Cisco データセンターとパブリッククラウドの接続

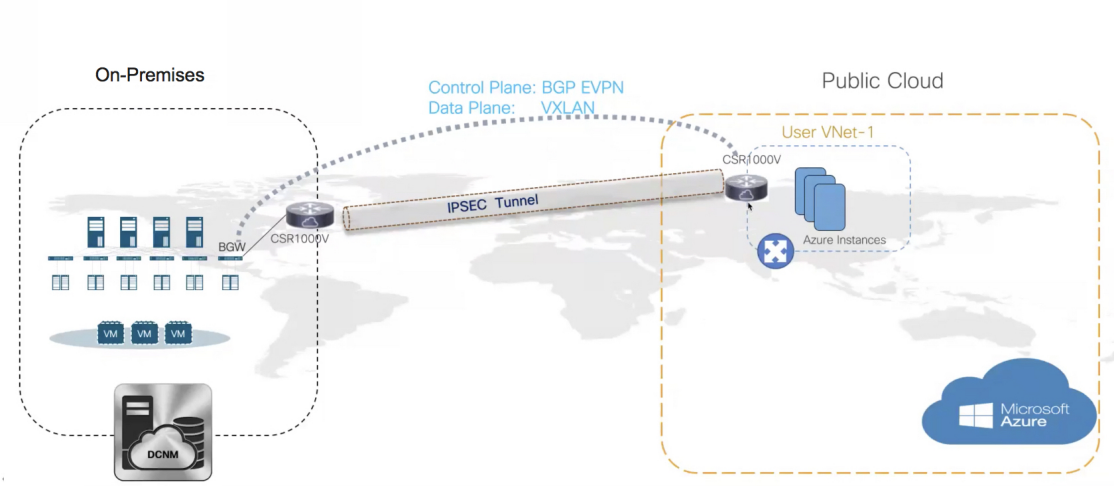
Cisco データセンターとパブリッククラウドの接続

このセクションでは、Cisco DCNM でプロビジョニングされた VXLAN EVPN ファブリックから Microsoft Azure パブリッククラウドへのパブリッククラウド接続を可能にする 機能について説明します。 レイヤ 3 接続により、オンプレミスのワークロードと Microsoft Azure クラウド間のシームレスで安全な通信が保証されます。接続は、Cisco DCNM によって管理される シスコ クラウド サービス ルータ 1000v（Cisco CSR 1000v）を介してプロビジョニングされます。コントロール プレーンには BGP EVPN が採用され、データ プレーンには VXLAN が採用されています。オンプレミスの Cisco CSR 1000v とパブリッククラウドの Cisco CSR 1000v の間に、セキュアな IPsec トンネルが確立されます。

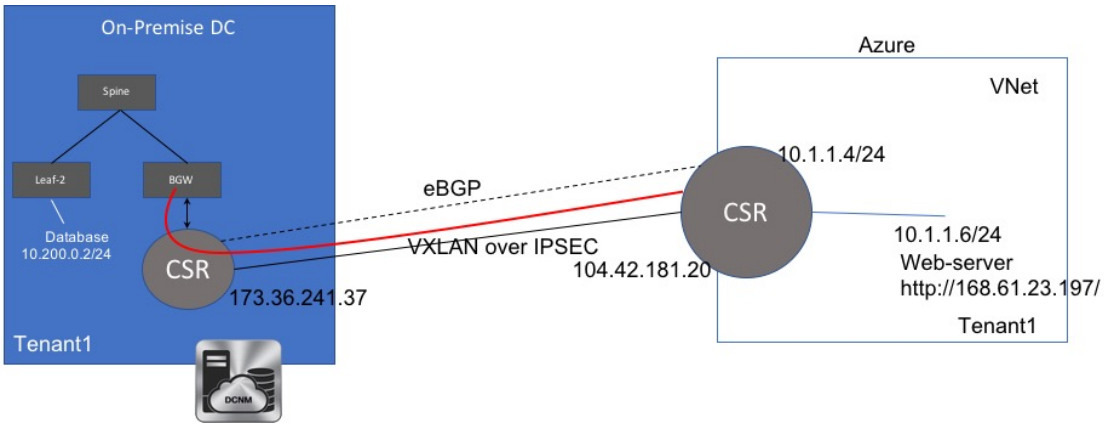
（注） Cisco DCNM は、 Cisco CSR 1000v の検出と管理をサポートします。この機能は、Cisco DCNM リリース 11.2(1) のプレビュー機能です。Cisco DCNM リリース 11.3(1) へのインライン アップグレード後、この機能はデフォルトで有効になります。

トポロジ概要

図 *1*: トポロジの概要



オンプレミスのデータセンターには、必要なスイッチがあります。これらのスイッチの 1 つは、パブリッククラウドへの WAN 接続向けに、コア ルータとインターフェイス接続するボーダーゲートウェイ（BGW）です。Cisco CSR 1000v は、この使用例のコア ルータです。このコア ルータを Cisco DCNM の外部ファブリックにインポートできます。次の図は、採用されているサンプル トポロジを示しています。



この例では、スタンドアロン リーフの背後にある VM と特定のユーザ VNET 内の Microsoft Azure クラウド内の VM との間にレイヤ 3 接続を提供するために必要なタスクをリストします。

パブリッククラウドには、Cisco CSR 1000v、Microsoft Azure インスタンス、Azure 仮想ネットワーク（Azure VNet）、および VM があります。クラウドの Cisco CSR 1000v には、VM とのインターフェイスがあります。

アンダーレイ ルーティングと到達可能性を交換するために、2 つのコア ルータ間で eBGP を使用しています。VXLAN は、オンプレミスの BGW と Microsoft Azure のコア ルータを IPsec トンネル経由で接続します。

このユースケースでは、次のようにセットアップを構成します。

ガイドラインと制約事項

オンプレミス データ センターとパブリッククラウドを接続するためのガイドラインと制限は次のとおりです。

- Cisco CSR 1000v シリーズ ルータは、ルートベースの IP セキュリティ（IPsec）トンネル インターフェイスをサポートしています。
- Cisco DCNM の VXLAN EVPN Easy ファブリックで Cisco Nexus 9000 シリーズ スイッチまたは Cisco Nexus 3000 シリーズ スイッチを使用します。
- このドキュメントで指定されている IP アドレスは、サンプル アドレスです。セットアップに実稼働ネットワークで使用されている IP アドレスが反映されていることを確認します。

前提条件

- Microsoft Azure でアカウントを作成します。
- Microsoft Azure でパブリッククラウド コア ルータの VNet を作成します。
- Microsoft Azure に Cisco CSR 1000v を展開します。この Cisco CSR 1000v は、パブリッククラウド コア ルータです。詳細については、Microsoft Azure での Cisco CSR 1000v の展開（25 ページ）を参照してください。
- ボーダーゲートウェイが必要なため、Cisco NX-OS リリース 7.0(3)I7(x) 以降のバージョンをサポートするスイッチを使用します。
- パブリック インターネットにアクセスできるように、DMZ または同等のゾーン内の Cisco DCNM、スイッチ、Cisco CSR 1000v、およびその他のデバイスをセットアップします。
- VXLAN BGP EVPN データセンター ファブリック アーキテクチャおよび DCNM を介した構成に精通していること。
- MSD ファブリックに精通していること。

（注） 設定に必要なさまざまなタスクについては、『*Cisco DCNM LAN* ファブリックの構成ガイド』の「制御」の章を参照してください。

タスクの概要

次のセクションでは、オンプレミスデータセンターとパブリッククラウド間の接続を確立するためのタスクの概要を示します。

オンプレミス データセンター

1. ポーリング時間を設定します。
2. オンプレミスデータセンター用のスイッチを備えたファブリックを作成し、いずれかのスイッチに BGW ロールを構成します。
3. オンプレミス コア ルータの外部ファブリックを作成します。コア ルータとして Cisco CSR 1000v を検出します。
4. BGW 上のオンプレミス ホストとして IP アドレスをシミュレートします。

パブリック クラウド

1. パブリッククラウド コア ルータの外部ファブリックを作成します。
2. コア ルータであるパブリッククラウドの Cisco CSR 1000v を検出します。

接続

1. MSD ファブリックを作成し、以前に作成したファブリックをインポートします。
2. BGW とオンプレミスのコア ルータを接続します。
3. オンプレミス コア ルータとパブリッククラウド コア ルータの間に IPsec トンネルを作成します。
4. IPsec トンネル上で実行されるコア ルータ間に eBGP アンダーレイ接続を作成します。
5. VXLAN EVPN を使用して、BGW とパブリッククラウド コア ルータを接続します。
6. ファブリック内の VRF を拡張します。

