalyst 8000V デバイスに使用される物理 IP アドレスのサブネットを示します。CIDR ブロックは通常、2 つの /24 サブネットにさらにサブネット化される /16 サブネットです。各サブネットの最初の 3 つの IP アドレスは、Azure ルートテーブルおよびその他のサービス用に予約されます。IP 割り当てはサブネットの 4 番目の IP から始まり、動的に割り当てられるパブリック IP に自動的にマッピングされます。パブリック IP はインターネットへのアクセスを可能にするため、DMVPN シナリオの NBMA アドレスになります。

ステップ 9 [Configure the Subnets] の横にある矢印をクリックし、[OK] をクリックします。

ステップ 10 [Summary] 画面で、設定されたパラメータを確認します。テンプレートを検証したら、[OK] をクリックします。

ステップ 11 [Create] をクリックして、TVNet スポークソリューションを展開します。

Note 作成する追加のスポークごとに、手順 1 ～ 10 に従います。

設定の確認

トランジット VNET ハブでの確認

次のコマンドは、スポークがトランジット VNet Hub1 への DMVPN トンネルを正常に確立し、EIGRP ルートを Transit VNet Hub1 と交換できることを示しています。このソリューションにより、DMVPN フェーズ 3 の機能である NHRP ショートカットスイッチングが有効になります。これらのコマンドを Transit VNet Hub2 で実行すると、コマンド出力は Transit VNet Hub1 と同様になります。これは、スポークが両方のトランジット VNet ハブの Cisco Catalyst 8000V への DMVPN トンネルを正常に確立し、EIGRP ルートを両方のハブと正常に交換したことを示しています。ハブは、復元力を高めるためにアクティブ-アクティブモードで展開されます。

ステップ 1 `show ip interface brief` コマンドを実行します。

Example:

```
Transit-Hub# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.1.0.4        YES DHCP   up                    up
GigabitEthernet2       10.1.1.5        YES DHCP   up                    up
Tunnel11               172.16.1.1      YES TFTP   up                    up
VirtualPortGroup0      192.168.35.1    YES TFTP   up                    up
p1-tvnet-csr-1#
```

設定出力の強調表示されている部分に注目してください。これは、トンネルが稼働していることを示しています。システムがこの設定出力にトンネルを表示しない場合は、ゲストシェルに移動して TVNet のログを確認する必要があります。`show log` コマンドを実行して、TVNet のログにアクセスします。

ステップ 2 スポークからの 2 つの DMVPN 接続の IKE セッションを表示するには、`show crypto isakmp sa` コマンドを実行します。

Example:

```
Transit-Hub# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.1.0.4        168.62.164.228  QM_IDLE           1042 ACTIVE
10.1.0.4        40.114.69.24    QM_IDLE           1043 ACTIVE
IPv6 Crypto ISAKMP SA
```

ステップ 3 スポークからの 2 つの DMVPN 接続の IPsec セッションを表示するには、`show crypto session` コマンドを実行します。

Example:

```
Transit-Hub# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
```

```
Peer: 40.114.69.24 port 4500 fvrf: (none) ivrf: tvnet-Tun-11
      Phase1_id: 12.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 10.1.0.4/4500 remote 40.114.69.24/4500 Active
          Capabilities:DN connid:1043 lifetime:18:32:04
  IPSEC FLOW: permit 47 host 10.1.0.4 host 40.114.69.24
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 32 drop 0 life (KB/Sec) 4607996/3474
        Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4607998/3474
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 168.62.164.228 port 4500 fvrf: (none) ivrf: tvnet-Tun-11
      Phase1_id: 11.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 10.1.0.4/4500 remote 168.62.164.228/4500 Active
          Capabilities:DN connid:1042 lifetime:18:02:01
  IPSEC FLOW: permit 47 host 10.1.0.4 host 168.62.164.228
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 32 drop 0 life (KB/Sec) 4607970/2427
        Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4607982/2427
```

ステップ 4 `show dmvpn` コマンドを実行して、デバイスの DMVPN のステータスを表示します。

Example:

```
Transit-Hub# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel11, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 40.114.69.24       172.16.1.137    UP     1w3d    DN
     1 168.62.164.228     172.16.1.147    UP     1w3d    DN
```

ステップ 5 `show vrf` コマンドを実行して、トランジット VNet 上の各スポークからの表示ルートを表示します。

Example:

```
Transit-Hub# show vrf
  Name                             Default RD            Protocols   Interfaces
  tvnet-Tun-11                     64512:11              ipv4        Tu11
```

