cisco.



Cisco NX-OS のハイブリッド クラウド接続展開

初版:2023年1月31日 最終更新:2023年4月17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/ © Cisco Systems, Inc. All rights reserved.



Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at:

http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



はじめに:	Trademarks iii
第 1 章	 新機能と更新情報 1 新機能と更新情報 1
第 部:	 ハイブリッド クラウドとマルチクラウド接続展開のインフラ構成を設定する 3
第 2 章	—— 概要 5
	ハイブリッド クラウド接続のコンポーネントを理解する 5
	ハイブリッド クラウド接続を構築 7
	用語 10
	前提条件 13
	注意事項と制約事項 13
	関連資料 14
第3章	ーー サポートされるトポロジ 15
	[Connection] のオプション 15
	IPsec(シングルクラウド)でサポートされるトポロジ 16
	IPsec(マルチクラウド)でサポートされるトポロジ 21
	IPSec なしてサポートされているトポロジ(シングル クラウド) 25
	IPsec なしでサポートされるトポロジ(マルチクラウド) 29
第4章	 ハイブリッド クラウドとマルチクラウド接続展開のインフラ構成を設定する 35
	ハイブリッド クラウドとマルチクラウド接続展開のインフラ構成のトポロジ例 35

オンプレミス NDFC ファブリックを設定 37

NDFC VXLAN ファブリックを作成 37

NDFC VXLAN ファブリックを作成 38

VXLAN ファブリックへのスイッチの追加 41

NDFC 外部ファブリックを構成 45

NDFC 外部ファブリックを作成 46

オンプレミス Cisco Catalyst 8000V を外部ファブリックに追加 49

クラウド サイト上のクラウド ネットワーク コントローラを展開します 55

AWS クラウド サイトのクラウド ネットワーク コントローラを展開 56

AWSの詳細設定で必要なパラメータを構成します 57

AWS のリージョン管理の必要なパラメータを構成します 58

Azure クラウド サイトのクラウド ネットワーク コントローラを展開 63 Azure の詳細設定で必要なパラメータを構成します 63

Azure のリージョン管理で必要なパラメーターを構成する 65

NDFC とクラウドサイトを ND と NDO に導入準備する 70

Complete サイト間の接続 NDFC と クラウド サイトの間 78

必要なコントロール プレーン構成を完了する 78

オンプレミス IPsec デバイス と IPSec トンネル サブネット プールを追加 80

NDFC 外部ファブリック内の外部デバイスのポートを追加する 87

VXLAN ファブリック サイトのマルチサイト VIP を定義します。 89

IPSec デバイスを VXLAN ファブリック サイトにマップする 90

NDFC VXLAN ファブリック内の BGW スパイン デバイスにポートを追加する 92 1 つ目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続する 94

1つ目のクラウドサイトを2つ目のクラウドサイトに接続する 97

2 つ目のクラウド サイトを NDFC VXLAN ファブリック サイトに接続する 99 Nexus ダッシュボード オーケストレータの構成を展開 102

第Ⅱ部: 使用例 107

第5章 テナントを展開 109

テナントを展開 109

vi

第6章

- ストレッチされた VRF ユース ケース 117 ストレッチされた VRF ユース ケースについて 117 ストレッチされた VRF ユース ケースの構成 118
- 第7章 ルートリークの使用例 155

ルートリークの使用例について 155

- 必要なテンプレートの構成 157
 - オンプレミス サイト テンプレートの構成 157
 - Azure サイトテンプレートの構成 166
 - AWS サイトテンプレートの構成 172
- ルートリークの設定 177
 - Azure VRF から NDFC VRF へのルート リークの構成 177 Azure VRF から AWS VRF へのルート リークの構成 179 AWS VRF から NDFC VRF へのルート リークの構成 182 AWS VRF から Azure VRF へのルート リークの構成 184 NDFC VRF から AWS VRF へのルート リークの構成 186 NDFC VRF から Azure VRF へのルート リークの構成 188 構成の確認 191

目次

I



新機能と更新情報

•新機能と更新情報 (1ページ)

新機能と更新情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、 今リリース までの変更点や新機能の一部は表に記載されていません。

リリース バージョン	特長	説明
NDFC リリース 12.1.2e	このユースケースドキュメン トの初版。	このユースケースドキュメン トの初版。

I



第 ■ 部

ハイブリッドクラウドとマルチクラウド 接続展開のインフラ構成を設定する

- •概要 (5ページ)
- ・サポートされるトポロジ (15ページ)
- ハイブリッドクラウドとマルチクラウド接続展開のインフラ構成を設定する(35ページ)



概要

- •ハイブリッドクラウド接続のコンポーネントを理解する (5ページ)
- •ハイブリッドクラウド接続を構築(7ページ)
- •用語 (10ページ)
- •前提条件 (13ページ)
- 注意事項と制約事項(13ページ)
- •関連資料 (14ページ)

ハイブリッドクラウド接続のコンポーネントを理解する

このドキュメントでは、Cisco Nexus ダッシュボードファブリック コントローラ (NDFC) に よって管理される Cisco Nexus 9000 NX-OS ベースのファブリックと Cisco クラウドネットワー クコントローラ (CNC) によって管理されるパブリッククラウドサイトを備えた、Cisco Nexus ダッシュボードオーケストレータ (NDO) によって強化された Cisco ハイブリッドクラウド ネットワーキング ソリューションの導入手順について説明します。

Cisco Nexus Dashboard Orchestrator(NDO)ベースのハイブリッドクラウドソリューションは、 オンプレミスネットワークとクラウドネットワーク間のシームレスな接続を提供します。こ のソリューションは、NDFC を使用してオンプレミスの VXLAN ベースのファブリックとオン プレミスの Cisco Catalyst 8000V を管理しますが、クラウドサイト(AWS または Microsoft Azure)は Cisco Cloud Network Controller(CNC)によって管理されます。NDOは、オンプレミ スサイトとクラウドサイト間、および2つ以上のクラウドサイト間の接続を調整するために 使用されます。VXLAN は、サイト間にオーバーレイトンネルを構築するために使用されま す。

次の図は、これらのコンポーネントを使用したハイブリッドクラウド接続のトポロジ例を示しています。詳細については、「サポートされるトポロジ(15ページ)」を参照してください。



このトポロジ例では、NDFC が管理するオンプレミス サイトに AWS および Azure クラウド サ イトへの安全な接続が設定されています。そこではインフラ VPC/VNet の上の Cisco Catalyst 8000Vは、オンプレミスデータセンターから来るそしてオンプレミスデータセンターへ向かう 全てのトラフィックのクラウド ゲートウェイの役割があります。

ボーダー ゲートウェイ (BGWs) でもある、様々なオンプレミス VXLAN EVPN サイトのシー ムレス Layer-2/Layer-3 DCI 拡張をサポートするオンプレミス サイト上で、 パブリック クラウ ドへ Layer-3 拡張もサポートします。

クラウド内の BGW と Cisco Catalyst 8000V 間のコントロール プレーンには BGP-EVPN が使用 され、データ プレーンには VXLAN が使用されます。

前の図に示すように、Cisco Hybrid クラウドネットワーキング ソリューションは次のコンポー ネントで構成されています。

- Cisco Nexus ダッシュボードオーケストレータ(NDO): NDOは、セントラルポリシー コントローラとして働き、様々なNDFCインスタンスに管理されている複数のオンプレミスファブリックに渡ってポリシーを管理します。そして、各クラウドサイトは、自分の Ciscoクラウドネットワークコントローラに抽象化されます。NDOはNexus ダッシュボー ド上のサービスとして実行されます。Nexus ダッシュボードは、VMware ESXi、Linux KVM、Amazon Web Services、または Microsoft Azure で実行される物理アプライアンスまたは仮想マシンのクラスタとして展開できます。以前にバージョン間サポートが導入されているため、NDOは、異なるソフトウェアバージョンを実行している Cisco クラウドネットワークコントローラを管理できます。
- •[Cisco Nexus ダッシュボードファブリック コントローラ (NDFC)]: NDFC は、LAN、 VXLAN、SAN、および Cisco IP Fabric for Media (IPFM) ファブリックを構築するための ネットワーク自動化およびオーケストレーションツールです。NDFC は、物理クラスタま たは仮想クラスターのいずれかである Nexus ダッシュボード クラスター上でサービスと して実行されます。ハイブリッド クラウド ネットワーキング ソリューションの場合、

NDFC はオンプレミスの VXLAN ファブリックとオンプレミスの Cisco Cloud Router (Catalyst 8000V)を管理します。

- オンプレミス VXLAN ファブリック:オンプレミス VXLAN ファブリックは、NDFC に よって管理される Nexus 90000/3000 スイッチで構築されています。ファブリックには、オ ンプレミス サイトとクラウドサイト間の VXLAN マルチサイト オーバーレイ トンネルの 開始と終了を担当する1つ以上のボーダー ゲートウェイ (BGW) デバイスが必要です。 NDFC には、VXLAN ファブリックを作成するための事前に作成されたテンプレートがあ ります。このドキュメントでは、VXLAN ファブリックに External_Fabric テンプレート を使用しています。
- オンプレミスの Cisco Cloud Router (CCR) : CCR は、オンプレミスの VXLAN ファブ リックとクラウドサイト間の到達可能性を提供するために使用されます。CCR は、パブ リックインターネットまたはプライベート接続(AWS Direct Connect や Azure ExpressRoute など)を使用してクラウドサイトへの接続を提供します。オンプレミスの CCR は、事前 に構築された External_Fabric テンプレートを使用して NDFC によって管理され、コア ルー タロールを割り当てる必要があります。

Cisco Catalyst 8000V は、Cisco ハイブリッド クラウド ネットワーキング ソリューション のオンプレミス CCR として使用されます。

- Cisco クラウドネットワークコントローラ(CNC): Cisco クラウドネットワークコント ローラは、サポートされているパブリッククラウド上で仮想インスタンスとして実行さ れ、パブリッククラウド内の自動接続、ポリシー変換、およびワークロードのさらなる可 視性を提供します。Cisco クラウドネットワークコントローラは、NDO から受け取った すべてのポリシーを変換し、それらをクラウドネイティブの構造、AWS の VPC やセキュ リティグループやMicrosoft Azure の VNet などにプログラムします。Cisco Cloud Network Controller は、AWS Marketplace や Azure Marketplace などのパブリッククラウドマーケッ トプレイスを通じて展開されます。
- Cisco Catalyst 8000V: Cisco Catalyst 8000Vは、パブリッククラウドプラットフォームの 重要なコンポーネントです。Cisco Catalyst 8000Vは、オンプレミスサイトおよびパブリッ ククラウドプラットフォームへのサイト間通信に使用されます。さらに、Cisco Catalyst 8000Vは、オンプレミスのクラウド接続と、さまざまなクラウドプロバイダー間の接続 (たとえば、Azure から AWS)に使用されます。

ハイブリッド クラウド接続を構築

このセクションでは、ハイブリッドクラウド接続を構築するために使用されるプロセスについて説明します。

- ・開始点 (8ページ)
- アンダーレイレイヤーの構築(8ページ)
- •オーバーレイの構築 (9ページ)

開始点

次の図は、ハイブリッドクラウド接続の開始点を示しています。ここには、ハイブリッドクラウド接続のコンポーネントを理解する (5ページ)で説明されているさまざまな部分があります:

- Nexus ダッシュボード ファブリック コントローラ (NDFC) のファブリック:
 - ・オンプレミスの VXLAN ファブリック
 - 外部ファブリック
- ・クラウドネットワーク コントローラによって管理されるクラウド サイト (AWS および Azure)

図2:



アンダーレイ レイヤーの構築

次に、後でアンダーレイがどのように構築されるかを示します。

- 1. まず、VXLANファブリックのボーダーゲートウェイスパインスイッチと外部ファブリッ クの Cisco Catalyst 8000V の間に BGP 接続が確立されます。
- 2. 次に、BGP ピアリングを使用して、外部ファブリックのオンプレミス Cisco Catalyst 8000V とクラウド サイトの各クラウド ルータ間のアンダーレイ接続を確立します。
- 3. 最後に、OSPF はクラウドサイト間でクラウド間アンダーレイ接続に使用されます。



図3:

オーバーレイの構築

最後に、前の手順で確立されたアンダーレイ接続の上にVXLANマルチサイトオーバーレイを 確立する方法を示します:

- 1. VXLAN マルチサイトが確立されます。これは、VXLAN ファブリックのボーダーゲート ウェイ スパイン スイッチから始まり、クラウド サイトの Cisco Catalyst 8000V で終了しま す。
- 2. 接続タイプとしてパブリックインターネットを選択した場合、IPsec と OSPF を使用して NDFC VXLAN ファブリック サイトとクラウド サイトの間を接続します。

図4:



用語

このマニュアルでは、次の用語を使用します。

用語	略語	定義
ボーダーゲートウェイ	BGW	NDFC 簡単ファブリック (VXLAN EVPN ファブリック など)でサポートされている スイッチロールの1つ。BGW は、オンプレミスファブリッ ク間のレイヤー2/レイヤー3 DCI 接続と、パブリック クラ ウドサイトへのレイヤー3 接 続(ハイブリッドクラウド接 続など)を拡張するために使 用されます。

用語	略語	定義
コア ルータ		NDFC 外部ファブリックでサ ポートされる役割の1つ。
		コア ルータは、一方の側で VXLAN EVPN ファブリック と、もう一方の側でクラウド サイトの Catalyst 8000V とのレ イヤ3 接続(アンダーレイ) を確立するために使用されま す。
直接接続		AWS クラウドで使用されま す。AWS 直接接続は、ネット ワークを AWS に直接リンクし て、一貫した低遅延のパ フォーマンスを提供するクラ ウドサービスです。
ExpressRoute		Azure クラウドで使用されま す。Azure ExpressRoute を使用 して、Azure データセンターと オンプレミスまたはコロケー ション環境のインフラストラ クチャとの間にプライベート 接続を作成できます。
サイト間ネットワーク	ISN	オンプレミスの VXLAN ファ ブリック間、およびパブリッ ククラウド(「アンダーレ イ」とも呼ばれる)と、オン プレミスの VXLAN ファブ リックをインターコネクトす るために使用されるレイヤー 3インフラストラクチャ。その ため、ISNには、インターネッ トまたは直接接続および ExpressRoute 専用回線を含める こともできます。

用語	略語	定義
IP セキュリティ ルータ	IPSec ルータ	オンプレミスサイトとクラウ ドサイト Cisco クラウドネッ トワーク コントローラの間で IPsec 接続を確立するには、イ ンターネット プロトコル セ キュリティ (IPsec)対応の ルータが必要です。
ルーティング サーバ	RS	コントロールプレーンノード は、オンプレミスの BGW デ バイス間の EVPN 隣接関係 (アジャセンシー)の確立を 容易にするために使用され、 それらすべての間にフルメッ シュピアリングを作成する必 要性を軽減します。ルート サーバーは BGP プロトコルを 実行し、2 つ以上の BGP ピア 間でルートを渡すために使用 されます。 ルート サーバ機能は、iBGP セッションに従来使用されて いた「ルートリフレクタ」機 能に相当する eBGP です。必 要な BGP ピアリングの数を減 らすのに役立ちます。
仮想ネットワーク	VNet	Azure クラウドで使用されま す。Azure Virtual Network (VNet) は、Azure のプライ ベートネットワークの基本的 な構成要素です。VNet を使用 すると、Azure 仮想マシン (VM) などのさまざまな種類 の Azure 情報技術が、相互、 インターネット、およびオン プレミスネットワークと安全 に通信できます。 クラウドネットワークコント ローラに関連して、クラウド ネットワーク コントローラの VRF は Azure の VNet にマッピ ングされます。

I

用語	略語	定義
仮想プライベートクラウド	VPC	AWS クラウドで使用されま す。Amazon 仮想 プライベー トクラウド (VPC) は、お客 様が定義する仮想ネットワー クでAWSの情報技術を起動で きるようにします。この仮想 ネットワークは、お客様自身 のデータセンターで運用され ている可能性がある従来型の ネットワークとよく似ている だけでなく、AWSの拡張可能 なインフラストラクチャを活 用するというメリットがあり ます。
		クラウドネットワークコント ローラに関連して、クラウド ネットワークコントローラの VRF は AWS の VPC にマッピ ングされます。

前提条件

次のソフトウェア バージョンが必要です。

- ・Cisco Nexus ダッシュボード (ND) バージョン 2.3.1c 以降(物理または仮想クラスタ)
- ・Cisco Nexus ダッシュボード ファブリック コントローラ (NDFC) バージョン 12.1.2e 以降
- Cisco Nexus ダッシュボード オーケストレータ (NDO) バージョン 4.1 (1) 以降
- AWS サイトおよび Microsoft Azure サイト用の Cisco クラウドネットワーク コントローラ (CNC) バージョン 25.1 (1e) 以降

注意事項と制約事項

以下は、ハイブリッドクラウド接続ソリューションを展開するときに理解する必要がある特定 のガイドラインと制限事項です。

・現在、各 Cisco クラウドネットワーク コントローラは、AWS および Azure クラウドで最大16のリージョンを管理できます。16を超えるリージョンを管理する場合は、追加のCisco クラウドネットワーク コントローラを展開する必要があります。詳細については、AWS インスール ガイドの Cisco クラウドネットワーク コントローラまたはAzure インスー

ルガイドの *Cisco* クラウドネットワーク コントローラ、リリース 25.1 (x) 以降の「サイト、リージョン、および CCR の数の制限について」セクションを参照してください。

関連資料

Cisco ハイブリッド クラウド ネットワーキング ソリューションを構成するコンポーネントの ドキュメントは、次の場所にあります:

- Cisco Nexus ダッシュボードオーケストレータ (NDO) ドキュメント
- Cisco Nexus ダッシュボードファブリック コントローラ (NDFC) ソリューション
- Cisco クラウドネットワーク コントローラ (CNC) ドキュメント
- Cisco キャタリスト 8000V ドキュメント
- Amazon Web Services (AWS) ドキュメント
- Microsoft Azureドキュメント



サポートされるトポロジ

- [Connection] のオプション (15 ページ)
- IPsec (シングルクラウド) でサポートされるトポロジ (16ページ)
- IPsec (マルチクラウド) でサポートされるトポロジ (21 ページ)
- IPSec なしてサポートされているトポロジ(シングル クラウド) (25 ページ)
- IPsec なしでサポートされるトポロジ(マルチクラウド) (29 ページ)

[Connection] のオプション

Cisco ハイブリッド クラウド ネットワーキング ソリューションでは、次の接続オプションを 使用できます:

- 「IPsec付き(With IPsec)]: オンプレミスのデータセンターからクラウドへの接続がパブ リックインターネットを介している場合、安全なチャネルを確立するために IPsecトンネ ルが必要です。この場合、ボーダーゲートウェイ(BGW)は、ASR 1000または、Cisco Catalyst 8000Vなどのオンプレミス IPsec-capable デバイスに接続されます。このデバイス は、クラウド内の Catalyst 8000Vとの IPsecトンネルを確立します。オンプレミスの BGW は、この「IPsec で保護されたアンダーレイ」を利用して、クラウド内の Catalyst 8000Vで VXLANトンネルを構築できます。
- •[IPsec 抜き(Without IPsec)]: BGW が直接接続(AWS) または、ExpressRoute(Azure) を使用してパブリック クラウドに接続されている場合、IPsec を有効にするのはオプショ ンです。この場合、オンプレミスの VXLAN EVPN データセンターとそれらの専用回線上 の Cisco Catalyst 8000V との間で VXLAN 接続が採用されます。

次のセクションでは、これらの接続オプションのいずれかを使用して使用できる、サポートさ れているトポロジに関する詳細情報を提供します。

- IPsec(シングルクラウド)でサポートされるトポロジ(16ページ)
- IPsec (マルチクラウド) でサポートされるトポロジ (21 ページ)
- IPSec なしてサポートされているトポロジ(シングル クラウド) (25 ページ)
- IPsec なしでサポートされるトポロジ(マルチクラウド) (29 ページ)

IPsec(シングルクラウド)でサポートされるトポロジ

次の表は、オンプレミスサイトとオンプレミスとクラウドサイトの間で BGP EVPN コント ロール プレーンの隣接関係を確立する方法と、オンプレミスサイトと1つのクラウドサイト 間のアンダーレイ接続を確立するために IPsec を利用する方法を示しています。



次の各図は、簡単な例を表示します。実際のシナリオでは、各ロールにデバイスが重複で展開 されている可能性があります。

オンプレミスの間の BGP EVPN	クラウドサイトへの BGP EVPN と IPsec		
	フルメッシュ	バフ サイトのみを通して	・BGP EVPN からクラウ ド サイトへ : フルメッ シュ
			・クラウド サイトへの IPsec:共有 IPsec ルー ター経由のみ
フルメッシュ	オプション1 (16ページ)	オプション3(18ページ)	オプション5(20ページ)
ルーティング サーバ付き	オプション2(17ページ)	オプション4(19 ページ)	該当なし

オプション1

次の図は、IPsec を使用してシングル クラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュBGPEVPN隣接関係(ア ジャセンシー)を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000V は、各オンプレミスサイトに展開されたコアルー タと IPsec トンネルを確立し、オンプレミスサイトのすべての BGW デバイスとフルメッシュ BGP EVPN 隣接関係(アジャセンシー)全てのを確立します。



次の図は、IPsec を使用してシングル クラウド接続の例を示しています。

- •BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係(アジャセンシー)と一緒 にルート サーバー (RS) コントロール プレーン ノードを確立 します。
- クラウドサイトの Cisco Catalyst 8000V は、各オンプレミスサイトに展開されたコアルー タとフルメッシュ IPsec トンネルを確立し、オンプレミスサイトのすべての BGW デバイ スと BGP EVPN 隣接関係(アジャセンシー)全てのを確立します。



(注) 現在、ルート サーバ コントロール ノードと Cisco Catalyst 8000V をピアリングすることはサポートされていません。



次の図は、IPsecを使用してシングルクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュBGPEVPN隣接関係(ア ジャセンシー)を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000V は、特定のオンプレミスハブサイトに展開された コアルータとのみ IPsec トンネルを確立し、ハブサイトの BGW デバイスとのみ BGP EVPN 隣接を確立します。
- ・サイト2(Cisco Catalyst 8000Vが EVPNに現れる)内で展開された BGW は、後ろにファ ブリックを持つことはできません。オンプレミスとクラウドサイトの間でプレフィックス を交換するためにのみ使用されます。



次の図は、IPsec を使用してシングル クラウド接続の例を示しています。

- •BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係(アジャセンシー)と一緒 にルート サーバー コントロール プレーン ノードを確立 します。
- クラウドサイトの Cisco Catalyst 8000V は、特定のオンプレミスハブサイトに展開された コアルータとのみ IPsec トンネルを確立し、ハブサイトの BGW デバイスとのみ EVPN 隣 接を確立します。
- ・サイト2(Cisco Catalyst 8000V が EVPNに現れる)内で展開された BGW は、後ろにファ ブリックを持つことはできません。オンプレミスとクラウドサイトの間でプレフィックス を交換するためにのみ使用されます。



次の図は、IPsecを使用してシングルクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュEVPN隣接関係(アジャセンシー)を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000Vは、オンプレミスサイトのすべての BGW デバイ スとのフルメッシュ BGP EVPN 隣接関係を確立します。
- ・クラウドサイトへの IPsec 接続は、共有 IPsec ルータのみを介して行われます。

図 **9**:



IPsec(マルチクラウド)でサポートされるトポロジ

次の表は、オンプレミスサイトとオンプレミスとクラウドサイトの間で BGP EVPN コント ロール プレーンの隣接関係を確立する方法と、オンプレミスサイトと複数のクラウドサイト 間のアンダーレイ接続を確立するために IPsec を利用する方法を示しています。



(注) 次の各図は、簡単な例を表示します。実際のシナリオでは、各ロールにデバイスが重複で展開 されている可能性があります。

オンプレミスの間 の BGP EVPN	クラウド サイトへの BGP EVPN と IPsec			クラウド サイト 間の BGP EVPN と IPsec
	フルメッシュ	バフ サイトのみ を通して	・BGP EVPN からクラウド サイトへ : フ ルメッシュ ・IPsec からク ラウド サイ トへ : ハブ サイト経由の み	
フルメッシュ	オプション 1 (21 ページ)	オプション 3 (23 ページ)	オプション 5 (24 ページ)	フルメッシュ
ルーティング サーバ付き	オプション 2 (22 ページ)	オプション 4 (23 ページ)	該当なし	

オプション1

次の図は、IPsecを使用したマルチクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュBGPEVPN隣接関係(ア ジャセンシー)を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000V は、各オンプレミスサイトに展開されたコアルー タと IPsec トンネルを確立し、オンプレミスサイトのすべての BGW デバイスとフルメッシュ EVPN 隣接関係(アジャセンシー)全てのを確立します。
- ・異なるクラウドサイトの Cisco Catalyst 8000V は、フルメッシュ IPsec トンネルとそれらの 間の EVPN 隣接を確立します。



次の図は、IPsec を使用したマルチクラウド接続の例を示しています。

- BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係(アジャセンシー)と一緒 にルート サーバー コントロール プレーン ノードを確立 します。
- クラウドサイトの Cisco Catalyst 8000V は、各オンプレミスサイトに展開されたコアルー タと IPsec トンネルを確立し、オンプレミスサイトのすべての BGW デバイスとフルメッシュ BGP EVPN 隣接関係(アジャセンシー)全てのを確立します。
- ・クラウドルータは、ハブサイトのBGWとBGP EVPNをピアリングします。

図 11:



次の図は、IPsecを使用したマルチクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュEVPN隣接関係(アジャセンシー)を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000V は、特定のオンプレミスハブサイトに展開された コアルータとのみ IPsec トンネルを確立し、ハブサイトの BGW デバイスとのみ EVPN 隣 接を確立します。
- ・異なるクラウドサイトの Cisco Catalyst 8000V は、フルメッシュ IPsec トンネルとそれらの 間の EVPN 隣接を確立します。
- サイト2(Cisco Catalyst 8000Vが EVPNに現れる)内で展開された BGW は、後ろにファ ブリックを持つことはできません。オンプレミスのとクラウドサイトの間のプレフィック スの交換のみに使用されています。

図 12:



オプション4

次の図は、IPsecを使用したマルチクラウド接続の例を示しています。

- •BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係(アジャセンシー)と一緒 にルート サーバー コントロール プレーン ノードを確立 します。
- クラウドサイトの Cisco Catalyst 8000V は、特定のオンプレミスハブサイトに展開された コアルータとのみ IPsecトンネルを確立し、ハブサイトの BGW デバイスとのみ BGP EVPN 隣接を確立します。
- ・クラウドルータは、ハブサイトのBGWとBGP EVPNをピアリングします。

 サイト2(Cisco Catalyst 8000V が EVPNに現れる)内で展開された BGW は、後ろにファ ブリックを持つことはできません。オンプレミスのとクラウドサイトの間のプレフィック スの交換のみに使用されています。

図 13:



オプション5

次の図は、IPsec を使用したマルチクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュEVPN隣接関係(アジャ センシー)を間に確立させます。
- クラウド サイトの Cisco Catalyst 8000V は、オンプレミス サイトのすべての BGW デバイ スとのフルメッシュ BGP EVPN 隣接関係を確立します。
- クラウドサイトの Cisco Catalyst 8000V は、特定のオンプレミス ハブサイトに展開された コア ルータとのみ IPsec トンネルを確立します。
- ・異なるクラウドサイトの Cisco Catalyst 8000V は、フルメッシュ IPsec トンネルとそれらの 間の EVPN 隣接を確立します。



IPSec なしてサポートされているトポロジ(シングルク ラウド)

次の表は、オンプレミス サイト間またはオンプレミスとクラウド サイト間で BGP EVPN コン トロール プレーンの隣接関係(アジャセンシー)を確立する方法を示しています。

オンプレミス サイト間の BGP EVPN	クラウド サイトへの BGP EVPN	
	フルメッシュ	ハブ サイト経由
フルメッシュ	オプション1 (25ページ)	オプション3(27ページ)
ルーティング サーバ付き	オプション2(26ページ)	オプション4(28ページ)

(注) 次の各図は、簡単な例を表示します。実際のシナリオでは、各ロールにデバイスが重複で展開 されている可能性があります。

オプション1

次の図は、IPsecを使用しないシングルクラウド接続の例を示しています。

 全てのオンプレミスサイトにあるBGWノードは、フルメッシュBGPEVPN隣接関係(ア ジャセンシー)を間に確立させます。 • クラウド サイトの Cisco Catalyst 8000V は、オンプレミス サイトのすべての BGW デバイ スとのフルメッシュ BGP EVPN 隣接関係を確立します。



オプション2

次の図は、IPsec を使用しないシングル クラウド接続の例を示しています。

- •BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係(アジャセンシー)と一緒 にルート サーバー (RS) コントロール プレーン ノードを確立 します。
- クラウド サイトの Cisco Catalyst 8000V は、オンプレミス サイトのすべての BGW デバイ スとのフルメッシュ BGP EVPN 隣接関係を確立します。



次の図は、IPsecを使用しないシングルクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュBGP EVPN隣接関係(ア ジャセンシー)を間に確立させます。
- クラウドサイトの Cisco Catalyst 8000Vは、ハブサイトの BGW デバイスとだけ BGP EVPN 隣接関係を確立します。
- サイト2(Cisco Catalyst 8000V が EVPNに現れる)内で展開された BGW は、後ろにファ ブリックを持つことはできません。オンプレミスとクラウドサイトの間でプレフィックス を交換するためにのみ使用されます。



次の図は、IPsec を使用しないシングル クラウド接続の例を示しています。

- BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係(アジャセンシー)と一緒 にルート サーバー コントロール プレーン ノードを確立 します。
- クラウドサイトの Cisco Catalyst 8000Vは、ハブサイトの BGW デバイスとだけ BGP EVPN 隣接関係を確立します。
- サイト2(Cisco Catalyst 8000V が EVPNに現れる)内で展開された BGW は、後ろにファ ブリックを持つことはできません。オンプレミスとクラウドサイトの間でプレフィックス を交換するためにのみ使用されます。


IPsec なしでサポートされるトポロジ (マルチクラウド)

次の表は、オンプレミス サイト間またはオンプレミスとクラウド サイト間で BGP EVPN コン トロール プレーンの隣接関係(アジャセンシー)を確立する方法を示しています。

オンプレミスの間の BGP EVPN	クラウド サイトへの B	クラウド サイト間の BGP EVPN	
	フルメッシュ	ハブ サイト経由	
フルメッシュ	オプション1(29 ページ)	オプション 3 (31 ページ)	フルメッシュ
ルーティング サーバ	オプション 2 (30 ページ)	オプション 4 (32 ページ)	

(注) 次の各図は、簡単な例を表示します。実際のシナリオでは、各ロールにデバイスが重複で展開 されている可能性があります。

オプション1

次の図は、IPsec を使用しないマルチクラウド接続の例を示しています。

 全てのオンプレミスサイトにあるBGWノードは、フルメッシュBGPEVPN隣接関係(ア ジャセンシー)を間に確立させます。

- クラウドサイトの Cisco Catalyst 8000Vは、オンプレミスサイトのすべての BGW デバイ スとのフルメッシュ BGP EVPN 隣接関係(アジャセンシー)を確立します。
- ・異なるクラウドサイトのCisco Catalyst 8000Vは、フルメッシュBGPとそれらの間のEVPN 隣接を確立します。

図 19:



オプション2

次の図は、IPsecを使用しないマルチクラウド接続の例を示しています。

- •BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係(アジャセンシー)と一緒 にルート サーバー コントロール プレーン ノードを確立 します。
- クラウドサイトの Cisco Catalyst 8000Vは、オンプレミスサイトのすべての BGW デバイ スとのフルメッシュ BGP EVPN 隣接関係(アジャセンシー)を確立します。
- ・異なるクラウドサイトのCisco Catalyst 8000Vは、フルメッシュ BGP とそれらの間の EVPN 隣接を確立します。



オプション3

次の図は、IPsecを使用しないマルチクラウド接続の例を示しています。

- 全てのオンプレミスサイトにあるBGWノードは、フルメッシュBGPEVPN隣接関係(ア ジャセンシー)を間に確立させます。
- ・クラウドサイトのCisco Catalyst 8000Vは、ハブサイトのBGWデバイスとだけBGP EVPN 隣接関係(アジャセンシー)を確立します。
- ・異なるクラウドサイトのCisco Catalyst 8000Vは、フルメッシュ BGP とそれらの間の EVPN 隣接を確立します。
- サイト2(Cisco Catalyst 8000Vが EVPNに現れる)内で展開された BGW は、後ろにファ ブリックを持つことはできません。オンプレミスのとクラウドサイトの間のプレフィック スの交換のみに使用されています。



オプション4

次の図は、IPsec を使用しないマルチクラウド接続の例を示しています。

- •BGW ノードは、全てのオンプレミス サイトに EVPN 隣接関係(アジャセンシー)と一緒 にルート サーバー コントロール プレーン ノードを確立 します。
- クラウドサイトのCisco Catalyst 8000Vは、ハブサイトのBGWデバイスとだけBGP EVPN 隣接関係(アジャセンシー)を確立します。
- ・異なるクラウドサイトのCisco Catalyst 8000Vは、フルメッシュ BGP とそれらの間の EVPN 隣接を確立します。
- サイト2(Cisco Catalyst 8000Vが EVPNに現れる)内で展開された BGW は、後ろにファ ブリックを持つことはできません。オンプレミスのとクラウドサイトの間のプレフィック スの交換のみに使用されています。



Cisco NX-OS のハイブリッド クラウド接続展開



ハイブリッド クラウドとマルチクラウド 接続展開のインフラ構成を設定する

- ハイブリッドクラウドとマルチクラウド接続展開のインフラ構成のトポロジ例(35ページ)
- •オンプレミス NDFC ファブリックを設定 (37 ページ)
- クラウド サイト上のクラウド ネットワーク コントローラを展開します (55 ページ)
- NDFC とクラウド サイトを ND と NDO に導入準備する (70ページ)
- Complete サイト間の接続 NDFC と クラウド サイトの間 (78ページ)