このセクションの各タスクに含まれる手順については、次のセクションで説明します。

ポーリング時間の設定

Cisco DCNM は、オンプレミス コア ルータにクエリを実行し、設定したポーリング時間に応じてルーティング テーブルの状態を更新します。Cisco DCNM Web UI からのポーリング時間を設定するには、次の手順を実行します。

Procedure

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

[サーバー プロパティ（Server Properties）] ウィンドウが表示されます。

ステップ 2 **[プライベート クラウドとパブリッククラウドの接続（Private and public cloud connectivity）]** プロパティを見つけます。

ステップ 3 **[private_public_cloud_connectivity.stats.polling_time]** フィールドにポーリング時間を設定します。

値はミリ秒単位です。

```
# Private and public cloud connectivity
#
                                    preview_features.enable true

        private_public_cloud_connectivity.stats.polling_time 300000


#
```

ステップ 4 [Apply Changes] をクリックします。

ステップ 5 **appmgr restart dcnm** コマンドを使用して Cisco DCNM を再起動します。

Cisco DCNM Web UI にログインすると、有効になっているプレビュー機能に関する警告が表示されます。

Note これはプレビューのみの機能です。この機能は、実稼働環境ではなく、実験用セットアップでのみ使用することが推奨されています。

CSR1000vを使用したオンプレミスの外部ファブリックのセットアップ

オンプレミス エッジ ルータの外部ファブリックを作成します。

外部ファブリックの作成

Cisco DCNM Web UI から外部ファブリックを作成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

[ファブリックの追加（Add Fabric）] ダイアログボックスが表示されます。

ステップ 3 **[ファブリック名（Fabric Name）]** フィールドにファブリック名を **[CSR-OnPrem]** として入力します。

ステップ 4 [ファブリック テンプレート（Fabric Template）] ドロップダウンリストから **[External_Fabric_11_1]** を選択します。

ステップ 5 **[BGP AS #]** フィールドに BGP AS 番号を入力します。

ステップ 6 **[ファブリック モニタ モード（Fabric Monitor Mode）]** チェックボックスをオフにします。

ステップ 7 [保存（Save）] をクリックします。

ファブリックが作成され、[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。

What to do next

オンプレミスのコア ルータを検出します。

オンプレミス コア ルータの検出

Cisco CSR 1000v は、オンプレミスのコア ルーティングに使用されます。ファブリック トポロジ ウィンドウでコア ルータを検出するには、次の手順を実行します。

Before you begin

コア ルータのログイン情報を確認してください。

Procedure

ステップ 1 [アクション（Actions）] ペインで **[スイッチの追加（Add switches）]** をクリックします。

[インベントリ管理（Inventory Management）] ダイアログボックスが表示されます。

ステップ 2 [既存スイッチの検出（Discover Existing Switches）] タブの次のフィールドに値を入力します。

フィールド	説明
シードIP	コア ルータの IP アドレスを入力します。
デバイスタイプ（Device Type）	ドロップダウンリストから **[IOS XE]** を選択して、**[CSR]** ラジオ ボタンをクリックします。
ユーザ名	SSH アクセス向けのコア ルータのユーザー名を入力します。
パスワード	SSH アクセス向けのコア ルータのパスワードを入力します。

Note すでに検出されているスイッチを検出しようとすると、エラーが表示されます。

ステップ 3 [検出の開始（Start Discovery）] をクリックします。

ファブリック トポロジ ウィンドウが表示され、検出に関するポップアップ メッセージが右下に表示されます。

次に例を示します。<*ip-address*> 検出用に追加されました。

Note スイッチの検出には時間がかかる場合があります。

ステップ 4 [アクション（Actions）] ペインで **[表形式ビュー（Tabular view）]** をクリックします。

スイッチとリンクのウィンドウが表示され、スキャンの詳細を確認できます。検出が進行中の場合、検出ステータスは赤色の [検出中（discovering）] でありその横に警告アイコンが表示されます。

ステップ 5 コア ルータの詳細を表示します。

ルーターが検出された後：

- 検出ステータスが緑色の [OK] に変わり、横のチェックボックスがオンになります。
- **[ファブリック ステータス（Fabric Status）]** 列のルータの値が **[同期中（In-Sync）]** と表示されます。

ステップ 6 ファブリック トポロジ ウィンドウに戻り、トポロジを更新します。

What to do next

ルータのロールを **[コア ルータ（Core Router）]** に設定します。ルータを右クリックして、**[ロールの設定（Set role）] > [コア ルータ（Core Router）]** を選択します。

BGW を備えたオンプレミス データセンターの VXLAN EVPN ファブリックを設定します。

VXLAN EVPN ファブリックの設定

BGW のファブリックを作成します。

VXLAN EVPN ファブリックの作成

Cisco DCNM Web UI から VXLAN EVPN ファブリックを作成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

[ファブリックの追加（Add Fabric）] ダイアログボックスが表示されます。

ステップ 3 **[ファブリック名（Fabric Name）]** フィールドにファブリック名を **[site2]** として入力します。

ステップ 4 **[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[Easy_Fabric_11_1]** を選択します。

ステップ 5 すべての必須フィールドに値を入力します。

ステップ 6 [保存（Save）] をクリックします。

ファブリックが作成され、[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。

What to do next

このファブリックにスイッチを追加し、いずれかのスイッチに BGW ロールを割り当てます。

BGW ロールの割り当て

BGW スイッチにロールを割り当てるには、次の手順を実行します。

Before you begin

[site2] ファブリックにスイッチを追加します。

Procedure

ステップ 1 BGW ロールを設定する必要があるスイッチを右クリックします。

スイッチで実行できるアクションのリストが表示されます。

ステップ 2 **[ロールの設定（Set role）] > [ボーダーゲートウェイ（Border Gateway）]** を選択します。

What to do next

パブリッククラウドのファブリックを設定します。

Azure での CSR を使用した外部ファブリックのセットアップ

パブリッククラウド コア ルータの外部ファブリックを作成します。

外部ファブリックの作成

Cisco DCNM Web UI から外部ファブリックを作成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

[ファブリックの追加（Add Fabric）] ダイアログボックスが表示されます。

ステップ 3 **[ファブリック名（Fabric Name）]** フィールドにファブリック名を **[CSR-Azure]** として入力します。

ステップ 4 **[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[External_Fabric_11_1]** を選択します。

ステップ 5 **[BGP AS # フィールド（BGP AS # field）]** に BGP AS 番号を入力します。

ステップ 6 **[ファブリック モニタ モード（Fabric Monitor Mode）]** チェックボックスをオフにします。

ステップ 7 [保存（Save）] をクリックします。

ファブリックが作成され、[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。

What to do next

このファブリックでパブリッククラウド コア ルータを検出します。

コア ルータの検出

Cisco CSR 1000v シリーズ ルータは、パブリッククラウド コア ルーティングにも使用されます。ファブリック トポロジ ウィンドウでコア ルータを検出するには、次の手順を実行します。

Before you begin

コア ルータのログイン情報を確認してください。

Procedure

ステップ 1 [アクション（Actions）] ペインで [スイッチの追加（Add switches）] をクリックします。

[インベントリ管理（Inventory Management）] ダイアログボックスが表示されます。

ステップ 2 [既存スイッチの検出（Discover Existing Switches）] タブの次のフィールドに値を入力します。

フィールド	説明
シードIP	コア ルータの IP アドレスを入力します。
デバイスタイプ（Device Type）	ドロップダウンリストから **[IOS XE]** を選択して、**[CSR]** ラジオ ボタンをクリックします。
ユーザ名	SSHアクセス向けのコア ルータのユーザー名を入力します。

フィールド	説明
パスワード	SSHアクセス向けのコアルータのパスワードを入力します。

Note すでに検出されているスイッチを検出しようとすると、エラーメッセージが表示されます。

ステップ 3 [検出の開始（Start Discovery）] をクリックします。

ファブリック トポロジ ウィンドウが表示され、右下にスイッチ検出に関するポップアップ メッセージが表示されます。次に例を示します。 **<ip-address> added for discovery**

Note スイッチの検出には時間がかかる場合があります。

ステップ 4 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

スイッチとリンクのウィンドウが表示され、スキャンの詳細を確認できます。検出が進行中の場合、検出ステータスは赤色の [検出中（discovering）] でありその横に警告アイコンが表示されます。

ステップ 5 コア ルータの詳細を表示します。

ルータの検出後：

- 検出ステータスが緑色の [OK] に変わり、横のチェックボックスがオンになります。
- **[ファブリック ステータス（Fabric Status）]** 列のルータの値が **[同期中（In-Sync）]** に変わります。

ステップ 6 ファブリック トポロジ ウィンドウに戻り、トポロジを更新します。

What to do next

ルータのロールを **[コア ルータ（Core Router）]** に設定します。ルータを右クリックして、**[ロールの設定（Set role）] > [コア ルータ（Core Router）]** を選択します。