ステップ 6 `show ip eigrp vrf <vrf-name> neighbors` コマンドを実行して、EIGRP ネイバーのステータスを表示します。

Example:

```
Transit-Hub# show ip eigrp vrf tvnet-Tun-11 neighbors
EIGRP-IPv4 Neighbors for AS(64512) VRF(tvnet-Tun-11)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
```

```
1   172.16.1.137            Tu11                     14 1w3d       13  1398  0  12
0   172.16.1.147            Tu11                     10 1w3d       12  1398  0  12
```

ステップ 7 `show ip route vrf <vrf-name>VRF` コマンドを実行して VRF に固有のルートを表示します。

Example:

```
Transit-Hub# show ip route vrf tvnet-Tun-11
Routing Table: tvnet-Tun-11
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
      11.0.0.0/24 is subnetted, 2 subnets
D EX     11.1.0.0 [170/26880256] via 172.16.1.147, 1w1d, Tunnel11
D EX     11.1.1.0 [170/26880256] via 172.16.1.147, 1w1d, Tunnel11
      12.0.0.0/24 is subnetted, 2 subnets
D EX     12.1.0.0 [170/26880256] via 172.16.1.137, 1w1d, Tunnel11
D EX     12.1.1.0 [170/26880256] via 172.16.1.137, 1w1d, Tunnel11
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Tunnel11
L        172.16.1.1/32 is directly connected, Tunnel11
D EX  192.168.35.0/24 [170/26905600] via 172.16.1.147, 1w1d, Tunnel11
                      [170/26905600] via 172.16.1.137, 1w1d, Tunnel11
```

スポークとハブ間の接続の確認

次のコマンドは、スポークが両方の Cisco Catalyst 8000V TVNET ハブに接続されていて、両方のハブからの EIGRP ルートを交換できることを示しています。DMVPN ソリューションは DMVPN-Phase3（NHRP ショートカットスイッチング）として展開され、ハブはアクティブ-アクティブモードで展開されるため、スポーク 2 への EIGRP ルートはスポーク 2 のトンネルオーバーレイ IP アドレスを指します。

ステップ 1 `show ip interface brief` コマンドを実行して、デバイスのインターフェイスの IP アドレスを表示します。

Example:

```
Spoke# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       11.1.0.4        YES DHCP   up                    up
GigabitEthernet2       11.1.1.4        YES DHCP   up                    up
Tunnel11               172.16.1.147    YES TFTP   up                    up
VirtualPortGroup0      192.168.35.1    YES TFTP   up                    up
```

ステップ 2 `show dmvpn` コマンドを実行して、デバイスの DMVPN のステータスを確認します。

Example:

```
Spoke# show dmvpn
```

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================
Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 40.117.131.133       172.16.1.1    UP     1w3d     S
     1 40.117.128.85        172.16.1.2    UP     1w3d     S
```

強調表示されている設定出力に注目してください。これは、スポークが作動していて、ハブとの接続が確立されていることを示しています。

ステップ 3 スポークからの 2 つの DMVPN 接続の IKE セッションを表示するには、`show crypto isakmp sa` コマンドを実行します。

Example:

```
Spoke# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
40.117.131.133  11.1.0.4        QM_IDLE           1025 ACTIVE
40.117.128.85   11.1.0.4        QM_IDLE           1026 ACTIVE
IPv6 Crypto ISAKMP SA
```

ステップ 4 スポークからの 2 つの DMVPN 接続の IPsec セッションを表示するには、`show crypto session` コマンドを実行します。

Example:

```
Spoke# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.131.133 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.131.133/4500 Active
          Capabilities:DN connid:1025 lifetime:17:33:41
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.131.133
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 2250 drop 0 life (KB/Sec) 4607927/726
        Outbound: #pkts enc'ed 2251 drop 0 life (KB/Sec) 4607957/726
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.128.85 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.5
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.128.85/4500 Active
```

```
        Capabilities:DN connid:1026 lifetime:17:33:44
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.128.85
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 2252 drop 0 life (KB/Sec) 4607960/2046
        Outbound: #pkts enc'ed 2253 drop 0 life (KB/Sec) 4607976/2046
```

ステップ 5 EIGRP ネイバーのステータスを表示するには、`show up eigrp neighbor` コマンドを実行します。

Example:

```
Spoke# show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(64512)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   172.16.1.2              Tu11                     13 1w3d       24  1362  0  23
0   172.16.1.1              Tu11                     12 1w3d        8  1362  0  23
```

ステップ 6 EIGRP ルート情報を表示するには、show ip route eigrp コマンドを実行します。

Example:

```
Spoke# show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 11.1.0.1 to network 0.0.0.0
      12.0.0.0/24 is subnetted, 2 subnets
D EX     12.1.0.0 [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
                  [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
D EX     12.1.1.0 [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
                  [170/28160256] via 172.16.1.137, 1w3d, Tunnel11
```

スポーク間の接続の確認

次のコマンドは、2 つのスポーク間の接続をテストするのに役立ちます。サポートされる機能は DMVPN フェーズ 3 であるため、**traceroute** コマンドはスポーク 1 からスポーク 2 に送信されたパケットを表示します。ただし、スポーク 1 がパケットをハブに送信してスポーク 2 のアドレスを取得するため、NHRP 解決のために最初のパケットが失われます。スポーク 1 がアドレスを受信すると、スポーク 1 とスポーク 2 の間に動的 IPsec トンネルが確立されます。

```
Spoke1# clear crypto sa counters
Spoke1# ping 12.1.1.4 source gigabitEthernet 2 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 12.1.1.4, timeout is 2 seconds:
Packet sent with a source address of 11.1.1.4
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 1/1/6 ms
Spoke# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
```