ハイブリッドクラウドとマルチクラウド接続展開のイン フラ構成のトポロジ例

次の図は、ハイブリッドクラウドおよびマルチクラウド接続の展開のインフラ構成に使用でき る、サポートされているトポロジの1つを示しています。



このドキュメントの手順では、IPsec(マルチクラウド)でサポートされるトポロジ(21ページ)のオプション1(21ページ)に基づく特定のユースケースとしてこのトポロジを使用し、このトポロジのユースケースに特化したハイブリッドクラウド接続オプションを構成する方法について説明します。

この展開手順では、IPsecを使用してマルチクラウド接続を構成し、これらのハイブリッドクラウド接続エリアのそれぞれで特定の構成を行います。全体的な構成手順は次のとおりです。

•NDFC のインストール

詳細については、次を参照します:

- Cisco Nexus ダッシュボードファブリック コントーラのインストールとアップグレードガイド、リリース 12.1.2 以降
- Cisco NDFC-Fabric コントローラ 構成ガイドリリース 12.1.2 以降
- *Cisco Nexus* ダッシュボードファブリック コントローラ導入ガイド、リリース 12.1.2 以降

•初期設定:

- ・オンプレミス NDFC ファブリックの設定
- Cisco Cloud ネットワーク コントローラのインスール
- クラウド サイトの設定
- •NDOのインストール
- •NDOを使用したハイブリッドクラウド接続の設定

- テナントとスキーマの展開:
 - ユース ケース1: ストレッチ VRF (VRF 内)
 - ユース ケース 2: ルートリーク (VRF 間)

オンプレミス NDFC ファブリックを設定

このセクションでは、2つのオンプレミス NDFC ファブリックを設定します:

- NDFC VXLAN ファブリック
- •NDFC 外部ファブリック

次のセクションの手順を実行して、2つのオンプレミス NDFC ファブリックを設定します。

NDFC VXLAN ファブリックを作成

この手順では、下で強調表示されているトポロジ例の一部を構成します。

図 24 :



VXLAN ファブリックには、オンプレミスファブリックとクラウドサイト間のVXLANマルチ サイト接続を構築するために使用される1つ以上のボーダーゲートウェイ(BGW)デバイス が含まれている必要があります。

次のセクションの手順を実行して、NDFC VXLAN ファブリックを構成します。

NDFC VXLAN ファブリックを作成

- **ステップ1** NDFC がインストールされている Nexus ダッシュボードにログインします。
- **ステップ2** NDFC アカウントにログインします。
- ステップ3 [ローカルエリアネットワーク(LAN)]>[ファブリック(ファブリック)]に移動します。 [LAN ファブリック(LAN Fabrics)] ウィンドウが表示されます。
- **ステップ4** [アクション(Actions)]>[ファブリックの作成(Create Fabric)をクリックします。 [ファブリックの作成(Create Fabric)] ウィンドウが表示されます。
- ステップ5 Easy Fabric テンプレートを使用して、NDFC VXLAN ファブリックの作成プロセスを開始します。
 - a) [ファブリック名(Fabric Name)] フィールドに NDFC VXLAN ファブリックの名前を入力します。
 - b) [テンプレートを選ぶ (Pick a Template)]エリアで、[テンプレートを選択 (Choose Template)]しま す。

[ファブリック テンプレートの選択(Select Fabric Template)] ウィンドウが表示されます。

- c) Easy_Fabric テンプレートを見つけてクリックします。
- d) [選択 (Select)]をクリックします。

図 **25** :

Select Fabric Template	\times
Q Search Fabric Template	
Easy_Fabric Fabric Template for a VXLAN EVPN deployment with Nexus 9000 and 3000 switches.	
Easy_Fabric_IOS_XE Fabric Template for a VXLAN EVPN deployment with CAT9000 switches.	
Easy_Fabric_eBGP Fabric Template for an eBGP based Fabric with Nexus 9000 and 3000 switches.	
External_Fabric Fabric Template for support of Nexus and non-Nexus devices.	
Fabric_Group Fabric Template that can contain other LAN Classic fabrics	
LAN_Classic Fabric Template to manage various switches and topologies	
LAN_Monitor This fabric template is used for NI in Monitor Mode Only.	
Selec	

ステップ6 必要な一般的な VXLAN ファブリック パラメータ構成を完了します。

Easy_Fabric テンプレートの次のパラメーター タブに入力する必要がありますが、このハイブリッドクラウドトポロジのユース ケースに固有のパラメーターは含まれていません。

- 一般的なパラメータ
- Replication
- VPC
- Protocols

通常どおり、これらのパラメータ タブで VXLAN ファブリック構成を完了します。詳細については、 [*Cisco Nexus* ダッシュボードファブリック コントローラ導入ガイド (*Cisco Nexus Dashboard Fabric Controller Deployment Guide*)]、リリース 12.1.2 以降を参照します。

たとえば、トポロジ例の情報を使用すると、**[一般パラメータ(General Parameters)]** ページの **[BGP ASN]** フィールドに 65084 と入力します。

図 **26** :

abric Name	
sydney	
ick Template	
asy_Fabric >	
General Parameters Replication VPC Protocols Adva	nced Resources Manageability Bootstrap Configuration Backup Flow Monitor
BGP ASN*	
65084	1-4294967295 1-65535[.0-65535] It is a good practice to have a unique ASN for each Fabric.
Enable IPv6 Underlay	If not enabled, IPv4 underlay is used
Enable IPv6 Link-Local Address	If not enabled, Spine-Leaf Interfaces will use global IPv6 addresses
Fabric Interface Numbering*	Numbered(Point-to-Point) or Unnumbered
Underlay Subnet IP Mask*	
30 ~	Mask for Underlay Subnet IP Range
Underlay Subnet IPv6 Mask	
Select an Option \checkmark	Mask for Underlay Subnet IPv6 Range
Underlay Routing Protocol*	
ospf 🗸 🗸	Used for Spine-Leaf Connectivity
Route-Reflectors*	
2 ~	Number of spines acting as Route-Reflectors

- **ステップ7** [詳細(Advanced)] パラメータ タブで、このハイブリッド クラウド トポロジのユース ケースに特に必要な構成を行います。
 - •[エニーキャスト ボーダー ゲートウェイの advertise-pip (Anycast Border Gateway advertise-pip)] フィールドを見つけ、ボックスをオンにしてこのオプションを有効にします。これにより、エニー キャスト ボーダー ゲートウェイ PIP が VTEP としてアドバタイズされます。

これは、サイト間でレイヤー3のみの接続(レイヤー2拡張機能がないなど)が確立されている場合に必要です。これは、ハイブリッドクラウドおよびマルチクラウドの展開に常に当てはまります。

•通常どおり、[詳細(Advanced)]パラメータ タブで残りの構成を完了します。

図 27:

Fabric Name sydney		VTEP HoldDown Time 180	NVE Source Inteface HoldDown Time (Min:1, Max:1500) in seconds
Pick Template		Brownfield Overlay Network Name Format	
Easy_Fabric >		Auto_Net_VNI\$\$VNI\$\$_VLAN\$\$VLAN_ID\$\$	Generated network name should be < 64 characters
General Parameters Replication VPC Protocols Adva	nced Resources Manageability Bootstrap	Enable CDP for Bootstrapped Switch	Enable CDP on management interface
VRF Template*		Enable VXLAN OAM	
Default_VRF_Universal	Default Overlay VRF Template For Leafs		Enable the Next Generation (NG) OAM feature for all switches in the fabric to aid in trouble-shooting VXLAN EVPN fabrics
Network Template*		Enable Tenant DHCP	
Default_Network_Universal	Default Overlay Network Template For Leafs		
VRF Extension Template*			Enable NX-API on port 443
Default_VRF_Extension_Universal \sim	Default Overlay VRF Template For Borders	Enable NX-API on HTTP port	
Network Extension Template*			Enable NX-API on port 80
Default_Network_Extension_Universal \sim	Default Overlay Network Template For Borders	Enable Policy-Based Routing (PBR)	
Overlay Mode		Enable Strict Config Compliance	
config-profile \checkmark	VRF/Network configuration using config-profile or CLI, default is config-profile		Enable bi-directional compliance checks to flag additional configs in the running config that are not in the intent/expected
Site Id			config
82	For EVPN Multi-Site Support (Min:1, Max: 281474976710655). Defaults to Fabric ASN	Enable AAA IP Authorization	Enable only, when IP Authorization is enabled in the AAA Server
Intra Fabric Interface MTU*		Enable NDFC as Trap Host	
9216	(Min:576, Max:9216). Must be an even number		Configure NDFC as a receiver for SNMP traps
Layer 2 Host Interface MTU*		Anycast Border Gateway advertise-pip	
9216	(Min:1500, Max:9216). Must be an even number		to advertise Anycast border cateway PIP as VTEP. Effective on MSD fabric 'Recalculate Config'

- **ステップ8** [情報技術 (Resources)] パラメータ タブをクリックし、このページに必要な値を入力します。
 - ・このハイブリッドクラウドのユースケース専用に、次のフィールドに適切な情報を入力します。
 - •[アンダーレイ ルーティング ループバック IP 範囲 (Underlay Routing Loopback IP Range)]: 通常、これは loopback0 の IP アドレス範囲です。
 - •[アンダーレイ VTEP ループバック IP 範囲(Underlay Routing Loopback IP Range)]: 通常、こ れは loopback1 の IP アドレス範囲です。
 - •[アンダーレイ VTEP ループバック IP 範囲(Underlay RP Loopback IP Range): エニーキャス トまたはファントム ランデブー ポイント (RP) IP アドレスの範囲.
 - •[アンダーレイサブネット IP 範囲(Underlay Subnet IP Range)]: アドレス範囲ピアリンク SVI IP アドレスの番号付されたものを割り当てする。
 - [VRF Lite サブネット IP 範囲(VRF Lite Subnet IP Range)]: P2P ファブリック間接続を割り 当てるアドレス範囲。
 - ・通常どおり、[情報技術(Resources)]パラメータタブで残りの構成を完了します。

図 28;

		Layer 2 VXLAN VNI Range*	
		30000-49000	Overlay Network Identifier Range (Min:1, Max:16777214)
		Layer 3 VXLAN VNI Range*	
		50000-59000	Overlay VRF identifier Range (Min:1, Max:16777214)
		Network VLAN Range*	
Fabric Name		2300-2999	Per Switch Overlay Network VLAN Range (Min:2, Max:4094)
sydney		VRF VLAN Range*	
Pick Template		2000-2299	Per Switch Overlay VRF VLAN Range (Min:2, Max:4094)
Easy_Fabric >		Subinterface Dot1q Range*	
Conoral Parameters - Paplication - VPC - Protocolo - Adu	anad Baseuraas Managashility Roststran	2-511	Per Border Dot1q Range For VRF Lite Connectivity (Min:2, Max:4093)
		VRF Lite Deployment*	
Manual Underlay IP Address Allocation		Manual ~	VRF Lite Inter-Fabric Connection Deployment Options
	Checking this will disable Dynamic Underlay IP Address Allocations	Auto Deploy Both	
			Whether to auto generate VRF LITE sub-interface and BGP
Underlay Routing Loopback IP Range*			peering configuration on managed neighbor devices. If set, auto
20.2.0.0/22	Typically Loopback0 IP Address Range	VDE Lite Subnet ID Pange*	created viol the inclinits will have who beputy ring related.
Underlay VTEP Loopback IP Range*		20.33.0.0/16	Address range to assign P2P Interfabric Connections
20.3.0.0/22	Typically Loopback1 IP Address Range	VDE Lite Subset Meets	
Underlay RP Loopback IP Range*	, ,	30	(Min:8, Max:31)
20.254.254.0/24	Assessed on Diseastone DD ID Address Danses		
20.234.234.0/24	Anycast of Phantom RP IP Address hange	Service Network VLAN Range*	
Underlay Subnet IP Range*		3000-3199	Per Switch Overlay Service Network VLAN Range (Min:2, Max:4094)
20.4.0.0/16	Address range to assign Numbered and Peer Link SVI IPs	Route Map Sequence Number Range*	
		1-65534	(Min:1, Max:65534)

ステップ9 [管理性]および[ブートストラップパラメータ]タブで、必要な一般的な VXLAN ファブリックパラメー タ設定を完了します。

> [管理性(Manageability)]および[ブートストラップ(Bootstrap)]パラメータタブの構成を完了する必要がある場合がありますが、これらには、このハイブリッドクラウドトポロジのユースケースに固有の パラメータは含まれていません。

ステップ10 [構成バックアップ(Configuration Backup)]パラメータ タブをクリックし、[毎時のファブリック バッ クアップ(Hourly Fabric Backup)]フィールドのチェックボックスをオンにして、その機能を有効にし ます。

通常どおり、[構成バックアップ(Configuration Backup)]パラメータタブで残りの構成を完了します。

ステップ11 VXLANファブリックの[ファブリックを作成(Create Fabric)]ウィンドウで必要な構成を完了したら、 [保存(Save)]をクリックします。 [LAN ファブリック(LAN Fabrics)]ウィンドウに戻り、作成したばかりのVXLANファブリックが表示 されます。

次のタスク

VXLAN ファブリックにスイッチを追加し、VXLAN ファブリックへのスイッチの追加(41 ページ)に記載されている手順を使用して、スイッチに必要な役割を設定します。

VXLAN ファブリックへのスイッチの追加

この手順では、スイッチをVXLANファブリックに追加し、スイッチに必要な役割を設定します。

始める前に

NDFC VXLAN ファブリックを作成 (38 ページ) で提供されている手順を使用して、NDFC VXLAN ファブリックを作成します。

ステップ1 [ローカル エリア ネットワーク(LAN) ファブリック(LAN Fabrics)] ウィンドウで、作成したばかりの VXLAN ファブリックをクリックします。

ファブリックの[概要(Overview)] ウィンドウが表示されます。

- (注) 次の手順では、NDFC がスイッチを検出できるようにするために必要な情報を手動で入力する方法について説明します。代わりに、管理IPアドレス、デフォルトルートとスイッチに構成済みの発見されなければならないスタートアップ構成などの特定のパラメータが既にない場合に便利な NDFC の Power On Auto Provisioning (POAP)機能を使用することもできます。POAPは、ネットワークに初めて展開されるデバイスに構成ファイルをインストールするプロセスを自動化し、手動構成を実行せずにデバイスを起動できるようにします。POAPの詳細については、「外部ファブリックおよびローカルエリアネットワーク(LAN)クラシックファブリックでのインバンド POAP 管理」および「NDFC でのインバンド POAP を使用したVXLAN ファブリックのゼロ タッチプロビジョニング」を参照してください。
- **ステップ2** [アクション(Actions)]>[スイッチを追加(Add Switches)]をクリックします。 [スイッチの追加(Add Switches)]ウィンドウが表示されます。
- **ステップ3** スイッチを検出するために必要な情報を追加します。
 - ・シード IP、ユーザー名、パスワードなど、スイッチを検出するために必要な情報をこのページに入力します。
 - スイッチの既存の構成を保持するかどうかを決定します。
 - これが既存の構成をスイッチに保持するブラウンフィールド展開の場合は、[構成を保持(Preserve Config)]チェックボックスをオンにして、それらの既存の設定を保持します。
 - これがグリーンフィールド展開の場合は、[構成を保持(Preserve Config)]チェックボックスを オフにして、スイッチの構成をクリーンアップします。
- ステップ4 [スイッチの検出(Discover Switches)] をクリックします。

表示される確認ポップアップウィンドウで[確認(Confirm)]をクリックします。

ステップ5 スイッチが検出されたら、スイッチを NDFC VXLAN ファブリックに追加します。

[発見結果(Discovery Results)]エリアで、適切なスイッチを選択します(該当する各スイッチの横にあるボックスをクリックします)。

例として、次の図は、ファブリックに追加される2つのリーフ スイッチと1つのスパイン スイッチを示 しています。 図 29:

sydney Password • Set		172.16.0.67-68,172.16.0	1.76	MD5	admin	
		Max Hops 2		Preserve config Disabled		
ck						
scovery Results						
ilter by attributes						
Switch Name	Serial Number	IP Address	Model	Version	Status	Progress
10.18.1.2		10.18.1.2	cisco C8000V	17.7.1a,		
ndfc-spine1	FD0243503ZG	172.16.0.76	N9K-C9332C	9.3(9)	Manageable	
ndfc-leaf2	FD02442054U	172.16.0.68	N9K-C9348GC-FXP	9.3(9)	Manageable	
ndfc-leaf1	FD02442051Z	172.16.0.67	N9K-C9348GC-FXP	9.3(9)	Manageable	
leaf1	96O0UQZJFTJ	172.16.0.77	N9K-C9300v	9.3(9)	Already Managed In Vsite1	
leaf2	97UVLYWGPAN	172.16.0.78	N9K-C9300v	9.3(9)	Already Managed In Vsite1	
spine1	95INZNPCD1D	172.16.0.79	N9K-C9500v	9.3(9)	Already Managed In Vsite1	
ACI-TA-SW	FOC1752R19H	172.16.0.3	N6K-C6001-64P	7.1(4)N1(1)	Manageable	
bgw2	91P6JV6YK6U	172.16.0.83	N9K-C9300v	9.3(9)	Manageable	
aci-tme-lab-mgmt	SAL184436V9	172.16.0.50	N9K-C9372PX	9.3(9)	Manageable	
10 ~ Rows					Page 1	of 2 ≪ < 1-10 of 14 > ≫

ステップ6 [スイッチの追加(Add Switches)]をクリックします。

- (注) [構成を保持(Preserve Config)]オプションがオンになっている場合、スイッチは NDFC VXLAN ファブリックに追加された後に再起動します。
- ステップ7 適切なスイッチの役割を[ボーダー ゲートウェイ スパイン (Border Gateway Spine)]に設定します。

これらの手順例では、1 つのスパインスイッチがスパインスイッチとボーダーゲートウェイスパイン スイッチの二重の役割を果たしているため、これらの手順例では、スパインスイッチの役割をボーダー ゲートウェイスパインスイッチに変更します。ただし、ご使用の環境では、2 つの別個のスイッチがあ り、1 つはスパインスイッチの役割を持ち、もう1 つはボーダーゲートウェイの役割を持っている場合 があります。

- a) NDFC VXLAN ファブリック概要ウィンドウの[スイッチ(Switches)] タブをクリックします。 このファブリックに追加されたスイッチが表示されます。
- b) スパイン スイッチの横にあるボックスをクリックしてそのスイッチを選択し、[アクション (Actions)]>[役割を設定(Set Role)]をクリックします。

図 **30**:

図 31 :

viev	v Switches Links	Interfaces Interfac	e Groups Po	olicies Networks \	/RFs Services E	vent Analytics His	tory Resources Vir	tual Infrastructure			
ilter	by attributes										Actions ~
	Switch	IP Address	Role	Serial Number	Config Status	Oper Status	Discovery Status	Model	VPC Role	VPC Peer	Add Switches
	ndfc-leaf1	172.16.0.67	Leaf	FDO2442051Z	In-Sync	Minor	Ok	N9K-C9348GC-FXP	Secondary	ndfc-leaf2	Preview
	ndfc-leaf2	172.16.0.68	Leaf	FDO2442054U	In-Sync	Minor	• Ok	N9K-C9348GC-FXP	Primary	ndfc-leaf1	Discovery
2	ndfc-spine1	172.16.0.76	Spine	FDO243503ZG	In-Sync	O Mir Spine	• Ok	N9K-C9332C			Set Role VPC Pairing
											TOR Pairing
											vPC Overview

c) [ロールの選択 (Select Role)] リストで [ボーダー ゲートウェイ スパイン (Border Gateway Spine)] ロー ルを見つけて選択し、[選択 (Select)]をクリックします。

Select Role	×
Q Search Role	
Spine (current)	
Leaf	
Border	
Border Spine	
Border Gateway	
Border Gateway Spine	
Super Spine	
Border Super Spine	
Border Gateway Super Spine	
ToR	
	Select

ステップ8 [ローカルエリアネットワーク(LAN)]>[ファブリック(Fabrics)]に移動し、作成した NDFC VXLAN ファブリックを選択します。

NDFC VXLAN ファブリックの [概要(Overview)]ページが表示されます。

- ステップ9 [スイッチ (Switches)]タブをクリックして、追加したスイッチが正しく表示されることを確認します。
- ステップ10 [アクション(Actions)]>[再計算と展開(Recalculate and Deploy)]をクリックします。

図 32:

Fat	orio	Overview	v - sydney								Actions 🔿	0? -
Ove	rview	/ Switches Lin	sks interfaces interfac	ce Groups Pol	icies Networks	VRFs Services E	vent Analytics His	tory Resources Vir	tual Infrastructure	Ed Að	l Fabric d Switches	
E	-ilter i	by attributes								Rec	re >	Actions ~
		Switch	IP Address	Role	Serial Number	Config Status	Oper Status	Discovery Status	Model	VPC Role	VPC Peer	Mode
		ndfc-leaf1	172.16.0.67	Leaf	FDO2442051Z	In-Sync	O Minor	Ok	N9K-C9348GC-FXP	Secondary	ndfc-leaf2	Normal
		ndlc-leaf2	172.16.0.68	Leaf	FDO2442054U	In-Sync	O Minor	• Ok	N9K-C9348GC-FXP	Primary	ndfc-leaf1	Normal
		ndfc-spine1	172.16.0.76	Border Gateway Spine	FDO243503ZG	In-Sync	© Minor	• Ok	N9K-C9332C			Normal

前述のように、これらの手順では、1 つのスパインスイッチがスパインスイッチとボーダー ゲートウェ イスパインスイッチの二重の役割を果たしているため、以下に示すように、これらの手順例ではスパイ ンスイッチの役割をボーダー ゲートウェイ スパイン スイッチに変更しました。これらの手順例では、 次の図に示すように、vPC ペアも 2 つのリーフ スイッチにすでに構成されています。vPC ペアの構成の 詳細については、*Cisco NDFC-Fabric* コントローラ構成ガイドリリース 12.1.2e 以降を参照してください。 図 33:

Fabric Overview - sydney											0?->
Overview Switches Links Interfaces Interface Groups Policies Networks VRFs Services Event Analytics History Resources Virtual Infrastructure											
Filte	r by attributes										Actions ~
	Switch	IP Address	Role	Serial Number	Config Status	Oper Status	Discovery Status	Model	VPC Role	VPC Peer	Mode
	ndfc-leaf1	172.16.0.67	Leaf	FD02442051Z	In-Sync	♥ Minor	• Ok	N9K-C9348GC-FXP	Secondary	ndfc-leaf2	Normal
	ndfc-leaf2	172.16.0.68	Leaf	FD02442054U	In-Sync	♥ Minor	Ok	N9K-C9348GC-FXP	Primary	ndfc-leaf1	Normal
	ndfc-spine1	172.16.0.76	Border Gateway Spine	FDO243503ZG	In-Sync	♥ Minor	• Ok	N9K-C9332C			Normal

次のタスク

NDFC 外部ファブリックを構成(45 ページ)で提供されている手順を使用して、NDFC 外部 ファブリックを設定します。

NDFC 外部ファブリックを構成

この手順では、下で強調表示されているトポロジ例の一部を構成します。下の図の例および ユースケースの手順全体では、Cisco Catalyst 8000V が外部ファブリックの IPsec デバイスとし て使用されていますが、IPsec をサポートしNDFC によって管理されていれば(たとえば、ASR 1000 および Catalyst 8000V)、外部ファブリックにはさまざまなタイプのデバイスが存在する 可能性があります。



NDFC 管理の外部ファブリックには、1 つ以上の IPsec デバイスが含まれています。IPsec デバ イスは、インターネット (パブリック)を介して、または直接接続(AWS)や ExpressRoute (Azure) などのプライベート接続によってクラウド ネットワークに接続できます。パブリッ クインターネットを使用してクラウドサイトに接続する場合、オンプレミスの IPsec デバイス とクラウド サイトの Catalyst 8000V の間に IPsec トンネルが確立されます。

次のセクションの手順を実行して、NDFC 外部ファブリックを構成します。

NDFC 外部ファブリックを作成

始める前に

これらの手順に進む前に、NDFC VXLAN ファブリックを作成 (38 ページ) に提供されてい る手順を完了してください。

- ステップ1 まだログインしていない場合は、NDFC アカウントにログインします。
- **ステップ2 [ローカルエリアネットワーク(LAN)]>[ファブリック(ファブリック)]**に移動します。
- ステップ3 [アクション(Actions)]>[ファブリックの作成(Create Fabric)をクリックします。 [ファブリックの作成(Create Fabric)] ウィンドウが表示されます。

ステップ4 External Fabric テンプレートを使用して、外部ファブリックを作成するプロセスを開始します。

External_Fabric テンプレートは、Nexus および Catalyst 8000V などの非 Nexus デバイスを使用して従来の LAN ファブリックを構築するために使用されます。

- a) [ファブリック名(Fabric Name)]フィールドに外部ファブリックの名前を入力します。
- b) [テンプレートを選ぶ (Pick a Template)] エリアで、[テンプレートを選択 (Choose Template)]しま す。

[ファブリック テンプレートの選択(Select Fabric Template)] ウィンドウが表示されます。

- c) External_Fabric テンプレートを見つけてクリックします。
- d) [選択 (Select)]をクリックします。

図 35 :

ې Search Fabric Template Easy_Fabric	
C Search Fabric Template Easy_Fabric	
Easy_Fabric	
Fabric Template for a VXLAN EVPN deployment with Nexus 900 switches.	00 and 3000
Easy_Fabric_IOS_XE Fabric Template for a VXLAN EVPN deployment with CAT9000 s	switches.
Easy_Fabric_eBGP Fabric Template for an eBGP based Fabric with Nexus 9000 and	d 3000 switches.
External_Fabric Fabric Template for support of Nexus and non Nexus devices.	
Fabric_Group Fabric Template that can contain other LAN Classic fabrics	
LAN_Classic Fabric Template to manage various switches and topologies	
LAN_Monitor This fabric template is used for NI in Monitor Mode Only.	
	Select
Choose Template	

- **ステップ5** [一般パラメータ (General Parameters)]タブで、このハイブリッドクラウドトポロジのユース ケースに 特に必要な構成を行います。
 - •BGP ASN フィールドで、BGP ASN を定義します。

たとえば、トポロジ例の情報を使用すると、このユース ケースの **BGP ASN** フィールドに 65080 と入 力します。

- •外部ファブリックをモニタリングするかどうかを決定します。
 - オンプレミスの IPSec デバイスを NDFC で管理する場合は、[ファブリックモニタモード(Fabric Monitor Mode)]フィールドの横にあるボックスをオフにして、このオプションの選択を解除します。
 - オンプレミスの IPsec デバイスが NDFC (Cisco 以外のサードパーティ ファイアウォールなど)に よって管理されない場合、ファブリックが監視のみされる場合は、[ファブリック モニタ モード (Fabric Monitor Mode)]フィールドの横にあるチェックボックスをオンにします。

図 **36** :

Create Fabric		
	Fabric Name ext-fab-1 Pick Template External_Fabric > Conserved Decemptors Addressed Decemptors Configuration	Pooluun Boototron FlourMonitor
	BGP AS #* 65080	1-4294967295 1-65535[.0-65535] It is a good practice to have a unique ASN for each Fabric.
	Enable Performance Monitoring (For NX-OS Switches Only)	If enabled, fabric is only monitored. No configuration will be deployed

ステップ6 必要な一般的な外部ファブリック パラメータ設定を完了します。

External_Fabric テンプレートの次のパラメーター タブに入力する必要がありますが、このハイブリッド クラウド トポロジのユース ケースに固有のパラメーターは含まれていません。

•詳細設定

• 関連資料

- ・コンフィギュレーションのバックアップ
- ・ブートストラップ
- Flow Monitor

たとえば、[構成バックアップ(Configuration Backup)]パラメータタブで、[時間単位のファブリックバッ クアップ(Hourly Fabric Backup)] フィールドのボックスをチェックして、その機能を有効にすることが できます。

詳細については、[*Cisco Nexus* ダッシュボードファブリックコントローラ導入ガイド(*Cisco Nexus Dashboard Fabric Controller Deployment Guide*)]、リリース 12.1.2 以降を参照します。

ステップ7 外部ファブリックの[ファブリックを作成(Create Fabric)]ウィンドウで必要な構成を完了したら、[保存 (Save)]をクリックします。

[LAN ファブリック(LAN Fabrics)] ウィンドウに戻り、作成したばかりの外部ファブリックが表示されます。

次のタスク

オンプレミスの Cisco Catalyst 8000V を外部ファブリックに追加し、オンプレミス Cisco Catalyst 8000V を外部ファブリックに追加 (49 ページ) で提供されている手順を使用して必要なロールを設定します。

オンプレミス Cisco Catalyst 8000V を外部ファブリックに追加

次の手順に従って、オンプレミスの Cisco Catalyst 8000V を外部ファブリックに追加し、Cisco Catalyst 8000V に必要な役割を設定します。

始める前に

NDFC 外部ファブリックを作成(46 ページ)で提供されている手順を使用して、NDFC 外部 ファブリックを作成します。

ステップ1 [ローカル エリア ネットワーク(LAN) ファブリック(LAN Fabrics)] ウィンドウで、作成したばかりの 外部ファブリックをクリックします。

ファブリックの[概要(Overview)] ウィンドウが表示されます。

- **ステップ2** [アクション(Actions)]>[スイッチを追加(Add Switches)] をクリックします。 [スイッチの追加(Add Switches)] ウィンドウが表示されます。
- **ステップ3** Cisco Catalyst 8000V を検出するために必要な情報を追加し、[スイッチを発見(Discover Switches)]をク リックします。
 - Cisco Catalyst 8000V の[シード IP (Seed IP)]フィールドに必要な情報を入力します。
 - •[デバイスタイプ(Device Type)]フィールド内で IOS-XEを選択します。
 - ・[デバイス タイプ (Device Type)]フィールドが表示されたら、その下にある [CSR/C8000V] オプション を選択します。

図 37:

Add Switches	? ×
Critich Addition Michanism* More Weighbor Switches Seed Switch Details Seed 200* Seed 200* Device Type* Device Type* </td <td></td>	
	Close Discover Switches

ステップ4 [スイッチの検出 (Discover Switches)]をクリックします。

表示される確認ポップアップウィンドウで[確認(Confirm)]をクリックします。

ステップ5 Cisco Catalyst 8000V が検出されたら、Cisco Catalyst 8000V を外部ファブリックに追加します。

[発見結果(Discovery Results)]エリアで、Cisco Catalyst 8000V を選択し(Cisco Catalyst 8000Vの隣のボックスをクリック)、[スイッチを追加(Add Switches)]をクリックします。

図 **38** :

dd S	witches							? >
Switch A	ddition Mechanism* over O Move Neighb	or Switches						
Seed	Switch Details							
Fabric ext-fal	o-1		Switch 172.16.0.234		Authentication Protocol MD5	Username admin		
Passwe Set	ord		Max Hops 0		Preserve config Enabled			
← Back								
Disco	very Results							
Filter	by attributes							
	Switch Name	Serial Number	IP Address	Model	Version	Status	Progress	_
	C8K3-Fab2	98JE1U8CZ8M	172.16.0.234	C8000V	17.7.1a	Manageable		
							Close	d Switch

ステータスが[スイッチが追加されました(Switch Added)]に変わります。[閉じる(Close)]をクリック してウィンドウを閉じます。

図 **39**:

dd S	witches						?	
Switch A	ddition Mechanism* over O Move Neighbo	or Switches						
Seed	Switch Details							
Fabric ext-fal	p-1		Switch 172.16.0.234		Authentication Protocol MD5	Username admin		
Password Max Hops Set 0				Preserve config Enabled				
← Back								
Disco	very Results							
Filter	by attributes							
	Switch Name	Serial Number	IP Address	Model	Version	Status	Progress	
	C8K3-Fab2	98JE1U8CZ8M	172.16.0.234	C8000V	17.7.1a	Switch Added		

ステップ6 Cisco Catalyst 8000Vの役割を[コアルータ (Core Router)]に設定します。

a) Cisco Catalyst 8000Vの横にあるボックスをクリックしてそのルータを選択し、[アクション(Actions)]> [セットロール(Set Role)]をクリックします。 図 40:

Fab	Fabric Overview - ext-fab-1										O? –	
Over	Overview Switches Links Interfaces Policies Event Analytics History Resources Virtual Infrastructure											
F	Filter by attributes											
		Switch	IP Address	Role	Serial Number	Config Status	Oper Status	Discovery Status	Model	VPC Role	VPC Peer	Add Switches
	-	C8K3-Fab2	172.16.0.234	Edge Router	98JE1U8CZ8M	• NA	Healthy	• Ok	C8000V			Preview Deploy
												Discovery Set Role
												vPC Pairing
												vPC Overview
												More

b) [ロールの選択(Select Role)] リストで [コア ルータ (Core Router)] ロールを見つけて選択し、[選択 (Select)] をクリックします。

NDFC が BGP プロトコルを自動的に有効にするように、すべての Catalyst 8000V を [コア ルータ (core Router)] ロールに設定する必要があります。

図 41 :

Select Role	×
Q Search Role	
Spine	
Leaf	
Super Spine	
Edge Router (current)	
Core Router	
Se	elect

ステップ7 [ローカルエリアネットワーク(LAN)]>[ファブリック(Fabrics)]に移動し、作成した外部ファブリッ クを選択します。

外部ファブリックの[概要(Overview)]ページが表示されます。

ステップ8 [スイッチ (Switches)] タブをクリックして、追加した Cisco Catalyst 8000V が正しく表示されることを確認します。

図 42:

Fabr	abric Overview - ext-fab-1										ン? - ×
Overvi	Overview Switches Links Interfaces Policies Event Analytics History Resources Virtual Infrastructure										
Filt	er by attributes										Actions >
	Switch	IP Address	Role	Serial Number	Config Status	Oper Status	Discovery Status	Model	VPC Role	VPC Peer	Mode
	C8K3-Fab2	172.16.0.234	Core Router	98JE1U8CZ8M	• NA	C Healthy	Ok Ok	C8000V			Normal
											_