MSD ファブリックを作成し、以前に作成した他のファブリックをそこにインポートします。

MSD ファブリックの接続の設定

接続のためにすべてのスタンドアロン ファブリックを結合する MSD ファブリックを作成します。

MSD ファブリックの作成

Cisco DCNM Web UI から MSD ファブリックを作成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

[ファブリックの追加（Add Fabric）] ダイアログボックスが表示されます。

ステップ 3 **[ファブリック名（Fabric Name）]** フィールドにファブリック名を **[Cloud-Connect]** として入力します。

ステップ 4 **[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[MSD_Fabric_11_1]** を選択します。

ステップ 5 すべての必須フィールドに値を入力します。

ステップ 6 [保存（Save）] をクリックします。

ファブリックが作成され、[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。

What to do next

他のファブリックをこの MSD ファブリックに移動します。

他のファブリックを MSD ファブリックに移動する

他のファブリックをファブリック トポロジ ウィンドウから **[Cloud-Connect]** ファブリックに移動するには、次の手順を実行します。

Procedure

ステップ 1 **[アクション（Actions）]** ペインで **[ファブリックの移動（Move Fabric）]** をクリックします。

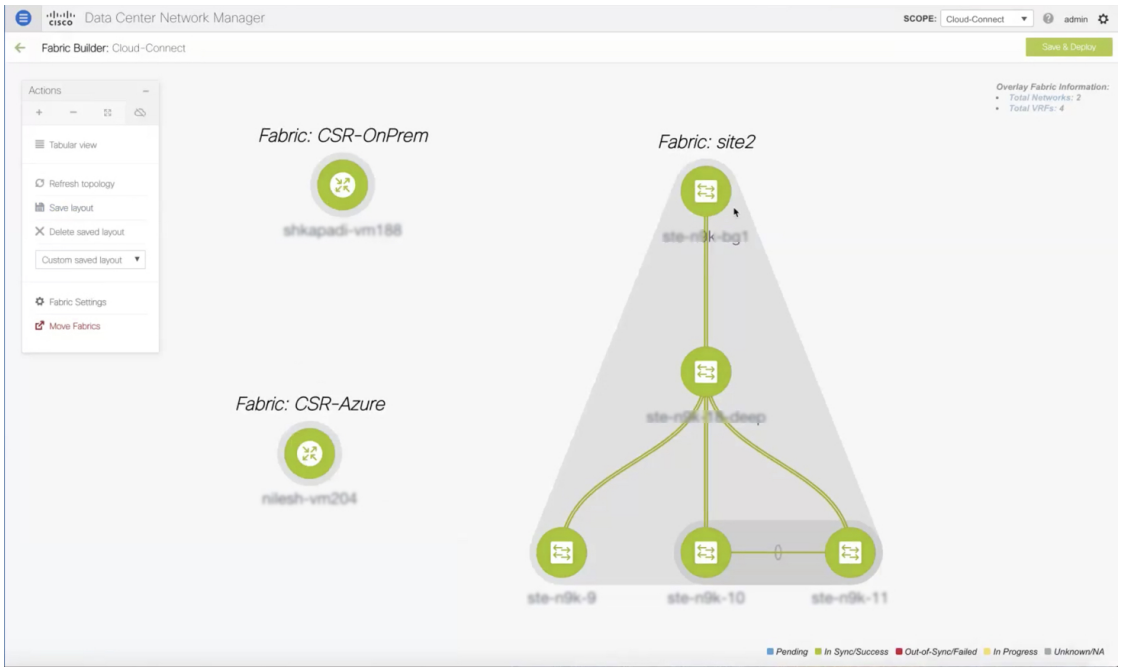
[ファブリックの移動（Move Fabric）] ダイアログボックスが表示されます。ファブリックのリストが含まれています。

ステップ 2 **[CSR-OnPRem]**、**[site2]**、および **[CSR-Azure]** ファブリックを選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 ダイアログボックスを閉じて、ファブリック トポロジを更新します。

すべてのメンバー ファブリックが **[Cloud-Connect]** ファブリックに表示されます。



What to do next

ファブリック間の接続をセットアップします。

接続設定

異なるリンクを使用して、以前に作成したファブリックを接続します。

オンプレミス BGW とオンプレミス コア ルータの接続

オンプレミス BGW とオンプレミス コア ルータの間にリンクを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[Cloud-Connect]** トポロジ ウィンドウの任意の場所を右クリックします。

ファブリックで実行できるアクションがリストに表示されます。または、ファブリック トポロジ ウィンドウから、**[アクション（Actions）]** ペインの **[表形式ビュー（Tabular view）]** を選択し、**[リンク（Links）]** タブをクリックします。

ステップ 2 **[リンクの追加（Add Link）]** を選択します。

[リンク管理（Link Management）- リンクの追加（Add Link）] ダイアログボックスが表示されます。

ステップ 3 次のフィールドに値を入力します。

フィールド	説明
リンクタイプ	ドロップダウンリストから **[ファブリック間（Inter-Fabric）]** リンク タイプを選択します。
リンク サブタイプ	ドロップダウンリストから **[MULTISITE_UNDERLAY]** リンク サブタイプを選択します。
リンク テンプレート	ドロップダウンリストから **[csr_ext_multisite_underlay_setup]** リンク テンプレートを選択します。 **Note** このテンプレートは、プレビュー機能を有効にして DCNM を再起動した後にのみ使用できます。
送信元ファブリック	ドロップダウンリストから送信元ファブリックとして **[site2]** を選択します。
接続先ファブリック	ドロップダウンリストから接続先ファブリックとして **[CSR-OnPrem]** を選択します。
送信元デバイス（Source Device）	ドロップダウン リストから BGW を選択します。
送信元インターフェイス（Source Interface）	BGW のインターフェースを選択します。
接続先デバイス	ドロップダウンリストからオンプレミス コア ルータを選択します。
宛先インターフェイス	ドロップダウンリストからオンプレミス コア ルータのインターフェイスを選択します。

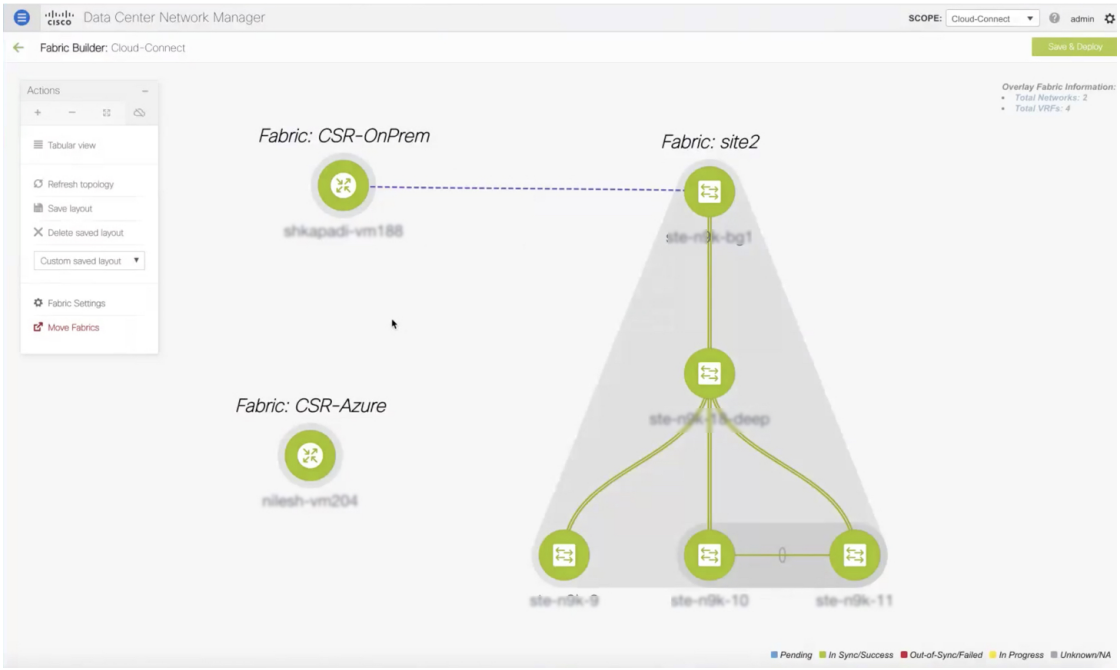
ステップ 4 **[全般（General）]** タブの **[リンク プロファイル（Link Profile）]** エリアにある次のフィールドに値を入力します。

フィールド	説明
IP_MASK	サブネットを持つ送信元インターフェイスの IPv4 アドレスを入力します。
NEIGHBOR_IP	接続先インターフェイスの IPv4 アドレスを入力します。

Cisco DCNM Web UI から IP アドレスを確認するには、**[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** を選択します。**[範囲（Scope）]** ドロップダウンリストからファブリックを選択し、デバイスを検索します。デバイスの IP アドレスが **[IP/プレフィックス（IP/Prefix）]** 列に表示されます。