```
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel11, IPv4 NHRP Details
Type:Spoke, NHRP Peers:3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 40.117.131.133       172.16.1.1    UP     1w3d     S
     1 40.117.128.85        172.16.1.2    UP     1w3d     S
     1 40.114.69.24       172.16.1.137    UP 00:00:07    DN
Spoke# traceroute 12.1.1.4 source gigabitEthernet 2
Type escape sequence to abort.
Tracing the route to 12.1.1.4
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.137 2 msec *  3 msec
p1spoke1#
p1spoke1#
p1spoke1#sh crypto sess detail | i pkts
        Inbound:  #pkts dec'ed 101 drop 0 life (KB/Sec) 4607985/3581
        Outbound: #pkts enc'ed 100 drop 0 life (KB/Sec) 4607989/3581
        Inbound:  #pkts dec'ed 12 drop 0 life (KB/Sec) 4607924/621
        Outbound: #pkts enc'ed 14 drop 0 life (KB/Sec) 4607955/621
        Inbound:  #pkts dec'ed 13 drop 0 life (KB/Sec) 4607957/1941
        Outbound: #pkts enc'ed 13 drop 0 life (KB/Sec) 4607975/1941
Spoke# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
Interface: Tunnel11
Uptime: 00:00:36
Session status: UP-ACTIVE
Peer: 40.114.69.24 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 12.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.114.69.24/4500 Active
          Capabilities:DN connid:1027 lifetime:23:59:23
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.114.69.24
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 101 drop 0 life (KB/Sec) 4607985/3563
        Outbound: #pkts enc'ed 100 drop 0 life (KB/Sec) 4607989/3563
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.131.133 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.4
      Desc: (none)
  Session ID: 0
  IKEv1 SA: local 11.1.0.4/4500 remote 40.117.131.133/4500 Active
          Capabilities:DN connid:1025 lifetime:17:31:38
  IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.131.133
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 16 drop 0 life (KB/Sec) 4607923/603
        Outbound: #pkts enc'ed 18 drop 0 life (KB/Sec) 4607955/603
Interface: Tunnel11
Uptime: 1w3d
Session status: UP-ACTIVE
Peer: 40.117.128.85 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.1.0.5
      Desc: (none)
  Session ID: 0
```

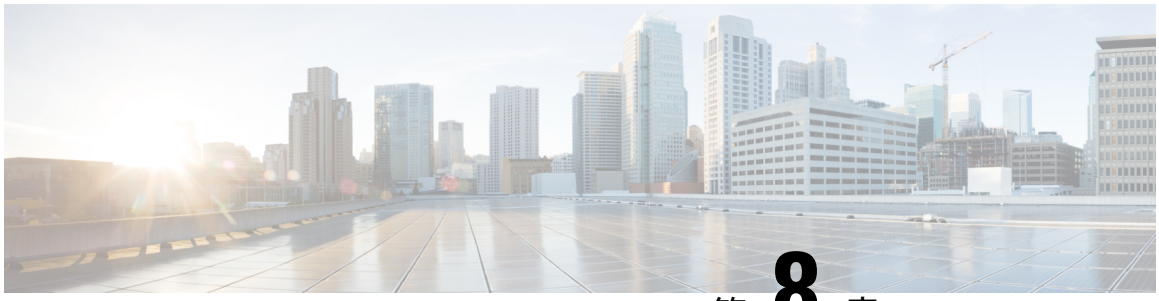
```
IKEv1 SA: local 11.1.0.4/4500 remote 40.117.128.85/4500 Active
        Capabilities:DN connid:1026 lifetime:17:31:41
IPSEC FLOW: permit 47 host 11.1.0.4 host 40.117.128.85
      Active SAs: 2, origin: crypto map
      Inbound:  #pkts dec'ed 17 drop 0 life (KB/Sec) 4607957/1923
      Outbound: #pkts enc'ed 17 drop 0 life (KB/Sec) 4607975/1923
```

トラブルシューティング

展開のステータスを表示するには、Cisco Catalyst 8000V インスタンスにログインして `show log` コマンドを実行します。展開が成功すると、「[AzureTransitVNET] Success.Configured all the required IOS configs」というメッセージが表示されます。

トランジット VNet ソリューションの設定中にこのメッセージが表示されず、エラーが発生した場合は、次のことを確認してください。

- DMVPN トンネルがハブとスポークの間に確立されているか確認します。ほとんどの場合、次の値に問題がある可能性があります。TransitVNETname、TransitVNETStoragename、または TransitVNETStoragekey。
- Guestshell が、インストールされる TVNet パッケージ用に立ち上がり、稼働しているか確認します。



第 8 章

LISP レイヤ 2 拡張の設定

Cisco Catalyst 8000V インスタンスは、パブリッククラウド、プライベートクラウド、およびハイブリッドクラウドに展開できます。企業がハイブリッドクラウドに移行する場合、サーバーに対して一切変更を加えずに、サーバーをクラウドに移行する必要があります。企業はクラウド内で同じサーバー IP アドレス、サブネットマスク、デフォルトゲートウェイ設定、独自の IP アドレス方式を使用し、クラウドプロバイダーのインフラストラクチャのアドレス方式によって制限されないことを望む可能性があります。