ステップ9 [アクション(Actions)]>[再計算と展開(Recalculate and Deploy)]をクリックします。

プロセスのこの時点で、[ローカルエリアネットワーク(LAN)]>[ファブリック(Fabrics)]に移動する と表示されるように、VXLAN と外部ファブリックは NDFC で構成されます。

図 **43** :

≡ داندان دانده Nexus Dashboard	d 🕴 💮 One V	iew ~				Feedback 👤 (
F Fabric Controller										
🎓 Dashboard	Dashboard LANL Fabrica									
💥 Topology	LANTA	brics				e				
≡ LAN ^	Filter by at	tributes				(Actions ~				
Fabrics		Palada Nama	Polode Technology	Pakels Torra	400	Patrix Hardet				
Switches	_	Fabric Name	Fabric Technology	Fabric Type	ASN	Fabric Health				
Interfaces	0	Sydney	VXLAN Fabric	Switch Fabric	65084	♥ Minor				
Services	0	ext-fab-1	External	External	65080	♥ Healthy				
📥 Virtual Management 🗸 🗸										

[トポロジ(Topology)] ビューを使用して、プロセスのこの時点で次の構成を決定することもできます:

• VXLAN と外部ファブリックの間にまだ接続がないこと:

図 44:



この NDFC では VMM ビジュアライザ機能が有効になっているため、IP アドレスが 172.16.0.252 の vCenter アイコンがトポロジビューに表示されます。VMM 機能の詳細については、*Cisco NDFC-Fabric* コントローラ 構成ガイドの仮想インフラストラクチャ マネージャの章を参照してください。

• VXLAN ファブリックにネットワークまたは VRF がまだ作成されていないこと:

図 45 :

≡	🔅 One View 🗸			
F Fabric Controller				
🏫 Dashboard	Data Center / Sydney			
% Topology	View A Searc	h by Attributes		
	(+ - / 0 🗎 X)			
Fabrics	Show Logical Links			
Switches	Operation Configuration		NET	
Interfaces	Ceperation comingatured			
Services	Hierarchical		INCLINITIES (U) VRFS (U)	VIVI (3)
📥 Virtual Management 🔍	In-Sync			
🔅 Settings 🗸 🗸	Pending			
_r⁰ Operations ∨	In Progress			
	Out-of-Sync			
	• NA			
	Multi-select			
	0 selected			
			ndfc/spine1	
			ndfc-leaf2 ndfc-	leaf1

次のタスク

クラウド サイト上のクラウド ネットワーク コントローラを展開します (55 ページ) で提供 されている手順を使用して、クラウド サイトにクラウド ネットワーク コントローラを展開し ます。

クラウド サイト上のクラウド ネットワーク コントロー ラを展開します

このセクションでは、下で強調表示されているトポロジ例の一部を構成します。



ハイブリッドクラウドトポロジの例に基づいて、これらの手順では、クラウドネットワーク コントローラを介して2つのクラウドサイト(AWSおよびAzureクラウドサイト)をセット アップすることを想定しています。したがって、これらの手順全体で次のドキュメントを参照 します。

- AWS インストール ガイド、リリース 25.1 (x) 以降の Cisco クラウド ネットワーク コント ローラ
- AWS ユーザー ガイド、リリース 25.1 (x) 以降の Cisco クラウド ネットワーク コントロー ラ
- Azure インストール ガイド、リリース 25.1 (x) 以降の Cisco クラウド ネットワーク コン トローラ
- Azure ユーザーガイド、リリース 25.1 (x) 以降の Cisco クラウドネットワーク コントロー ラ

以下のセクションの手順を実行して、クラウドネットワーク コントローラをクラウドサイト に展開します。

AWS クラウド サイトのクラウド ネットワーク コントローラを展開

これらのセクションの手順に従って、AWS クラウド サイトにクラウド ネットワーク コント ローラを展開します。

AWS の詳細設定で必要なパラメータを構成します

このセクションでは、この例のハイブリッドクラウドトポロジ専用に、[クラウドネットワー クコントローラのセットアップ(Cloud Network Controller Setup)]ページの[詳細設定 (Advanced Settings)]エリアで、AWS クラウド サイトに必要な構成を行います。

[Azure インストールガイドの Cisco クラウドネットワーク コントローラ (Cisco Cloud Network Controller for AWS Installation Guide)]の「Configuring Cisco Cloud Network Controller Using the Setup Wizard」の章に記載されている手順を使用しますが、[クラウドネットワークコントロー ラ 設定 (Cloud Network Controller Setup)]ページには、この例のハイブリッド クラウドト ポロジの場合のために具体的に構成する必要がある2つのエリアがあることに注意してください:

- コントラクトベースのルーティング(Contract-based routing): クラウドネットワーク コントローラは、次の2種類のモードをサポートしています。
 - 契約ベースのルーティング
 - •ルートマップベースのルーティング

契約ベースのルーティングとは、EPG 間の契約が VRF 間のルーティングを駆動すること を意味しますが、このタイプの契約ベースのルーティングは NDFC では使用できないた め、この特定の例のハイブリッド クラウド トポロジでは、契約ベースのルーティングを オフにして、代わりにルート マップ ベースのルーティングを使用します。詳細について は、AWS ユーザー ガイドの Cisco クラウド ネットワーク コントローラ、リリース 25.1 (x) 以降の「ルーティング ポリシー」および「グローバル Inter-VRF ルート リーク ポリ シー」 セクションを参照してください。

- クラウドネットワークコントローラのアクセス権限:デフォルトでは、クラウドネット ワークコントローラにはルーティングとセキュリティのアクセス権限があります。つま り、クラウドネットワークコントローラはネットワークを自動化できるだけでなく、ク ラウド上のセキュリティグループを自動化および構成することもできます。クラウドネッ トワークコントローラがセキュリティグループを自動化して構成する場合、EPGと契約 も構成する必要があります。ただし、EPGと契約は、ルーティングの自動化のみが必要な NDFC エンドユーザーには適用されません。NDO および NDFC とうまく統合するには、 クラウドネットワークコントローラのアクセス権限オプションをルーティングのみに設 定する必要があります。
- ステップ1 AWS の Cisco Cloud Network Controller にログインします。
- **ステップ2** この例のハイブリッド クラウド トポロジ用に、1 番目のクラウド サイトである AWS クラウド サイトを セットアップするプロセスを開始します。

AWS インストールガイドの Cisco クラウド ネットワーク コントローラ、リリース 25.1 (x) 以降の最初の 数章には、このハイブリッド クラウド トポロジのユース ケースに固有ではない一般的な情報が含まれて いるため、そのドキュメントのこれらの章の手順を完了してから、ここに戻ります:

• 概要

• Cisco クラウド ネットワーク コントローラのインストールの準備

・Cisco Cloud Network Controller のクラウド形成テンプレート情報の構成

ステップ3 Cisco Cloud Network Controller GUI で、インテントアイコン(²) をクリックし、[Cloud Network Controller **セットアップ**(Cloud Network Controller Setup)] を選択します。

[基本を構成しましょう(Let's Configure the Basics)] ページが表示されます。

- ステップ4 [詳細設定(Advanced Settings)]エリアを探し、[構成の編集(Edit Configuration)]をクリックします。
- ステップ5 [詳細設定(Advanced Settings)]ページで、次の構成を設定します。
 - [契約に基づいたルーティング (Contract Based Routing)]:ボックスがオフになっていることを確認 します(この機能が有効になっていないことを確認します)。これにより、契約ベースのルーティング が無効になり、代わりにルートマップベースのルーティングが使用されます。
 - ・クラウドネットワークコントローラのアクセス権限:[ルーティングのみ(Routing Only)]オプションを選択します。
- ステップ6 [保存して続行 (Save and Continue)]をクリックします。

[基本を構成しましょう(Let's Configure the Basics)]ページに戻ります。

次のタスク

AWSのリージョン管理の必要なパラメータを構成します(58ページ)の手順を実行します。

AWS のリージョン管理の必要なパラメータを構成します

このセクションでは、この例のハイブリッドクラウドトポロジー専用に、[クラウドネット ワークコントローラ (Cloud Network Controller Setup)]のセットアップページの[リージョン 管理 (Region Management) エリアで AWS クラウド サイトに必要な構成を行います。

始める前に

AWS の詳細設定で必要なパラメータを構成します (57 ページ) に挙げられている手順を完 了します。

ステップ1 [リージョン管理(Region Management)エリアを探して適切なボタンをクリックします。

クラウドネットワーク コントローラを初めてセットアップする場合は [開始(Begin)] をクリックし、 以前にこのクラウドネットワーク コントローラでリージョン管理を既に構成している場合は [構成の編 (Edit Configuration)] をクリックします。

ステップ2 AWS トランジット ゲートウェイを有効化

普段、Transit Gateway を使用して、リージョン内および TGW ピアリングがサポートされているリージョン間の接続に VPN トンネルを使用しないようにします。詳細については、ドキュメント「AWS トラン

ジット ゲートウェイまたは AWS トランジット ゲートウェイ コネクトを使用した VPC 間の帯域幅の増加」を参照してください。

特に、このハイブリッドクラウドトポロジのユースケースの例では、[トランジットゲートウェイの使用(Use Transit Gateway)]エリアで、[有効化(Enable)]の横にあるチェックボックスをクリックして AWS Transit Gateway を使用します。これにより、以降の手順で TGW Connect を有効にするために必要な ハブネットワークを追加できます。

ステップ3 [管理するリージョン (Regions to Manage)]領域で、Cisco Cloud Network Controller のホーム リージョン が選択されていることを確認します。

Cisco Cloud ネットワーク コントローラを AWS に最初に展開したとに選択したリージョンは、ホーム リージョンであり、このページで既に選択されいているはずです。これは、Cisco Cloud Network Controller が展開されるリージョン (Cisco Cloud Network Controller によって管理されるリージョン) で、[リージョン (Region)]列に「Cisco Cloud Network Controller」というテキストが表示されます。

ステップ4 Cisco クラウドネットワーク コントローラ で追加のリージョンを管理します。他のリージョンで Inter-VPC 通信と Hybrid-Cloud、Hybrid Multi-Cloud、または Multi-Cloud 接続を行うように Cisco Catalyst 8000Vs を 展開する場合は、追加のリージョンを選択します。

Cisco Catalyst 8000V は、Cisco Cloud Network Controller が導入されているホーム リージョンを含む、最大 4 つのリージョンにハイブリッド クラウドおよびマルチクラウド接続を提供できます。

ステップ5 リージョンにローカルにクラウドルータを展開するには、そのリージョンの Catalyst 8000Vs チェック ボックスにチェック マークをつけるためにクリックします。

> Catalyst 8000V が展開されているリージョンが少なくとも1つ必要です。ただし、このページで複数の リージョンを選択した場合は、選択したすべてのリージョンに Catalyst 8000V を設定する必要はありません。

ステップ6 AWS トランジット ゲートウェイ統計を使用する場合は、1 つ以上のリージョンの [TGW 統計(TGW Stats)]列のボックスをオンにします。

チェックボックスをオンにすると、指定したリージョンのインフラ テナントの AWS トランジット ゲー トウェイ トラフィック統計の収集が有効になります。

(注) AWS トランジット ゲートウェイの統計情報を収集するには、フロー ログを作成する必要もあります。AWS ユーザー ガイドの Cisco クラウド APIC リリース 25.1 (x) 以降の「Cisco Cloud APIC Statistics」の章の「Enabling VPC Flow Logs」セクションを参照してください。

特に、この例のハイブリッド クラウド トポロジのユース ケースでは、次のようになります。

- ・米国東部(バージニア北部)リージョンと米国西部(北カリフォルニア)リージョン(us-east-1およびus-west-1 リージョン)の隣のチェックボックスにチェックマークを付けます。
- Cisco クラウド ネットワーク コントローラ ホーム リージョンの Catalyst 8000V および TGW Stats 列のチェック ボックスにチェック マークを付けます。

図 47:

Setup -	- Region Managem	nent				×
		0	2			
		Regions to Manage	General Connectivity			
		External Cload Network Controller	Enter-Site Connectivey	Transit Gateway	Inter-Region Connectivity	
		Di-Premises ACI Ste	work Controller and which regions should host Clo	Catalyst 8000V	be deployed in at least one region to enable connectivity	
		(i) Please note that CSR is now changed t	o Catalyst 8000V.			
		Use Transit Gateway () C Enable Regions to Manage * ()				
		Region Name	Region	Catalyst 8000Vs 🔮	TGW Stats 🔴	
		Africa (Cape Town)	af-south-1			
		Asia Pacific (Hong Kong)	ap-east-1			
		Asia Pacific (Tokyo)	ap-northeast-1			
		Asia Pacific (Seoul)	ap-northeast-2			
		Asia Pacific (Osaka-Local)	ap-northeast-3			
		Asia Pacine (Mumbai)	ap-south- i			
		Asia Pacific (Singapore)	ap-southeast-1			
		Asia Pacific (Sydney)	ap-southeast-2			
		Asia Pacific (Jakarta)	ap-southeast-3			
		Canada (Central)	ca-central-1			
		EU (Frankfurt)	eu-central-1			
		EU (Stockholm)	eu-north-1			
		Europe (Milan)	eu-south-1			
		EU (Ireland)	eu-west-1			
		EU (London)	eu-west-2			
		EU (Paris)	eu-west-3			
		Middle East (Bahrain)	me-south-1			
		South America (Sao Paulo)	sa-east-1			
		US East (N. Virginia)	us-east-1		V	
		US East (Ohio)	us-east-2		V	
		US West (N. California)	us-west-1			
		US West (Oregon)	US-West-2 Cloud Network Controller Deployed		Z	
					Back to Overvi	W Previous Next Save and Continue

ステップ7 適切なリージョンをすべて選択したら、ページの下部にある[Next]をクリックします。

[General Connectivity]ページが表示されます。

ステップ8 [一般接続(General Connectivity)]ページで必要な構成を行います。

詳細については、[AWS 設置ガイドの Cisco クラウド ネットワーク コントローラ (Cisco Cloud Network Controller for AWS Installation Guide)]リリース 25.1 (x) 以降のセットアップウィザードを使用した Cisco Cloud Network Controller の構成の章を参照してください。

特に、このハイブリッドクラウドトポロジのユースケースの例では、次の手順の手順を使用してハブネットワークを追加します。

Cisco クラウドネットワーク コントローラ では、2 つ以上の AWS Transit Gateway の集合を[ハブネット ワーク(hub network)]と呼びます。ハブネットワークは、VRFのネットワーク分離を提供します。VRF のグループをハブネットワークに接続して、VRFのグループを他のハブネットワークに接続されている 他のVRFから分離することができます。ハブネットワークは、リージョンごとに少なくとも2つのAWS Transit Gateway を作成します。

ステップ9 [ハブネットワーク(Hub Network)]領域で、[ハブネットワークの追加(Add Hub Network)]をクリッ クします。

[ハブネットワークの追加(Add Hub Network)] ウィンドウが表示されます。

- **ステップ10 [名前 (Name)]**フィールドにハブ ネットワークの名前を入力します。
- ステップ11 [BGP Autonomous System Number] フィールドに、AWS でゼロを入力して番号を選択するか、各ハブネットワークの値を 64512 〜 65534 の範囲で入力し、フィールドの横にあるチェック マークをクリックします。

たとえば、ハイブリッドクラウドトポロジの例の情報を使用すると、このフィールドに 65091 と入力します。

ステップ12 AWS Transit Gateway Connect 機能を有効にする場合は、[**TGW Connect**] フィールドで[**有効化**(**Enable**)] の横のチェック ボックスをクリックします。

このハイブリッドクラウドトポロジのユースケースの例では、AWS Transit Gateway Connect 機能を有効 にします。詳細については、AWSトランジットゲートウェイまたはAWSトランジットゲートウェイ コ ネクトを使用した VPC 間の帯域幅の増加 を参照してください。

ステップ13 [CIDR] 領域で、[Add CIDR] をクリックします。

これは、AWS トランジット ゲートウェイ接続 CIDR ブロックで、トランジット ゲートウェイ側の接続 ピア IP アドレス(GRE 外部ピア IP アドレス)として使用されます。

- a) [Region (リージョン)]フィールドで、[リージョンを選択 (Select Region)]をクリックして適切な リージョンを選択します。
- b) CIDR フィールドに、中継ゲートウェイ側の接続ピア IP アドレスとして使用される CIDR ブロック を入力します。

図 **48** :

IDR		
Region *	CIDR *	
Select Region >		

- c) この CIDR ブロックのこれらの値を受け入れるには、チェックマークをクリックします。
- d) AWSトランジットゲートウェイ接続機能を使用するすべての管理対象リージョンに対して、これらの管理対象リージョンのそれぞれに使用する CIDR ブロックを追加します。

図 49:

Add Hub Network		×
Name *		
hub1		
BGP Autonomous System Number *		
65091		
TGW Connect		
C Enable		
Changing the use of TGW Connect will cause to	emporary traffic loss.	
CIDR		
Region *	CIDR *	
US West (Oregon)	176.16.11.0/24	/ 🖮
Add CIDR		
TGW Route Table Association Labels 💿		
Name *		
Add TGW Route Table Association Label		
		Add

ステップ14 通常どおりに残りの構成を完了します。

- [一般接続(General Connectivity)]ページの残りの構成を通常どおりに完了し、[保存して続行(Save and Continue)]をクリックします。
- ・通常どおり、[スマート ライセンス (Smart Licensing)]ページで必要な設定を完了します。

詳細については、[AWS 設置ガイドの Cisco クラウド ネットワーク コントローラ (Cisco Cloud Network Controller for AWS Installation Guide)]リリース 25.1 (x) 以降のセットアップウィザードを使用した Cisco Cloud Network Controller の構成の章を参照してください。

プロセスのこの時点で、Cisco クラウドネットワーク コントローラの最初のクラウドサイト(この例の ハイブリッドクラウドトポロジではAWS クラウドサイト)の基本設定が完了しました。次の手順に進 んで、Cisco クラウドネットワーク コントローラの2番目のクラウドサイト(この例のハイブリッドク ラウドトポロジでは、Azure クラウドサイト)の基本構成を完了します。

ステップ15 必要に応じて、AWSの Direct Connect を構成します。

Catalyst 8000V ルータからクラウドネットワークへの接続にプライベート接続が必要な場合は、直接接続 を構成します。AWS 用の 直接接続 の構成については、[AWS ユーザー ガイドの Cisco クラウド ネット ワーク コントローラ (Cisco Cloud Network Controller for AWS User Guide] リリース 25.1 (x) 以降を参照 してください。

次のタスク

Azure クラウドサイトのクラウドネットワークコントローラを展開 (63ページ) で提供され ている手順を使用して、2番目のクラウドサイト (Azure クラウドサイト) にクラウドネット ワークコントローラを展開します。

Azure クラウド サイトのクラウド ネットワーク コントローラを展開

これらのセクションの手順に従って、Azure クラウド サイトにクラウド ネットワーク コント ローラを展開します。

Azure の詳細設定で必要なパラメータを構成します

このセクションでは、この例のハイブリッドクラウドトポロジ専用に、[クラウドネットワー クコントローラのセットアップ(Cloud Network Controller Setup)]ページの[詳細設定 (Advanced Settings)]エリアで、Azure クラウドサイトに必要な構成を行います。

AWS クラウド サイトに対して行ったのと同じ構成を Azure クラウド サイトに対して行います。

[Azure インストール ガイドの Cisco クラウドネットワーク コントローラ (Cisco Cloud Network Controller for Azure Installation Guide)]の「Configuring Cisco Cloud Network Controller Using the Setup Wizard」の章に記載されている手順を使用しますが、[クラウドネットワークコントロー ラ 設定 (Cloud Network Controller Setup)]ページには、この例のハイブリッドクラウドト ポロジの場合のために具体的に構成する必要がある2つのエリアがあることに注意してください:

- コントラクトベースのルーティング(Contract-based routing): クラウドネットワーク コントローラは、次の2種類のモードをサポートしています。
 - 契約ベースのルーティング
 - •ルートマップベースのルーティング

契約ベースのルーティングとは、EPG 間の契約が VRF 間のルーティングを駆動すること を意味しますが、このタイプの契約ベースのルーティングは NDFC では使用できないた め、この特定の例のハイブリッド クラウド トポロジでは、契約ベースのルーティングを オフにして、代わりにルート マップ ベースのルーティングを使用します。詳細について は、AWS ユーザー ガイドの Cisco クラウド ネットワーク コントローラ、リリース 25.1 (x) 以降の「ルーティング ポリシー」および「グローバル Inter-VRF ルート リーク ポリ シー」 セクションを参照してください。

 クラウドネットワークコントローラのアクセス権限:デフォルトでは、クラウドネット ワークコントローラにはルーティングとセキュリティのアクセス権限があります。つま り、クラウドネットワークコントローラはネットワークを自動化できるだけでなく、ク ラウド上のセキュリティグループを自動化および構成することもできます。クラウドネッ トワークコントローラがセキュリティグループを自動化して構成する場合、EPGと契約 も構成する必要があります。ただし、EPGと契約は、ルーティングの自動化のみが必要な NDFC エンドユーザーには適用されません。NDO および NDFC とうまく統合するには、 クラウドネットワークコントローラのアクセス権限オプションをルーティングのみに設 定する必要があります。

始める前に

AWS クラウド サイトのクラウド ネットワーク コントローラを展開 (56 ページ) で提供され ている手順を使用して、最初のクラウド サイト (AWS クラウド サイト) にクラウド ネット ワーク コントローラを展開します。

- **ステップ1** Azure の Cisco クラウド ネットワーク コントローラにログインします。
- **ステップ2** この例のハイブリッドクラウドトポロジ用に、2番目のクラウドサイトである Azure クラウドサイトを セットアップするプロセスを開始します。

Azure インストールガイドの Cisco クラウドネットワーク コントローラ、リリース 25.1 (x) 以降の最初の 数章には、このハイブリッド クラウド トポロジのユース ケースに固有ではない一般的な情報が含まれて いるため、そのドキュメントのこれらの章の手順を完了してから、ここに戻ります:

• 概要

- Cisco クラウド ネットワーク コントローラのインストールの準備
- Azure での Cisco Cloud Network Controller の展開
- ステップ3 Cisco Cloud Network Controller GUI で、インテントアイコン(2) をクリックし、[Cloud Network Controller Lットアップ (Cloud Network Controller Setup)]を選択します。

[基本を構成しましょう(Let's Configure the Basics)] ページが表示されます。

- ステップ4 [詳細設定(Advanced Settings)]エリアを探し、[構成の編集(Edit Configuration)]をクリックします。
- ステップ5 [詳細設定(Advanced Settings)] ページで、次の構成を設定します。
 - [契約に基づいたルーティング(Contract Based Routing)]:ボックスがオフになっていることを確認 します(この機能が有効になっていないことを確認します)。これにより、契約ベースのルーティング が無効になり、代わりにルートマップベースのルーティングが使用されます。
 - ・クラウドネットワークコントローラのアクセス権限:[ルーティングのみ(Routing Only)]オプションを選択します。
- **ステップ6** [保存して続行 (Save and Continue)] をクリックします。

[基本を構成しましょう(Let's Configure the Basics)]ページに戻ります。
次のタスク

Azureのリージョン管理で必要なパラメーターを構成する(65ページ)の手順を実行します。

Azure のリージョン管理で必要なパラメーターを構成する

このセクションでは、この例のハイブリッドクラウドトポロジー専用に、[クラウドネット ワークコントローラ (Cloud Network Controller Setup)]のセットアップページの[リージョン 管理 (Region Management) エリアで Azure クラウド サイトに必要な構成を行います。

始める前に

Azureの詳細設定で必要なパラメータを構成します(63ページ)の手順を実行します。

ステップ1 [リージョン管理(Region Management)エリアを探して適切なボタンをクリックします。

クラウドネットワーク コントローラを初めてセットアップする場合は [開始(Begin)] をクリックし、 以前にこのクラウドネットワーク コントローラでリージョン管理を既に構成している場合は [構成の編 (Edit Configuration)] をクリックします。

ステップ2 [内部ネットワークの接続(Connectivity for Internal Network)] エリア内の [仮想ネットワーク ピアリン グ(Virtual Network Peering)]が自動的に有効化されていることを検証します。

> グローバルレベルの VNet ピアリングは、[内部ネットワークの接続(Connectivity for Internal Network)] エリアで設定されます。これにより、Cisco Cloud Network Controller レベルで VNet ピアリングが有効に なり、CCR を使用してすべてのリージョンに NLB が展開されます。リリース5.1 (2) 以降では、グロー バルレベルのVNetピアリングはデフォルトで有効になっており、無効にすることはできません。詳細に ついては、[Azure 向け Cloud APIC の VNet ピアリングを構成する (Configuring VNet Peering for Cloud APIC for Azure) Jを参照してください。

ステップ3 [管理するリージョン (Regions to Manage)]領域で、Cisco Cloud Network Controller のホーム リージョン が選択されていることを確認します。

> Cisco Cloud ネットワーク コントローラを AWS に最初に展開したとに選択したリージョンは、ホーム リージョンであり、このページで既に選択されいているはずです。これは、Cisco Cloud Network Controller が展開されるリージョン (Cisco Cloud Network Controller によって管理されるリージョン) で、[リージョ ン (Region)]列に「cisco cloud Network controller」というテキストが表示されます。

- (注) Azure VNet ピアリングは自動的に有効化されているので、Cisco クラウドネットワーク コントローラ ホーム リージョンの Catalyst 8000Vs カラムのボックスがチェックを既にされていない場合、チェックする必要があります。
- ステップ4 Cisco クラウドネットワークコントローラで追加のリージョンを管理します。他のリージョンで Inter-VNet 通信と Hybrid-Cloud、Hybrid Multi-Cloud、または Multi-Cloud 接続を行うように Cisco Catalyst 8000Vs を 展開する場合は、追加のリージョンを選択します。

Cisco Catalyst 8000V は、Cisco Cloud Network Controller が導入されているホーム リージョンを含む、最大 4 つのリージョンにハイブリッド クラウドおよびマルチクラウド接続を提供できます。

ステップ5 リージョンにローカルにクラウドルータを展開するには、そのリージョンの Catalyst 8000Vs チェック ボックスにチェック マークをつけるためにクリックします。

> Catalyst 8000V が展開されているリージョンが少なくとも1つ必要です。ただし、このページで複数の リージョンを選択した場合は、選択したすべてのリージョンに Catalyst 8000V を設定する必要はありません。

> 特に、このハイブリッド クラウド トポロジのユース ケースの例では、Cisco クラウド ネットワーク コ ントローラ ホーム リージョンの Catalyst 8000V 列のチェック ボックスにチェック マークを付けます。

図 **50**:

Setup - Region Mar	nagement		
	Please note that CSR is now changed to Catalyst 8000V.		
	Connectivity for Internal Network		
	Regions to Manage *		
	Region Name	Region	Catalyst 8000Vs 👦
	Australia Central 2	australiacentral2	
	Australia East	australiaeast	
	Australia Southeast	australiasoutheast	
	Brazil South	brazilsouth	
	Canada Central	canadacentral	
	Canada East	canadaeast	
	Central India	centralindia	
	Central US	centralus	
	East Asia	eastasia	
	East US	eastus Cloud Network Controller Deployed	

ステップ6 適切なリージョンをすべて選択したら、ページの下部にある[Next]をクリックします。 [General Connectivity]ページが表示されます。

ステップ7 [一般接続(General Connectivity)]ページで必要な構成を行います。

詳細については、[*Cisco Cloud Network Controller for Azuru* 設置ガイド(*Cisco Cloud Network Controller for Azure Installation Guide*)]リリース25.1 (x) 以降のセットアップウィザードを使用した Cisco Cloud Network Controller の構成の章を参照してください。

特に、このハイブリッドクラウドトポロジのユースケースの例では、次の手順の手順を使用して、Cisco Catalyst 8000V に対して次の設定を行います。

ステップ8 [全般(General)]エリアの[クラウドルータのサブネット プール(Subnet Pools for Cloud Routers)]
 フィールドで、Catalyst 8000V のサブネットを追加する場合は、[クラウドルータのサブネット プールの
 追加(Add Subnet Pool for Cloud Routers)] をクリックします。

最初のサブネットプールが自動的に入力されます(System Internalとして表示)。このサブネットプール のアドレスは、Cisco Cloud Network Controller で管理する必要がある追加のリージョンのリージョン間接 続に使用されます。このフィールドに追加するサブネットプールは、マスク/24の有効なIPv4サブネット である必要があります。

次の状況では、この手順で Catalyst 8000V のサブネットを追加します。

- Cisco Cloud Network Controller ホーム リージョンに Catalyst 8000V を展開している場合は、自動的に 生成される[システム内部 (System Internal)]サブネット プールに加えて、1 つのサブネット プールを追加します。
- 前のページで Cisco Cloud Network Controller により管理対象となる追加のリージョンを選択した場合:
 - 管理対象リージョンごとに 2~4 の Catalyst 8000V を持つすべての管理対象リージョンに 1 つの サブネットプールを追加します(このページの[リージョンごとのルータの数(Number of Routers Per Region)]フィールドに2、3、または4を入力した場合)。
 - 管理対象リージョンごとに5つ以上の Catalyst 8000V があるすべての管理対象リージョンに2つのサブネットプールを追加します(このページの[リージョンごとのルータの数(Number of Routers Per Region)]フィールドに5~8 を入力した場合)。

特に、このハイブリッドクラウドトポロジのユースケースの例では、サブネットエントリとして 10.90.1.0/24 を使用してサブネットプールを1つ追加します。

図 51:

Setup - Region Management		
External Cloud External Router Network Controller	Inter-Site Connectivity Catal	y st 8000V
Configure the fabric infra connectivity for the the configuration template used for the Clo	the Cloud Site. The Fabric Autonomous System Number is used for BGF loud Routers in the Cloud Site.	Peering insid
Conorol		
Sublet Polis for Globa Robers Regio	ions Created By	
10.90.0.0/24	System Internal	
10.90.1.0/24	User 🛛 🔊	
Add Subnet Pool for Cloud Route	iers	

ステップ9 Catalyst 8000V エリアの [C8kVs の BGP 自律システム番号(BGP Autonomous System Number for C8kVs)] フィールドに、このサイトに固有の BGP 自律システム番号(ASN)を入力します。

BGP自律システム番号は1~65534の範囲で指定できます。追加の制限は、[*Cisco Cloud Network Controller for Azuru* 設置ガイド(*Cisco Cloud Network Controller for Azure Installation Guide*)]リリース 25.1 (x) 以降 のセットアップウィザードを使用した Cisco クラウドネットワーク コントローラの構成の章を参照して ください。

具体的には、このハイブリッドクラウドトポロジのユース ケースの例では、[**C8kV の BGP 自律システ ム番号(BGP Autonomous System Number for C8kVs)**]フィールドに 65092 を入力します。

义	52 :
---	------

Catalyst 8000Vs	
RCD Autonomeuro Sustane Number fau CRIVIA :	
65092	
Assign Public IP to CBkV Interface ●	
Changing C8kV connectivity from private to public (or vice versa) may cause disruption in your network.	
Number of Routers Per Region	
Username * cisco	
Password	
Please ensure that the license account has licenses corresponding to the Router's throughput entered below.	
Pricing Type * BYOL V	
Throughput of the routers Tier1 (up to 100M throughput)	
TCP MSS * •	
1300	
License Token	

ステップ10 [次へ(Nexr)]をクリックし、通常どおりに残りの構成を完了します。

- [一般接続(General Connectivity)]ページの残りの構成を通常どおりに完了し、[保存して続行(Save and Continue)]をクリックします。
- ・通常どおり、[スマート ライセンス(Smart Licensing)]ページで必要な設定を完了します。

詳細については、[*Cisco Cloud Network Controller for Azuru* 設置ガイド(*Cisco Cloud Network Controller for Azure Installation Guide*)]リリース25.1 (x) 以降のセットアップウィザードを使用した Cisco Cloud Network Controller の構成の章を参照してください。

ステップ11 必要に応じて、Azure の ExpressRoute を構成します。

Catalyst 8000V ルータからクラウドネットワークへの接続にプライベート接続が必要な場合は、ExpressRoute を構成します。Azure 用の ExpressRoute の構成については、[*Azure* ユーザーガイドの *Cisco* クラウドネットワーク コントローラ(*Cisco Cloud Network Controller for Azure User Guide*]リリース 25.1 (x) 以降を参照してください。

次のタスク

NDFC とクラウド サイトを ND と NDO に導入準備する (70 ページ) で提供されている手順 を使用して、NDFC 管理サイト (VXLAN ファブリック、外部ファブリック、およびクラウド サイト)を Nexus ダッシュボード (ND) および Nexus ダッシュボード オーケストレータ (NDO) にオンボードします。

NDFC とクラウドサイトを ND と NDO に導入準備する

始める前に

- NDFC VXLAN ファブリックを作成(38ページ)で提供されている手順を使用して、NDFC VXLAN ファブリックを作成します。
- NDFC 外部ファブリックを作成(46 ページ)で提供されている手順を使用して、NDFC 外部ファブリックを作成します。
- AWS クラウド サイトのクラウド ネットワーク コントローラを展開 (56 ページ)で提供 されている手順を使用して、最初のクラウド サイトにネットワーク クラウド コントロー ラを展開します。
- Azure クラウドサイトのクラウドネットワークコントローラを展開(63ページ)で提供 されている手順を使用して、2番目のクラウドサイトにネットワーククラウドコントロー ラを展開します。
- ステップ1 Nexus Dashboard Orchestrator (NDO) を使用して Nexus Dashboard (ND) クラスタにログインします。
- ステップ2 Nexus ダッシュボードで、[サイト (Sites)]>[サイトを追加 (Add Site)]をクリックします。 図 53:

≡ cisco Nexus	Dashboa	rd 🛛 🗐 o Admin Console						Feedback 💄 🕐
= Admin Consol	le	C fab2nd2						۵
C Overview		Sites						٢
III Services		Filter by attributes						Add Site
System Resources		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
 Infrastructure 								
<u>1</u> ° Administrative								
					No rows found			
		10 × Rows					Page 1 of 1 《	<0-0 of 0 > >>

[サイトの追加(Add Site)]ページが表示されます。

- ステップ3 [サイトの追加(Add Site)]ページの [NDFC] ボックスをクリックします。
- ステップ4 NDFC サイトを追加するために必要な情報を入力します。

- •[ホスト名/IP アドレス(Hostname/IP Address)]フィールド内で NDFC のデータ インターフェイス IP アドレスを入力します。
- •[ユーザー名(Username)]および[パスワード(Password)]フィールドに、NDFCのユーザー名と パスワードログイン情報を入力します。
- ステップ5 [サイトの選択 (Select Sites)] をクリックします。

🗵 54:

≡ ^{•1 •1 •} Nexus Dashboard ⊕ ©	Dne View 🗸			Feedback 💄
Admin Console G fab2nd2				0 🗅 🖸
G Overview				
© Sites				
III Services	Site Type			
🖉 System Resources 🗸 🗸		0	0	۲
🖽 Operations	ACI	Cloud Network Controller	MDFC	
O Infrastructure V				
🖍 Administrative 🧹	In inschability is required between Nexus Dasboard data metwork. Use the DCMAND/CD Leaves IP address to oriooxide the test of test	sk and DCMM/NOFC Intend BOMM/NOFC steet.		