ステップ 5 [保存（Save）] をクリックします。

[ファブリック トポロジ（fabric topology）] ウィンドウが更新されます。**site2** ファブリックのオンプレミス BGW と **CSR-OnPrem** ファブリックのオンプレミス コア ルータの間にリンクが追加されます。



What to do next

オンプレミス コア ルータとパブリック クラウド コア ルータを接続します。

IPsec トンネルを使用したオンプレミス コア ルータとパブリッククラウド コア ルータの接続

オンプレミス コア ルータ とパブリッククラウド コア ルータの間にリンクを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[Cloud-Connect]** トポロジ ウィンドウの任意の場所を右クリックします。

ファブリックで実行できるアクションがリストに表示されます。または、ファブリック トポロジ ウィンドウから、**[アクション（Actions）]** ペインの **[表形式ビュー（Tabular view）]** を選択し、**[リンク（Links）]** タブをクリックします。

ステップ 2 **[リンクの追加（Add Link）]** を選択します。

[リンク管理（Link Management）- リンクの追加（Add Link）] ダイアログボックスが表示されます。

ステップ 3 次のフィールドに値を入力します。

フィールド	説明
リンクタイプ	ドロップダウンリストから**[ファブリック間（Inter-Fabric）]** リンク タイプを選択します。
リンク サブタイプ	ドロップダウンリストから **[BGP_OVER_IPSEC]** リンク サブタイプを選択します。
リンク テンプレート	ドロップダウンリストから **[csr_link_template]** リンク テンプレートを選択します。
送信元ファブリック	ドロップダウンリストから送信元ファブリックとして **[CSR-OnPrem]** を選択します。
接続先ファブリック	ドロップダウンリストから接続先ファブリックとして **[CSR-Azure]** を選択します。
送信元デバイス（Source Device）	ドロップダウンリストからオンプレミス コア ルータを選択します。
送信元インターフェイス（Source Interface）	オンプレミス コア ルータのインターフェイスを選択します。
接続先デバイス	ドロップダウンリストからパブリッククラウド コア ルータを選択します。
宛先インターフェイス	ドロップダウンリストからパブリッククラウド コア ルータのインターフェイスを選択します。

ステップ 4 **[全般（General）]** タブの **[リンク プロファイル（Link Profile）]** エリアで、IPSec トンネルに使用されるパス キーを **[SHARED_KEY]** フィールドに入力します。

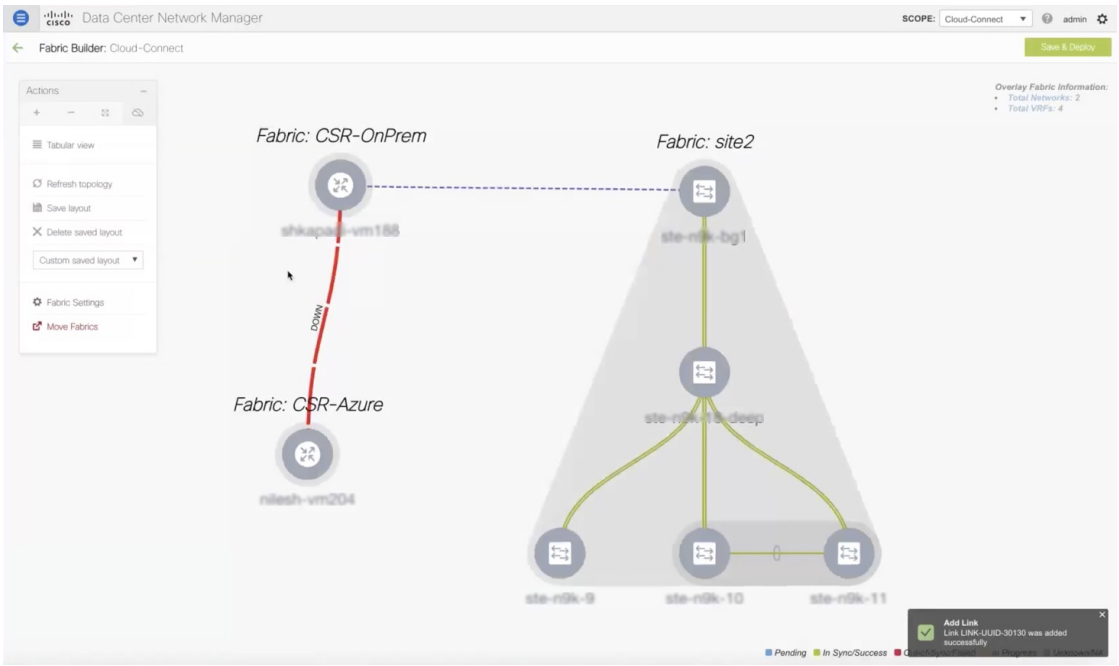
ステップ 5 (Optional) [リンク プロファイル（Link Profile）] エリアで、**[詳細（Advanced）]** タブを選択します。

このタブの下のフィールドには、デフォルト値が入力されています。必要に応じて値を変更します。これにより、2 つのコア ルータ間で eBGP ピアリングが構成されるループバックが作成されます。

ステップ 6 [保存（Save）] をクリックします。

ファブリック トポロジ ウィンドウが更新され、**[CSR-OnPrem]** ファブリックのコア ルータと **[CSR-Azure]** ファブリックのコア ルータの間にリンクが追加されます。

Note 構成内にプッシュするまで、リンク ダウンします。



What to do next

オンプレミス BGW とパブリッククラウド コア ルータを接続します。

EVPN ピアリングを使用したオンプレミス BGW とパブリッククラウド コア ルータの接続

オンプレミス コア ルータ とパブリッククラウド コア ルータの間にリンクを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[Cloud-Connect]** トポロジ ウィンドウの任意の場所を右クリックします。

ファブリックで実行できるアクションがリストに表示されます。または、ファブリック トポロジ ウィンドウから、**[アクション（Actions）]** ペインの **[表形式ビュー（Tabular view）]** を選択し、**[リンク（Links）]** タブをクリックします。

ステップ 2 **[リンクの追加（Add Link）]** を選択します。

[リンク管理（Link Management）- リンクの追加（Add Link）] ダイアログボックスが表示されます。

ステップ 3 次のフィールドに値を入力します。

フィールド	説明
リンクタイプ	ドロップダウンリストから **[ファブリック間（Inter-Fabric）]** リンク タイプを選択します。
リンク サブタイプ	ドロップダウンリストから **[MULTISITE_OVERLAY]** リンク サブタイプを選択します。
リンク テンプレート	ドロップダウンリストから **[csr_ext_evpn_multisite_overlay_setup]** リンク テンプレートを選択します。
送信元ファブリック	ドロップダウンリストから送信元ファブリックとして **[site2]** を選択します。
接続先ファブリック	ドロップダウンリストから接続先ファブリックとして **[CSR-Azure]** を選択します。
送信元デバイス（Source Device）	ドロップダウンリストからオンプレミス BGW を選択します。
送信元インターフェイス（Source Interface）	オンプレミス BGW のループバック インターフェイスを選択します。
接続先デバイス	ドロップダウンリストからパブリッククラウド コア ルータを選択します。
宛先インターフェイス	ドロップダウンリストからパブリッククラウド コア ルータのインターフェイスを選択します。 **Note** インターフェイスを作成していない場合、接続先インターフェイスはドロップダウンリストに表示されないため、接続先インターフェイスを入力する必要があります。

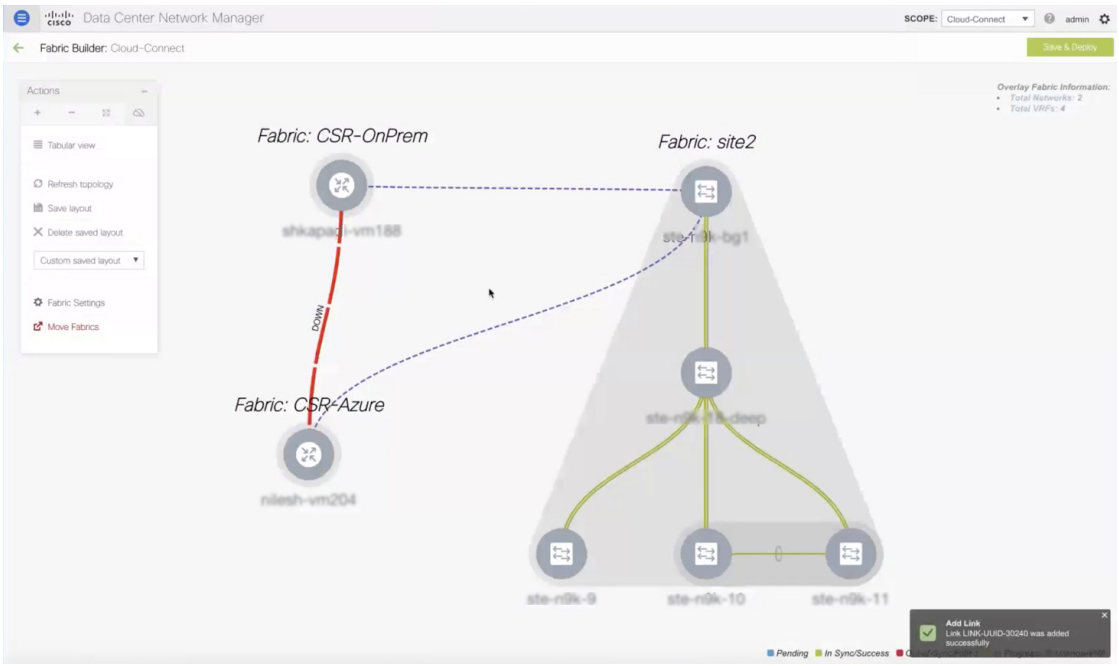
ステップ 4 **[全般（General）]** タブの **[リンク プロファイル（Link Profile）]** エリアにある次のフィールドに値を入力します。