この要件を満たすために LISP を使用できます。LISP は、場所（エンタープライズデータセンターまたはパブリッククラウド）と ID（サーバー IP アドレス）を分離できるアーキテクチャであり、同じ IP アドレスでクラウド上に新しいサーバーを作成できます。LISP アーキテクチャでは、サーバーのエンドポイント ID からルータロケータ（EID-to-RLOC）マッピングが更新され、クラウドに移動される新しい場所が反映されます。さらに、LISP が ID と場所の間のマッピングを処理するため、エンドシステム、ユーザー、またはサーバーに変更を加える必要はありません。

LISP はオーバーレイとして動作し、サーバーからの元のパケットを、追加の外部 IPv4 または IPv6 ヘッダーと共にユーザーデータグラムプロトコル（UDP）パケットにカプセル化します。このカプセル化により、送信元と宛先のルータロケータが保持され、サーバー管理者は、クラウドプロバイダーのアドレッシング構造に関係なく、独自の IP アドレス方式に従ってクラウド内のサーバーにアドレスを指定できます。

Microsoft Azure で実行されている Cisco Catalyst 8000V インスタンスでレイヤ 2 拡張を設定できます。インスタンスは、エンタープライズデータセンターとパブリッククラウドの間のブリッジとして機能します。レイヤ 2 拡張を設定すると、プライベートデータセンター内のレイヤ 2 ネットワークをパブリッククラウドに拡張して、サイトとパブリッククラウド間でのホストの到達可能性を実現できるようになります。また、データセンターとパブリッククラウド間のアプリケーションワークロードの移行を有効にすることもできます。

利点

- パブリック IP アドレスを地理的に異なる場所間で移動するか、異なるパブリッククラウド間で分割します。いずれの場合も、LISP IP モビリティソリューションは、場所に関係なく、インターネット上のクライアントと移動したパブリック IP アドレス間の最適なルーティングを提供します。Azure クラウドの IP モビリティの実現について詳しくは、「Achieving IP Mobility」をご覧ください。

- データ移行が容易になり、ネットワークのワークロード IP アドレスが最適化されます。通常、IP アドレスの変更により、ソリューションが複雑になり、さらに遅延が発生します。クラウド用の L2 拡張機能を使用することで、ネットワークの制約を受けることなく、元の IP アドレスを保持しながらワークロードを移行できます。このユースケースの詳細については、「Data Migration Use Case」を参照してください。
- プロバイダーサイトで VM を仮想的に追加し、VM がプロバイダーサイトで実行されている間に、クラウドバーストを活用して、仮想的に VM をエンタープライズサーバーに挿入できるようにします。
- 部分的な障害回復と障害回避のためのバックアップサービスを提供します。

LISP レイヤ 2 拡張の設定の前提条件

- L2 拡張を設定する前に、ソリューションのアンダーレイの準備ができていることを確認してください。
- クラウドは Address Resolution Protocol（ARP）をサポートしておらず、クラウドインフラストラクチャはリモートサイトのホストを認識していないため、仮想 IP を追加して、クラウドがパケットをエッジルータに適切にルーティングできるようにする必要があります。仮想 IP またはエイリアス IP を追加するには、「Add an IP address for an Azure interface」を参照してください。
- それぞれの Cisco Catalyst 8000V インスタンスは、1 つの外部 IP アドレスで設定されている必要があります。この場合、2 つの Cisco Catalyst 8000V インスタンスの IP アドレス間、または Cisco Catalyst 8000V インスタンスと ASR1000 デバイス間に IPsec トンネルが構築されます。IPsec トンネルにプライベートアドレスがあることを確認します。
- 2 つの Cisco Catalyst 8000V インスタンスの IP アドレス間、または Cisco Catalyst 8000V インスタンスと ASR1000 デバイス間で IPsec トンネルが機能していることを確認します。
- ソリューションに応じて、2 つの Cisco Catalyst 8000V インスタンス間、Cisco Catalyst 8000V と ASR1000 デバイス間、および VM とホスト間で ping が成功することを確認します。

LISP レイヤ 2 拡張の設定の制約事項

- ホストをデータセンターからクラウドに、またはその逆に移動する場合は、最初にクラウドの仮想 IP テーブルにセカンダリアドレスを追加または削除する必要があります。

- VM をクラウドに移動する場合は、VM がデータセンターからクラウドに追加されたことを Cisco Catalyst 8000V デバイスが認識できるように、Cisco Catalyst 8000V インスタンスへのパケットを開始する必要があります。
- 高可用性は、L2 拡張機能では機能しません。
- Azure は、最大 256 個の IP をサポートします。したがって、リモートサイトまたはデータセンターのホストの最大数は 256 です。

LISP レイヤ 2 拡張の設定方法

L2 拡張機能を設定するには、まず Microsoft Azure で Cisco Catalyst 8000V インスタンスを展開し、インスタンスを xTR として設定する必要があります。その後、展開を完了するためにマッピングシステムを設定する必要があります。

LISP サイトは、アップストリーム プロバイダーへの 2 系統の接続を持つ、ITR と ETR の両方として設定された（xTR とも呼ばれる）Cisco Catalyst 8000V インスタンスを使用します。次に LISP サイトは、ネットワークコアのマップリゾルバ/マップサーバー（MR/MS）として設定されたスタンドアロンデバイスに登録されます。マッピングシステムは、Azure 内で移行済みのパブリック IP に送信されるパケットの LISP カプセル化およびカプセル化解除を実行します。Azure からのトラフィックについては、必要に応じて（接続先へのルートが C8000V のルーティングテーブルで見つからない場合は常に）、Cisco Catalyst 8000V インスタンスがエンタープライズ データセンターの PxTR を介してルーティングします。

LISP マップサーバーおよびマップリゾルバをマッピングサービスに使用する際、LISP xETR 機能を設定して有効化するには、次の手順を実行します。

複数のインターフェイスを持つ Cisco Catalyst 8000V を展開する

複数のインターフェイスを持つ Cisco Catalyst 8000V を展開するには、次の手順を実行します。

ステップ 1 左側のパネルで [Virtual machines] を選択します。

ステップ 2 [Add]をクリックします。

ステップ 3 「C8000V」と入力します。

Azure Marketplace で Cisco Catalyst 8000V VM の展開を検索します。

ステップ 4 2、4、または 8 つの NIC を持つ展開を選択します。

ステップ 5 [Create] をクリックします。