ステップ6 以前に追加した2つのNDFCサイト(VXLANファブリックと外部ファブリックサイト)の横にあるボックスをクリックし、[選択(Select)]をクリックします。

🗵 55 :

≡ cisco Nexus Dashboard €	> One View				Particles
🗐 Admin Console 🛛 🙆 🕬					0 🖸
Coverview Sites					
© öftes					
	Site Type				
E Gysters Resources		0		0	۲
III Operations	ACI	Clou	d Network Controller	NDFC	
C lotrastructure	Selec	t		×	
£ Advantative	Prostability is required bitment second. Use the CONNECT Case Houses Houses Houses Houses Login Domain () Login Domain () Box Sist frame Society Domain Houses Houses	446-1	No term Selected Select them For Details		
	Add Security Domains				
					Canon Canon

[サイトの追加(Add Site)]ページに戻ります。

- ステップ7 Nexus ダッシュボードの [サイトの追加(Add Site)]ページに2つの NDFC サイト(VXLAN ファブリッ クと外部ファブリック サイト)が正しく表示されていることを確認し、[保存(Save)]をクリックしま す。
- ステップ8 Nexus ダッシュボードで、最初のクラウドサイトを追加するために[サイト(Sites)]>[サイトを追加 (Add Site)]もう一度をクリックします。

図 56:

Admin Consol	e	6 fab2nd2						00
Overview		Sites						
lervices		Filter by attributes						Add S
System Resources		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
ifrastructure		A Minor	Sydney	NDFC	(Ø Up	12.1.2.275	o	
dministrative		() Healthy	ext-fab-1	NDFC	(Q) Up	12.1.2.275	0	

[サイトの追加(Add Site)]ページが表示されます。

ステップ9 [サイトの追加(Add Site)]ページで[クラウドネットワークコントローラ(Cloud Network Controller)] ボックスをクリックし、必要な情報を入力して最初のクラウドサイト(この例のトポロジではAWSサ イト)を追加します。

- •[ホスト名/IP アドレス(Hostname/IP Address)]フィールドに、最初のクラウドサイトのクラウド ネットワーク コントローラ(CNC)の IP アドレスを入力します。
- •[ユーザー名(Username)]と[パスワード(Password)]フィールドに、最初のクラウドサイトのク ラウドネットワーク コントローラ(CNC)のユーザー名とパスワードのログイン情報を入力しま す。
- クラウドネットワークコントローラ(CNC)の場合、CNCがプロキシを通して到達可能ならば、 [プロキシを有効化(Enable Proxy)]プロキシは、Nexus Dashboardのクラスタ設定ですでに設定されている必要があります。プロキシが管理ネットワーク経由で到達可能な場合は、プロキシIPアドレスに対して静的管理ネットワークルートも追加する必要があります。プロキシとルートの構成の詳細については、お使いのリリースのNexus Dashboard ユーザーガイドを参照してください。

図 57:

≡ cisco Nexus Da	ashboard	- One View					
	C fab	2nd2					٥
C Overview	∢ Sites						
U sites							
System Resources		Site Type				7	
Operations		ACI		Cloud Network Cont	roller	NDFC	
O Infrastructure							
<u>1</u> ° Administrative		General					
		Name •					
		Settings					
		Hostname/IP Address *					
		10.00.00 m					
		Username * 🕢					
		Password = ()					
			•				
		Login Domain 💿					
		Enable Proxy					
		Security Domains Name					
		Add Security Domains					
							Cancel Save

- ステップ10 [保存 (Save)] をクリックして、最初のクラウドサイトを追加します。
- ステップ11 Nexus ダッシュボードで、2番目のクラウドサイトを追加するために[サイト(Sites)]>[サイトを追加 (Add Site)]もう一度をクリックします。

🗵 58 :

≡ cisco Nexus Dashboa	ard 🛛 🗐 🖉 Admin Console 🗸						Feedback 🛓 🔍
	C fab2nd2						000
Overview Sites	Sites						٥
III Services	Filter by attributes						Add Site
System Resources	Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
C Infrastructure	di Major	AWS	Cloud Network av Controller	3 (O up)	25.1(te)	0	
⊥° Administrative ∨	A Minor	Sydney	NDFC	(O up)	12.1.2.275	0	
	() Healthy	ext-fab-1	NDFC	(0 Up)	12.1.2.275	0	
	10 V Rows					Page 1 of 1	$\ll < 1\text{-3 of } 3 > \gg$

[サイトの追加(Add Site)]ページが表示されます。

ステップ12 [サイトの追加(Add Site)] ページで [クラウド ネットワーク コントローラ] ボックスをクリックし、必要な情報を入力して、2番目のクラウドサイト(このトポロジ例の Azure サイト)のクラウドネットワーク コントローラ(CNC)を追加します。

前の一連の手順を繰り返します。今度は、2番目のクラウドサイトのクラウドネットワークコントロー ラ(CNC)の[ホスト名/IPアドレス(Hostname/IP Address)]、[ユーザー名(Username)]、および[パ スワード(Password)]フィールドに必要な情報を入力し、2番目のクラウドのCNCの場合は[プロキシ を有効にする(Enable Proxy)]をクリックします。サイトはプロキシ経由で到達可能です。 図59:

> Admin Console © trazvaz © overview © state B Services Site Type Ø system Bessurces	0
Overview 4 Stes © Sites	
E Services Site Type	
Gereations G	
O Infrastructure V	
L' Administrative General	
Name *	
Part	
Settings	
Hostname/IP Address =	
Username • 🔘 admin	
Password * 🔿	
Login Domain 🔿	
Chable Provy	
Security Domains Hame	
Add Security Domains	

- **ステップ13** Nexus ダッシュボードで[サイト (Sites)]をクリックし、4つのサイトが正しく表示されていることを確認します。
 - •NDFC の2つのサイト (VXLAN ファブリックと外部ファブリック サイト)
 - クラウドネットワークコントローラが展開されたクラウドサイト(この例のハイブリッドクラウドトポロジでは、AWSおよびAzureクラウドサイト)

図 60:

≡ cisco Nexus	Dashboa	ard and Admin Console						Feedback 💄 🔮
	le	6 fab2nd2						o 🕽 🕄
 Overview Sites 		Sites						Ó
Services		Filter by attributes						Add Site
Operations		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
 Infrastructure 		A Major	Azure	Cloud Network	oup)	T 25.1(1e)	o	57253
⊥° Administrative		🖄 Májor	AWS	Cloud Network Controller	O Up	25.1(1e)	0	
		A Minor	Sydney	NDFC	(Ø Up	12.1.2.275	0	-
		Healthy	ext-fab-1	NDFC	(⊘up)	12.1.2.275	0	
		10 V Rows					Page 1 of 1 《	< 1-4 of 4 > >>>

ステップ14 Nexus ダッシュボードオーケストレータ (NDO) にアクセスします。

Nexus ダッシュボードで、ウィンドウの上部にある [一つの表示 (One View)]>[オーケストレータ (Orchestrator)]をクリックします。

巡 61:



ステップ15 NDO で、[サイト (Sites)]をクリックします。

ND で追加した 4 つのサイトが表示されますが、[管理対象外(Unmanaged)]の状態で表示されます。 図 62:

	Sites					TEROBER Z
 Sites 	ones					0 ()
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
 Operations O Infrastructure 	⊘ок	AWS	AWS	Unmanaged	~ 25.1(1e)	2770
@ Integration	⊘ок	Azure	Azure	Unmanaged	~ 25.1(1e)	
	⊘ок	ext-fab-1	NDFC	Unmanaged	- 12.1.2.275	·
	ØОК	Sydney	NDFC	Unmanaged	12.1.2.275	
	10 V Rows				Page 1	of 1 《<1-4 of 4>》

ステップ16 NDOから、4つのサイトを管理します。

NDO の各サイトに対して次の手順を実行します。

a) NDOにリストされている最初のサイトの[状態(State)]列で、状態を[管理対象外(Unmanaged)] から[管理対象(Managed)]に変更します。

図 **63**:

E cisco Nexus Dashi	board A Orchestrator					Feedback 上 🤇
Sites						0 0
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
Operations Infrastructure	⊘ок	AWS	😑 AWS	Unmanaged ~	25.1(1e)	
✓ Integration	⊘ок	Azure	Azure	Managed	25.1(1e)	
	⊘ок	ext-fab-1	NDFC	Unmanaged ✓	12.1.2.275	
	⊘ок	Sydney	NDFC	Unmanaged ~	12.1.2.275	
	10 V Bows				Page 1	of 1 ≪ < 1-4 of 4 > ≫

b) この特定のサイトに固有のサイト識別子(このNDOを通じて管理されている他のサイトのサイト識別子と競合しないサイト識別子)を指定し、[追加(Add)]をクリックします。

図 64 :

	01000					
Application Management						
	Controller Connectivity	Name	Туре	State	Version	
) Infrastructure	Øок		AWS	Unmanaged		
	Øок	Azure	Azure	Unmanaged		
	ØOK	ext-		Unmanaged		
	⊘ок	Syd	d Configuration	× Unmanaged		
		Site ID *	•			
				Add		

c) NDO の残りのサイトに対してこれらの手順を繰り返して、各サイトを[管理対象(Managed)]状態 に変更し、各サイトに一意のサイト ID を提供します。

次の図は、4 つのサイトすべて(2 つの NDFC サイトと2 つのクラウド サイト)の例を示しており、状態が[管理対象(Managed)]に変更され、各サイトに一意のサイト ID が提供されています。 図 65:

Dashboard	01000					
Sites						€ <u>0</u> 1
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
Infrastructure	⊘ок	AWS Site ID: 91	aws	Managed	25.1(1e)	
Integration	ØOK	Azure Site ID: 92	Azure	Managed	25.1(1e)	
	ØOK	ext-fab-1 Site ID: 80	NDFC	Managed	12.1.2.275	
	ØOK	Sydney Site ID: 82	NDFC	Managed	12.1.2.275	

次のタスク

Complete サイト間の接続 NDFC と クラウド サイトの間 (78 ページ)に記載されている手順 を使用して、NDFC とクラウド サイト間のサイト間接続を完了します。

Complete サイト間の接続 NDFC と クラウド サイトの間

次のセクションの手順に従って、NDFC とクラウドサイト間のサイト間接続を完了します。

必要なコントロール プレーン構成を完了する

始める前に

NDFC とクラウド サイトを ND と NDO に導入準備する (70 ページ) で提供されている手順 を使用して、ND および NDO で NDFC およびクラウド サイトをオンボードします。

ステップ1 NDO 内で、[インフラストラクチャ(Infrastructure)]>[サイト接続(Site Connectivity)]に移動します。 図 66:

≡ cisco Nexus Dashi	board 🙏 Orchestrator 🗸					Feedback 上 🤨
 Dashboard Sites Application Management 	Sites					0 ()
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
C Infrastructure	Infrastructure	AWS Site ID: 91	😑 AWS	Managed	25.1(1e)	
@ Integration	System Configuration	Azure Site ID: 92	Azure	Managed	25.1(1e)	
	e un	ext-fab-1 Site ID: 80	NDFC	Managed	12.1.2.275	
	⊘ок	Sydney Site ID: 82	NDFC	Managed	12.1.2.275	
	10 V Rows				Page 1	of 1 $\ll\!<\!$

この時点で、世界地図にサイトが表示されますが、サイト間にリンクはありません。つまり、この時点で はサイト間に接続がありません。 図 67:

≡ cisco Nexus Dashboar	rd 🍨 Orchestrator 🗸	Feedback 💄 🔮
Dashboard Sites	Site Connectivity	ti Configure
Application Management Application Management Dentitions Infrastructure Infrastructure Infrastructure Integration	Connectivity Settings	Croup Markers

- ステップ2 [サイト接続 (Site Connectivity)]ウィンドウの右上のエリアで、[構成 (Configure)]をクリックします。 [一般設定 (General Settings)]エリアの[サイト接続 (Site Connectivity)]ウィンドウが表示されます。
- ステップ3 [一般設定(General Settings)]エリアで、[コントロール プレーン構成(Control Plane Configuration)]タ ブをクリックし、このページで必要な構成を行います。

図 **68**:

Connectivity		DEPLOY V D13 X
ios	Control Plana Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDPC Settings	
. anotiga	RGD	
D AWS	BCP Neering Type Tub neerb v	
Azure	teop Join Internal Becombi ⊘ 100	
est-fab-1	10 10 1 10 1 10 1 10 1 10 1 10 1 10 1	
Sydney	Carolina and Carol	
	OSPF 0/# 4xx 0 6880	~
	CloudSec Control	^
	NNA Assigned Forn Q	
	Data Path	^
	VYLAN UDP destination port change will cause traffic disruption for evidors flows. Change with eaction:	

BGP はオンプレミスとクラウドサイト間のアンダーレイ接続に使用され、OSPF はクラウド間のアンダー レイ接続に使用されることに注意してください。

 (注) これらの一般的な BGP 設定は、アンダーレイ接続とオーバーレイ接続の両方での BGP の使用 に適用され、オーバーレイ ピアリングにのみ適用される次のステップの [BGP ピアリングタイ プ(BGP Peering Type)]オプションを除き、通常は変更しないでください。 ステップ4 オンプレミスとクラウドサイト間のオーバーレイ接続の場合、BGP エリアの [BGP ピアリング タイプ (BGP Peering Type)]フィールドで、[フルメッシュ(full-mesh)]または[ルートサーバー(route-server)] のいずれかを選択します。

> フル メッシュまたはルート サーバー接続を使用するトポロジを確認するには、サポートされるトポロジ (15ページ) を参照してください。

この特定のユースケースでは、IPsec(マルチクラウド)でサポートされるトポロジ(21ページ)のオプ ション1(21ページ)トポロジに基づいて展開を構成しているため、このユースケースでは[フルメッ シュ(full-mesh)]を選択します。

- ステップ5 必要に応じて、BGP エリアで残りのパラメータを定義します。
- ステップ6 クラウド間アンダーレイ接続の場合、OSPF エリアで、[OSPF エリア識別子(OSPF Area ID)] フィール ドに適切な値を入力します。

2 つのクラウド サイト間のアンダーレイ ルーティングは OSPF を使用するため、この構成はクラウド間接 続に必要です。この例では、このフィールドに OSFP エリア識別子0.0.0.0 を入力します。

ステップ7 [データ パス(Data Path)]で、[カプセル化タイプ(Encapsulation Type)]エリアを見つけて、[VXLAN] を選択します。

> デフォルトでは、NDOは、オンプレミスファブリックに基づく NDFC のハイブリッド クラウドのデータ プレーンで標準規格 VXLAN を使用します。もう1つのオプションは iVXLAN です。これは、ACI サイト のハイブリッド クラウド接続を構築するときに使用する必要があります(ACI は iVXLAN を使用するた め)。

次のタスク

オンプレミス IPsec デバイスと IPSec トンネル サブネット プールを追加 (80 ページ) の手順 を実行します。

オンプレミス IPsec デバイス と IPSec トンネル サブネット プールを追加

このセクションでは、オンプレミスのIPsecデバイス(NDFC外部ファブリックサイトのCisco Catalyst 8000V)を追加し、IPsec トンネルプールを構成します。

始める前に

必要なコントロールプレーン構成を完了する (78ページ) の手順を実行します。

- ステップ1 同じ[一般設定(General Settings)]ページで、[オンプレミス IPsec デバイス(On Premises IPsec Devices)] タブをクリックします。
- ステップ2 [オン プレミス IPsec デバイスを追加(Add On Premises IPsec Device)] をクリックします。

図 69:

≡ cisco Nexus Dashb	oard 📄 🏩 Orchestrator 🗸	
Site Connectivity		
SETTINGS	Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDFC Settings	
General Settings		
SITES	On Premises IPsec Devices	
• 🤤 AWS disabled	Name Type IP Address Next Hop Address Add On Premises IPsec Device IP Address IP Address IP Address	
• Azure		
◦ ● ext-fab-1 ⊘		
• • Sydney		

[オンプレミス IPsec デバイスを追加(Add On Premises IPsec Device)] ページが表示されます。

ステップ3 [タイプ(Type)]フィールドで、[非管理(Unmanaged)]または[管理(Managed)]を選択します。

オンプレミスの IPsec デバイスでは、[非管理(Unmanaged)]と[管理(Managed)]管理対象の両方のオプ ションがサポートされています。

 オンプレミスの IPsec デバイスに対して [管理対象外(Unmanaged)] オプションを選択した場合は、 [名前(Name)]、[IP アドレス(IP Address)]、[ネクストホップアドレス(Next Hop Address)]など、この管理対象外のオンプレミス IPsec デバイスに必要な情報を入力する必要があります。オンプレミスの IPsec デバイスが NDFC で管理されていない場合 (そのデバイスが NDFC でサポートされていないか、サードパーティのデバイスである場合)、[管理対象外(Unmanaged)]を使用します。次に、 NDO は、管理対象外の IPsec デバイスに必要な構成を生成します。これをダウンロードして、オンプレミスの IPsec デバイスに手動で適用できます。

≡ "cisco Nexus	Dashboard Schestrator V
Site Connectivit	у
	Control Plane Configuration On Premises (Psec Devices External Devices (Psec Tunnel Subnet Pools, NDEC Settions
	On Premises IPsec Devices
	Name Type IP Address Add On Premises IPsec Device Add On Premises IPsec Device X
o Azure disabled	O Type Unmanaged Managed
∞ ● ext-fab-1	Name * P Address *
Sydney	⊘ ASN *
	Next Hop Address * 1.1.1.1

 オンプレミスの IPsec デバイスに対して[管理対象(Managed)]オプションを選択すると、[サイト (Site)]フィールドが[管理対象(Managed)]オプションの下に表示されます。[サイト(Site)] フィールドで使用できるサイトは、NDFC で構成された外部ファブリックについて NDO が NDFC か らプルする情報に基づいています。 図 71:

	ivity						
		Control Plane Confic	uration On Pr	emises IPsec Devices	External Devices	Psec Tunnel Subnet Pool	s NDFC Settings
		On Premise	es IPsec De	vices			
		Name	Туре	IP Address	Next Hop Addr	355	
		Add On Premises I	Psec Device				-
Azure							_
					Add On Pren	nises IPsec Devic	e ×
					Turce		<u>^</u>
ext-fab-1					1 1 / / 1 1 4 4		
e 🔵 ext-fab-1					Unmanaged Mana	ged	
 ext-fab-1 Sydney 					Unmanaged Mana Site *	ged	
e ext-fab-1					Unmanaged Mana Site * Select	ged	
e ext-fab-1					Unmanaged Mana Site * Select ext-fab-1	ged	<u>^</u>

管理対象のオンプレミス IPsec デバイスを備えた NDFC 外部ファブリックを選択します。この場合、 選択したサイトに基づいて、ASN フィールドが自動的に入力されます。

このユース ケースの例では、オンプレミスの IPsec デバイスのタイプとして [管理対象(Managed)]を選択します。

a) [デバイス (Device)]フィールドで、この展開に使用するオンプレミスの IPsec デバイスを選択します。

[デバイス(Device)] フィールドで使用できるデバイスは、上で選択した NDFC サイトで構成された オンプレミスの IPsec デバイスについて、NDO が NDFC からプルする情報に基づいています。[デバイ ス(Device)] フィールドで選択したオンプレミスの IPsec デバイスに基づいて、ASN フィールドが自 動的に入力されます。

b) [インターフェイス(Interface)] フィールドで、オンプレミスの IPsec デバイスに使用する適切なイン ターフェイスを選択します。

このインターフェースの[IPアドレス(IPAddress)]フィールドは、[インターフェイス(Interface)] フィールドで選択したインターフェースに基づいて自動的に入力されます。

c) [ネクストホップアドレス(Next Hop Address)]フィールドに、IPsec で構成するルートに使用するアドレスを入力します。

义	72	:
---	----	---

Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDFC Set			
AVS disabled AXUE disabled Sydney Sydney Marrie Sydney Marrie		Control Plane Configuration On Premises IPsec Devices	External Devices IPsec Tunnel Subnet Pools NDFC Setting
On Premises IPsec Devices MVS diabled Azure diabled Azure diabled Azure diabled Managed			
Add On Premises IPsec Device Add On Premises IPsec Device Add On Premises IPsec Device Type Umanaged Manged Sife * ext-fab-1 ASN 65000 Device * C&K3-Fab2 Interface * GigabitEthernet2 Interface * GigabitEthernet2 INTerface * GigabitEthernet2 Interface *		On Premises IPsec Devices	Add On Dramiana IDaga Davies
Name Type IP Address Isabled Add On Premises IPace Device Jisabled Image: Sydney Sydney Sydney Sydney Image: Sydney Im			Add On Premises iPsec Device
Add On Premises Preci Device Add On Premises Preci Device Managed Managed Managed Managed Managed Managed Managed Managed Managed Interface* GigabitEthernet2 Interface* GigabitEthernet2 IP Address 64 104 255 12 Next Hop Address *		Name Type IP Address	T
Azure disabled ext-fab-1 ASN ext-fab-1 ASN ext-fab-1 ASN ext-fab-1 ASN ext-fab-2 Interface * GigabitEthernet2 IP Address 64.104.255.12 Next Hop Address *		Add On Premises IPsec Device	Unmanaged Managed
ext-fab-1	Azure		Site *
ext-fab-1 ASN S5000 Device * C8K3-Fab2 Interface * GigabitEthernet2 IP Address 84.104.255.12 Next Hop Address *			ext-fab-1 🗸
• • ext-fab-1 • • • ext-fab-1 • • • • • • • • • • • • • • • • •			ASN
© Sydney © CBK3-Fab2 Interface * GigabitEthernet2 IP Address 64.104.255.12 Next Hop Address *	ext-fab-1		65080
© Sydney © Sydney © G8K3-Fab2 Interface * GigabitEthernet2 IP Address 64.104.255.12 Next Hop Address *			Device *
Sydney Interface * GigabitEthernet2 IP Address 64.104.255.12 Next Hop Address *			C8K3-Fab2 V
GigabitEthernet2 IP Address 64.104.255.12 Next Hop Address *	Sydney		Interface *
IP Address 64.104.255.12 Next Hop Address *			GigabitEthernet2 V
64.104.255.12 Next Hop Address *			IP Address
Next Hop Address *			64.104.255.12
			Next Hop Address *
64.104.255.1			64.104.255.1

ステップ4 [オンプレミス IPsec デバイスを追加(Add On Premises IPsec Device)] ページで必要な情報の入力が完了 したら、Ok をクリックします。

[オンプレミス IPsec デバイス (On Premises IPsec Device)] ページに戻ります。このページには、構成されたオンプレミスの IPsec デバイスが表示されています。

ステップ5 IPsec トンネル サブネットプールを構成するために[IPSec トンネル サブネット プール (IPsec Tunnel Subnet Pools)] タブをクリックします。

クラウドトンネルの IP 割り当てには、[IPSec トンネル サブネット プール(IPsec Tunnel Subnet Pools)] の情報が必要です。

ステップ6[外部サブネット プール(External Subnet Pool)]エリアで、[IP アドレスの追加(Add IP Address)]をク リックします。 図 73:

≡ יווייווי cisco Nexus Dasht	board Archestrator V	
Site Connectivity		
SETTINGS	Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools	NDFC Settings
General Settings		
SITES	External Subnet Pool 💿	
• 😝 AWS disabled	IP Address 169.254.0.0/16	
• Azure	Add IP Address	
◦ ● ext-fab-1	Site Specific Subnet Pool Name IP Address	
• • Sydney	Add Site Specific Subnet Pool	

ステップ7 IPsec トンネルに使用する IP サブネット プールを入力します。

IPsec トンネルのパブリックまたはプライベート IP アドレスを使用して、IP サブネット プールを定義しま す。これは、オンプレミスの外部デバイスと Cisco Catalyst 8000V の間、およびクラウドサイトに展開され た Cisco Catalyst 8000V の間の IPsec トンネル アドレスの IP アドレスのプールです。

- IPsec トンネルごとに /30 サブネットが必要です。
- ・プールサイズは、すべての IPsec トンネルに対応できる必要があります。
- ・許可される最小プールサイズは512アドレス(/23サブネット)です。
- ・環境内の他の IP アドレスと重複しない IP アドレスの範囲(パブリックまたはプライベート)を使用 します。

図 74:

≡ •I uI u cisco Nexus Dashboard A Orchestrator →						
Site Connectivity						
SETTINGS	Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDEC Settings					
General Settings						
SITES	External Subnet Pool 💿					
• 🤤 AWS	IP Address 🚳					
disabled	169.254.0.0/16					
• 🔿 Azure	170.1.0.0/16					
disabled	Add IP Address					
👓 🕒 ext-fab-1						
0	Site Specific Subnet Pool 💿					
o Sydney	Name IP Address					
\odot	Add Site Specific Subnet Pool					

ステップ8 チェックボックスをクリックして、入力した IP サブネット プールを受け入れます。

[外部サブネット プール (External Subnet Pool)]エリアの下に IP サブネット プールが表示されます。 図 75:

Site Connectivity		
ETTINGS	Control Plane Configuration On Premises IPsec Devices Exte	rnal Devices IPsec Tunnel Subnet Pools NDFC Settings
eneral Settings		
ITES	External Subnet Pool 💿	
• 🤤 AWS	IP Address 🚳	
disabled	169.254.0.0/16	
• 🔷 Azure	170.1.0.0/16	~ m
disabled	🔁 Add IP Address	
• ext-fab-1		
\odot	Site Specific Subnet Pool 💿	
🔊 🌘 Sydney	Name IP Address	
\odot	🚯 Add Site Specific Subnet Pool	

ステップ9 必要に応じて、[NDFC 設定(NDFC Settings)] タブをクリックし、[自動ルート ターゲット プレフィック ス(Auto Route Target Prefix)]に必要な情報を入力します。

図 76:

≡ داندان Nexus Dashb	oard 📃 🌨 Orchestrator 🗸
Site Connectivity	
SETTINGS	Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDFC Settings
General Settings	
SITES	NDFC Settings
disabled Ø	Layer 2 VXLAN VNI Range 130000-149000
👳 🔕 Azure	Layer 3 VXLAN VNI Range 150000-159000
disabled	Multi-Site Routing Lookback IP Range
♥ ● ext-fab-1	Anycast Gateway MAC 2020.0000.00aa
🔹 🌘 Sydney ⊘	Auto Route Target Prefix * 23456
	Advanced Settings

NDO の NDFC 設定では、ルートターゲット生成のルートターゲットプレフィックスが NDFC のデフォル ト値 23456 に設定されています (クラウドネットワーク コントローラーにはこの設定に対して異なる値が あります)。したがって、重複を避けるために必要な場合、この値は[自動ルートターゲットプレフィック ス (Auto Route Target Prefix)]フィールドで変更できます。このフィールドに値を設定すると、NDO は NDO によってこの値を NDFC にプッシュできます。

次のタスク

NDFC 外部ファブリック内の外部デバイスのポートを追加する (87 ページ) の手順を実行します。

NDFC 外部ファブリック内の外部デバイスのポートを追加する

このセクションでは、NDFC外部ファブリックの外部デバイスに必要なポートを追加して構成 します。これらは、コアルータを BGW ノードに接続するインターフェイスです。

始める前に

オンプレミス IPsec デバイスと IPSec トンネル サブネット プールを追加 (80 ページ) の手順 を実行します。

- ステップ1 [一般設定:サイト(General Settings: Sites)]の下の左側のウィンドウで、NDFC外部ファブリック(この 例では ext-fab-1 サイト)をクリックします。
- ステップ2 中央のペインで、NDFC 外部ファブリックの最初の外部デバイスをクリックします。

ステップ3 右側のペインで [ポートを追加 (Add Port)] をクリックします。

図 77:

≡ disco Ne	xus Dashbo	ard 📃 🙏 Orchestrator 🗸			Fe	edback 上 😏
Site Connect	ivity			1	DEPLOY V	X 650 [
SETTINGS			0 0	8K3-Fab2		
General Settings		P Site ext-fab-1 Refresh	-		1.	
SITES		Core Router C8K3-Fab2	critical	major	minor	warning
disabled	0		Ports	et Port ID		
• 🔕 Azure	0		C Add	non		
disabled						
o ext-fab-1	0					
🔹 🌒 Sydney	0					

ステップ4 IP アドレス、リモート IP アドレス、リモート ASN など、ポート構成に必要な情報を入力します。

- (注) [クラウドルータに向かう(Towards Cloud Router)]オプションは、ハブサイトのボーダー ゲートウェイにのみ適用されます。次の理由により、このウィンドウでこのオプションを有効 にしません。
 - この導入例に使用しているトポロジは、ハブサイトを使用していないのでのこ導入例に[ク ラウドルータに向かう(Towards Cloud Router)]をイネーブル化しません。
 - IPsec (マルチクラウド)でサポートされるトポロジ (21ページ)のオプション3 (23ページ)のようなハブサイトを使用するトポロジを構成していた場合でも、そのハブサイト トポロジの NDFC 外部ファブリックの外部デバイスに対して、このページでこのオプションを有効にしません。代わりに、NDFC VXLAN ファブリック内の BGW スパイン デバイスにポートを追加する (92ページ)で説明されているように、NDFC VXLAN ファブリックの BGW スパイン デバイスのページでこのオプションを有効にします。

図 78:

Ethernet Port ID * GigabitEthernet4 IP Address * 10.140.1.1/30 Description towards on-prem Spine BGW E1/32 Remote Address * 10.140.1.2 Remote ASN * 65084 MTU * 9216 Inherit BGP Authentication and BFD ①			
GigabitEthernet4 P Address * 10.140.1.1/30 Description towards on-prem Spine BGW E1/32 Remote Address * 10.140.1.2 Remote ASN * 65084 MTU * 9216 Inherit BGP Authentication and BFD ○ Imperit BGP Authentication and BFD ○ Imperit BGP Authentication Imperi	Ethernet Port ID *		
IP Address * 10.140.1.1/30 Description towards on-prem Spine BGW E1/32 Remote Address * 10.140.1.2 Remote ASN * 65084 MTU * 9216 Inherit BGP Authentication and BFD ① SBGP Authentication ③ None	GigabitEthernet4	\times \sim	
10.140.1.1/30 Description towards on-prem Spine BGW E1/32 Remote Address * 10.140.1.2 Remote ASN * 65084 MTU * 9216 Inherit BGP Authentication and BFD () Imple Cisco Towards Cloud Router () BFD Enabled	P Address *		
Description towards on-prem Spine BGW E1/32 Remote Address • 10.140.1.2 Remote ASN • 65084 MTU • 9216 Inherit BGP Authentication and BFD ①	10.140.1.1/30		
towards on-prem Spine BGW E1/32 Remote Address * 10.140.1.2 Remote ASN * 65084 MTU * 9216 Inherit BGP Authentication and BFD ① BGP Authentication None Simple Cisco Towards Cloud Router ① BFD Enabled	Description		
Remote Address * 10.140.1.2 Remote ASN * 65084 MTU * 9216 Inherit BGP Authentication and BFD ③ BGP Authentication None Simple Cisco Towards Cloud Router ④ BFD Enabled	towards on-prem Spine BGW E1/32		
10.140.1.2 Remote ASN * 65084 MTU * 9216 Inherit BGP Authentication and BFD ⑦ Inherit BGP Authentication ● None Simple Cisco Towards Cloud Router ⑦ BFD Enabled	Remote Address *		
Remote ASN * 65084 MTU * 9216 Inherit BGP Authentication and BFD ① BGP Authentication None Simple Cisco Towards Cloud Router ① BFD Enabled	10.140.1.2		
65084 MTU * 9216 Inherit BGP Authentication and BFD ① ✓ BGP Authentication ● None ○ Simple ○ Cisco Towards Cloud Router ① BFD Enabled	Remote ASN *		
MTU * 9216 Inherit BGP Authentication and BFD ① BGP Authentication None Simple Cisco Towards Cloud Router ① BFD Enabled	65084		
9216 Inherit BGP Authentication and BFD ① Image: Simple Organization Organizatio Organization Organizatio Organization Organiz	MTU *		
Inherit BGP Authentication and BFD ① BGP Authentication None Simple Cisco Towards Cloud Router ① BFD Enabled	9216		
BGP Authentication None Simple Cisco Towards Cloud Router BFD Enabled	nherit BGP Authentication and BFD ①		
Towards Cloud Router ① BFD Enabled	BGP Authentication Image: None Simple Cisco		
BFD Enabled	Towards Cloud Router 🕢		
	BFD Enabled		