フィールド	説明
IP_MASK	サブネットを持つ送信元インターフェイスの IPv4 アドレスを入力します。
NEIGHBOR_IP	接続先インターフェイスの IPv4 アドレスを入力します。

ステップ 5 [保存（Save）] をクリックします。

ファブリック トポロジ ウィンドウが更新され、**[site2]** ファブリックの BGW と **[CSR-Azure]** ファブリックのコア ルータの間にリンクが追加されます。

Note 構成内にプッシュするまで、リンク ダウンします。



What to do next

構成を保存して展開します。

構成の保存と展開

ファブリック トポロジ ウィンドウで構成を保存して展開するには、次の手順を実行します。

Procedure

ステップ 1 [保存して展開（Save & Deploy）] をクリックします。

[構成の展開（Config Deployment）] ダイアログ ボックスが表示され、**[構成のプレビュー（Configuration Preview）]** ステップが表示されます。BGW、オンプレミス データセンター、パブリッククラウドの間で作成されたリンクのインテントが生成されます。

ステップ 2 (Optional) **[構成のプレビュー（Preview Config）]** 列で BGW の反対側のフィールドをクリックします。

BGW の **[構成プレビュー（Config Preview）]** ダイアログ ボックスが表示されます。

ステップ 3 (Optional) **[保留中の構成（Pending Config）]** 列で構成の詳細を表示します。

アンダーレイ ピアリングとオーバーレイ ピアリングに関する詳細が含まれています。

ステップ 4 (Optional) **[構成のプレビュー（Preview Config）]** 列でオンプレミス コア ルータの反対側のフィールドをクリックします。

オンプレミス コア ルータの **[構成プレビュー（Config Preview）]** ダイアログ ボックスが表示されます。

ステップ 5 (Optional) **[保留中の構成（Pending Config）]** 列で構成の詳細を表示します。

これには、インターフェイス、IPsec トンネル、共有キー、コア ルータ間の BGP ピアリング、および EVPN ピアリングに関する詳細が含まれます。すべての BGP トラフィックとデータ トラフィックがトンネルを通過する必要があることを示すルートマップが追加されます。

ステップ 6 (Optional) **[構成のプレビュー（Preview Config）]** 列でパブリッククラウド コア ルータの反対側のフィールドをクリックします。

オンプレミス コア ルータの **[構成プレビュー（Config Preview）]** ダイアログ ボックスが表示されます。

ステップ 7 (Optional) **[保留中の構成（Pending Config）]** 列で構成の詳細を表示します。

これには、オンプレミス コア ルータについて説明されている詳細に加えて、VTEP に関する詳細が含まれています。

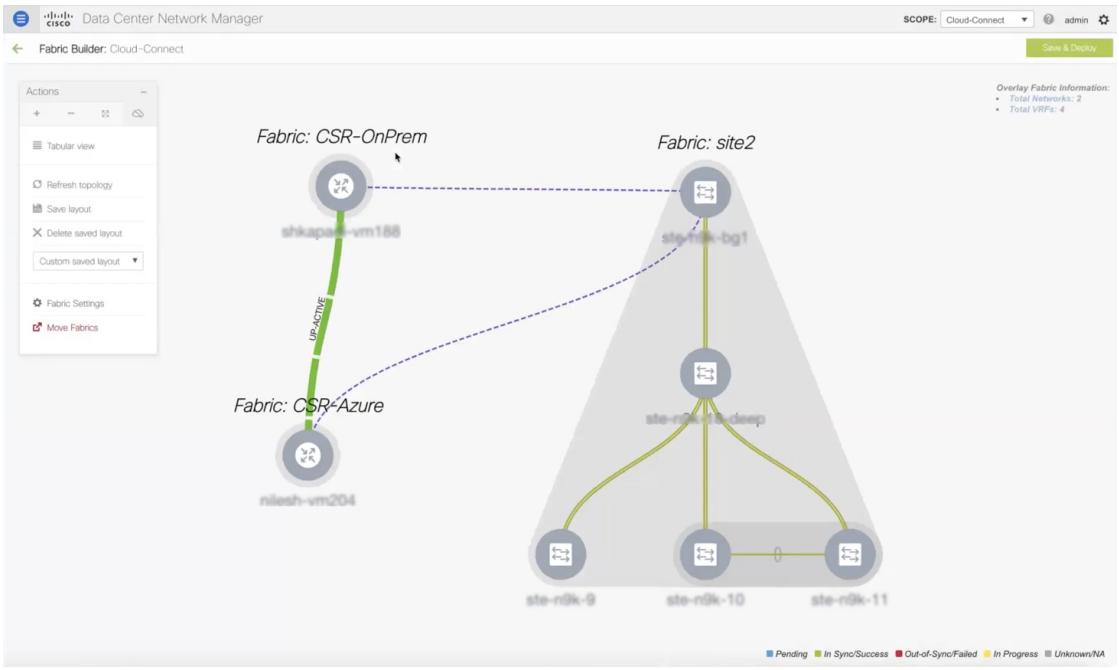
ステップ 8 **[構成の展開（Deploy Config）]** をクリックします。

[構成の展開ステータス（Configuration Deployment Status）] ステップが表示され、構成の展開ステータスを確認できます。

ステップ 9 正常に展開された後、**[閉じる（Close）]** をクリックします。

ファブリック トポロジ ウィンドウが表示されます。IPsec トンネルが起動し、アクティブになります。

Note 展開には時間がかかる場合があります。



What to do next

VRF を拡張して展開します。

VRF の拡張

VRFは、データセンターとパブリッククラウドの間でワークロードを共有できるように拡張されています。

VRF オンプレミス コア ルータの展開と拡張

MSD ファブリックのファブリック トポロジ ウィンドウから VRF を拡張してオンプレミス コア ルータに展開するには、次の手順を実行します。

Procedure

ステップ 1 **[保存と展開（Save & Deploy）]** アイコンの下にある **[オーバーレイ ファブリック情報（Overlay Fabric Information）]** エリアの **[トータル VRF（Total VRF）]** リンクをクリックします。

ファブリックの VRF ウィンドウの **[ネットワーク / VRF 選択（Network / VRF Selection）]** エリアが表示されます。

ステップ 2 オンプレミス コア ルータの VRF を選択し、**[続行（Continue）]** をクリックします。

VRF ウィンドウの **[ネットワーク / VRF 展開（Network / VRF Deployment）]** エリアが表示されます。ファブリックのネットワーク トポロジが表示されます。未検出のクラウドを隠すことができます。

ステップ 3 BGW をダブルクリックします。

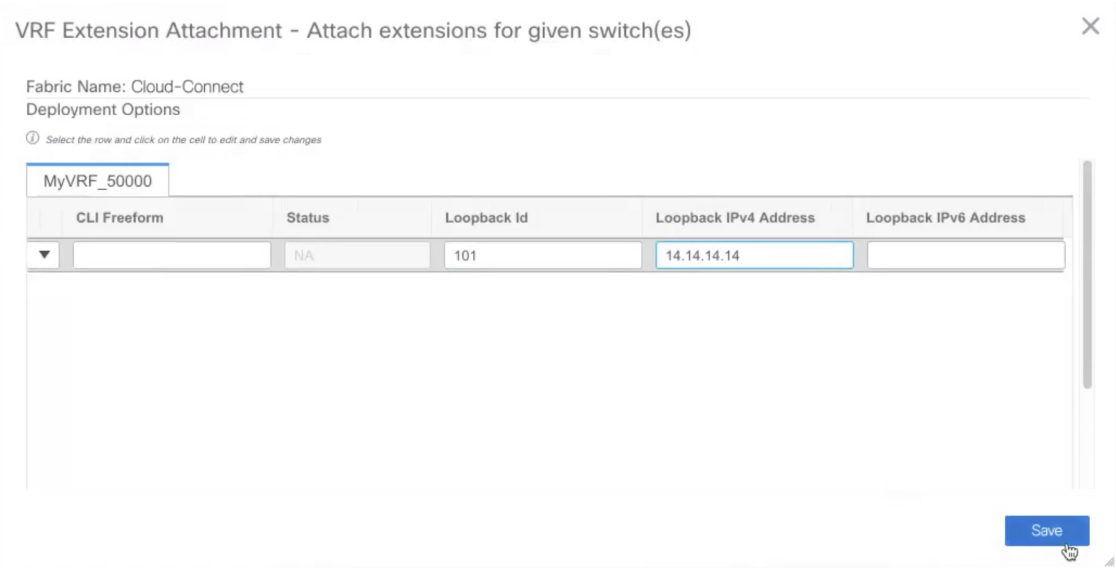
[VRF 拡張アタッチメント（VRF Extension Attachment）] ダイアログボックスが表示されます。