ステップ 6 [Virtual Machine Name] で [Basics] サブメニューを選択し、仮想マシン名を入力します。

プライベートネットワークを表すために Microsoft Azure が使用するクラウドベースのネットワークの名前です。

ステップ 7 [Username] でユーザー名を選択します。

Cisco Catalyst 8000V インスタンスへのログインに使用できる Cisco Catalyst 8000V 仮想マシンのユーザー名です。

ステップ 8 [Authentication type] でパスワード（デフォルト）または SSH 公開キーを入力します。

ステップ 9 [Cisco IOS XE Image Version] で Cisco IOS XE バージョンを選択します。

ステップ 10 [Subscription] でサブスクリプション名を変更（任意）します。

仮想マシンの名前に基づいて、デフォルトのサブスクリプション名が提供されます。このデフォルトのサブスクリプション名は変更できます。

ステップ 11 [Resource Group] で [Create new] または [Use existing] を選択します。

Cisco Catalyst 8000V は、新しいリソースグループ（または完全に空の既存のリソースグループ）にのみ作成できます。リソースグループを削除するには、Cisco Catalyst 8000V VM を削除してから、リソースグループを削除します。

ステップ 12 [OK] をクリックします。

ステップ 13 [Cisco C8000V Settings] サブメニューを選択してから、[Number of Network Interfaces in C8000V] を選択します。

ステップ 14 インターフェイスの数を 2、4、または 8 から選択します。

ステップ 15 [License Type] でライセンスタイプとして [BYOL] または [PAYG] を選択します。

ステップ 16 [Managed Disk] で [Enabled] を選択します。

ステップ 17 [Storage Account] でストレージアカウントの名前を入力します。

ストレージアカウントの詳細については、このガイドの「Microsoft Azure Resources」セクションを参照してください。

ステップ 18 [Virtual machine size] で適切な仮想マシンのサイズを選択します。

使用しているインターフェイスの数に基づいて、適切な仮想マシンのサイズを選択します。Microsoft Azure は、期待されるパフォーマンスが異なるさまざまなイメージタイプをサポートしています。サポートされているインスタンスタイプと仮想マシンサイズを表示するには、次のリンクを参照してください。

- 「Dv2 and DSv2 series」
- 「Fsv2 series」

ステップ 19 [Custom Data] で、ブートストラップ設定ファイルを提供する場合は、[Yes] を選択します。

Cisco Catalyst 8000V インスタンスにブートストラップ設定ファイルを提供する方法の詳細については、「Deploying a Cisco Catalyst 8000V VM Using a Day 0 Bootstrap File」セクションおよび「Customdata-examples」セクションを参照してください。

ステップ 20 [Availability Set] で [Yes] を選択します。

ステップ 21 [Availability Set name] で可用性セットの名前を入力します。

ステップ 22 [Availability Set fault domain count] で可用性セットの障害ドメイン数を入力します。

障害ドメインは、共通の電源とネットワークスイッチを共有する VM のグループを定義します。可用性セットは、障害ドメイン全体に仮想マシンを配置します。

ステップ 23 [Availability Set update domain count] で可用性セットの更新ドメイン数を入力します。

更新ドメインは、同時に再起動できる VM と基礎となる物理ハードウェアのグループです。

ステップ 24 [Boot diagnostics] で起動診断を入力します。

起動診断の詳細については、「Information About Deploying Cisco Catalyst 8000V in Microsoft Azure」セクションを参照してください。

ステップ 25 [Diagnostics Storage account] でストレージアカウント名を入力します。

ステップ 26 [Public IP Address] でパブリック IP アドレス名を入力します。

パブリック IP アドレスの詳細については、「Microsoft Azure Resources」セクションを参照してください。

ステップ 27 [DNS label] で DNS ラベルの名前を変更（任意）します。

DNS ラベルは、Cisco Catalyst 8000Vに割り当てられるパブリック IP アドレスの名前です。DNS ラベルのデフォルト値がテキストボックスに表示されます。これは、VM 名の後に「`-dns`」が続きます。

ステップ 28 [Virtual network] で [Create New] または [Use existing] のいずれかを選択します。

新しい仮想ネットワークの場合、名前と IP アドレスを入力します。

ステップ 29 [Subnets] をクリックし、サブネット名と IP アドレスを入力します。

ステップ 30 すべての Cisco Catalyst 8000V 設定が許容範囲であることを確認し、[OK] をクリックします。

[3 Summary] サブメニューが強調表示されます。

ステップ 31 [OK] をクリックします。

[4 Buy] サブメニューが強調表示されます。

ステップ 32 [Create] をクリックします。

VM が作成され、購入が確定されます。

ステップ 33 左側のパネルで [Virtual machines] をクリックします。

数分後、最近作成された VM のステータスが [Creating] から [Running] に変わります。パブリック IP アドレス名をメモします。

AzureのCiscoCatalyst8000Vとエンタープライズシステムの CiscoCatalyst 8000V 間のトンネルの設定

エンタープライズデータセンター内に展開された Cisco Catalyst 8000V インスタンスとパブリッククラウド内に展開された Cisco Catalyst 8000V インスタンス間の通信は、両者の間に確立された IP セキュリティ（IPsec）トンネルによって保護されます。LISP カプセル化トラフィックは、パブリッククラウドと企業間のデータ発信元認証、完全性保護、アンチリプライ保護、および機密性を実現する IPsec トンネルで保護されます。

ステップ 1 Microsoft Azure で Cisco Catalyst 8000V インスタンスを設定します。

interface loopback コマンドを実行します。ループバックは、移行された顧客の IP スペースがどこにあるかを識別する LISP RLOC として使用されます。

interface Tunnel コマンドを実行して、クラウド上の Cisco Catalyst 8000V インスタンスに接続します。