ステップ5 完了したら、[OK] をクリックします。 ステップ6 残りの外部デバイスに対してこの手順を繰り返します。

次のタスク

VXLAN ファブリック サイトのマルチサイト VIP を定義します。 (89 ページ) の手順を実行 します。

VXLAN ファブリック サイトのマルチサイト VIP を定義します。

このセクションでは、VXLAN ファブリック サイトのマルチサイト VIP を定義します。

始める前に

NDFC 外部ファブリック内の外部デバイスのポートを追加する (87 ページ) の手順を実行します。

- **ステップ1** [一般設定: サイト (General Settings: Sites)]の下の左側のペインで、NDFC VXLAN ファブリック サイト をクリックします。
- ステップ2 中央のペインで、スパインデバイスをクリックします。
- ステップ3 右側のペインの[サイト間接続(Inter-Site Connectivity)]で、[マルチサイトVIP(Multi-Site VIP)]フィールドにマルチサイト VIP を定義します。

[自動割り当て(Auto Allocate)]をクリックするか、マルチサイト VIP の IP アドレスを明示的に定義できます。

図 79:

≡ ^{•• •• •} Nexus Dashi	oard 📄 🗶 Orchestrator 🗸	Feedback 🛓 ᠑
Site Connectivity		DEPLOY V Oth X
SETTINGS		Sydney Settings
General Settings	Site Sydney	
SITES	Switch ndfc-spine1	Inter-Site Connectivity
e AWS	· · · · · · · · · · · · · · · · · · ·	General A
 Azure disabled 		Multi-Site VIP 10.10.1 IPsec Device ①
♥ ● ext-fab-1		Name Device ID IP Address Add IPacc Device
 Sydney 		
	-	

次のタスク

IPSec デバイスを VXLAN ファブリック サイトにマップする (90 ページ) の手順を実行します。

IPSec デバイスを VXLAN ファブリック サイトにマップする

このセクションでは、IPsec デバイスを VXLAN ファブリック サイトにマッピングします。

始める前に

VXLAN ファブリック サイトのマルチサイト VIP を定義します。 (89 ページ) の手順を実行 します。

- ステップ1 [一般設定:サイト (General Settings: Sites)]の下の左側のペインで、NDFC VXLAN ファブリックサイト をクリックします。
- **ステップ2** 中央のペインで、スパインデバイスをクリックします。
- ステップ3 右側のペインの[サイト間接続(Inter-Site Connectivity)]で、[IPsec デバイスの追加(Add IPsec Device)] をクリックします。

図 **80**:

≡ cisco Nexus Dashbo	ard 🙏 Orchestrator 🗸	Feedback 1
Site Connectivity		DEPLOY V O() X
SETTINGS General Settings	•	Sydney Settings O
SITES	P Site Sydney Refresh	r-Site Connectivity
AWS disabled	Switch ndfc-spine1 Gen Site 82	eral ^
e 🔕 Azure	84.0 10 1956	-Site VIP 10.0.1 Auto Allocate c Device ③
• • ext-fab-1		e Device ID IP Address
💿 🕽 Sydney 📀		

ステップ4 [選択 (Select)]をクリックして、適切な IPsec デバイスを選択します。

図 **81** :

	xus Dashb	aard 🌐 🙏 Orchestrator 🗸	Feedback 🛓 🕐
Site Connect	ivity		DEPLOY V Ott X
SETTINGS			Sydney Settings
General Settings		Refresh Refresh	s of an of a commission of a commi
SITES		Switch ndfc-spine1	Inter-Site Connectivity
 AWS disabled 	0		General A Site ID 82
 Azure disabled 	ø		Multi-Site VIP 10.10.0.1 IPsec Device
• • ext-fab-1	0		Name Device ID IP Address
Sydney	0		C8K3-Fab2

これで、オンプレミスの IPsec デバイスが VXLAN ファブリック サイトにマップされました。 図 82:

≡ disco Ne	xus Dasht	oard 🔔 Orchestrator ~	Feedback 👤 💿
Site Connect	ivity		DEPLOY V Otl X
SETTINGS			Sydney Settings
General Settings		Site Sydney Befresh	• Sydney Settings
SITES			Inter-Site Connectivity
 AWS 	0	Switch ndre-spiner	General
disabled	0		Site ID 82
🛛 🗿 Azure			Multi-Site VIP 10.10.0 1 Auto Allocate
disabled	0		IPsec Device O
🔹 🔵 ext-fab-1			Name Device ID IP Address
	0		C8K3- Fab2 98JE1U8CZ8M 64.104.255.12 \checkmark 1
Surfaceu			Add IPsec Device
C) C) G) GI (C)			

ステップ5 NDFC VXLAN サイトをクラウドサイトに接続するために使用されるオンプレミスの IPsec デバイス (Cisco Catalyst 8000V) ごとに、この手順を繰り返します。

次のタスク

NDFC VXLAN ファブリック内の BGW スパイン デバイスにポートを追加する (92 ページ) で提供されている手順を使用して、コア ルータ (Cisco Catalyst 8000V) に接続する BGW スパ イン デバイスのポートを構成します。

NDFC VXLAN ファブリック内の BGW スパイン デバイスにポートを追加 する

このセクションでは、オンプレミスの IPsec デバイスに面する NDFC VXLAN ファブリックの BGW スパイン デバイスに必要なポートを追加して構成します。

始める前に

IPSec デバイスを VXLAN ファブリック サイトにマップする (90 ページ) の手順を実行します。

- ステップ1 [一般設定:サイト (General Settings: Sites)]の下の左側のペインで、NDFC VXLAN ファブリック サイト をクリックします。
- **ステップ2** 中央のペインで、スパインデバイスをクリックします。
- ステップ3 右側のペインで [ポートを追加(Add Port)]をクリックします。

図 **83** :

	kus Dasht	aard 🔔 Orchestrator 🗸			Fe	edback 上 📀
Site Connecti	vity				DEPLOY V	<i>€19</i>
SETTINGS			•	dfc-spine1		
General Settings		Refresh Refresh				
SITES		Switch ndfc-spine1	critical	major	minor	warning
disabled	0		BGP-E1	/PN ROUTER-ID		
• 🔕 Azure			BGW P	IP		
disabled	0		Ports	10.10		
• • ext-fab-1	0		C Add	Port		
	0					
 Sydney 						

ステップ4 必要な情報をこのページに入力します。

このページでポートパラメータを定義します。

াগ্যা	QЛ	
	04	٠

≡ cisco Nexus Dashboard	🔹 Orchestrator 🗸				Feedback 🛓 💿
Site Connectivity					DEPLOY V Ott X
				o ndfc-spir	net
	Site Sydney		Refresh		
		Add Port	×	majo	r minor warning
	Switch ndfc-spine1	Ethernet Port ID *			-P-ID
		Ethernet1/32 × V		20.2.0.3	
e 💿 Azure		IP Address * 10.140.1.2/30		BGW PIP	
		Description			
a evidab-1		towards on-prem CSKv Gi-4		Ethernet Port ID	<u> </u>
0		10.140.1.1		Add Port	
		Remote ASN *			
• Sydney		MTU *			
		9216			
		BGP Authentication None Simple			
		Towards Cloud Router () BFD Enabled			
			OK		

- •[イーサネットポート識別子(Ethernet Port ID)]フィールドで、オンプレミスの Cisco Catalyst 8000V の方を向いているインターフェイスを選択します。
- •[IP アドレス (IP Address)]フィールドに、このインターフェイスの IP アドレスを入力します。これ らの手順の後半で、Nexus ダッシュボード オーケストレータ は、VXLAN ファブリックに存在する BGW スパイン スイッチで、このインターフェイスのこの IP アドレスを構成します。
- •[リモートアドレス(Remote Address)]フィールドに、オンプレミスの IPsec デバイスのギガビット 4インターフェイスの IP アドレスを入力します。
- ・[リモートASN (Remote ASN)]フィールドに、オンプレミスのIPsec デバイスのASNを入力します。 たとえば、このユースケースの例では、オンプレミスのIPsec デバイスのASN として 65080 を入力し ます。
- (注) [クラウドルータに向かう(Towards Cloud Router)]オプションは、オンプレミスハブサイトのボーダーゲートウェイにのみ適用されます。IPsec(マルチクラウド)でサポートされるトポロジ(21ページ)のオプション3(23ページ)などのハブサイトを使用しているトポロジでは、このオプションを有効にする必要があります。
 この導入例に使用しているトポロジは、ハブサイトを使用していないのでのこ導入例に[クラウ

ドルータに向かう(Towards Cloud Router)]をイネーブル化しません。

ステップ5 [OK] をクリックします。

BGW スパイン デバイスのポートが NDFC VXLAN ファブリックに追加されました

図 85 :

≡ disco Nex	us Dashboar	d 🌐 🏥 Orchestrator 🗸			Fe	edback 👤 📀
Site Connecti	vity				DEPLOY V	× €7@ [
SETTINGS			0	dfc-spine1		
General Settings		Refresh Refresh				
SITES		Switch ndfc-spine1	critical	major	minor	warning
disabled	Ø		BGP-E 20.2.0	/PN ROUTER-ID		
💌 🔕 Azure			BGW P	IP 1.4		
disabled	0		Ports	net Port ID		
🔹 🌒 ext-fab-1	0		Ether	met1/32		/ =
			C Ada	Port		
 Sydney 	0					

次のタスク

1つ目のクラウドサイトを NDFC VXLAN ファブリックサイトに接続する (94 ページ) の手 順を実行します。

1つ目のクラウドサイトを NDFC VXLAN ファブリック サイトに接続する

このセクションでは、1番目のクラウドサイトをNDFC VXLAN ファブリックサイトに接続します。

始める前に

NDFC VXLAN ファブリック内の BGW スパイン デバイスにポートを追加する (92ページ) の手順を実行します。

- ステップ1 [一般設定:サイト (General Settings: Sites)]の下の左側のペインで、最初のクラウドサイト (AWS サイトなど)をクリックします。
- ステップ2 右側のペインで、[サイト間接続(Inter-Site Connectivity)]をクリックし、[マルチサイト(Multi-Site)] の下にあるチェックボックスをオンにして、その機能を有効にします。

この機能は、サイト間に VXLAN マルチサイト オーバーレイ トンネルを構築するために必要です。

ステップ3 右側のペインで [サイトの追加(Add Site)]をクリックします。

図 **86**:

Site Connect	ivity		DEPLOY V Otl
ETTINGS			AWS Settings
eneral Settings		Site AWS	Refresh Inter-Site Connectivity External Connectivit
AWS disabled Aure disabled e Arure disabled e ext-fab-1	0	Region us-west-2 C.couterp_us- west-2,5 casv Casv Casv	General Sile D H Mars-Sile O BOP BOP Autonomous System Humber 5591
Sydney	0		Contract Based Routing Inter-Site Connectivity Protocol Site Protocol

[サイトの追加(Add Site)]ページが表示されます。

ステップ4 [サイトの追加(Add Site)]ページ内で[サイトを選択(Select a Site)]をクリックします。 図 87:

≡ cisco Nexus Das	board 🔶 Orchestrator 🗸				Feedback 上
Site Connectivity					DEPLOY V Oth X
					AWS Settings
	Site AWS			Refresh	· Arro Securigs
					Inter-Site Connectivity External Connectivity
	Region us-wes	d Sito			General
	♥ ct_routerp_us-	u Site			
a Arma	west-2_0	ected to Site			Muti-Site O
0	CSRV Selec	ection Type *			BGP
				~	
👳 🕘 ext-fab-1	Proto	COL			
	Hub	ite O			
 Sydney 					Inter-Site Connectivity Site Protocol
	IPsec				Add Site
	On Pr	emises IPsec Devices	IP Arkings		
	СВКЗ	I-Fab2	64.104.255.12		

[サイトを選択(Select a Site)]ページが表示されます。

ステップ5 NDFC VXLAN ファブリック(この例ではシドニーサイト)を選択し、[選択(Select)]をクリックします。

図 **88**:

図 **89**:

Site Connectivity	Doard Prochestrator V			
				AWS Set
	Site AWS		Ref	resh Inter-Site Conne
	C Region us-wes	Add Site		× General Site ID 91
e 🖸 Azure	C8KY	Select Site	Site Sydney	× Multi-Site ① BOP BOP-Autonomous 5
≂ ● ext-fab-1		Azure Sydney	Site ID 82	Contract Based Ro
s 🕈 Sydnay			Type N/A URL https://172.16.0.191:443	Site Add Site
			Sate	
			6	3

[サイトの追加(Add Site)]ページに戻ります。

ステップ6 [サイトの追加(Add Site)] ページの[接続タイプ(Connection Type)] フィールドで、1番目のクラウド サイトから NDFC VXLAN ファブリック サイトに使用する接続のタイプを選択します。

Site Connectivity				
SETTINGS				
General Settings	Site AWS	Add Site		×
	Region us-wes ct routero us-	AWS → Sydney Connected to Site Sydney ×		Â
e 💽 Azure 🧭 disabled	west-2,0 C8kV	Connection Type * Public Internet Public Internet		<u>^</u>
e ● ext-fab-1		Private Connection		
a 🖲 Sydney		On Premises IPsec Devices Device Name	IP Address	
		C8K3-Fab2	64.104.255.12	
		Sydney ● → AWS ⑤	ed with Public IPs for Public Underlay connection	
		Connected to Site		

[パブリックインターネット(Public Internet)]を選択するか、AWSで直接接続またはAzureでExpressRoute を使用している場合は[プライベート接続(Private Connection)]を選択できます。

- オンプレミスサイトでは[パブリックインターネット(Public Internet)]と[プライベート接続(Private Connection)]の両方のオプションを使用できますが、クラウドサイトでは[パブリックインターネット(Public Internet)]接続オプションのみを使用できます。
- IPsecは、[パブリックインターネット(Public Internet)]接続タイプでは必須であり、その接続タイプでは自動的に有効になりますが、[プライベート接続(Private Connection)]タイプではIPsecはオプションです。
- (注) IPsec (マルチクラウド) でサポートされるトポロジ (21ページ) のオプション3 (23ページ) などのハブ サイトを使用しているトポロジでは、[ハブサイト (Hub Site)]オプションを 有効にする必要があります。

この導入例に使用しているトポロジは、ハブ サイトを使用していないのでのこ導入例に[**ハブ** サイト(Hub Site)]オプションをイネーブル化しません。

ステップ7 このページでの構成が完了したら、[OK] をクリックします。

次のタスク

1 つ目のクラウド サイトを2 つ目のクラウド サイトに接続する (97 ページ) の手順を実行します。

1つ目のクラウドサイトを2つ目のクラウドサイトに接続する

このセクションでは、最初のクラウドサイトを2つ目のクラウドサイトに接続します。

始める前に

1つ目のクラウドサイトを NDFC VXLAN ファブリックサイトに接続する (94 ページ) の手順を実行します。

- ステップ1 [一般設定:サイト (General Settings: Sites)]の下の左側のペインで、最初のクラウドサイト (AWS サイトなど)をクリックします。
- ステップ2 右側のウィンドウで、[サイト間の接続(Inter-Site Connectivity)]をクリックします。
- ステップ3 右側のペインで [サイトの追加 (Add Site)] をクリックします。

図 *90*:

≡ cisco Ne	xus Dashboar	rd 📃 🏩 Orchestrator 🗸	Feedback 🛓 🕤
Site Connect	ivity		DEPLOY V O(1 X
SETTINGS			AWS Settings
General Settings		Site AWS	efresh
SITES	_	Region Heuwert-2	Inter-Site Connectivity External Connectivity
AWS	0	nografi wa-weat-z	General
boldene		ct_routerp_us- west-2_0 west-2_1	Site ID 91
👳 🔕 Azure	0	CBKV CBKV	Multi-Site 🔘
disabled	0		BGP Autonomous System Number
• ext-fab-1			65091
	0		Contract Based Routing
o 🔵 Sydney			Inter-Site Connectivity
	0		Sydney BGP-EVPN 2
			Add Site
			Add Site

[サイトの追加(Add Site)]ページが表示されます。

ステップ4 [サイトの追加(Add Site)]ページ内で[サイトを選択(Select a Site)]をクリックします。

[サイトを選択(Select a Site)]ページが表示されます。

ステップ5 2番目のクラウドサイト(たとえば、Azureクラウドサイト)を選択し、[選択(Select)]をクリックします。

図 **91** :

≡ cisco Ne:	xus Dashboar	d 🙏 Orchestrator 🗸				Feedback	L 0
Site Connect	ivity					DEPLOY ~ Oth	×
						AWS Settings	0
		Site AWS			Refresh	Inter-Site Connectivity External Connectivity	y
		 ct_routerp_us- west-2_0 	Add Site		×	General Site/D 91	
a Azure disablod		CBKV	Select Site	s Site	×	Autor Site () ECP BCD Autorspectral Sectors Namber	
is 🔵 ext-fab-1			Azure	Site ID 92			
Sydney				Type Azure URL		Inter-Site Connectivity Site Protocol Sydney Connection Type Public BOP-EVPN	· =
				https://20127114.214.443	Select	C And the	

[サイトの追加(Add Site)]ページに戻ります。

ステップ6 [サイトの追加(Add Site)] ページページの[接続タイプ(Connection Type)] フィールドで、最初のクラ ウド サイトから 2 番目のクラウド サイトに使用する接続のタイプを選択します。

一部のタイプのクラウド間接続では、次のオプションを使用できます。

・パブリック インターネット

・クラウド バックボーン

クラウドバックボーンを使用して、同じプロバイダーのクラウドサイト間の接続を確立できます(たとえ ば、1つのクラウドネットワーク コントローラによって管理される AWS サイト1と2番目のクラウド ネットワーク コントローラによって管理される AWS サイト2)。ただし、次の図に示すように、異なる クラウドプロバイダーのサイト間(AWS から Azure など)では、パブリック インターネットが唯一のオ プションです。

図 *92 :*

E cisco No	xus Dashboan	d 🙏 Orchestrator 🗸			Feedback 1
Site Connect	ivity				DEPLOY V Ota X
					AW/S Settings
		Site AWS	Add Site	×	• Ano Settings
		Region us-wes	AWS	1	Inter-Site Connectivity External Connectivity
		* ct_routerp_us- west-2_0	Please check if C8kVs are configured with Public IPs for Public Underlay connection		
e Azure		CRKV	Connected to Site Asure ×		BOP
e 🔵 ext-fab-1			Connection type - Public Internet Protocol	~	
 Sydney 			BGP-EVPN		Contract Based Routing
			Psec V		Sydney BOP-EVPN X 11
			Azure ♥ → AWS ●		Actd Site
			Please check If C8kVs are configured with Public IPs for Public Underlay connection		
			Connected to Site AWS	_	
			Connection Type *	_	

パブリック インターネット 接続タイプが選択されている場合、**IPsec** オプションは必須であり、その接続 タイプでは自動的に有効になりますが、**クラウド バックボーン タイプ** では **IPsec** はオプションです。

- (注) トポロジが ハブサイト を使用している場合でも、クラウド間接続のハブ サイト オプションを 有効にしません (その場合、クラウド サイトと NDFC VXLAN ファブリック サイト間の接続を 構成するときに ハブサイト オプションを有効にします)。
- ステップ1 このページでの構成が完了したら、[OK] をクリックします。

次のタスク

2 つ目のクラウドサイトを NDFC VXLAN ファブリックサイトに接続する (99 ページ) の手 順を実行します。

2 つ目のクラウドサイトを NDFC VXLAN ファブリック サイトに接続する

このセクションでは、2番目のクラウドサイトを NDFC VXLAN ファブリック サイトに接続します。

このセクションの手順は、前のセクションで実行した手順と基本的に同じです。ここで、次の ことを行います。

- ・最初のクラウドサイトを1つ目のクラウドサイトをNDFC VXLAN ファブリックサイト に接続する (94ページ) の NDFC VXLAN ファブリックサイトに接続しました。
- ・最初のクラウドサイトを1つ目のクラウドサイトを2つ目のクラウドサイトに接続する (97ページ)の2番目のクラウドサイトに接続しました。

このセクションでは、2番目のクラウドサイトをNDFC VXLAN ファブリックサイトに接続します。1つ目のクラウドサイトを2つ目のクラウドサイトに接続する(97ページ)内のAWS とAzure 間の接続は既に構成されているため、2番目のクラウドサイト(Azure)からAWSへの接続を構成する必要はありません。その接続は前のセクションで既に構成されているためです。

始める前に

1 つ目のクラウドサイトを2 つ目のクラウドサイトに接続する (97 ページ) の手順を実行します。

- ステップ1 [全般設定:サイト(General Settings: Sites)]の下の左側のウィンドウで、2番目のクラウドサイト(Azure サイトなど)をクリックします。
- ステップ2 右側のペインで、[サイト間接続(Inter-Site Connectivity)]をクリックし、[マルチサイト(Multi-Site)] の下にあるチェックボックスをオンにして、その機能を有効にします。
- ステップ3 右側のペインで [サイトの追加 (Add Site)] をクリックします。

図 **93**:

≡ cisco Nex	us Dashboar	d 🌐 🙏 Orchestrator 🗸	Feedback 土 🔍
Site Connectiv	vity		DEPLOY V Otl X
SETTINGS			• Azure Settings •
General Settings		Site Azure Refr	Inter-Site Connectivity External Connectivity
 AWS enabled 	0	Region eastus Schooleguestus Schooleguestus Schooleguestus	General A
e Azure	0	cav cav	BGP Autonomous System Number
.♥ ● ext-fab-1	0		6592 Contract Based Routing
🤊 🌘 Sydney	0		Inter-Site Connectivity Frotocol
			Add Site

[サイトの追加(Add Site)]ページが表示されます。

ステップ4 [サイトの追加(Add Site)]ページ内で[サイトを選択(Select a Site)]をクリックします。 [サイトを選択(Select a Site)]ページが表示されます。

ステップ5 NDFC VXLAN ファブリック(この例ではシドニーサイト)を選択し、[選択(Select)]をクリックします。
[サイトの追加(Add Site)]ページに戻ります。

ステップ6 [サイトの追加(Add Site)]ページの[接続タイプ(Connection Type)]フィールドで、2番目のクラウド サイトから NDFC VXLAN ファブリック サイトに使用する接続のタイプを選択します。

図 **94** :

≡ cisco Ne	xus Dashboard	j 🙏 Orchestrator 🗸				Feedbac	× 1 0
Site Connect	ivity					DEPLOY V	X fj
						A Azura Sattings	
		Site Azure	Add Site		×	· Azure Settings	
					-	Inter-Site Connectivity External Connec	
		🔞 Region eastus	Azure ^O → Sydney ●			General	
		♥ ct_routerp_eastur	Connected to Site Sydney × Connection Turns 1				
		CBKV	Public Internet		.~	Multi-She ()	
			Protocol BGP-EVPN				
a 🌒 ext-fab-1			Hub Site () 			Gootract Rased Rousing	
👘 🔎 Sydney			On Premises IPsec Devices			Site Protocol	
			Device Name	IP Address		AWS BOP-EVPN	/ 8
			C8K3-Fab2	64.104.255.12		Add Site	
			Sydney ● → Azure ● Please check if CBxVs are configure Connected to Site	d with Public IPs for Public Underlay connection			

ステップ1 このページでの構成が完了したら、[OK] をクリックします。

構成されたサイトが表示されます。

図 **95**:

Site Connectivity set Tikes General Settings	©EPLOY → Oth X • Azure Settings •
AETTINOS Oerwal Settings	• Azure Settings •
Oeneral Settings	
Refresh Refresh	
srts	General Connectivity
exasted J J	Site ID 92
CRV CRV	Multi-Site () BCP
© ● et/4o-1	BGP Autonomous System Number 65092
0	Contract Based Routing
s Sydney	Site Protocol
	AWS BGP-EVPN 2 T
	Sydney BGP-EVPN / T
	To Add Sile

次のタスク

Nexus ダッシュボードオーケストレータの構成を展開 (102ページ) の手順を実行します。

Nexus ダッシュボードオーケストレータの構成を展開

このセクションでは、Nexusダッシュボードオーケストレータ(NDO)に構成を展開します。

始める前に

2 つ目のクラウドサイトを NDFC VXLAN ファブリックサイトに接続する (99 ページ) の手順を実行します。

ステップ1 NDO で構成を展開します。

オンプレミス IPsec デバイス と IPSec トンネル サブネット プールを追加 (80 ページ) でオンプレミス IPsec デバイスの [管理対象外 (Unmanaged)] オプションを選択した場合は、ページの右上にある [展開(Deploy)]>[展開して外部デバイス構成ファイルをダウンロード (Deploy & Download External Device Config files)]をクリックします。

このオプションにより、オンプレミス IPsec デバイスの構成に使用する必要な構成情報を含む zip ファ イルがダウンロードされます。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選 択できるようにするための、フォローアップ画面が表示されます。

オンプレミス IPsec デバイス と IPSec トンネル サブネット プールを追加 (80 ページ) でオンプレミス IPsec デバイスの [管理対象 (Managed)] オプションを選択した場合は、ページの右上にある[展開 (Deploy)]>[展開 (Deploy)]をクリックします。

図 *96 :*

≡ disco Ne	exus Dashboard	1. Orchestrator	Feedback	1 0
Site Connect	tivity		DEPLOY A Ota	×
SETTINGS			Deploy Only Deploy & Download On Premises IPsec Device Config files	0
General Settings	_	Site Azure Refresh	Deploy & Download External Device Config files Download On Premises IPsec Device Config files Inectivit	ty
💌 🤤 AWS	0	Region eastus	Download External Device Config files General On to	^
enabled enabled enabled	0	* ctrouterp.eastus J csev	Site ID 92 Mutti-Site () 80P	^
💌 🔵 ext-fab-1	ø		BGP Autonomous System Number 65092 Contract Based Routing	
🔋 🌘 Sydney	0		Inter-Site Connectivity Site Protocol	
			AWS Connection Type: Public BOP-EVPN	1 =
			Sydney Connection Type: Public BGP-EVPN	=
			Add Site	

ステップ2 [確認 (Confirmation)] ウィンドウで、[はい (Yes)] をクリックします。

この時点で、NDO は次のことを行います。

- ・クラウドネットワーク コントローラを介して NDFC およびクラウド サイト (AWS および Azure) と の通信を開始して、IPsec トンネルを自動化します。
- Azure Catalyst 8000V と AWS Catalyst 8000V の間で OSPF を構成します。

- BGW スパイン スイッチ、オンプレミス IPsec デバイス、および Azure Catalyst 8000V および AWS Catalyst 8000V 間の eBGP を構成します。
- ・サイト間の BGP-EVPN ピアリング セッションを確立します。

ステップ3 NDO で構成が正しく行われたことを確認します。

 ・左側のナビゲーションバーで[インフラストラクチャ(Infrastructure)]>[サイト接続(Site Connectivity)]をクリックし、[接続設定(Connectivity Settings)]エリアでサイト間の接続を確認し ます。

図 **97**:

≡ ^{•1 •1 •} Nexus Dashboa	rd 🔶 Orchestrator 🗸	Feedback 💄 🤇
Dashboard Sites	Site Connectivity	ڑ¢ Configure
Application Management Application Management Corrections Integrations Integration	Connectivity Settings	C Group Markers

 ・同じページで、最初のクラウドサイト(AWSサイトなど)のエリアまで下にスクロールし、[接続ス テータスを表示(Show Connectivity Status)]をクリックしてから、[サイト間接続(Inter-Site Connections)]エリアで[アンダーレイステータス(Underlay Status)]をクリックして、アンダーレ イステータスを確認します。

この例では、最初のクラウドサイト(AWS)に2つの Cisco Catalyst 8000V があり、2番目のクラウド サイト(Azure)にある2つの Cisco Catalyst 8000V と、2番目のクラウドサイト(Azure)にある1つ の Cisco Catalyst 8000V に IPsec トンネルがあるため、6つの IPsec トンネルがあります。オンプレミス の外部ファブリック。 図 **98**:

AWS 😑	ACI Multi-Site On	Site ID 91	BGP ASN 65091		^
Z Inter-Site Connections Overlay Status Underlay Status					Hide Connectivity Status \wedge
Device	Device Status	Interface Status	Peering Status	BGP Peer	Destination
ct_routerp_us-west-2_1	↑ Up	tunn-7 🕇 Up	OSPF 🛧 Up	-	
ct_routerp_us-west-2_1	↑ Up	tunn-6 🛧 Up	BGP 🛧 Up	170.1.254.6	64.104.255.12
ct_routerp_us-west-2_1	↑ Up	tunn-8 🛧 Up	OSPF 🕇 Up		
ct_routerp_us-west-2_0	↑ Up	tunn-7 🕇 Up	OSPF 🕇 Up		
ct_routerp_us-west-2_0	↑ Up	tunn-8 🕈 Up	OSPF 🛧 Up		·
ct_routerp_us-west-2_0	↑ Up	tunn-6 ↑ Up	BGP ↑ Up	170.1.254.2	64.104.255.12

 ・2番目のクラウドサイト(Azure サイトなど)のエリアまでスクロールダウンし、[接続ステータスの 表示(Show Connectivity Status)]をクリックしてから、[サイト間接続(Inter-Site Connections)]エ リアで[アンダーレイステータス(Underlay Status)]をクリックして、アンダーレイのステータスを 確認します。

この例では、6 つの IPsec トンネルがあります。これは、2 番目のクラウド サイト (Azure) に 2 つの Cisco Catalyst 8000V があり、最初のクラウド サイト (AWS) にある 2 つの Cisco Catalyst 8000V と、 オンプレミスの外部ファブリック。

図 **99**:

Azure C Regions 1 Inter-Site Connections	ACI Multi-Site On	Site ID 92	80P ASN 65092		A Hide Connectivity Status A
Device	Device Status	Interface Status	Peering Status	BGP Peer	Destination
ct_routerp_eastus_0	↑ Up	tunn-3 🛧 Up	OSPF ↑ Up	-	
ct_routerp_eastus_0	↑ Up	tunn-2 🛧 Up	OSPF ↑ Up	12.1	
ct_routerp_eastus_0	↑ Up	tunn-1 🛧 Up	BGP 🕈 Up	170.1.255.2	64.104.255.12
ct_routerp_eastus_1	↑ Up	tunn-2 🛧 Up	OSPF ↑ Up		•
ct_routerp_eastus_1	↑ Up	tunn-3 🛧 Up	OSPF ↑ Up	(*)	
ct_routerp_eastus_1	↑ Up	tunn-1 🛧 Up	BGP 🕈 Up	170.1.255.6	64.104.255.12

 NDFC 外部ファブリック サイトのエリアまでスクロール ダウンし、[接続ステータスの表示 (Show Connectivity Status)]をクリックしてから、[サイト間接続 (Inter-Site Connections)]エリアで[アン ダーレイステータス (Underlay Status)]をクリックして、アンダーレイのステータスを確認します。

外部ファブリックの機能は、オンプレミスのIPsec デバイスから VXLAN ファブリックおよびクラウド サイトへのアンダーレイの到達可能性を提供することです。アンダーレイ プロトコルは eBGP を使用 します。

 NDFC VXLAN ファブリックサイトのエリアまでスクロールダウンし、[接続ステータスの表示 (Show Connectivity Status)]をクリックしてから、[サイト間接続 (Inter-Site Connections)]エリアで [アン ダーレイ ステータス (Underlay Status)]をクリックして、アンダーレイ ステータスを確認します。

アンダーレイ ステータスは、BGW スパイン スイッチとオンプレミス IPsec デバイス間の eBGP セッション ステータスを示します。

図 100:

Sydney •						^
Nodes Situ 1 82	ID	Multi-Site VIP 10.10.0.1	BGP ASN 65084		Fabric Type VXLAN Fabric	
						Hide Connectivity Status 🔿
Overlay Status Underlay Status						
Device	Device Status	Interface Status	Peering Status	BGP Peer		
ndfc-spine1	↑ Up	Ethernet1/32 🛧 Up	BGP 🕈 Up	10.140.1.1		

・これらの各画面で、[オーバーレイステータス(Overlay Status)]をクリックして、それぞれのオー バーレイステータスを確認します。

図 101 :