ステップ 4 BGW を選択し、**[拡張（Extend）]** 列の下にある編集アイコンをクリックして、マルチサイトを有効にします。

[拡張（Extend）] 列の下にドロップダウンリストが表示されます。

ステップ 5 ドロップダウンリストから **[MULTISITE]** を選択します。

ステップ 6 ループバック ID とループバック IPv4 アドレスをそれぞれの列に入力して、BGW のホストをシミュレートします。



ステップ 7 [保存（Save）] をクリックします。

ファブリックのネットワーク トポロジが表示され、BGW が青色に変わり、展開が保留中であることを示します。

ステップ 8 [プレビュー（Preview）] オプションをクリックします。

[構成のプレビュー（Preview Configuration）] ダイアログボックスが表示されます。EVPN 構成がプッシュされ、ループバック インターフェイスが作成されます。

ステップ 9 **[展開（Deploy）]** をクリックします。

What to do next

VRF を作成し、パブリッククラウドに展開します。

パブリッククラウドでの VRF の作成と展開

VRF を拡張して、ファブリック トポロジ ウィンドウからパブリッククラウド コア ルータに展開するには、次の手順を実行します。

Before you begin

VM が稼働していることを確認します。VM は、パブリッククラウド コア ルータに接続する必要があります。

Procedure

ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから **[CSR-Azure]** ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 パブリッククラウド コア ルータを右クリックします。

ルータで実行できるアクションのリストが表示されます。

ステップ 3 リストから **[ポリシーの表示/編集（View/edit policies）]** を選択します。

[ポリシーの表示/編集（View/Edit Policies）] ダイアログボックスが表示されます。

ステップ 4 **[ポリシーの追加（Add Policy）]** アイコンをクリックします。

[ポリシーの追加（Add Policy）] ダイアログボックスが表示されます。

ステップ 5 **[ポリシー（Policy）]** ドロップダウンリストから **[csr_vrf_evpn]** ポリシーを選択します。

ステップ 6 **[全般（General）]** タブの必須フィールドに値を入力します。

ステップ 7 [保存（Save）] をクリックします。

[ポリシーの表示/編集（View/Edit Policies）] ダイアログボックスが表示されます。

ステップ 8 **[すべて表示（View All）]** をクリックして、作成されたネットワークとインターフェイスを表示します。

[生成された構成（Generated Config）] ダイアログ ボックスが表示されます。VRF、ブリッジ ドメイン、およびマッピングされた VNI に関する詳細も、このダイアログ ボックスで表示できます。

What to do next

パブリッククラウド内の VM のパブリッククラウド コア ルータでデフォルトゲートウェイを構成します。

VM のデフォルトゲートウェイの構成

ファブリック トポロジ ウィンドウからパブリッククラウド コア ルータのデフォルトゲートウェイを構成するには、次の手順を実行します。

Procedure

ステップ 1 [ファブリック ビルダ（Fabric Builder）] ウィンドウから **[CSR-Azure]** ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 パブリッククラウド コア ルータを右クリックします。

ルータで実行できるアクションのリストが表示されます。

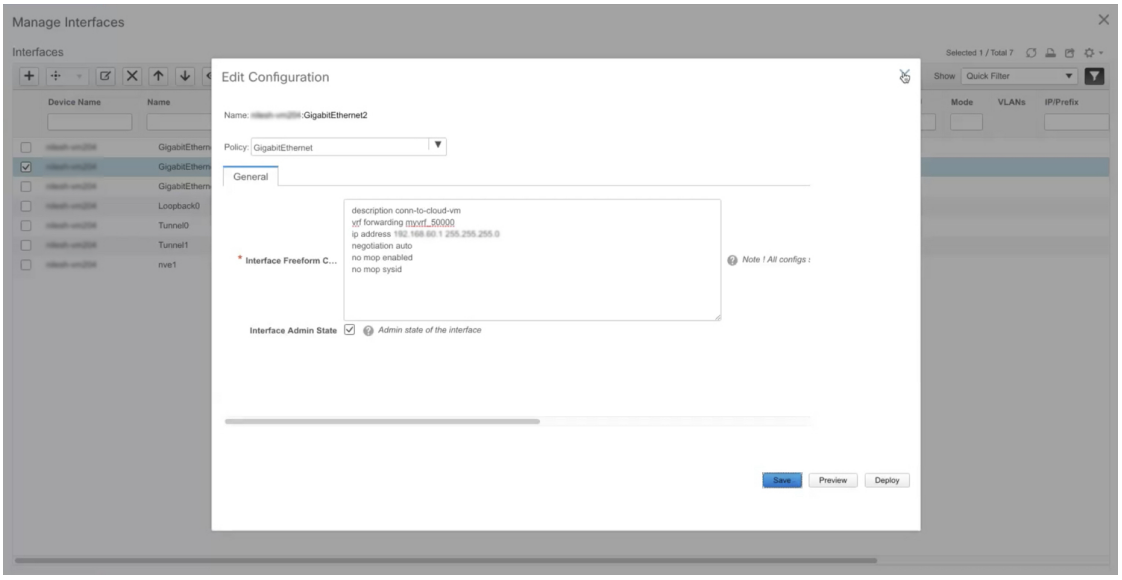
ステップ 3 リストから **[インターフェイスの管理（Manage Interface）]** を選択します。

[インターフェイスの管理（Manage Interface）] ダイアログボックスが表示されます。

ステップ 4 **[構成の編集（Edit Configuration）]** をクリックして、ポリシーを作成するインターフェイスを編集します。

[構成の編集（Edit Configuration）] ダイアログボックスが表示されます。

ステップ 5 自由形式構成を編集し、**[保存（Save）]** をクリックして、**[インターフェイスの管理（Manage Interfaces）]** ダイアログ ボックスを閉じます。



ファブリック トポロジ ウィンドウが表示されます。

ステップ 6 パブリッククラウド コア ルータを右クリックし、リストから **[構成の展開（Deploy Config）]** を選択します。

[構成展開（Config Deployment）] ダイアログ ボックスが表示されます。

ステップ 7 **[構成のプレビュー（Preview Config）]** 列の下の値をクリックして、構成のプレビューを確認します。

ステップ 8 構成を展開するには、**[展開の展開（Deploy Config）]** をクリックします。

構成がプッシュされて展開されます。

ステップ 9 [閉じる（Close）] をクリックします。

ステップ 10 CLI にログオンして、トラフィック フローを表示します。

トラフィックはコア ルータ間を流れ、VRF を経由します。

接続の確認

Cisco DCNM Web UI からオンプレミス データセンターとパブリッククラウド間の接続を確認するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [VRF]** を選択します。

[VRF] ウィンドウが表示されます。

ステップ 2 **[Cloud-Connect]** ファブリックを選択します。

このファブリックの VRF が一覧表示されます。

ステップ 3 VRF を選択して **[続行（Continue）]** をクリックします。

ステップ 4 BGW を右クリックします。

[VRF 拡張アタッチメント（VRF Extension Attachment）] ダイアログボックスが表示されます。

ステップ 5 チェックボックスをオフにして、**[保存（Save）]** をクリックします。

[ネットワークトポロジ（network topology）] ウィンドウが表示されます。

ステップ 6 **[展開（Deploy）]** をクリックして、構成をプッシュします。

BGW で VRF が無効になっています。

ステップ 7 CLI を確認します。

トラフィックが停止します。

ステップ 8 BGW で VRF を再度有効にします。

ステップ 9 CLI を確認します。

トラフィックが流れます。または、パブリッククラウドの Web サーバーの HTTP アドレスにアクセスします。**[データベースの到達可能性（Database Reachable）** メッセージが表示されます。