```
interface Loopback1
 ip address 33.33.33.33 255.255.255.255
!
interface Tunnel2
 ip address 30.0.0.2 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 173.39.145.79
 tunnel protection ipsec profile p2p_pf1
!
interface GigabitEthernet2
 ip address 10.10.10.140 255.255.255.0
 negotiation auto
 lisp mobility subnet1 nbr-proxy-reply requests 3
 no mop enabled
 no mop sysid
!
```

ステップ 2 企業サイトで 2 番目の Cisco Catalyst 8000V インスタンスを設定します。

```
interface Loopback1
 ip address 11.11.11.11 255.255.255.255

interface Tunnel2
 ip address 30.0.0.1 255.255.255.0
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 52.14.116.161
 tunnel protection ipsec profile p2p_pf1
!
!
interface GigabitEthernet3
 ip address 10.10.10.2 255.255.255.0
 negotiation auto
 lisp mobility subnet1 nbr-proxy-reply requests 3
 no mop enabled
 no mop sysid
!
```

Azure で実行されている Cisco Catalyst 8000V インスタンスでの LISP xTR の設定

サービスプロバイダーで実行されている Cisco Catalyst 8000V インスタンスで LISP xTR を設定するには、「Configuring LISP (Location ID Separation Protocol)」のセクションの設定手順に従います。

Azure の Cisco Catalyst 8000V インスタンスは、エンタープライズ LISP ルータをプロキシ ETR として使用します。ルーティングテーブルがデフォルトルートを指す場合は常に、トラフィックを PETR に送信します。

router lisp コマンドを実行して、LISP を有効にします。**itr map resolver** および **itr map server** コマンドを実行して、エンタープライズの Cisco Catalyst 8000V インスタンスを LISP マップサーバーやマップリゾルバとして設定します。

例：

```
router lisp
 locator-set azure
  33.33.33.33 priority 1 weight 100
  exit-locator-set
 !
 service ipv4
  itr map-resolver 11.11.11.11
  itr
  etr map-server 11.11.11.11 key cisco
  etr
  use-petr 11.11.11.11
  exit-service-ipv4
 !
 instance-id 0
  dynamic-eid subnet1
   database-mapping 10.10.10.0/24 locator-set azure
   map-notify-group 239.0.0.1
   exit-dynamic-eid
  !
  service ipv4
   eid-table default
   exit-service-ipv4
  !
  exit-instance-id
 !
 exit-router-lisp
!
router ospf 11
 network 30.0.0.2 0.0.0.0 area 11
 network 33.33.33.33 0.0.0.0 area 11
!

router lisp
 locator-set dmz
  11.11.11.11 priority 1 weight 100
  exit-locator-set
 !
 service ipv4
  itr map-resolver 11.11.11.11
  etr map-server 11.11.11.11 key cisco
  etr
  proxy-etr
  proxy-itr 11.11.11.11
  map-server
  map-resolver
  exit-service-ipv4
 !
 instance-id 0
  dynamic-eid subnet1
   database-mapping 10.10.10.0/24 locator-set dmz
   map-notify-group 239.0.0.1
   exit-dynamic-eid
  !
```

```
  service ipv4
   eid-table default
   exit-service-ipv4
  !
  exit-instance-id
 !
 site DATA_CENTER
  authentication-key cisco
  eid-record 10.10.10.0/24 accept-more-specifics
  exit-site
 !
 exit-router-lisp
!
router ospf 11
 network 11.11.11.11 0.0.0.0 area 11
 network 30.0.0.1 0.0.0.0 area 11
!