AWS 😑								
2	On On		91		65091			
2								
								Hide Connectivity Status -
er-site Connections								
Overby Status Under	tay Mature							
ite Name		Deployment Status 🔘		Operational Status 📀		BGP EVPN Status	Tunnel Status	
2110		© CK		© ok		41 1 4 4 0 © OK	41 + 4 + 0	
ydney		© CK		⊙ ok		21 ↑ 2 ↓ 0 ⊙ CK	21 + 2 4 0	
zure								
Regions	ACI Multi-Site		Site ID		BOP ASN			
1	On		92		65092			
								Hide Connectivity Status
er-Site Connections	by Status							Hide Connectivity Status
er-Site Connections Nortay Status Under te Name	try Status	Deployment Status 🔿		Operational Status 🔿		BOP EVPN Status	Tunnel Status	Hide Connectivity Status
er-Site Connections Nortay Status Under Ite Name	try Status	Deployment Status 🔿		Operational Status 🔘		60P EVPN Status 41 ↑ 4 → 0 ② 0K	Tunnel Status 41 + 4 + 4	Hide Connectivity Status
er-Site Connections Northy Status Under te Name MS concy	try Stand	Deplayment Status () () OX () OX		Operational Status) O OK O OK		60P EVYN Stanus 41 ↑ 4 ÷ 0 © 0K 21 ↑ 2 ÷ 0 © 0K	Tunnel Status 41 ↑ 4 ÷ 0 21 ↑ 2 ÷ 0	Hide Connectivity Status
er-Site Connections Nextry Status Under te Name VS (Only	tay Statur	Deployment Eature () () OK () OK		Operational Status O		BOP EVMI Status 41 + 4 ÷ 0 0 21 + 2 ÷ 0 0	Turnet Status 41 € 4 ÷ 0 21 € 2 ÷ 0	Hide Connectivity Status
er-Site Connections Newtry Status Under te Name AS (Shely ydney I)	99 Ross	Deployment Status () () OX () OX		Operational Status ○ ○ OK ○ OK		80P EV/N Status 41 ↑ 4 ÷ 0 © 04 21 ↑ 2 ÷ 0 © 04	Tunnit Sistua 41 + 4 ÷ 0 31 + 2 ÷ 0	Hide Connectivity Status
er-Site Connections Noticy Status Under tis Name MS concy ydney • Nodes	See D	Deployment Status () () OK () OK	Mail Day VP	Operational Status () () () () () () () () () () () () () () () () () (529 43	BOP EVPN Blauss 41 ↑ 4 ↓ 0 ○ ○ K 21 ↑ 2 ↓ 0 ○ ○ K	Teened Series 41 ⊕ 4 ⊕ 0 31 ⊕ 2 ⊕ 0 Falent Type	Nide Connectivity Status
e-Site Connections weeky Mater Under Is Name VS Oney Vdney • Nodes 1	504 10 mm	Deployment Elation () () OX () OX	Vuit-Ste V/P 1036.01	Operational Status () () CK () CK	80 ⁰ AD 6004	509 EVM Suma 41 ↑ 4 ÷ 0 ⊙ ∞ 21 + 2 ÷ 0 ⊙ ∞	Transit Status 4 + + 4 + 0 21 + 2 + 0 Falsit Type VELINITADIR	Nide Connectivity Bates
er-Site Connections Nortry Status te Name MS concy wdney • Nootes 1	Sty these	Depiryment fathas ○ ○ OC ○ OC	4.00 USA V/P 1038.03	Operational Status () : () Ori	50P A29 60084	EOF EVMI BALINA 41 ↑ 4 ↓ 0 ○ ○ 21 ↑ 2 ↓ 0 ○ ○	Tennel Status 41 ± 4 ± 0 31 ± 2 ± 0 France Type VGLANTAINE	Hide Connectivity Dates /
er-Site Connections Newtry total of the Name rds colory ychney • Notice 1 er-Site Connections	try there.	Bephyser Bins () () OL () OL	Multi-Dia V/P 1039.03	Operational Status) C CK C CK	BOP AD SODA	827 0195 50mi 41 ↑ 4 ÷ 0 ⊙ 01 21 ↑ 2 ÷ 0 ⊙ 01	Twend Series 4 1 7 4 4 0 21 7 2 0 21 7 2 0 21 7 2 21 7 2	Nills Connectivity Status
en-Site Connections Newty Status Under NS Connections Notes 1 Status 2 Status 1 Status 2 Status Status 2 Status Status 2 Status 2 Status S	ογ θαια 22 92 92 92 92	Biglingment Balava ○ ○ OF ○ OF	Mail: Dar V/P 1038.03	Operational Status O	50P A2 60084	607 DVM 5044 41 ↑ 4 ÷ 0 ⊕ 00 21 + 2 ÷ 0 ⊕ 00	Normal Tabala 41 + 4 + 6 31 + 2 + 0 7 - 20 7 - 20 7 7 - 20 7 7 7 - 20 7 7 7 7 7 7 7 7	Nills Connectivity Status /
er Sie Connections hwere Manne of S ydney • ydney • Noden 1 ser Sie Connections bwere Manne (bes	ny MAN Sire D 82 Ny MAN	Dephyment Same O C C C C C C C C C C C C C C C C C C	Vue:-C24 VP 1019.01	Operational Subst ○ ○ or: ○ or:	SOP AD 80084	607 01% 5uns 41 ± 4 ÷ 0 ⊕ 0r 11 ± 2 ÷ 0 ⊕ 0r	All + 4 + 6 21 + 2 + 6 21 + 2 + 6 21 + 2 + 6 rates Tate VEX.NTDO: Outling Name Description	Nida: Connectivity Status
en-Site Connections Charley Material Internet Sydney • Notes 1 State-Site Connections 1 State Site Connections Internet Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site	Sty Rides) Silve C 82 Ny Mone	Depityment Estina	Must Cas VP 1018.01	Operational Barrier () :	107 A U 6004 Operational Status O © 0 K	B# DWR Sissa 41 ↑ 4 ÷ 0 0 00 21 ↑ 2 ÷ 0 0 00	Twee flate 41 + 4 + 6 31 + 2 + 6 31 + 2 + 6 7 False fair 7 False fair 7 Table fair 0 Table fair 0	Hida Connectivity Status

•NDFC 画面に戻り、[トポロジ(Topology)] 画面でハイブリッド クラウド接続を確認します。次の例 では、NDFC VXLAN ファブリック サイト (シドニー サイト) が1番目と2番目のクラウドサイト (AWS および Azure クラウドサイト)に接続されていることがわかります。

I

図 102:







使用例

- テナントを展開 (109 ページ)
- •ストレッチされた VRF ユース ケース (117 ページ)
- •ルートリークの使用例(155ページ)



テナントを展開

テナントを展開(109ページ)

テナントを展開

サイト間にアンダーレイとオーバーレイの接続が確立されたら、エンドポイントネットワーク/VPC/VNetを展開して、オンプレミスとクラウドサイトに展開されたテナントエンドポイント間の通信を確立する必要があります。

NDOは、VRFとネットワークを定義するためにスキーマとテンプレートの概念を使用します。 NDFCのコンテキストでは、VRFは、あるテナントを別のテナントから分離するために使用さ れます。1つのテナントのすべてのエンドポイントネットワーク(サブネット)は、それぞれ の VRF にマッピングされます。VRF の同じ概念をクラウドに拡張することもできます。VRF は AWS の VPC および Azure の VNet に対応します。

テナントを展開するための次の手順は、前述のすべてのトポロジに適用され、展開された特定 のインフラ構成を活用します。また、次のユース ケースのいずれにも適用されます。



(注) NDOには、事前に構築された dcnm-default-tn テナントがあり、オンプレミス サイトとクラ ウドサイトに関連付けることができます。ハイブリッド クラウド接続を展開するときに、こ の事前構築済みの dcnm-default-tn テナントを NDFC およびクラウドサイトに関連付けること をお勧めしますが、必要に応じて、独自のテナントを最初から作成することもできます。

ステップ1 NDO で [アプリケーション管理(Application Management)] > [テナント(Tenants)]に移動します。

図 103:



テナントウィンドウが表示されます。

図 104:

≡ cisco Nexus Dashb	oard 🏩 Orchestrator 🗸					Feedback 💄 🔮
 Dashboard Sites 	Tenants					④ ද ়ি Add Tenant
Application Management	Filter by attributes					
Fabric Management	Name	Description	Assigned To Sites	Assigned To Users	Assigned to Templates	
Operations Infrastructure	common	Common tenant for use with all other tenants	4	1	0	1000
& Integration	infra	Infra tenant for use with all other tenants	2	1	0	
	dcnm-default-tn	Default tenant for NDFC	1	1	0	
	10 V Rows				Page 1 of 1	\ll $<$ 1-3 of 3 $>$ \gg

ステップ2 dcnm-default-tn テナントをクリックします。

dcnm-default-tn テナントの [テナントの更新(Update Tenant)] ページが表示されます。

図 105:

≡ cisco Nexus Dashi	board 🔺 Orchestrator 🗸			Feedback 💄 🇿
Update Tenant dcnn	n-default-tn			Ot} X
	General Settings			
	Display Name *			
	dcnm-default-tn			
	Internal Name: donm-default-tn Description			
	Default tenant for NDFC			
	Associated Sites			
	Site Name	Site Type		
	Sydney 12.1.2.275	NDFC		
	Azure 25.1(10)	Azure		
	AWS 25.1(1e)	AWS		
	5 V Rows		Page 1 of 1 $\ll <1-3$ of 3 $> \gg$	
	Associated Users			
	No user is available			
Cancel				Save

ステップ3 画面に表示されているサイトを選択します。

外部ファブリックサイトはリストに表示されないことに注意してください。外部サイトは、オンプレミス サイトとクラウドサイト間の接続を提供するためにのみ使用され、外部ファブリックにはエンドホストが ないため、外部ファブリックにテナントを展開する必要はありません。

図 106:

≡ cisco Nexus Dashboard	单 Orchestrator 🗸		
Update Tenant dcnm-defa	ult-tn		
Gen	eral Settings		
Display	Name *		
dcnm-	default-tn		
Internal N	Name: dcnm-default-tn		
Descrip	ation It tenant for NDFC		
Asso	ociated Sites		
0	There are cloud site settings that need to be configured.		
(2)	Sites selected		Unselect items
	Site Name	Site Type	
	Sydney 12.1.2.275	NDFC	/
	Azure 25.1(1e)	Azure	/
	AWS 25.1(1e)	e Aws	
5	~ Rows		Page 1 of 1 $\ll <1-3$ of 3 $> \gg$

ステップ4 クラウド サイトの場合は、編集ボタン (鉛筆アイコン)をクリックして、各クラウドアカウントに必要な 情報を入力します。

ユーザーテナントにはAWSの追加アカウントが必要ですが、Azureの場合は、Azureインフラテナントと同じサブスクリプションを使用できます。

 たとえば、AWSクラウドサイトの編集ボタンをクリックした後、[AWSアカウント設定(AWSAccount Setting)]エリアで、[アクセスタイプ(Access Type)]で[信頼(Trusted)]をクリックし、関連する AWSアカウント識別子をそのフィールドに入力します。

図 107:

≡ cisco Nexus Da	shboard 🔶 Orchestrator 🗸		
Update Tenant dc	nm-default-tn		
	General Settings		
	Display Name *		
		Tenant Setting for AWS site ×	
		General Setting	
	Default tenant for NDFC	Security Domains	
		Select Security Domain(s)	
	Associated Sites	AWS Account Settings	
		AWS Account Id *	
	() There are cloud site settings that need to be	Access Type	
		Untrusted Trusted Organization	
	3 Sites selected		Unselect litems
	Site Name	Cancel	
	Sydney 1212.275	NDFC	/
	O Azure 25.1(3e)	O Azure	/
	💟 🌒 AWS 283(1e)	AWS	1
	5 V Rows		Page 1 of 1 《<1-3 of 3 >》

AWS のテナントのさまざまなアクセス タイプの詳細については、[AWS インストール ガイドの Cisco クラウド ネットワーク コントローラ(Cisco Cloud Network Controller for AWS Installation Guide)]、リ リース 25.1 (1) 以降の「Setting Up the AWS Account for the User Tenant」 セクションを参照してくださ い。

•同様に、Azure クラウドサイトの編集ボタンをクリックした後、テナントが管理されているかどうか に応じて、必要な情報を入力します。

date Tenant c	lcnm-default-tn		
	General Settings		
		Town to this for town the	
	Internal Name: dcnm-default-tn	lenant Setting for Azure site ×	
		General Settings	
	Default tenant for NDFC	Security Domains	
		Select Security Domain(s)	
	Associated Sites	azureAccount Settings	
		Mode	
		Create Own Select Shared	
		The second secon	
	Site Name		
	Sydney 12.1.2.375	Cancel Save	1
	Azure 25.1(1e)	Azure	1
	AWS (25.10)	S AWS	

Azure のテナントのさまざまなアクセスタイプの詳細については、[Azure インストールガイドの Cisco クラウドネットワークコントローラ(Cisco Cloud Network Controller for Azure Installation Guide)]、リ リース 25.1 (1) 以降の「Adding a Role Assignment」セクションを参照してください。

ステップ5 テナントが正しく展開されたことを確認します。

たとえば、次の図では、dcnm-default-tn テナントには3つのサイトがマップされています(1つのオンプレミス NDFC サイトと2つのクラウドサイト)。

図 109:

≡ cisco Nexus Dasht	ooard 📃 🙏 Orchestrator 🗸		s n Lisp			Feedback 💄 ?
Dashboard	Tenant dcnm-default-	tn has been successfully updated.				×
Sites	Tananta					
Application Management	lenants					
Fabric Management					ίΩ.	Add Ienant
Operations	Filter by attributes					
🔿 Infrastructure	Name	Description	Assigned To Sites	Assigned To Users	Assigned to Templates	
Integration	common	Common tenant for use with all other tenants	4	1	0	
	infra	Infra tenant for use with all other tenants	2	1	0	
	dcnm-default-tn	Default tenant for NDFC	3	1	0	
	10 V Rows				Page 1 of 1 \ll	< 1-3 of 3 > >>

≡ cisco Nexus Dash	nboard 🔶 🌲 Orchestrator 🗸				Feedback
Dashboard	Tenants			Sites	
Sites				Q Search	Sites Sydney
Application Management	Filter by attributes			Sydney	
Fabric Management	Name	Description	Assigned To Sites	- dcnm-default-tn Azure	Critical major minor warning
Operations Infrastructure	common	Common tenant for use with all other tenants	4	donm-default-tn	General
@ Integration	infra	Infra tenant for use with all other tenants	2	dcnm-default-tn	Sydney
	dcnm-default-tn	Default tenant for NDFC	3		Type on-premise
	10 v Rows				Cloudsec Encryption Not Enabled Site ID 82 Site Controller URLs URL https://172.16.0.191.44.3 Topology
					9 — 🧕

クラウドサイトの Cisco Cloud Network Controller に展開された dcnm-default-tn テナントを確認することも できます。

図 110:

Ŧ	al) Ci	cloud Netw	ork Controller (AWS)							Q 🛛 🔾	000 💶
Dashboard	Тег	nants							0		
Topology	101	lanto									
Cloud Resources		Actions >							Actions ~		
Application Management ^						Application	n Management			Cloud Resources	
Tenants		Health	Name	Description	Application Profiles	EPGs	VRFs	AWS Account	Regions	VPCs	Endpoints
Application Profiles		C Healthy	common		1	0	2		0	0	0
EPGs	G	•		De faith teach							
Contracts		Healthy	NDO	for NDFC	0	0	0	1	*	0	0
Filters			lades.	SILES		15		05750100500			
VRFs		O Major	mra		1	15	2	0	4	1.	12
Services		O Healthy	mgmt		0	0	2		0	0	0
Cloud Context Profiles											
External Networks	1	o 🗸 Rows							Page	1 ∨ of 1 4	

Ŧ	el c	Cloud Ne	Cloud Network Controller (AZURE) 🔥 Arure							000 💶	
Dashboard	То	nante	aanto								0
Topology	Te	nants									۷
Cloud Resources	Filte										Actions ~
Application Management						Applicat	tion Management			Cloud Resources	
Tenants		Health	Name	Description	Application Profiles	EPGs	VRFs	Azure Subscription	Regions	Virtual Networks	Endpoints
Application Profiles		• Healthy	common		1	0	2		0	0	0
EPGs											
Contracts		Healthy	dcnm-default-tn	tenant for	0	0	0	infra	0	0	0
Filters				NDFC sites		1.002					
VRFs		Major	infra		1	12	2	74094178- 785d-	1	1	7
Services								468a-bf23- 41e85a1a3a			
Cloud Context Profiles								da			
External Networks		Healthy	mgmt		0	0	2		0	0	0
Operations ~	1	5 🗸 Rows							Page 1	✓ of 1 < <	1-4 of 4 ▶ ▶
⊖ Infrastructure ∨											

次のタスク

次の使用例のいずれかまたは両方を構成します。

- •ストレッチされた VRF ユース ケース (117 ページ)
- •ルートリークの使用例(155ページ)



ストレッチされた VRF ユース ケース

- •ストレッチされた VRF ユース ケースについて (117 ページ)
- •ストレッチされた VRF ユース ケースの構成 (118 ページ)

ストレッチされた VRF ユース ケースについて

ストレッチ VRF(VRF内)は、すべてのサイト(オンプレミスおよびクラウドサイト)に関 連付けられたテンプレートで単一の(共通)VRFが定義される一般的な使用例です。オンプレ ミスサイトとクラウドサイト間でネットワークを拡張することはできないため、オンプレミ スサイトのネットワークの展開には別のテンプレートが使用されます。

同じ VRF をすべてのサイトに拡張すると、追加のルーティング構成を必要とせずに、サイト 間でプレフィックスを交換できます。CIDR ブロック(クラウド VPC/VNet でサブネットをプ ロビジョニングするために使用)は、この拡張 VRF にマッピングされます。



(注) オンプレミスとクラウドサイト間、またはクラウドサイト間でのレイヤー2サブネットの拡張はサポートされていません。

次の図は、デモスキーマの下で作成される2つのテンプレートを示しています:

- •3つのサイトすべてに展開される VRF を定義する[ストレッチ テンプレート (Stretched Template)]。クラウドサイトの場合、VRF の下でリージョンと CIDR ブロックを定義します。
- オンプレミスのVXLANファブリックに展開されるネットワークを含む on_Prem テンプレート。

図 111 :



ストレッチされた VRF ユース ケースの構成

ステップ1 NDO で、[アプリケーション管理(Application Management)]>[スキーマ(Schema)]に移動し、[ス キーマの追加(Add Schema)]をクリックします。 図 112:

≡ ^{•• ••• ••} cisco Nexus Dashb	ioard 🌐 🙏 Orchestrator	Feedback 上 💿
Dashboard Sites	Schemas	① (*) Add Schema
Application Management Fabric Management Operations	Filter by attributes	
☐ Infrastructure	No Data Found	

ステップ2 スキーマ名を指定し、[追加(Add)]をクリックします。

このユース ケースでは、新しいスキーマに [ストレッチ スキーマ (Stretched Schema)] という名前を付けま す。

図 113:

≡ cisco Nexus Dashboard Orchestrator ∨	الكوي المشاه				
Untitled Schema					
View Overview ~					
Overview					
General	0	Audit Logs			
Name Description Untitled Schema	General	Created	Deleted	Updated 0	Deployee 0
Sites	Name *				
APIC 0 AVIC 0	Description		Sync C)	
			_		
Application Management					

新しい [ストレッチスキーマ(Stretched Schema)] スキーマの [概要 (overview)] ページに戻ります。 ステップ3 [新しいテンプレートを追加(Add New Template)] をクリックします。 図 114:

≡ cisco Nexus Dashboard	rchestrator ~						Feedback 💄 🥑
Stretched Schema						0 / 100	0 Objects Save Schema たよ X
View Overview ~							Add New Template
General		0	Audit Logs				
Name Description Stretched Schema			Created 0	Deleted 0	Updated 0	Deployed 0	Other 0
Sites			Templates				
Type APIC ADIC ADIC ADIC			Sync Status ()	In Sync Out of Sync t	0		
Application Management							
Application Profiles (0) Filters (0) EPGs (0) External EPGs (0)	Contracts (0) E3Outs (0)	VRFs (0) Service Graphs (0)	Bridge Don Networks	nains (0) (0)			0 Total Objects
Topology							

ステップ4 NDFC テンプレートを選択し、[追加(Add)]をクリックします。

オンプレミスおよびクラウドサイトには、NDFC テンプレート タイプを使用する必要があります。 図 115:

≡ ^{• • •} Nexus Dashboard Orche	strator ~		edback 👤 🔮
Stretched Schema		0 / 1000 Objects Saw Sol	homa CJ 🗙
View Overview ~		(Add N	Rew Template
Overview	Select a Template type	×	
Ceneral Name Description Sites Type exercise of			
0 • Altro 0 B • Statio B * Douge Cloud Puttion D	ACI Multi-Cloud • On-pren ACI ate to site • On-pren ACI ate to cloud site • Cloud to cloud site	C state to site retreark retreark	
Application Management		(ALS)	
Application Profiles (0) Filters (0) External EPOy (0)	* Contracts (0) * VMFs (0) * (30uts (0) * Service Graphs (0)	Indigridomental (0) Tatul Objects Tatul Objects	

ステップ5 [表示名 (Display Name)]フィールドに名前を入力して NDFC タイプのテンプレート(たとえば、ストレッ チされたテンプレート)を作成し、[テナントの選択 (Select a Tenant)]フィールドで dcnm-default-tn テナン トを選択して、テンプレートをそのテナントにマップします。 図 116:



ステップ6 [テンプレート プロパティ(Template Properties)] で [オブジェクトの作成(Create Object)] をクリックし、[VRF] を選択して、全てのサイトにストレッチされたVRF を作成します。

図 117:

≡ altude cisco Nexus Dashboard Orchestrator ~	Feedback 🛓 🧿
Stretched Schema	0/1000 Objects Save Schema () 🗙
View Stretched Template ~ (Add New Template)	Template ×
Stretched Template Tenant: dcrm-default-in	Template Settings Display Name* Stretched Template Deployed Name:
Template Properties ~ Attoms ~	Description
Network	Tenant Settings
Let's create an object Click "Create Object" on template properties to create an object	

(注) 新しい VRF を作るより、既に使用したいオンプレミス VRF を作成した場合、[テンプレート プロパティ(Template Properties)]の下、[インポート(Import)]をクリックします。そし て既に作成された VRF をインポートします。

現在、オンプレミスサイトからのVRFとネットワークのインポートのみがサポートされています。

図 118:

≡ ^{ti]iti]it} Nexus Dashboard . Crchestrator ∨		Feed	back 上
Stretched Schema		1 / 1000 Object Save Scher	× 63 🖬
View Stretched Template ~		Add New Template VRF stretched-vrf	×
Stretched Template Tenant: dcnm-default-tn	Associated Sites • in Symc 0 • Out of Symc 0	company to state Common Properties Common Properties	
Template Properties ~	IMP	Actions - Description	
VRFs		Add VRF NDFC Properties VRF ID O	
stretched-vrf		VRF Profile *	
		Default_VRF_Universal VRF_tension Profile * Default_VRF_Exercise (Internal)	
		Loopback Routing Tag 12345	
		Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET	
		Disable RT Auto-Generate	

- ステップ8 拡張 VRF ユース ケースの [ストレッチされたテンプレート (stretched Template)]にすべてのサイト (オンプレミスおよびクラウド サイト)を関連付けます。
 - a) [テンプレート プロパティ(Template Properties)] エリア内で [アクション(Actions)] > [サイトの 関連付け(Sites Association)]をクリックします。

図 119:

≡ ^{d lid li} Nexus Dashboard				Feedback 💄 🥐
Stretched Schema			1 / 1000 Object	Same Scheme 💿 🤨 🗙
View Stretched Template ~	Add New	w Template	Template Stretched Template	×
Stretched Template Version 1 Tenant: dcnm-default-tn	0 Digday) no 0	to sites	Template Settings Display Name* Stretched Template Deployed Name:	^
Template Properties \vee		Actions ~	Description	
Filter VRFs ~	BMPORT - SELECT + Create Objec	Clone Template Delete Template History	ate Type	^
stretched-vrf		Rollback Sites Association	default-tn	
		Tag	-default-tn	
			Description Default tenant for NDFC	

b) すべてのサイトを選択し、[OK] をクリックします。

これにより、各サイトを個別に選択して、このテンプレートで定義されたオブジェクト(この特定のケースでは、拡張された VRF)のサイトレベルの構成をプロビジョニングすることもできます。

巡 120:

≡ cisco Nexus Dashboard . • Ore	hestrator v			Feedback 💄 🧿
Stretched Schema				× 63 ©
View Stretched Template \vee		Add New Template	Template Stretched Template	×
Stretched Template Version 1 Tenant: denmi-default-in	Associated Sites ** sync 0 ** optication 2	(Instanting)	Template Settings Display Name* d Template	
Template Properties ~	Add Sites To Stretched Template		× where on	
	AWS 251(a)		Type	
VRFs ~ stretched-vrf	O Azire ZSA(te) ZSA(te) Us.3275		erungs ame fault-tn	
			fault-tn on snant for NDFC	

サイトがテンプレートに関連付けられると、それらは[**テンプレートのプロパティ(Template Properties)**]の下に表示されます。

図 121 :

≡ dirdh tisco Nexus Dashboard . Crchestrator ∨		Foedback 💄 🥐
Stretched Schema	1 / 1000 Object	Save Schema 🛈 🗘 🗙
View Stretched Template ~	Template Stretched Template	×
Stretched Template Version 1 Applied to 3 sites Tenant: dcmi-default-in	Template Settings Display Name* Stretched Template Deployed Name: Description	^
Template Properties ~ Artises - Artises - Articles - Ar	Template Type NDFC	
Azure © Outet type Sydney @ Count type stretched-vrf	Tenant Settings Display name dcnm-default-tn Name dcnm-oefault-tn Description Default tenant for NDPC	^

- **ステップ9** [テンプレートのプロパティ(Template Properties)]をクリックして最初のクラウドサイト(このユースケースの例ではAWSサイト)を選択し、VRFを適切なリージョンに関連付けて VPC を作成します。
 - a) VRFをクリックし、[リージョンの追加(Add Region)]をクリックして、選択したリージョンにVPC を作成します。

図 122 :

≡ cisco Nexus Dashboard Orchestrator ∽	Feedback 上 🕄
Stretched Schema	1/1000 Object Save Schema の たと 🗙
View Stretched Template ~	Add New Template VRF stretched-vrf ×
AWS Version 1 Stretched Tamplate	Denixy in suise
Tenant: down-default-tn AWS © out at time: >> Filter	Actions Template Properties Actions Display Name * stratched-vrf Description N/A VRF ID O
VRFs ~	Site Local Properties
	Leak Routes Target VRF Routes Add Leak Route

[クラウド リージョン CIDRs を追加(Add Cloud Region CIDRs) ウィンドウ が表示されます。

b) [リージョン(Region)]フィールド内で VPC を作成したいリージョンを選択します。

図 **123**:

≡ ^{•(• •} Nexus Dashboard .	Orchestrator ~			Feedback 💄 💿
Stretched Schema			1 / 1000 Objec	savo Schema 🗿 🞲 🗙
View Stretched Template ~		[Add New Template]	VRF stretched-vrf	×
Add Cloud Region CIDRs	2			×
Region * Select region				<u></u>
us-west-2 us-east-1				
CIDR Add CIDRs VPN Gateway Router	Туре	VRF.		
Hub Network				¢k.

- c) CIDRフィールド内で[CIDR を追加(Add CIDRs)]をクリックし、VPCの CIDR ブロックを定義します。
- d) サブネットを作成するためと可用性ゾーンにマップするためにに[サブネットを追加(Add Subnet)] をクリックし、[保存(Save)]をクリックします。

図 124 :

císco Nexus Dashboard 🔶 Orchestrato	10. ×				Feedback
etched Schema					1/1000 Object Save Schema 🕥 🗘
dd Cloud Region CIDRs					
ion *					
s-west-2					×~
ntainer Overlav					
Enabled					
Rs					
)R				Туре	VRF
IDP Type () Primary Secondary Id Subnets Jubnet Name Private Link Labels	Availability Zone				
0.230.1.0/24	us-west-2a	~	×		
0.230.2.0/24	us-west-2b	~	\times		
Add Subnet					
	Cance	T	Save		
		_			

e) [ハブネットワーク(Hub Network)] フィールドの下にあるチェックボックスをオンにして、AWS 用の Cisco クラウド ネットワーク コントローラで作成されたハブ ネットワークを選択します。

Cisco クラウド ネットワーク コントローラがサブネットをトランジット ゲートウェイに付加するこ とを許可します。これは、トランジット ゲートウェイが既に接続のあるサブネットからクラウド上 の Cisco Catalyst 8000Vsにトランジット ゲートウェイに接続を積み上げます。

f) [サブネット (Subnet)] フィールド内でトランジット ゲートウェイに使われるサブネットをマップ します。

トランジットゲートウェイに専用のサブネットを使用するのがベストプラクティスです。

図 125:

Ξ cisco Nexus Dashboard Orchestrator ∨			Feedback 💄 🔮
Stretched Schema			1/1000 Object Save Schema 🛈 🗘 🗙
Add Cloud Region CIDRs			×
Region *			
us-west-2			X ~
Container Overlay Enabled			
CIDRs			
CIDR	Туре	VRF	
10.230.0.0/16	Primary	stretched-vrf	/=
🚯 Add CIDRs			
VPN Gateway Router Hub Network			
To change the selected Hub Network, uncheck the Hub Network option	on and deploy the template first. Then re-enable the option, select the new	lub Network, and redeploy the template.	
Hub Network			
hub-1 - infra			
Subnets			
10.230.1.0/24 × 10.230.2.0/24 ×			×
			Ok

- (注) または、ハブネットワーク(TGW)への接続に、アベイラビリティゾーンごとに専用の /25 サブネットを使用できます。これにより、エンドポイントサブネット全体をエンドホストに使用できるようになります。
- g) [OK]をクリックします。

AWS テンプレート ウィンドウに戻ります。

この構成が展開されると、CIDR 10.230.0.0/16の VPC が AWS クラウドに作成され、us-west-2a と us-west-2bの可用性ゾーンにまたがり、10.230.1.0/24 と 10.2302.0/24 サブネットがそれぞれ作成され ます。

27	176.
<u>×</u>	120.

図 127:

⊟ ^{-t]tull} t Nexus Dashboard . Orchestrator ∨			Feedback 💄 🥐
Stretched Schema	1/1000	Object Save S	chema の 代え X
View Stretched Template ~	VRF stretched-vrf		×
AWS Version 1 AWS transition AWS transition AWS transition	 critical major	- minor	- warning
AWS © Out of Spec V Filter VBFs Vistached-vvrf	Template Properties Display Name * stretchod-stretchod Description N/A VRF ID Q 150555 Site Local Properties Context Profiles		^
	Region		
	us-west-2 CIDR: 10.230.0.0/16		/ =
	Add Region		
	Leak Routes		
	Target VRF	Routes	
	😔 Add Leak Route		

- **ステップ10** [テンプレートのプロパティ(Template Properties)]をクリックして2番目のクラウドサイト(このユー スケースの例ではAzureサイト)を選択し、VRFを適切なリージョンに関連付けてVNetを作成します。
 - a) VRF をクリックし、[**リージョンの追加(Add Region**)] をクリックして、選択したリージョンに VNet を作成します。

≡ ^{- e} tisco Nexus Dashboard	Feedback 🛓
Stretched Schema	1/1000 Object Save Schema ⊙ €↓ 🗙
View Stretched Template ~	Add New Template VRF stretched-vrf
Azure Version 1 Stretched Template	centreal major minor warring
Tenant: donn-default-in	Actions
VRFs 😔	Ver ID () 150555 Site Local Properties Context Profiles Region
	Add Region Leak Routes Target VRF Routes Add Leak Route

[クラウドリージョン CIDRs を追加(Add Cloud Region CIDRs) ウィンドウ が表示されます。

- b) [リージョン(Region)]フィールド内で VNet を作成したいリージョンを選択します。
- c) CIDRフィールド内で[CIDR を追加(Add CIDRs)]をクリックし、VNetの CIDR ブロックを定義します。
- d) サブネットを作成するために[サブネットを追加(Add Subnet)]をクリックし、[保存(Save)]をク リックします。

図 128:

cisco Nexus Dashboard 🌲 Orchestrator 🗸			Feedback
etched Schema			1/1000 Object Save Scheme 🕢 🏷
dd Cloud Region CIDRs			
ion *			
istus			XX
tainer Overlay Enabled			
Rs			
R	Туре	VRF	
IDR *			
70.1.0.0/16			
DR Type 🔘			
Primary			
) Secondary			
Parent VRF Hosted VRF			
ubnet Name Private Link Labels Availability Zone			
0.1.1.0/24 × X			
Add Subnet			
Cancel Save			

e) [VNet ピアリング(VNet Peering)]フィールドの下にあるチェックボックスをオンにして、Azure 用のCisco クラウドネットワークコントローラで作成された [デフォルト(Default)] ハブネットワークを選択します。

≡ disco Nexus Dashboard . Crchestrator ∨		Feedback 💄 🔿
Stretched Schema		1000 Object Save Schema 🗿 🏷 🗙
View Stratchod Template v Add Cloud Region CIDRs	(Add New Template)	× ×
Region * eastus Container Overlay Enabled		× ~]
CIDRs CIDR Type	VRF	
70.1.0.0/16 Primary Q Add CIDRs	stretched-vrf	
VPN Gateway Router ↓ VNet pening Hub Network Default		× ~) @

f) [OK]をクリックします。

この構成が展開されると、構成した VNet(この例では 70.1.0.0/16)が Azure の適切なリージョン(この例では eastus Azure リージョン)に作成され、VNet ピアリングが Azure のインフラ テナント内の インフラ VNet に構成されます。。

27	120 .	
λ	130.	

Ξ cisco Nexus Dashboard					Feedback 上 🧿
Stretched Schema			1/1	000 Object Save	Schema 🛈 🗘 🗙
View Stretched Template \vee		Add New Template	VRF stretched-vrf		×
Azure Version 1 Stretched Template	Associated Sites In Sync Out of Sync 3	Deploy to siles	major	- minor	- warning
Filter VRFs Stretched-vrf		Actions -	Template Properties Display Name * stretched-wf Desloyed Name: stretched-wf Desloyed Name: stretched-wf NA VRF ID15055 Site Local Properties Context Profiles Region		^
			eastus CIDR: 70.1.0.0/16		/ =
			Add Region		
			Target VRF	Routes	
			🚯 Add Leak Route		

- ステップ11 [テンプレートプロパティ(Template Properties)]をクリックし、オンプレミスサイト(このユースケースの例ではシドニーサイト)を選択してから、stretched-vrf VRFを選択します。
- ステップ12 右側のペインで [静的リーフの追加(Add Static Leaf)] をクリックします。

図 **131** :

≡ ^{el}ede- cisco Nexus Dashboard .}	Feedback 💄	0
Stretched Schema	1/1000 Object Serve Schema 🕢 🗘 🗙	
View Stretched Template ~	Add New Template Stretched-vrf	¢
Sydney Wersion 1 Stretched Template	Crystay in salars	
Tenant: doim-default-in Sydney @ out of Syme. > Fifter VRFs >	Template Properties ^ Display Name * stretched-orf Description N/A VIAP ID O 150555	
Stretched-vrf	Site Local Properties Autocast Routed Muticast Routed Muticast Routed Muticast Routed Muticast Routed Muticast Routed Muticast Routed R	

[静的リーフの追加(Add Static Leaf)] ウィンドウが表示されます。

ステップ13 [リーフ(Leaf)]フィールド内で、VRFが展開されるべき場所のリーフ/ボーダー/ボーダー ゲートウェイ デバイスを選択し、Okをクリックします。

🗵 132 :

≡ ^{d lulli} Cisco Nexus Dashboard						Feedback
Stretched Schema				1 / 100	0 Object Save S	ichema 💿 t
View Stretched Template ~		Add New Template	VRF stretched			
Sydney Version 1 Stretched Template	Associated Sites		- critical	- major	- minor	- warning
Sydney Country - Service -	Add Static Leaf Leaf Indic-leaf1 - ndic-leaf2	× Actors ~	Template Pr Display Nam stratched-vi Depoyed Nam Description N/A VRF ID () 150555 Site Local Pr Tenant Rout RP External	operties 6 * f e structured-vert roperties ed Mutticast		
			Static Leaf Node/Swit	iodes ich : Leaf		

[ストレッチされたテンプレート (Stretched Template)] ページに戻ります。

ステップ14 [静的リーフの追加(Add Static Leaf)]を再度クリックして、このVRFが展開される追加のリーフ/境界/ 境界ゲートウェイデバイスを追加します。

> この例では、リーフノードに VRF を展開する必要があります(VRF にマップされたネットワークのエンドポイントに接続される)。そして、VRF からクラウドサイトへのレイヤー3 接続に拡張するために BGW スパインノードを展開する必要があります。

図 133 :

≡ cisco Nexus Dashboard . Orchestrator ∨						Feedback 👤 📀
Stretched Schema				1 / 100	0 Object Save S	chorma 🕘 🔃 🗙
View Stretched Template ~		Add New Template	VRF stretched			×
Sydney Version 1 Stretched Template	Associated Sites		- critical	- major	- minor	warning
Tenant: doon-default-in Sydney • to entropy	Add Static Leaf	× (Actions -)	Template Pro Display Name stretched-vrt Deployed Name Description	pperties s * f strutched-wrf		
VRFs V	VLAN	× ~)	N/A VRF ID () 150555 Site Local Pr	operties		
		OK	RP External Static Leaf N Node/Switz	odes		
			ndfc-leaf1 VLAM: N/A	~ ndfc-leaf2		/ 8
			Add Static	Leaf		

この VRF が展開されるすべてのリーフ/ボーダー/ボーダー ゲートウェイ デバイスを追加すると、[スト レッチされたテンプレート (Stretched Template)]ページに表示されます。

াগ্যা	12/
	104.