Microsoft Azure での Cisco CSR 1000v の展開

Microsoft Azure に Cisco CSR 1000v を展開するには、次の手順を実行します。

Procedure

ステップ 1 **[Microsoft Azure]** UI から、**[仮想マシン（Virtual Machines）]** を選択します。

[仮想マシン] ウィンドウが表示されます。

ステップ 2 [追加（Add）] をクリックします。

[仮想マシンの作成（Create a virtual machine）] ウィンドウが表示されます。

ステップ 3 **[Azure マーケットプレイスから VM を作成（Create VM from Azure Marketplace）]** ハイパーリンクをクリックします。

標準のクラシック VM を検索できる **[マーケットプレイス（Marketplace）]** ウィンドウが表示されます。

ステップ 4 マーケットプレイスで CSR 展開を検索します。

ステップ 5 検索結果から **[シスコ クラウド サービス ルータ（CSR）1000V（Cisco Cloud Services Router（CSR）1000V）]** を選択します。

ステップ 6 **[ソフトウェア プランの選択（Select a software plan）]** ドロップダウンリストから **[Cisco CSR 1000V 個人所有ライセンス可 - XE 16.9（Cisco CSR 1000V Bring Your Own License – XE 16.9）]** 以降のバージョンを選択します。

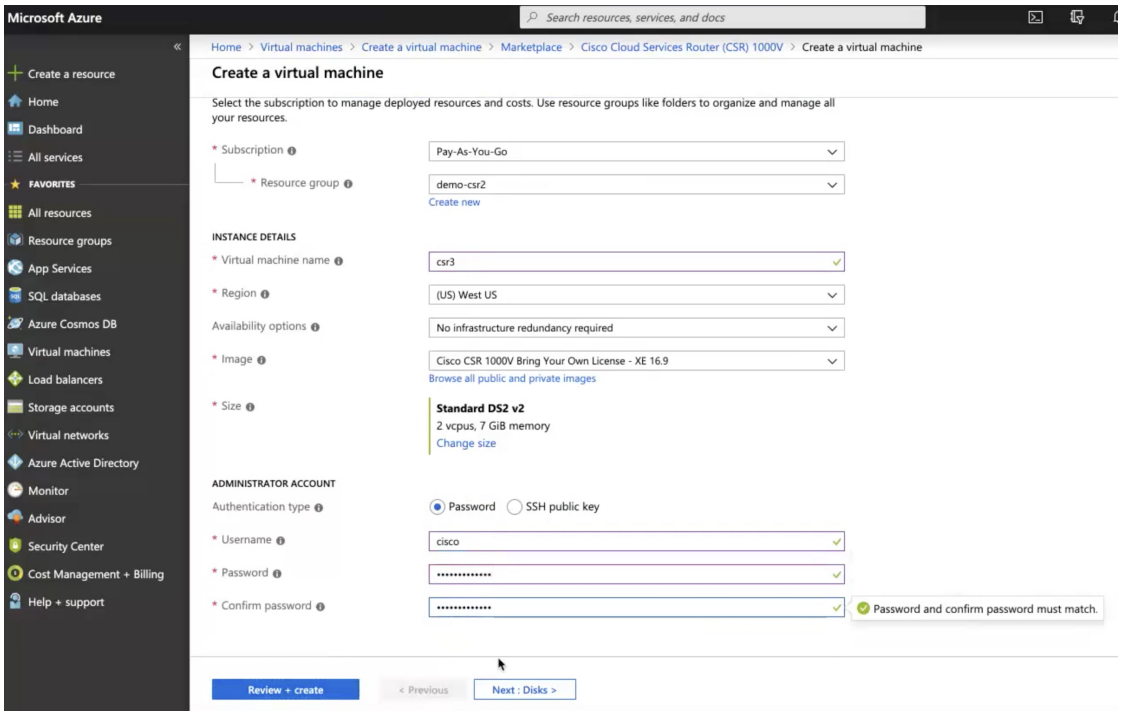
ステップ 7 [作成（Create）] をクリックします。

ステップ 8 **[仮想マシンの作成（Create a virtual machine）]** ウィンドウで、プロジェクトの詳細とインスタンスの詳細を入力します。

ステップ 9 管理者アカウントのセクションでは **[パスワード（Password）]** 認証タイプを選択します。

Cisco DCNM は、SSH 公開キーをサポートしていません。

ステップ 10 ユーザー名とパスワードを作成します。



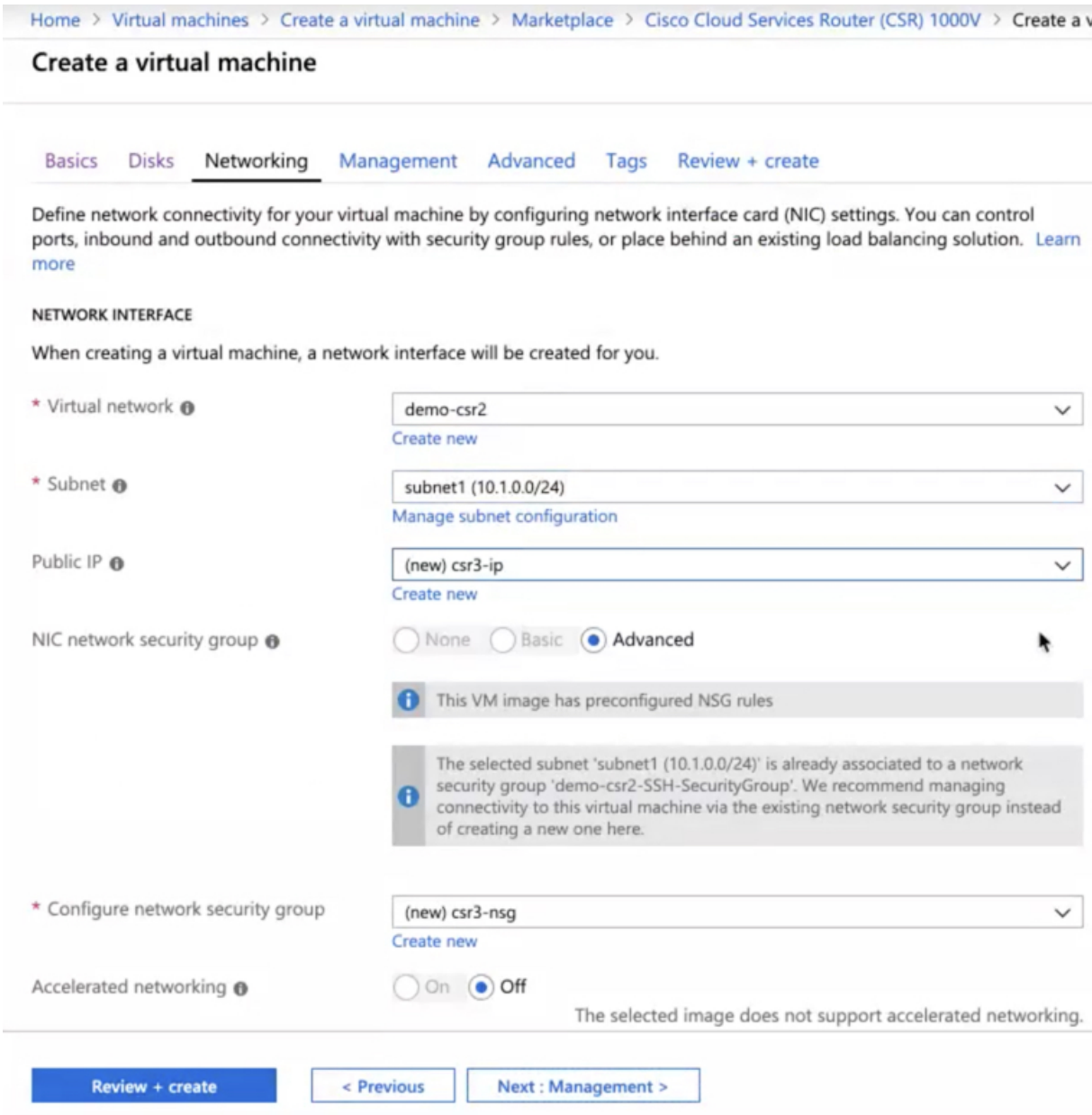
ステップ 11 **[次へ：ディスク >（Next : Disks >）]** をクリックします。