!
!
```

Azure での Cisco Catalyst 8000V とエンタープライズシステムでの Cisco Catalyst 8000V 間における LISP レイヤ 2 トラフィックの確認

LISP レイヤ 2 トラフィックを確認するには、次の show lisp コマンドを実行します。

例：

```
Router#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 2, no-route 0, inactive 0

10.0.1.1/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
33.33.33.33    1/100  cfg-addr   site-self, reachable
10.0.1.20/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
33.33.33.33    1/100  cfg-addr   site-self, reachable
Router-azure#show ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 4 entries

0.0.0.0/0, uptime: 00:09:49, expires: never, via static-send-map-request
  Negative cache entry, action: send-map-request
10.0.1.0/24, uptime: 00:09:49, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
10.0.1.4/30, uptime: 00:00:55, expires: 00:00:57, via map-reply, forward-native
  Encapsulating to proxy ETR
10.0.1.100/32, uptime: 00:01:34, expires: 23:58:26, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
11.11.11.11  00:01:34  up           1/100       -
Router-azure#show lisp dynamic-eid detail
% Command accepted but obsolete, unreleased or unsupported; see documentation.
```

```
LISP Dynamic EID Information for VRF "default"

Dynamic-EID name: subnet1
  Database-mapping EID-prefix: 10.0.1.0/24, locator-set dc
  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: 239.0.0.1
  Number of roaming dynamic-EIDs discovered: 2
  Last dynamic-EID discovered: 10.0.1.20, 00:01:37 ago
    10.0.1.1, GigabitEthernet2, uptime: 00:09:23
      last activity: 00:00:42, discovered by: Packet Reception
    10.0.1.20, GigabitEthernet2, uptime: 00:01:37
      last activity: 00:00:40, discovered by: Packet Reception

Router-DC#show ip lisp
Router-DC#show ip lisp data
Router-DC#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 1, no-route 0, inactive 0

10.0.1.100/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
11.11.11.11    1/100  cfg-addr   site-self, reachable
Router-DC#show ip lisp
Router-DC#show ip lisp map
Router-DC#show ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 2 entries

10.0.1.0/24, uptime: 1d08h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
10.0.1.20/32, uptime: 00:00:35, expires: 23:59:24, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
33.33.33.33  00:00:35  up           1/100

Router-DC#show lisp dynamic-eid detail
% Command accepted but obsolete, unreleased or unsupported; see documentation.

LISP Dynamic EID Information for VRF "default"

Dynamic-EID name: subnet1
  Database-mapping EID-prefix: 10.0.1.0/24, locator-set dc
  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: 239.0.0.1
  Number of roaming dynamic-EIDs discovered: 1
  Last dynamic-EID discovered: 10.0.1.100, 1d08h ago
    10.0.1.100, GigabitEthernet2, uptime: 1d08h
      last activity: 00:00:47, discovered by: Packet Reception

Router-DC#show lisp site
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
dc             never     no     --                            10.0.1.0/24
               00:08:41  yes#   33.33.33.33                   10.0.1.1/32
               00:01:00  yes#   33.33.33.33                   10.0.1.20/32
               1d08h     yes#   11.11.11.11                   10.0.1.100/32
Router-DC#show ip cef 10.0.1.20
10.0.1.20/32
  nexthop 33.33.33.33 LISP0
Router-DC#
```

```
Router#show lisp instance-id 0 ipv4 database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 7, no-route 0, inactive 4

10.20.20.1/32, locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.5/32, dynamic-eid subnet1, inherited from default locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.6/32, Inactive, expires: 01:20:16
10.230.1.7/32, Inactive, expires: 01:20:16
10.230.1.8/32, dynamic-eid subnet1, inherited from default locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.31/32, Inactive, expires: 01:21:52
10.230.1.32/32, Inactive, expires: 01:20:16
Router-OnPrem#show lisp instance-id 0 ipv4 map
Router#show lisp instance-id 0 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 6 entries

10.20.0.0/16, uptime: 22:39:53, expires: never, via static-send-map-request
Negative cache entry, action: send-map-request
10.230.1.0/24, uptime: 22:39:53, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request
10.230.1.6/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
10.230.1.7/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
10.230.1.31/32, uptime: 22:38:14, expires: 01:21:45, via map-reply, complete
Locator Uptime State Pri/Wgt Encap-IID
11.11.11.11 22:38:14 up 1/100 -
10.230.1.32/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
```

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。