⊟ diuth tisco Nexus Dashboard .≵ Orchestrator ∨	Feédback 🔔
Stretched Schema	1/1000 Object Save Schema の 代え X
View Stretched Template ~	Add New Temptate VRF ×
Sydney Version 1 Structured Template	Cheptory In survey.
Sydney O our at Sees	Template Properties Actions Actions Statichos' with Description N/A VIFI ID 150555 State Local Properties Temant Routed Multicast BP External Static Lies Nodes
	ndfc-leaf2 / 1
	VLAN INA ndfe-spinn1 / = VLAN INA

- ステップ15 シドニーサイトの横にある矢印をクリックし、ドロップダウンメニューから[テンプレートのプロパティ (Template Properties)]を選択します。
- **ステップ16 [サイトへ展開(Deploy to sites)]**をクリックします。 図 *135*:

≡ disc0 Nexus Dashboard . Crohestrator ~	Feedback 🛓 🕐
Stretched Schema	1/1000 Object Save Schema の たよ 🗙
View Stretched Template ~	Template X
Stretched Template Version 1 Applied to 3 plans Temant: dcmm-default-in	Template Settings ^ Display Name* Stocked Template Description
Elemplate Properties Actions - Filter IMPORT - SELECT	Template Type NDFC
VRFs ··· Add VRF	Tenant Settings

[サイトに展開(Deploy to Sites)] ウィンドウが表示され、拡張されたテンプレートが展開される3つの サイトが表示されます。

図 136:

cisco Nexu	Dashboard 🏩 o	rchestrator ~					Feedback 💄 🔇
retched Schen	na					1 / 1000 Object	0 03 X
ew Stretche	d Template 🗸				Add New Template	Template Stretched Template	×
Stretched	Template Version 2	I	9 Associa	Ited Sites	Deploy to sites	Template Settings Display Name*	^
Deploy to site	es						×
Deploy to site	əs					View Version History	X Deployment Plan
Deploy to site	es					View Version History	X Deployment Plan
Deploy to site nodifications	S 🖉 Modified <table-cell> 😭</table-cell>	f Deleted 🛛 🧭 Config Drif	t 🧹 🕈 Migrated			View Version History	X Deployment Plan
Deploy to site nodifications	S 🖉 🖉 Modified 🕑 📾	Deleted 🧭 « Config Drif Souther States (Config Drift)	t d Migrated	Sydney 12.1.2.275		View Version History	Deployment Plan

ステップ17 [展開プラン (Deployment Plan)]を追加認証のためにクリックします。そして、その特定のサイトの展開プランを表示するために各サイトをクリックします。

図 137:

≡ cisco Nexus Dashboard Ore	hestrator 🗸	Feedback 上 💿
Stretched Schema		1/ 1000 Object.
View Stretched Template ~		Add New Template Strenched Template
Deployment Plan		×
General Information		
Template Stretched Template	Schema Stretched Schema	Tenant dcnm-default-in
Plan		
AWS Azure Sydney		Ocreated ODeleted OModified OExisting Shadow
		View Payload
O dcnm-default-tn O stretchied-vrf	O route-target:as2-nn4:23456:150	
<u></u>		

図 138:

	back 上 💿
1/3000 Object. Terr Owen 1	× 67 ©
Add New Template Add New Template Stretched Template	×
	×
Tenant dcnm-default-tn	
Ocreated Oblieted OModified OExisting @Sha	idow
(View Pay	bool
	Aur rever rempter Tennet Gorrented Obeleted OModified OExisting State View Pay

図 **139**:

cisco Nexus Dashboard . Or	chestrator v	Feedback
tretched Schema		1/ 1000 Object
Deployment Plan		×
General Information		
Template Stretched Template	Schema Stretched Schema	Crim-default-tn
Plan		
AWS Azure Sydney		O Created O Deleted O Modified O Existing Shadow
		(View Payload)
	orute-target:as2-nn4:23456:301	
O dcnm-default-tn Stretched-vrf	© route-target:as2-nn4:23456:150	
	Indic-leaf1 ~ ndfc-leaf2	
	ndfc-spine1	

ステップ18 [展開(Deploy)]を NDO が構成をサイト固有のコントローラ(NDFC とクラウド ネットワーク コント ローラ)にプッシュするためにクリックします。

図 140:

Stretched Schema View Stretched Template	Associated Sites Associated S	Add New Template Add New Template Stretched Template Template Settings Display Name*	a C C X
View Stretched Template Stretched Template Wester 2 Deploy to sites Modifications	Associated Sites	Add terr Template Template Stretched Template Template Settings Display for stars	×
Stretched Template Verses Deploy to sites Modifications + Created C Modified C Defect C	Associated Sites	0 Duplay for kites	×
Deploy to sites Modifications	<table-cell> 🌌 Config Drift: 🕑 🗢 Migrated</table-cell>		×
Modifications	V / Config Drift V C Migrated		
🗸 + Created 🗸 Z Modified 🗹 🗂 Deleted 🗸	Config Drift 🗹 🧟 Migrated		View Version History Deployment Plan
Object Type Name State	AWS 25.1(1e)	8Y 2275	
VRF stretched-vrf + c	+ Created + Created +	eated	

- ステップ19 構成が正常に展開されたことを確認します。
 - NDFC での VRF 展開を表示するには、[トポロジ (Topology)]ビューに移動し、オンプレミス ファ ブリックの[シドニー (Sydney)]> VRFを選択してから、stretched-vrf を選択します。
 図 141:

A cisco Nexus Dashb	poard
= Fabric Controller	
	Data Center / default / Sydney / VRFs (1) / stretched_vrf View Search by Attributes Operation Configuration Hierarchical
	 In-Sync Pending In Progress Out-of-Sync NA Muti-select () Selected

•AWSに展開されたクラウドネットワークコントローラに接続して、最初のクラウドサイト(AWS)の構成が正常に展開されたことを確認します。

[アプリケーション管理(Application Management)]>**VRF**に移動し、stretched-vrf を見つけて、 列 **VPC** をクリックしてから、**[概要(Overview)]**ページに移動して、**[サブネット(Subnets)]**を クリックします。

 Azure に展開されたクラウドネットワークコントローラに接続して、2番目のクラウドサイト (Azure)の構成が正常に展開されたことを確認します。

[アプリケーション管理(Application Management)]>**VRF**に移動し、stretched-vrf を見つけて、 列[仮想ネットワーク(Virtual Networks)]をクリックしてから、[概要(Overview)]ページに移動 して、**[サブネット(Subnets)**]をクリックします。

- **ステップ20** オンプレミスサイトにネットワークを展開するために、[デモ スキーマ (Demo Schema)]の下に別のテンプ レートを作成します。
 - a) [デモ スキーマ (Demo Schema)]テンプレートで、[新しいテンプレートの追加 (Add New Template)] をクリックします。
 - b) NDFC テンプレートを選択します。
 - c) [表示名 (Display Name)] フィールドに名前を入力して NDFC タイプのテンプレート (たとえば、 On-Prem テンプレート)を作成し、[テナントの選択 (Select a Tenant)] フィールドで dcnm-default-tn テナントを選択して、テンプレートをそのテナントにマップします。

図 142:

≡ dituții. cisco Nexus Dashboard . Orchestrator ∨		Feedback 上 💿
Stretched Schema		1/1000 Object Save Schema ④
View On-Prem Template \vee		Add New Template On-Prem Template X
On-Prem Template	Associated Sites In Sync 0 Out of Sync 0	Discov for stars
Template Properties ~	MPORT - SELECT	Actions + Create Object Templata Type NOFC
Click "Create Ob	Let's create an object ject" on template properties to create an object	Tenant Settings Setect a Tenant* dcrem-default-In X Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y

ステップ21 On-Prem テンプレートの VRF の下に net20 ネットワークを作成します。

- (注) 新しい VRF を作るより、既に使用したい VRF を作成した場合、[テンプレート プロパティ (Template Properties)]の下、[インポート(Import)]をクリックします。そして既に作成 された ネットワーク をインポートします。
- a) [テンプレート プロパティ(Template Properties)]の下、[オブジェクトを作成(Create Object)] をクリックしてネットワークを作成するために[ネットワーク(Network)]を選択します。

図 143:

≡ disco Nexus Dashboard Archestrator ∨	Feedback 💄 💿
Stretched Schema	1/1000 Object Save Schema の たよ 🗙
View On-Prem Template ~ Add New Template	On-Prem Template
On-Prem Template On-P	Template Settings Display Name* On-Prem Template Deproyed Name: Description
BMPORT -> SELECT +Creater Diject -> VRF Network	Template Type NDFC Tenant Settings
Let's create an object Click "Create Object" on template properties to create an object	Select a Tenant * dcnm-default-tn X V

- b) ネットワークの[表示名 (Display Name)] フィールドに名前を入力します(例:net20)。
- c) [バーチャルルートと転送(Virtual Routing & Forwarding)] フィールドで、stretched-vrf VRF を 選択して、net20 をその VRF にマッピングします。

図 144 :	
---------	--

≡ dividio cisco Nexus Dashboard Orchestrator ∨		Feedback	1 0
Stretched Schema		2/1000 Objects Stora Science 🕢 th	×
View On-Prem Template ~		Add New Template net20	×
On-Prem Template Tenant: dotte-default-tri	Associated Sites • Sinc 0 • Our of Sinc 0	Common Properties Display funation	^
Template Properties > Fiter	IMPORT - SELECT	Actions Deployed Name: Description + Creatis Object	
Networks v		Add Network NDFC Properties	^
net20		Layer2 Only	
		Virtual Routing & Forwarding # 1 stretched-wrf X	-
		Network Profile *	
		Default_Network_Universal ×	
		Default_Network_Extension_Universal ×	
		VLAN ID	
		VLAN Name	
		* Gateway IP	
		Add Subnet Suppress ARP	_

d) [ゲートウェイ IP (Gateway IP)]フィールドで、[サブネットの追加 (Add Subnet)]をクリックします。

サブネットの追加ウィンドウが表示されます。
e) [ゲートウェイ IP の追加(Gateway IP)]をクリックしてゲートウェイ IP アドレスを入力し、チェッ クマークをクリックして値を受け入れ、[追加(Add)]をクリックします。

🗵 145:

≡ cisco Nexus Dashboard . Crchestrator ~		Feedback	10
Stretched Schema		2 / 1000 Objects	<i>62</i> ×
View On-Prem Template V	[Add Ways Tomption]	Network net20	• ×
On-Prem Template Tenser: down-default to	Associated Sites •• bire 0 •• bire 0 •• bire 0	O O O O O O O O O O O O O O	
Template Properties ~	(Attorn · ·)	Deployed Name Description	
Retworks · ·	Add Subnet × Cateway IP Type 17216.20.1/24 primary ✓ 😭 Add Network	NDPC Properties Notwork (0)	
		Usyot 2 Univ	
		Network Profile * Default_Network_Universal	
		Default_Network_Extension_Universal	
		Gateway IP Add Subnet Suppress ARP	

ゲートウェイ IP アドレスは[ゲートウェイ IP (Gateway IP)]フィールドに表示されます。 図 146:

≡ diadio Nexus Dashboard Orchestrator ~	Feedback
Stretched Schema	2/1000 Objects Sever Schema () ()
View On-Prem Template ~	Add New Template Network
Associated Sites	UNED IN CONSERVIT SCHOMA UNED IN YOTHIN ROHINAN 0 0
On-Prem Template Tenant: dcnm-default-tn O · Gut ef sync · Gut ef sync	Disclery In datas Common Properties
Template Properties V	net20 Deployed Name:
Filter	Actions Description MPORT SELECT + Create Object
Networks ~	Add Network Network ID 🕥
net20	Layer2 Only
	Virtual Routing & Forwarding 🗮 *
	stretched-vrf X V
	Network Profile *
	Default_Network_Universal
	Network Extension Profile *
	Default_Network_Extension_Universal 🛛 🕹 🗸
	VLANID
	VLAN Name
	* Gateway IP
	172.16.20.1/24

f) 必要な場合、ネットワークのオプショナルパラメータを定義します。

ステップ22 [テンプレート プロパティ (Template Properties)]エリア内で [アクション (Actions)]>[サイトの関連 付け (Sites Association)]をクリックします。

図 147:

E cisco Nexus Dashboard Crchestrator			Feedback 👤 (
Stretched Schema			2/1000 Objects Save Schema 🛈 🏌 🗙
View On-Prem Template ~		Add New Template	Network O ×
On-Prem Template Tenan: donm-default-tn	Associated Sites In Sync 0 Ot of Sync 0	Dejacy in same	USED IN CORRECT COLOMA O O Common Properties Display Name*
Template Properties V		Actions	net20 Deployed Name: Description late
🔘 Networks 🗸		Sites Associ	ation perties
net20			Layer2 Only
			stretched-vrf × ~
			Network Profile *
			Default_Network_Universal X V
			Network Extension Profile *
			Default_Network_Extension_Universal $\times \lor$
			VLAN ID
			VLAN Name
			* Gateway IP
			172.16.20.1/24 / 😭

ステップ23 このテンプレートをオンプレミス サイト (このユース ケースの例ではシドニー サイト) にのみ関連付け、[OK] をクリックします。

図 148:

≡ disco Nexus Dashboard . Orchestrator -				Feedback 1
Stretched Schema			27.1000 Objects	ave Schema の たえ X
View On-Prem Template ~			Network net20	© ×
On-Prem Template	Associated Sites * h byc 0 * h draf Size 0		Common Properties Display Name*	
Template Properties ~	Add Sites To On-Prem Template	×	net20 Description Description	
Networks ~	AMS 251mi 251mi		NDFC Properties Network ID ()	
	Sydney ULLER:		Victual Routing & Forwarding 🐧 * stretched wrf Network Profile *	
			Default_Network_Universal Network Extension Profile * Default_Network_Extension_Universal	
			VLAN ID VLAN Name	

[On-Prem テンプレート (On-Prem Template) ウインドウに戻ります。

ステップ24 [テンプレートプロパティ (Template Properties)]ドロップダウンから、オンプレミスサイト(このユースケースの例ではシドニーサイト)を選択し、net20ネットワークをクリックしてから、[静的ポートの追加(Add Static Port)]をクリックして、このネットワークを展開するポートを追加します。
 [静的ポートの追加(Add Static Port)]ウィンドウが表示されます。

図 149:

≘ -iju-iju cisco Nexus Dashboard ≛ Orchestrator ->				Feedback 1 0
Stretched Schema		2/100	Objects Save S	chema 🕘 tù 🗙
View On-Prem Template \sim	Add New Template	letwork et20		×
Sydney Christian Sydney Christian Sydney Sydney	Peoplely to white	- ical major	- minor	- warning
Tenant: domination: Sydney • Good statut: Fitter • Networks · Imt20	Actions Decision of the second	mmon Properties play: Name * 20 play: Name * 20 scription verk ID O tocal Properties ant: Routed Multicast bite L3 Gateway Boder CP Loceback ID		~
		CP Servers erver Address Add DHCP Server tic Ports h eaf VLAN Add Static Port	Ports	

- **ステップ25** [静的ポートの追加(Add Static Port)] ウィンドウで[パスを追加(Add Path)]をクリックします。 [静的ポートの追加(Add Static Port)] ウィンドウが表示されます。
- ステップ26 [リーフ(Leaf)]フィールドで展開したいネットワークのデバイスを選択します。
- ステップ27 (任意) VLANフィールドに必要な情報を入力します。
- ステップ28 [ポート (Port)]フィールドで展開したいネットワークのポートを選択します。
- ステップ29 [保存(Save)]をクリックします。

🗵 150:

=	hestrator ~			Feedback 💄 ?
Stretched Schema			2 / 1000 Objects Save S	thema 💿 tł 🗙
View On-Prem Template ~	AA	Id New Template	Network	×
Sydney	Add Static Port		x -: - major minor	warning
On-Prom Tamplate Tenant: dcnm-default-tn:	Path Leaf	VLAN Por	ts Properties	
Sydney Courd Syns	Leaf ndtc-leaf1 ~ ndtc-leaf2		iame.	
	VLNN 2320		10 O	
Networks			Il Properties	
	Add Path		3 Geteway Borden	
		Su	opback ID	
			Server Address	
			Static Ports Path	
			Add Static Port	

[静的ポートの追加(Add Static Port)] ウィンドウに戻ります。

ステップ30 [静的ポートの追加(Add Static Port)]ウィンドウで[送信(Submit)]をクリックします。 図 *151*:

≡ disco Nexus Dashboard . Crchestrator					Feed
Stretched Schema					
View On-Prem Template ~				Add New Template	Network met20
On-Prem Template Tensant done-default-in	Associated Sites Asociated Sites Asociated Sites Asocia				major critical minor was Common Properties Display Naria *
Sydney Constant V	Add Static Port	M AN	Porte	×	net20 Depayer Memoret20 Description N/A Network ID () 134736
Networks	cear ndfc-leaf1 ~ ndfc-leaf2	2320	vPC49 vPC51 vPC52 Hide All	/=	Site Local Properties Tenant Routed Mutlicast Finable L3 Gateway Border
	Add Path			Submit	DHOP Loopback ID DHOP Servers Servers Address
					Add Static Points Basic Points Pain Leaf VLAN Ports Add Static Point

[On-Prem テンプレート (On-Prem Template) ウィンドウに戻ります。

- **ステップ31** オンプレミス サイト (このユース ケースの例ではシドニー サイト)の横にある矢印をクリックし、ドロッ プダウン メニューから [テンプレート プロパティ (Template Properties)]を選択します。
- ステップ32 [サイトに展開(Deploy to Sites)]をクリックします。

19	152	
	132	٠

≘ disele. cisco Nexus Dashboard . L. Orchestrator ~		Feedback 上 💿
Stretched Schema	2 / 1000 Objects	iave Schema の たよ 🗙
View On-Prem Template ~	Template On-Prem Template	×
On-Prem Template Version 5 Applied to 1 sites Tenset: done-default-to Template Properties < Image: State Spectrum Spe	Template Settings Display Name* On-Prem Template Displayed Name: Description	^
Fiter BARGET - SELECT + Create Coget	Template Type NDFC	
Network: Add Network net20	Tenant Settings Display name dcnm-default-tn Name dcnm-default-tn	^
	Description Default tenant for NDFC	

[サイトに展開(Deploy to Sites)] ウィンドウが表示され、テンプレートが展開されるサイトが表示され ます。

図 **153**:

≡ cisco Nexus Dashboard	Orchestrator V			Feedback 👤 📀
Stretched Schema			2 / 1000 Objects	⊙ <i>€}</i> ×
View On-Prem Template ~		Add New Template	Template On-Prem Template	×
	Associated Sites		Template Settings	
Deploy to sites				×
Modifications			View Version Hi	istory Deployment Plan
V + Created V / Modified V 1	📅 Deleted 🧹 🖉 Config Drift 🔽 🗢 Migrated			
Object Type Name	Stydney 12.1.2.275			
Network Net20	+ Created			
				Deploy

ステップ33 [展開プラン (Deployment Plan)]を追加認証のためにクリックします。そして、その特定のサイトの展開プランを表示するためにそのオンプレミスサイトをクリックします。

図 154:

≡ difuito Nexus Dashboard Orchestrator ∨				Feedback 💄 📀
Stretched Schema				s (0 t) ×
View On-Prem Template ~		(Add New Template)	Template On-Prem Template	×
Deployment Plan				×
General Information Or Implate On-them Template	Schema Stretched Schema	G Tenant dorm-default-in		
Pian Sydney			Ocreated ODeleted OModified	OExisting Shadow
O dome default-tn O met20 O dome default-tn O met20 O stretched-vrf O vPC1	49 51 52			(Vew Payload)

ステップ34 [展開(Deploy)]をクリックして、NDOがNDFCに構成をプッシュします。

図 155 :

≡ cisco Nexus Dashboard . Contestrator ~	Feedback 🛓
Stretched Schema	2/1000 Objects (100 Science @ 11 🗙
View On-Prem Template ~	Add New Template On-Prem Template
On-Prem Template Version 6 Applied to 1 sites Temant: dom-default-in	65 Last Deployed: Jan 24, 2023 09:22 pm 5 Sync 0 Display for alter Display for alter
Template Properties ~	Actions -
Filter	IMPORT -> SELECT + Create Object Template Type NDFC
Networks ~	Add Network Tenant Settings
	Description Default tenant for NDFC

ステップ35 構成が正常に展開されたことを確認します。

これらの各検証ステップでは、表示されているこのユース ケースの構成のために特定のコマンドが使用 されることにご注意ください。構成に基づいて各コマンドの適切な変数を入れ替えます。

- a) NDO 内で構成が正常に展開されたことを確認します。
 - [ストレッチされた テンプレート (Stretched Template)]が正常に展開されたことを確認します。

义	156 :
---	-------

exition Management c Management c Management c Management c Management is or is or <	shhoard	Schemas			Templates	12-0 Sa
cation Management c Adaragement ations ations since the disclosema Seteched Schema 2 02 Term Produced Schema Seteched Schema 2 02 Seteched Schema 2 02 <th>es</th> <th>oonennao</th> <th></th> <th></th> <th>Q. Search</th> <th>Template Stretched Template</th>	es	oonennao			Q. Search	Template Stretched Template
Anangement ators ators threture ration Nme Templates Tennats 0 0 0 1 Descended Schward ators Descended Schw	plication Management	Filter by attributes			Stretched Template	General
tinder tructure tradien tructure tradien tructure tradien tructure tradient tructure tradient tructure tradient tructure t	bric Management	Name	Templates	Tenants	Stretched Schema	Change Control Status O Deployment Successful
stee By Type	rations istructure	Stretched Schema	2	1	Stretched Schema	Tenant Name dcnm-default-tn
0 0 0 0 0 0 0 0 0 0 0 0 0 0		10 v Rows				And And And And And And And And
0 0 						
0 NITHONG BURNEL BANKS						0 0 Pictee Laout
						O O SERVICE GRAPHS

・[On-Premテンプレート (On-Prem Template)]が正常に展開されたことを確認します。

図 157:

Desthered	Schemas			Templates	CDC.	6.7	
b Dashboard b Sites	Schemas			Q. Search	Template On-Prem Template	emplate	
Application Management	Filter by attributes			Stretched Template	General Chappen Control	Ctatus	^
j Fabric Management	Name	Templates	Tenants	On-Prem Template	O Deployment	Successful	
Operations Infrastructure	Stretched Schema	2 02	1	Stretched Schema	Tenant Name dcnm-default-tr	1	
7 Integration					Sites By Type		
						· APIC	
						Aws Azure	
					Total	• Google Cl	oud Platform
					Application Ma	nagement	^
	10 V Rows				O ANPS	O BRIDGE DOMAIN	
					0	0	
					CONTRACT	EXTERNAL EPO	
					0	0	
					PLTER	LIGUT	

・dcn-default-tn テナントが正常に展開されたことを確認します。

🗵 158 :

	Calan		Te	enants		×
Dashboard	Schemas				Tenants	cf
Sites			q	Search	dcnm-default-tn	
Application Management	Filter by attributes		der	nm-default-tn	General	^
(@ Fabric Management	Name	Templates	Tenants	atched Schema	Name dcnm-default-tn	
C Infrastructure	Stretched Schema	2	1.		Description Default tenant for NDFC	
& Integration					Associated Sites + Sites (3)	- 3 of 4
					Associated Users Users (1)	- 1 of 1
					Assigned Schemas	2 of 1
	10 ~ Rows				Topology	^
					0 0 3	

- b) NDFC で、以下が正常に実行されたことを確認します。
 - •1つの vrf と1つのネットワークが作成されていることを確認します。

🗵 159 :

≡ ¹¹¹¹¹¹¹ cisco Nexus Dashboard	🕀 One View 🗸	Feedback 💄
= Fabric Controller		
☆ Dashboard	Data Center / C default / Svdney	
χ∈ Topology	View A Search by Attributes	Actions
	$(+ - \angle \circ \mathbf{w} \times)$	
👝 Virtual Management 🗸 🗸	Show Logical Links	
Settings		
	Operation Conniguration	
	Hierarchical Virus (1) Virus (1)	meta-laudiuz-wvis meta-laudiuz-wzule vim (3)
	In-Sync Pending	
	 In Progress 	
	• Out-of-Sync	
	• NA	
	Multi-select () 0 selected	
		8
		ndfospine1
		ndfc-leaf2 ndfc-leaf1

• VRF が正常に展開されたことを確認します。

図 160:

\equiv cisco Nexus Dashboard	d 🔰 🗇 One View 🗸	F
F Fabric Controller		
n Dashboard	Data Center / default / Sydney / VRFs (1) / stretched-vrf	
¥ Topology	View A Search by Attributes	
	$(+ - 2 \circ) \times$	
📥 Virtual Management 🗸 🗸	Operation Configuration	
🔅 Settings 🗸 🗸	Hierarchical V	
<u>x</u> ^e Operations ∨	In Progress Out-of-Sync Na Mutii-select O D selected Image: Control of the select of the s	

・ネットワークが正常に展開されたことを確認します。

図 161 :



c) オンプレミスのボーダー ゲートウェイ スパイン デバイスで sh ip route vrf stretched-vrf を入力しま す。

■ ndfc-leaf1 - SecureCRT	– 🗆 ×
File Edit View Options Transfer Script Tools Window Help	
€∮⊑ 2 D D A 🖨 🗘 🛱 🕈 🖪	
ondfc-ext-c8k O Cat8K-AWS ✓ Cat8K-AZURE ✓ ndfc-leaf1 × O ndfc-spine O Cat8K-AWS(1) O Cat8K-AWS-2	4 Þ
Certain components of this software are licensed under the GNU General Public License (GPL) version 3.0 or the GNU Lesser General Public License (LGPL) Version 3.1 or Lesser General Public License (LGPL) version 2.1 or Lesser General Public License is available at http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/gpl-2.1.php and http://www.opensource.org/licenses/gpl-2.2.php and http://www.opensource.org/licenses/gpl-2.2.php and http://www.opensource.org/licenses/library.txt. ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# is prouver stretched-vrff P. Nouter Bable for V&F "stretched-vrff '* denotes best ucast next-hop '** <firiges' <string="" denotes="" in="" output="" vff="" via=""></firiges'>	^
10.230.0.0/16, ubest/mbest: 1/0	

10.230.0.0/16, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 00:16:32, bgp-65084, internal, tag 65091, segid: 150555 tunnelid: 0xa0a0001 encap: VXLAN 70.1.0.0/16, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 00:17:37, bgp-65084, internal, tag 65092, segid: 150555 tunnelid: 0xa0a0001 encap: VXLAN 172.16.20.0/24, ubest/mbest: 1/0, attached *via 172.16.20.1, vlan2320, [0/0], 00:04:48, direct, tag 12345 172.16.20.1/32, ubest/mbest: 1/0, attached *via 172.16.20.1, vlan2320, [0/0], 00:04:48, local, tag 12345 ndfc-leaf1# Default 🗸

このユース ケースでは、ルーティング テーブルを使用して、NDFC リーフ スイッチが次のサブネッ トに到達できることを確認できます。

- AWS : 10.230.0.0/1
- Azure : 70.1.0.0/16
- d) AWS に展開されたクラウド ネットワーク コントローラに接続し、次の検証を行います。
 - dcnm-default-tn テナントが作成され、1 つの VPC が展開されていることを確認します。

← → C ▲ Not secure Https://	44.238.203.132/#/application-mar	nagement/tenants -AWS @ cAPIC-Azure 🧰 AWS Infra	Azure 🙆 Images						ピ ☆	Update :
Ξ	cisco Cloud Ne	etwork Controller (A)	WS) aws						0000	000 💶
Dashboard	Tenants									0
Topology	Torianto									•
Cloud Resources ~	Filter by attributes									(Actions ~)
Application Management					Applica	ation Management			Cloud Resource	es
Tenants	Health	Name	Description	Application Profiles	EPGs	VRFs	AWS Account	Regions	VPCs	Endpoints
Application Profiles	P Healthy	common		1	0	2		0	0	0
EPGs		dcnm-default-to	Default	0	0	1	117378746	2	1	1
Contracts	Healthy	NDO	tenant for NDEC				411	~		
Filters		intra		1	15	2	257501685	2	1	12
VRFs	♥ Major				10	-	230	÷.	1	
Services	Thealthy	mgmt		0	0	2		0	0	0
Cloud Context Profiles	15 Davis							Daga 1	at 1 Id	4 1444 551
External Networks	15 V Rows							Page	○ 011 14	4 1-4014 P PI
Operations										
⊖ Infrastructure ∨										
1º Administrative 🗸										

• VPC が展開されていることを確認します。



- AWS に展開されたクラウドネットワーク コントローラのルーティング テーブル ビューを使用 して、到達可能なサブネットが次のようになっていることを確認します。
 - NDFC : 172.16.20.0/24
 - Azure : 70.1.0.0/16

			Actions 🗸 🔲 🔿 —	
Overview Topology Cloud Resources Application	n Management Event Analytics	Subnets for CIDR Block 10.230.	0.0/16	×
General Account dcmm-default-tn Region us-west-2 Cloud Resources 1 4 0 Bears 1 0 2	Settings Cloud Access Privilege Inherited (Routing & Security) Cloud Provider ID vpc-057x651679a0971d CIDRs CIDR Block Range 10.230.0.0/16	p y	Settings Cloud Access Privilege Inherited (Routing & Security) Cloud ODP's Subnet 10.230.1.0/24 Name - Route Table Settings Name stretched-wf.egress Oper State configured Cloud Provider ID	~
Application Management 0 0 1 Againsen hulles 0 1 Utra 0 0 Vers 0 0			rti-04.47/29694.43ce393 Direction egress Entries Destination Address * Next Hop 172.16.20.1/24 Hub Network 70.10.0/16 tgw-034.97dd5ed64b8 Hub Network 10.230.0.0/16 Essent local	377
			Actions 🗸 📕 🖬 🔿 –	- ×
Overview Topology Cloud Resources Application	1 Management Event Analytics	Subnets for CIDR Block 10.230.	Actions → 🕅 🖬 O -	- × ×
Overview Topology Cloud Resources Application General Account dcnm-offault-tn Region us-west-2	Management Event Analytics Settings Cloud Access Privilege Inherited (Routing & Security) Cloud Provider ID vpc-057/L951679a0971d CIDRs	Subnets for CIDR Block 10.230. 10.230.10/24 10.230.2.0/24	Actions V R => O - 0.0/16 Cloud Access Privilege: Inherited (Routing & Security) Cloud CDR*s Subnet 10:230 2.0/24 Name -	- × ×

- e) AWS コンソールで、次のことを確認します。
 - •1 つの VPC と 2 つのサブネットが表示されていることを確認します。



aws III Services Q Se	earch [Alt+5]		D & Ø (Dregon 🔻 demo @ 1173-7874-6411
VPC dashboard X EC2 Global View 🖄 New	Subnets (2) Info Q. Filter subnets		C Actio	ns Create subnet (1) ③
Filter by VPC:	Name T Subast ID T State T 105 T	ID-4 CIDD	10-6 CIDB	V Ausilable Dud addr
Juictorre	Name v Sublet ID v State v VPC v	IPV4 CIDR	V IPV6 CIDR	 Avaitable IPv4 addr
 Virtual private cloud 	subnet-[10.230.1.0/24] subnet-02e03f2bc17ffc9da OAvailable vpc-057fc951679a0971d con	10.230.1.0/24	-	250
Your VPCs	subnet-[10.230.2.0/24] subnet-0318aa2d5634350d1 O Available vpc-057fc951679a0971d con	10.230.2.0/24	-	250
Subnets				· ·
Route tables				
Internet gateways				
Egress-only internet gateways				
Carrier gateways				
DHCP option sets				
Elastic IPs				
Managed prefix lists				
Endpoints				
Endpoint services				
NAT gateways	-			
Peering connections	Select a subnet			
▼ Security				
Network ACLs				