ステップ 12 OS ディスク タイプのドロップダウンリストから、**[標準 HDD（Standard HDD）]** を選択します。

ステップ 13 **[次へ：ネットワーキング >（Next : Networking >）]** をクリックします。

ステップ 14 必要なフィールドに値を入力します。

ステップ 15 ネットワークのパブリック IP を選択します。



ステップ 16 他のフィールドではデフォルト値を使用します。

ステップ 17 **[確認して作成（Review + create）]** をクリックします。

パブリック IP アドレスを使用して、Microsoft Azure に Cisco CSR 1000v 用の VM が作成されます。

What to do next

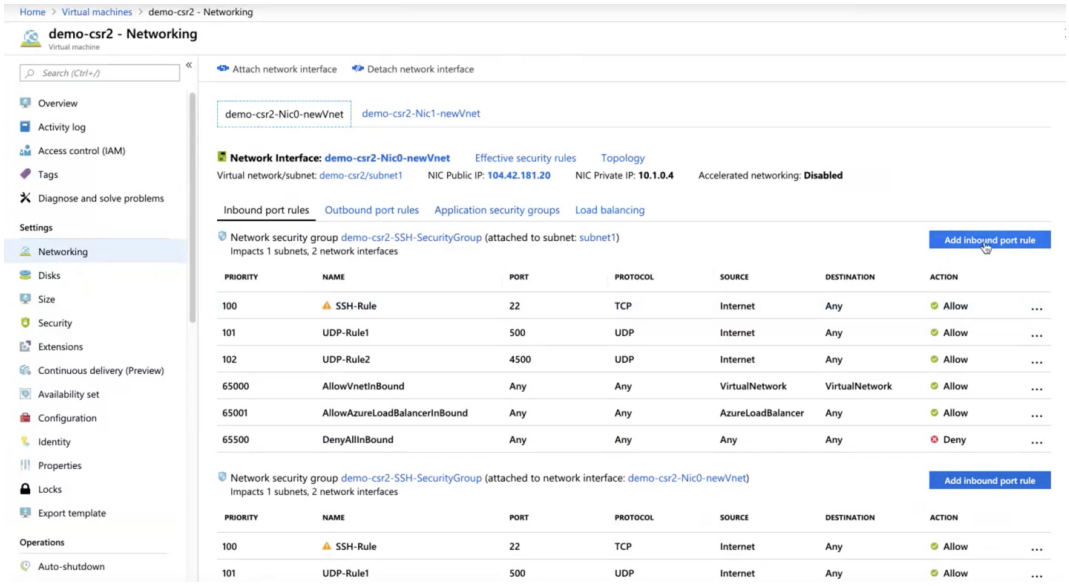
- ネットワーク インターフェイスの接続

1. VM の **[ネットワーキング（Networking）]** 設定を選択します。
2. **[ネットワーク インターフェイスの接続（Attach network interface）]** を選択して、NIC を追加します。

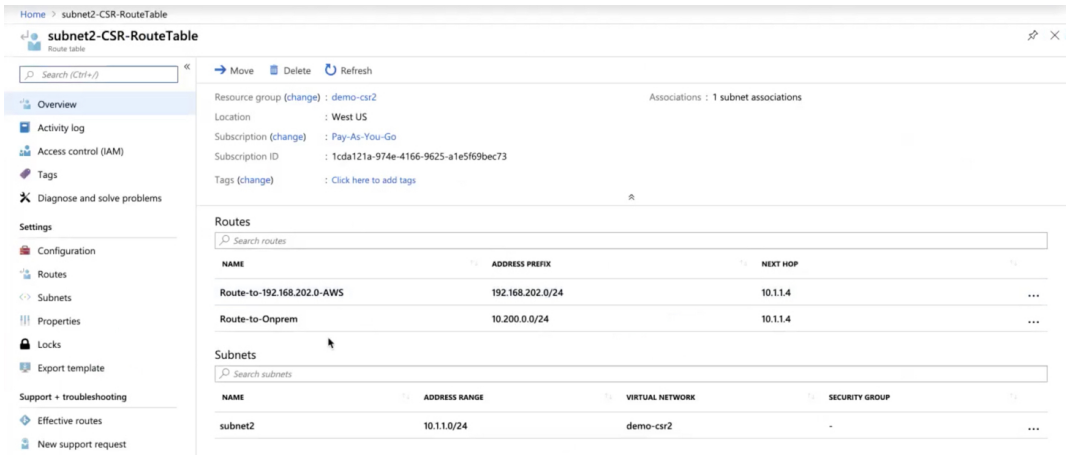
   両方のサブネットにそれぞれ 1 つの NIC を接続します。IP アドレスが自動的に割り当てられます。
3. ポート 22 を使用して SSH ルールを追加して、コア ルータの SSH アクセスを有効にします。

   Cisco DCNM は、この SSH アクセスを使用してコア ルータを検出します。

Note IPsec トンネルを有効にするためにポート 500 と 4500 を使用する 2 つの UDP ルールが自動的に追加されます。



- VM の **[ルート（Routes）]** 設定でルートを作成して、オンプレミス データ センターと Microsoft Azure 間のトラフィック ルートを作成します。デフォルトルートを使用して、トラフィックを VNet から Cisco CSR 1000v にリダイレクトできます。



詳細については、「*Microsoft Azure* 向け *Cisco CSR 1000v* 導入ガイド」を参照してください。

リンクおよびコア ルータの詳細の表示

ファブリック トポロジ ウィンドウからリンクとコア ルータの詳細を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[アクション（Actions）]** ペインで、**[表形式ビュー（Tabular view）] > [リンク（Links）]** を選択します。

[リンク（Links）] ウィンドウが表示されます。

ステップ 2 ウィンドウを更新します。

作成した 3 つのリンクがリストに表示されます。

ステップ 3 (Optional) オンプレミスのコア ルータをダブルクリックして、IP ルート情報を表示します。

[IP ルート情報（IP Route Information）] ダイアログボックスが表示されます。

ステップ 4 (Optional) **[暗号セッション（Crypto Session）]** タブをクリックして、IPsec トンネルの詳細を表示します。

ステップ 5 (Optional) **[BGP セッション（BGP Session）]** タブをクリックして、BGP セッションに関する詳細を表示します。

ステップ 6 (Optional) **[パケット カウンタ（Packet Counter）]** タブをクリックして、パケット カウンタの詳細を表示します。

[パケット カウンタ（Packet Counter）] タブに表示されるカウンタ値をリセットできます。詳細については、API を使用したパケット カウンタのリセット, on page 30を参照してください。

API を使用したパケット カウンタのリセット

ピーク カウンタをリセットするには、次の手順を実行します。

Procedure

ステップ 1 Cisco DCNM にログインします。

ステップ 2 https:// *DCNM-IP* /api-docs URL に移動します。

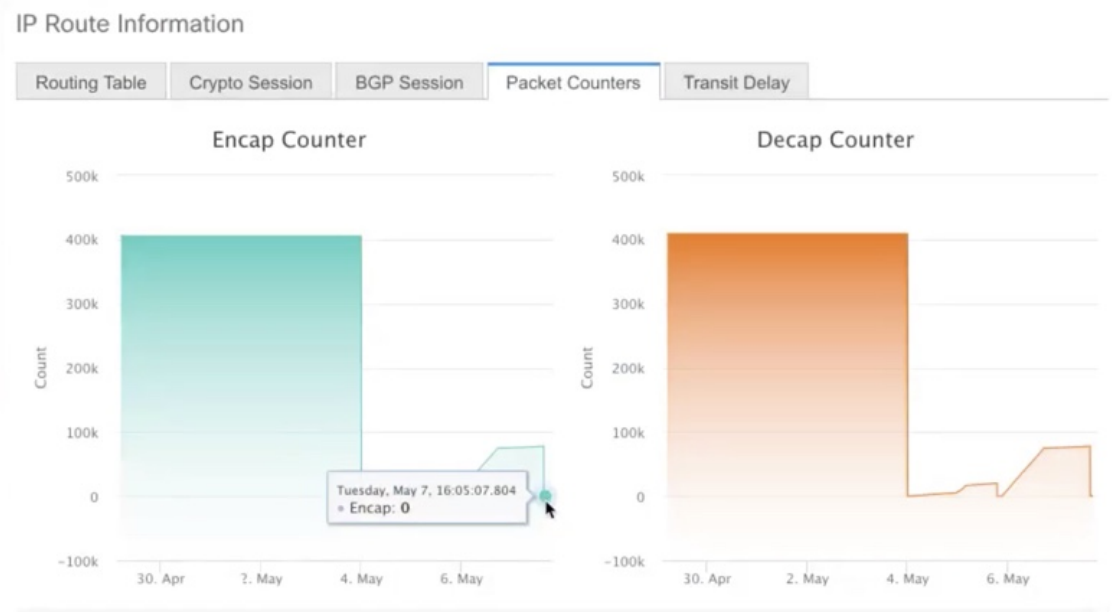
ステップ 3 クラウド拡張の下にある GET **/cloud-extension/status/{ipAddress}** API を展開します。

ステップ 4 on-prem コア ルータの IP アドレスを入力します。

ステップ 5 **[fetchLatestFromSwitch]** 値を **[true]** に設定します。

ステップ 6 [試行する（Try it out）] をクリックします。

パケット カウンタがクリアされ、カウントがゼロになります。



翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。