・ルーティングテーブルが表示されていることを検証する。

aws iii Services Q S	iearch	[Alt+S]		⊳	Oregon 🔻 demo @ 1173-7874-641
VPC dashboard X EC2 Global View 2 New Filter by VPC: Select a VPC V	 VPC > Route tables > rtb-04447 rtb-04d472959543 You can now check network co 	2959543ce393	ed-vrf:egress]	Run Re	Actions 🔻
 Virtual private cloud Your VPCs Subnets 	Details Info				
Route tables Internet gateways Egress-only internet gateways Carrier gateways DHCP option sets Elastic IPs	Route table ID Trb-0447299543ce393 VPC Vpc-057(c951679a0971d context vr1-addr-(10.230.0.0/16)	Main No Owner ID O 117378746411	Explicit subnet-0118aa2d5634350d1 / subnet-02803f2bc17ffc9da / su	Edna szezetetlene subnet-[10.230.2.0/24] X benet-[10.230.1.0/24]	
Managed prefix lists Endpoints Endpoint services	Routes Subnet associations	Edge associations Route propagation	Tags		
NAT gateways	Routes (3)				Edit routes
Peering connections	Q Filter routes		Both 🔻		< 1 > ©
▼ Security					
Network ACLs	Destination				∇
Security groups	10.230.0.0/16	local	⊘ Active	No	
Network Analysis	70.1.0.0/16	tgw-034a97dd5ed64b877	⊘ Active	No	
Reachability Analyzer	172.16.20.0/24	tgw-034a97dd5ed64b877	⊘ Active	No	
Network Access Analyzer					

- f) Azure に展開されたクラウドネットワーク コントローラに接続し、次の検証を行います。
 - dcnm-default-tn テナントが作成されていることを確認します。

Ŧ	cisco Cloud	Network Controller (Az	ure) 🔥 Azure						Q 💿 🖸	000 💶
Dashboard	Tenants									Ø
Topology	Filter by attributes									(Actions ~)
Cloud Resources					6.00	Section Management			Claud Resources	
Tenants	Health	Nama	Description	Application	EDGe	VBE	Azure	Regions	Virtual Networks	Endocinte
Application Profiles	Health	Name	Description	Profiles	EPGS	VIEFS	Subscription	Regions	Virtual Networks	Endpoints
EPGs	Healthy	common		1	0	2		0	0	0
Contracts	Healthy	dcnm-default-tn	Default tenant for NDFC	0	0	1	Shared from infra	1	1	0
Filters	O Major	infra		1	12	2	74094178-	1	1	10
VRFs							7850-468a- bf23- 41e85a1a3arta			
Services	C Healthy	mgmt		0	0	2		0	0	0
Cloud Context Profiles	C Preaking									
External Networks	15 V Rows								Page 1 v of 1	≪ ≪ 1-4 of 4 ⇒ ⇒
Infrastructure										
r ^o Administrative										
Ŧ	diale Cloud	Network Controller (Az	zure) 🔥 Azure						000	
🚍	Tenants	Network Controller (A	zure) 🔥 Azure dcnm-	·default-tn : \	/irtual Netwo	orks			@@	0000
E Deshboard Topology	Tenants	Network Controller (A	zure) Azure	-default-tn : \	/irtual Netwo	orks	O Vitual	Network	@ 00	000 9
Deshboard Topology Cloud Resources	Tenants	Network Controller (A	zure) Azure dcnm-	·default-tn : \	/irtual Netwo	orks	Virtual stratc	Network hed-vrf	000	000
Dashboard Topology Coul Resources Application Management Amagement Amagement Application Management Application Management	Tenants	Network Controller (A;	Zure) Azure dcnm- dcom-dc	-default-tn:\	/irtual Netwo	orks	Stretc	Network hed-vrf	Image: Second state Image: Second state Healthy	0000
Dashboard Topology Cload Resources Application Management Application Profiles	-II-II- Cloud CISCO Tenants Film in anticom	Network Controller (A;	Zure) Azure dcnm- Q stretchec De	-default-tn:\ 	/irtual Netwo	orks	General	Network hed-vrf	Image: Second state Image: Second state Image: Healthy	000
	Cloud Tenants Pres 1 and 2 and Health Health Healthy	Network Controller (A)	ZURE) Ature dcnm- c c c c c c c c c c c	-default-tn:\ d-wr 70.1.0.0/16 afaut-tn > eastus	/irtual Netwo	orks	© What stretc Ceneral Account dom-dra	Network hed-vrf	Sector Control Con	
	India Cloud	Network Controller (A)	Zure) Anne dcnm- Q b b b to	default-tn : ∖ 4-wr70.1.0.0/16 faalt-tn > eastus	/irtual Netwo	orks	S Weat stretc General Account dorm-defa Region	Network hed-vrf	C Healthy	
	India Cloud	Network Controller (A)	Zure) Arve	∙default-tn : \ d-wr70.1.0.0/16 faat-tn > eastus	/irtual Netwo	orks	Ceneral Account dorm-defa Region eastus	Network Ded-vrf	C Healthy	
	India Cloud	Network Controller (A)	zure) Arve dcnm- Q Q be for	-default-tn : \ -wr 70.1.0.0/16 fault-tn > eastus	/irtual Netwo	orks	Ceneral Account derm-defa Region eastus Citoud Ress	Network Meteoryrf	C Healthy	
Dashbaard Topology Topology Application Management Application Management Finis Contracts Finis Contracts Finis Viri5 Services	Cloud Tenants Print a minimum Health O Health O Healthy O Macc	Network Controller (A)	zure) Arve	default-tn : \ +r70100/16 fault-tn > eastes	/irtual Netwo	orks	Ceneral Account demonder Region eastus Cloud Resc	Network Inder-vrf uft-tn urces	C Healthy	
	Cloud Crece: Cloud Tenants Profile or intention • Heatthy • Heatthy • Heatthy • Heatthy	Network Controller (A)	zure) Arve	default-tn : \ +r70100/16 fault in > eastes	/irtual Netwo	orks	Ceneral Account demonder Region eastus Cloud Resc	Network ned-wrf uft-tn wrces 1	Healthy	1 1 1 1 1 1 1 1 1 1 1 1 1 1
Desiboard Topology Topology Could Resources Voires Application Management Application Profiles EPGs Contracts Fifters Virif's Services Could Contect Profiles Epclement Virif's Services Could Contect Profiles Epclement Virif's Services Could Contect Profiles Epclement Virif's Services Could Contect Profiles Destruction	Cloud Crece: Cloud Tenants Profile or electry O Heathy O Heathy I O Heathy I O Heathy I S V Rows	Network Controller (A2	zure) Arve	default-tn : \ 	/irtual Netwo	orks	Ceneral Account demonder Region eastus Cloud Rese	Network ned-wrf uit-tn urces	C Healthy	1 1 1
	Cloud Creating For the restore Heathy O Mary 15 Rows	Network Controller (Ad Name common dcom-default-in infra ingrit	ZURE) Asse dcnm- De De for	default-tn : \ 	/irtual Netwo	orks	Ceneral Account dom-afa Region estus Cloud Reso	Network Network ut-tn arces 1 nummers	Healthy 0 Ensure 0 Non-Non-Non-Non-Non-Non-Non-Non-Non-Non-	1 1 1 1 1 1 1 1 1 1 1 1 1 1
	Cloud Creates For the restore Heathy O Heathy O Heathy I to Heathy Nor Nor Nor Nor Nor Nor Nor Nor	Network Controller (Ad Name common dcom-default-in infra regent	ZURE) Asse dcnm- De De tor	default-tn : \ +r70:10.0/16 fault in > easted	/irtual Netwo	orks	Ceneral Account dom-data Region estus Cloud Reso	Network held-vrf arces 1 hypers 1 Security Onepo	C Healthy Healthy Marrier Name	1 1 1 1 1 1 1 1 1 1 1 1 1 1
	Cloud Creating For the restore Heating O Mage O Mage O Mage O Mage O Mage	Network Controller (Ad Name common dcom-default-in infra regent	ZURE) Asse dcnm- De De tor	default-tn : \ +r70100/16 fault in > easted	/irtual Netwo	orks	Ceneral Account dom-afa Region estus Cloud Reso Loud Reso Application	Network head-wrf ut-tn arces 1 hypers 5 search (Deeper Search (Deeper Management	C Healthy Healthy Marrier N Network N N N N N N N N N N N N N	1 1 1 1 1 1 1 1 1 1 1 1 1 1
Danhourd Topology CouR Resources CouR Resources CouR Resources CouR Resources Cour Application Management Application Management Application Management Prefix Courtest Prefix Courtest Prefix Services Courtest Profix Services Courtest Profix Services Services Courtest Profix Services S	Cloud Creating For the entering Heatthy Heatthy Heatthy Heatthy Heatthy Rows	Network Controller (Ad Name common dcom-default-m infra mgmt	ZURE) Acre	default-tn : \ 	/irtual Netwo	prks	Venational State	Network head-wrf uit-tn arces 1 1 1 Swath Grape Management 0	C Healthy C Heal	1 1 1 1 1 1 1 1 1 1 1
Courtext Profiles Context Profiles	Cloud Creating For the entering Healthy Healthy Healthy Healthy Healthy Rows	Network Controller (Ad Name common dcom-default-in infra mgmt	ZURE) Acre	default-tn : \ ⊷rt 70.1.0/j16 fraf-tn > eastan	/irtual Netwo	prks	Venat State General Account dom-offa Region estos Cloud Reso Loud Reso Application Application	Network head-wrf utt-tn utt-tn utt-tn l sevens Grappin Management 0 utton Polese	C Healthy C Healthy C Healthy C Healthy C Healthy C Healthy C Healthy C Healthy C Healthy C Healthy	
Courtest Profiles Contest Profiles	Cloud Ceneral For the enternance Healthy Healthy Healthy Healthy Healthy Rows	Network Controller (Ad Name common dcom-default-in intra mgmt	ZURE) Acres	default-tn:\ rt701.0.0/16 frad-tn > eastan	/irtual Netwo	prks	Venational State	Network head-vert utt-tn arces 1 Search Gauges Management 0 anon Pooles 1	C Healthy C Heal	

• VRF が展開されていることを確認します:

Ŧ	-ilis cise	Cloud Netw	work Controller (Azure)					9	00000 💶
Dashboard									
Topology	VIXI	3							0
▲ Cloud Resources ∨	VRFs	Leak Routes							
Application Management									(Actions ~)
Tenants					Fording Management			Deservices	
Application Profiles			-	App	ication management	B	Ciou	Resources	
EPGs		Health	Name	EPGS	Cloud Context Profiles	Regions	Virtual Networks	Routers	Endpoints
Contracts		Healthy	ave-ctrl infra	0	0	0	0	0	0
Filters		· Healthy	сору	0	0	0	0	0	0
VRFs			common						
Services		• Healthy	common	0	0	0	0	0	0
Cloud Context Profiles		Healthy	inb	0	0	0	0	0	0
External Networks			mgmt						
🖾 Operations 🗸 🗸		Healthy	oob mgmt	0	0	0	0	0	0
🔿 Infrastructure 🗸 🗸		· Healthy	overlay-1 Internal	12	1	1	1	2	10
1º Administrative \lor			infra						
		Healthy	dcnm-default-tn	0	1	1	1	0	0
	15	Rows						Page 1 V	of 1 4 4 1-7 of 7 ⊨ ⊨

- AWS に展開されたクラウド ネットワーク コントローラのルーティング テーブル ビューを使用 して、到達可能なサブネットが次のようになっていることを確認します。
 - NDFC : 172.16.20.0/24

• AWS : 10.230.0.0/1

erview Topology	Cloud Resource	es Application Mana	gement Event Analytics	Subnets for CIDR Block 70.1.0.0/1	16	
				1	70.1.1.0/24	
General Account Scrm-default-tn Region Heastus			Settings Cloud Access Phylioge Inheretes (Posting & Security) Cloud Context Profile stretched-vrf-eastus CIDRs CIDR Bock Range P	70.1.1.0/24	Settings Cloud Access Phylioge Inherited (Routing & Security) Cloud CDR's Subnet 70.1.10/24 Name -	
1	0	1	70.1.0.0/16 yr		Route Table Settings	
Regions	Routers	Network Security Groups	Cloud Provider ID		Name	
1 Application Security Groups	0 Virtual Machines	0 Endpoints	/subscriptions/74094178-785d-468a-br23-41e85a1a3ada/resourceGre vrf_eastus/providers/Microsoft.Network/virtualNetworks/stretched-vrf		stretcned-vrt-egress Oper State configured Cloud Provider ID	
Application Managem	ent				/subscriptions/74094178-785d-488a-b 41e85a1a3ada/resourceGroups/CAPIC_ tn_stretched- vrf_eastis/conviders/Microsoft Network/	f23- .dcnm-default- /routeTables/rt-stretched-
0 Application Profiles	O EPda	1 Cloud Context Profiles			vir_egress Direction egress	
1 VRFs	0 Service Graphs				Entries Destination Address *	Next Hop
					10.230.0.0/16	10.90.1.36 Hub Network
					172.16.20.1/24	Hub Network
					172.16.20.0/24 Copied	10.90.1.36

g) Azure コンソールで、サブネットが表示されることを確認します。

Microsoft Azure	₽ Search	resources, services, and docs (G+/)			2	Q @ 🖓 🖓	A ambsingh@cisco. cisco avseu	
Home > Virtual networks > stretched-vrf									
Virtual networks « Cisco-INSBU-MKT	stretched-vrf Sub Virtual network	onets 🛪 …							×
+ Create 🔘 Manage view 🗸 …	Search 0	+ Subnet + Gate	way subnet 🕐 Refres	h በ ⁸ ዓ. Manage users	Delete				
Filter for any field	Overview Activity log	Search subnets							
Name Tu	Access control (IAM)	Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs 1+	Delegated to ↑↓	Security group ↑↓	Route table ↑↓	
e> overlay-1 ····	Tags	subnet-70.1.1.0_24	70.1.1.0/24		251		subnet-70.1.1.0_24	rt-stretched-vrf_egress	
	Diagnose and solve problems								
	Settings								
	Address space								
	Ø Connected devices								
	 Subnets 								
	× Bastion								
	DDoS protection								

I



ルートリークの使用例

- ・ルートリークの使用例について (155ページ)
- ・必要なテンプレートの構成 (157 ページ)
- ルートリークの設定(177ページ)

ルートリークの使用例について

このルートリークのユースケースでは、オンプレミスサイトのVRFおよびネットワーク定義 を含むサイトごとに個別のテンプレートを使用しますが、クラウドサイトの場合、これらのテ ンプレートにはVRF 定義のみが含まれます。同じVRF が全てのサイトに渡っているのでサイ ト間でプレフィックスの交換のために構成を必要としない ストレッチされた VRF ユースケー ス(117ページ)で説明されている拡張VRF(内部VRF)の使用例とは異なり、各サイトは違 う VRF を使うのでこのユースケースでは VRF リーク構成する必要があります。

サイト (オンプレミスとクラウドサイト)間でプレフィックスを伝達するには、サイトに関連 付けられているそれぞれのテンプレートでルートリークを明示的に構成する必要があります。 図 162:



上の図に示すように、各サイトには個別に関連付けられたテンプレートがあり、そのサイトの みに固有の VRF/ネットワーク定義が含まれています。オンプレミス テンプレートは NDFC 管理の オンプレミス サイトに関連付けられていますが、AWS テンプレートと Azure テンプレートはそれぞ れ AWS と Azure クラウド サイトに関連付けられています。Inter-VRF ルート リークは、サイ ト間の通信を可能にするために、異なる VRF 間で明示的に構成されます。

必要なテンプレートの構成

次のセクションの手順を使用して、ルートリークのユースケースに必要なテンプレートを構成します。

オンプレミス サイト テンプレートの構成

このセクションでは、NDFC 管理のオンプレミス サイトに関連付けられる[オンプレミス テンプ レート (On-Prem Template)]を構成します。

- ステップ1 NDO で、[アプリケーション管理(Application Management)]>[スキーマ(Schema)]に移動し、[ス キーマの追加(Add Schema)]をクリックします。
- ステップ2 スキーマ名を指定し、[追加(Add)]をクリックします。

このユース ケースでは、新しいスキーマに [VRF ルート リーク スキーマ (VRF Route Leaking Schema)]という名前を付けます。

図 163:

≡ cisco Nexus Da	shboard 🔔 Orchestrate	er ~									ck 🛓 🤇
Untitled Schema									0	/ 1000 Objects Save Schema	() ×
View Overview ~										Add New Te	
Overview											
General						Audit Logs					
Name Untitled Schema						Created 0	Deleted 0	Updated 0	Deployed 0		
Sites			General				×				
Туре			Name *								
			VRF Route Leaking Schema	8			at of Sync. 0				
0			Description								
Application Managem	ient										
Application Profiles (0) External LPGe (0)	• EPGs (0) • L3Outs (0)	Contracts (0) Service Graphs (0)	• VRFs (0) • Nertworks (0)		• Bridge		• Fittaria (0)				

新しい **[VRF ルート リーク スキーマ(VRF Route Leaking Schema)]** スキーマの [概要 (Overview)] ページに戻ります。

- ステップ3 [VRF ルート リーク スキーマ (VRF Route Leaking Schema)] スキーマの下で[新しいテンプレートを追加しま す (Add New Template)]をクリックします。
- ステップ4 NDFC テンプレートを選択します。
- **ステップ5** [表示名 (Display Name)]フィールドに名前を入力して、NDFCタイプのテンプレートを作成します(例: [On-Prem テンプレート (On-Prem Template)])。
- **ステップ6** テナントにテンプレートをマップするために[テナントを選択(Select a Tenant)]フィールド内の dcnm-default-tn テナントを選択します。

図 164 :

≡ cisco Nexus Dashboard . Orchestrator ~				Feedback 🔔 3
VRF Route Leaking Schema				4/1000 Objects の代え 🗙
View On-Prem Template		Add New Template Sive	Template On-Prem Template	×
On-Prem Template Version 8 Applied to 1 sites Tenarit: doom-default-to	Associated Sites	Last Depkryed: Dec 3, 2022 12-53 pm Depkry to sites	Template Settings Display. Name* On-Prem Template Deployed Name:	^
Template Properties 🗸		Actions ~	Description	
Filter		IMPORT - SELECT SCREATE OBJECT -	Template Type NDFC	
😡 VRFs 🗸			Tenant Settings	^
			dcnm-default-tn	
			Name dcnm-default-tn Description Default tenant for NDFC sites	
Networks v				
net10				

- **ステップ7** [テンプレート プロパティ(Template Properties)]で[オブジェクトの作成(Create Object)]をクリッ クし、[VRF]を選択して、NDFC に管理されたオンプレミス サイトで使用される VRF を作成します。
 - (注) 新しい VRF を作るより、既に使用したいオンプレミス VRF を作成した場合、[テンプレート プロパティ(Template Properties)]の下、[インポート(Import)]をクリックします。そし て既に作成された VRF をインポートします。

現在、サポートはオンプレミスサイトからのVRFとネットワークのインポートに対してのみ 利用できます。

ステップ8 この VRF の [表示名 (Display Name)] フィールドに名前を入力します(例: v10)。

図 165:

≡ cisco Nexus Dashboard . Circhestrator ∨				Feedback 👤 🔮
VRF Route Leaking Schema			1 / 1000 Obje	Save Schema () X
View On-Prem Template ~		Add New Template	VRF v10	X
On-Prem Template	Associated Sites In Sync 0 Out of Sync 0	Solida (sugar)	0 Common Properties Display Name* ()	· ^
Template Properties ~		Actions -> IMPORT -> SELECT + Create Object ->	Deployed Name Description	
VRPs ~		Add VRF	NDFC Properties	^
			VRF Profile * Default_VRF_Universal	×v
			VRF Extension Profile *	
			Loopback Routing Tag 12345	~~
			Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET	
			Disable RT Auto-Generate	
			Select	

- ステップ9 [テンプレート プロパティ(Template Properties)]の下、[オブジェクトを作成 (Create Object)]をク リックしてネットワークを作成するために[ネットワーク (Network)]を選択します。
 - (注) 新しい VRF を作るより、既に使用したい VRF を作成した場合、[テンプレート プロパティ (Template Properties)]の下、[インポート(Import)]をクリックします。そして既に作成 された ネットワーク をインポートします。
- ステップ10 ネットワークの[表示名 (Display Name)]フィールドに名前を入力します(例:net10)。
- **ステップ11** [バーチャルルートと転送(Virtual Routing & Forwarding)] フィールドで、v10 VRF を選択して、net10 ネットワークをその VRF にマッピングします。

🗵 166 :

≡ ••(•• • cisco Nexus Dashboard . Orchestrator ~				Feedback 💄
VRF Route Leaking Schema			2 / 1000 Objects	x f3 million
View On-Prem Template \sim		Add New Template	Network net10	@ >
On-Prem Template Tenart: done-oefault-in	Associated Sites Sinc 0 O O O	Opping to aller.	O Common Properties Display Name*	OTHER SCHEMAS
Template Properties ~		Actions -	net10 Deployed Name: Description	
VRFs ~		Add VRF	NDFC Properties	^
VIU		Add Maturely	Layer2 Only	
Networks V		Add Network	Virtual Routing & Forwarding * v10 Network Profile *	×v
			Default_Network_Universal Network Extension Profile *	× ~
			Default_Network_Extension_Universal	×v
			VLAN Name	
			* Gateway IP	
			Add Subnet	

ステップ12 [ゲートウェイIP (Gateway IP)]フィールドで、[サブネットの追加 (Add Subnet)]をクリックしてゲートウェイの IP アドレスを入力し、[追加 (Add)]をクリックします。

図 167:

≡ ^{•(1+ +} Cisco Nexus Dashboard . Orchestrator ~				Feedback 1
VRF Route Leaking Schema			2 / 1000 Objects	X is
View On-Prem Template ~		Add New Template	Network	© ×
On-Prem Template Instant: domedication	Associated Sites • Baye • Baye • Data faye		Common Properties Display Name*	
Template Properties ~		Actions	Deproyed Name:	
	Add Subnet	× + Cresto Object -		
VBPs ~ VD	Gateway IP Type 172.16.10.1/24 primary Ø Add Gateway IP	Add VR#	NDFC Properties Network ID O	
Networks ·		Add Network		
			Default_Network_Universal Network Extension Profile * Default_Network_Extension_Universal	
			VLAN Name	
			Add Subnet Suppress ARP	

ゲートウェイ IP アドレスは[ゲートウェイ IP (Gateway IP)]フィールドに表示されます。

図 168:

≡ sico Nexus Dashboard A crowstrator ~	Feedback 上 🕄
VRF Route Leaking Schema	2/1000 Objects Save Schema () X
View On-Prem Template ~	Network net10
On-Prem Template On-P	O O Common Properties A Display Name* net10
Template Properties ~ Retorn - Fiber BAPORT - SELECT - Challe Caper	Depkyed Name: Description
V#9a ~ Add V#P [v10	NDFC Properties ^ Network (D O)
Networks Add Network net10	Virtual Routing & Forwarding * V10 × Network Profile * Datavir Naturoli Universal ×
	Vehaol, Extension, Drivles X V Default, Network, Extension, Drivlesal X V VLAN Name
	* Gateway IP 172:16:10:3/24 Tune reliner

- ステップ13 必要な場合、ネットワークのオプショナルパラメータを定義します。
- ステップ14 [テンプレート プロパティ(Template Properties)] エリア内で [アクション(Actions)] > [サイトの関連 付け(Sites Association)]をクリックします。

3	160	
	105	٠

≡ ^{et[tet]te} Nexus Dashboard Orchestrator ~		Feedback 🛓
VRF Route Leaking Schema		2/1000 Objects Save Schema C2 X
View On-Prem Template ~	Add New Yemplat	e Network net10 $\odot \times$
On-Prem Template Tenant: acrem-default to	Associated Sites • 0 and • 0	UND BY OTHER BOLEMAX UND BY OTHER BOLEMAX 0 0 Common Properties Automatic Address Address Setup Name* entit
Template Properties ~	Actors MPORT - SELECT + Create Object	Decrylot Name: Decrylotion Perplate
VRPs V	Citra A	Inspitate perties
v10 Networks ~	Add Network	Layer2 Only UP Virtual Routing & Forwarding *
net10		v10 X ~·· Network Profile * Default_Network_Universal X ~·
		Network Extension Profile * Default, Network, Extension, Universal
		VLAN Name
		* Gateway IP 172.15.10.1724 / 2 Type: primary
		Add Subnet

ステップ15 このテンプレートをオンプレミスサイト(このユースケースの例ではシドニーサイト)にのみ関連付け、 [OK] をクリックします。

図 170:

Ξ cisco Nexus Dashboard	istrator ∽			Feedback 💄 🅐
VRF Route Leaking Schema				4 / 1000 Objects のでえ 🗙
View On-Prem Template ~	Add No	w Template	Template On-Prem Template	×
On-Prem Template Version 8 Applied to 1 sites Tenant: dcnm-default-tn	Add Sites To On-Prem Template	x	s Settings lame* m Template	
Template Properties \vee	Name		vame: on	
	251(he) 5 6 7 2 5 1		Туре	
VRFs ~	Sydney 12.12.275		ettings ame fault-to	
		OK	fault-tn	
Networks				
net10				

- **ステップ16** [テンプレートプロパティ(Template Properties)]をクリックし、オンプレミスサイト(このユースケースの例ではシドニーサイト)を選択してから、v10 VRFを選択します。
- ステップ17 右側のペインで[静的リーフの追加(Add Static Leaf)]をクリックします。

図 171 :

≡ ^{alluth} Nexus Dashboard . ★ Orchestrator ->			Feedback 👤 🧐
VRF Route Leaking Schema		2 / 1000 Objec	ts Save Schema tl X
View On-Prem Template >	Add New Template VRF		×
Sydney On Pren Template	- critical	 major mino	e warning
Tenant: dom-default-to	Actions Act	perties	^
V10	Site Local Pro	perties I Multicast des	^
net10	ndfc-spine1		/ =
	ndfc-leaf1 ~ VLAN: N/A	ndfc-leaf2	/ =
	Add Static I	eat	

[静的リーフの追加(Add Static Leaf)] ウィンドウが表示されます。

ステップ18 [リーフ(Leaf)]フィールド内で、VRFが展開されるべき場所のリーフ/ボーダー/ボーダーゲートウェイ デバイスを選択し、Okをクリックします。

> この例では、リーフノードに VRF を展開する必要があります(VRF にマップされたネットワークのエンドポイントに接続される)。そして、VRF からクラウドサイトへのレイヤー3 接続に拡張するために BGW スパインノードを展開する必要があります。

- ステップ19 ネットワークをリーフスイッチに接続するには、net10ネットワークをクリックし、[静的ポートの追加]
 をクリックして、このネットワークを展開するポートを追加します。
 [静的ポートの追加(Add Static Port)]ウィンドウが表示されます。
- **ステップ20** [静的ポートの追加(Add Static Port)]ウィンドウで[パスを追加(Add Path)]をクリックします。 [静的ポートの追加(Add Static Port)]ウィンドウが表示されます。
- ステップ21 [リーフ(Leaf)]フィールドで展開したいネットワークのデバイスを選択します。
- ステップ22 (任意) VLANフィールドに必要な情報を入力します。
- ステップ23 [ポート (Port)]フィールドで展開したいネットワークのポートを選択します。
- ステップ24 [保存 (Save)]をクリックします。

3	172	
	1/2	

VRF Route Leaking Schema				2 / 1000 Objects	Save Schemu (L) X
View On-Prem Template ~		(Add New Template)	Network		>
Sydney	Associated Sites		- ritical ma	çar minor	warning
Tenant: dcnm-default-to	Add Static Port	×	Common Properties		
Sydney Out of Synce V	Path Leaf	VLAN Ports			
	Leaf ndfc-leaf1 ~ ndfc-leaf2	~			
VRFs	VLAN 2310		Site Local Properties		
	Ports				
networks	Add Path	Cancel			
			DHCP Servers Server Address		
			Static Ports Path	VI AN Ports	
			Add Static Port		

[静的ポートの追加(Add Static Port)] ウィンドウに戻ります。

ステップ25 [静的ポートの追加(Add Static Port)]ウィンドウで[送信(Submit)]をクリックします。 図 *173*:

≡ cisco Nexus Dashboard . Orchestrato	r.~						Føedback 👤 🕐
VRF Route Leaking Schema					-	/ 1000 Objects	Seve Scheme CJ 🗙
View On-Prem Template ~					Network		×
Sydney On-Prem Template Templat	Associated				eritical major	- minor	warning
Sydney Order type V	Add Static Port Path Leaf	VLAN	Ports	×	Common Properties Display Name * nat10 Deployed Name Description N/A Network ID (0) N/A		
V10	ndfc-leaf1 ~ ndfc-leaf2	2310	vPC49 vPC51 vPC52 Hide All	/≘	Site Local Properties		
Networks	Add Path						
	-		_	Submit	DHCP Servers Server Address		
					Static Ports Path Leaf VL	N Ports	
					Add Static Port		

オンプレミス テンプレート ウィンドウに戻ります。

図 174:

≡ disco Nexus Dashboard . ♣ Orchestrator >	Feedback 上 🕻
VRF Route Leaking Schema	2/1000 Objects Serve Schemal (1) 🗙
View On-Prem Template ~	Add New Template) Network
Sydney Sydney	Explanate to service and the service s
Tenact: dom-default-tin Sydney • Out of time Filter Vitifs Vitifs Vitifs • Networks	Common Properties Display Name * Description NN Network ID O Site Local Properties Temate Rooted Multicast Enable L3 Gateway Border Composition Colorback ID Common Properties Temate Rooted Multicast
Pnetto	DHCP Servers Server Address
	Add DRICP Server Static Ports Path
	Leaf VLAN Ports ndfc-leaf1 = ndfc- vPC40

- ステップ26 オンプレミス サイトの横にある矢印をクリックし、ドロップダウン メニューから [テンプレートのプロ パティ (Template Properties)]を選択します。
- ステップ27 [サイトに展開(Deploy to Sites)]をクリックします。

図 175:

≡ disco Nexus Dashboard Orchestrator -	Feedback 🛓 🕥
VRF Route Leaking Schema	2/1000 Objects Sove Schema CJ X
View On-Prem Template ~ Add New Template	Template × On-Prem Template
On-Prem Template Applied to 1 lates Temaric donn-default-in	Template Settings Display Name* Or-Phen Template Object Pane: Description
Filter Melost - SELOT + Onde Object -	Template Type NDFC
VR#s Add VRF v10	Tenant Settings
Add Network Add Network	
net0	

- ステップ28 [On-Prem テンプレート (AWS Template)]をサイトに展開ます。
 - ・追加認証のために[展開プラン(Deployment Plan)]をクリックします。

オンプレミス サイトをクリックして、その特定のサイトの展開プランを表示します。

図 176:

Cisco Nexus Dashboard + Orche	strator ~	Feedback 🛓
RF Route Leaking Schema		2/1000 Objects
		Template
Deployment Plan		x
Template On-Prem Template	C Schema VRF Route Leaking Schema	Tenant dorm-default-tn
Plan		
Sydney		Created Obeleted Modified Existing Shadow
		(View Reyload)
	- @ ndfc-spine1	
• v10	ndfc-leaf1 ~ ndfc-leaf2	
O dcrim-default-tn		
	● 172.16.10.1/24 ● vPC49	
@ net10	ndfc-leaft ~ ndfc-leaf2	
	VID VPCS2	

- •[展開(Deploy)]をクリックして、NDOがNDFCに構成をプッシュします。 これにより、NDO構成がNDFCにプッシュされます。
- ステップ29 NDFC で、VRF が正常に展開されたことを確認します。

図 177:

Fabric Controller	
🏫 Dashboard	💿 Data Center / 💿 default / 💿 VRFs (2) / 💿 v10
👷 Topology	View Search by Attributes
📥 Virtual Management 🗸 🗸	Operation Configuration
Settings	Hierarchical
_¢ Operations ∨	 In-Sync Pending In Progress Out-of-Sync NA Multi-select O Selected
	B ndtc-leaf2 ndtc-leaf1

次のタスク

Azure サイトテンプレートの構成 (166 ページ) の手順を実行します。

Azure サイト テンプレートの構成

このセクションでは、Azure サイトに関連付けられる Azure テンプレートを構成します。

始める前に

オンプレミスサイトテンプレートの構成(157ページ)の手順を実行します。

- ステップ1 [VRF ルート リーク スキーマ (VRF Route Leaking Schema)]スキーマの下で[新しいテンプレートを追加しま す (Add New Template)]をクリックします。
- ステップ2 NDFC テンプレートを選択します。
- **ステップ3** [表示名 (Display Name)]フィールドに名前を入力して、Azure サイトの NDFC タイプのテンプレートを 作成します (例: [Azure テンプレート (Azure Template)])。
- ステップ4 テナントにテンプレートをマップするために[テナントを選択(Select a Tenant)]フィールド内の dcnm-default-tn テナントを選択します。

2	178 ·	
짇	1/0.	

allalla	
E cisco Nexus Dashboard A Orchestrator ~	Feedback 上 🕥
VRF Route Leaking Schema	4/1000 Objects ① 代】 🗙
View Azure Template ~	Add News Template Azure Template Azure Template
Acure Template Version 17 Acycled to 1 alles Tenant down-default-in	Last Deployed: Dec 4, 2022 09:40 pm Coglegy for salars Template Settings Template Settings Acous Template Acou
Template Properties V	Actions -> Description
Filter	IMPORT U SELECT CCREATE OBJECT U Template Type
vra v azure10	Add VPF Tenant Settings Gisplay name Gispla

ステップ5 [テンプレート プロパティ(Template Properties)]で[オブジェクトの作成(Create Object)]をクリックし、[VRF]を選択して、Azure サイトで使用される VRF を作成します。

図 179:

E cisco Nexus Dashboard Crchestrator	Peedback
VRF Route Leaking Schema	3/1000 Objects Save Schema 💽 🏌
View Azure Template ~	Add New Template Add New Template Add New Template
Azure Template Tenant: dorm-default to Tenant: dorm-default to Template Properties >	Template Settings Display Name* Active Template Description
	INFORT SELECT + Creater Coject Tampiate Type NDFC NDFC Tenant Settings Select a Tenant * docrreorfeader in XX
Let's create an object Click "Create Object" on template properties to create an object	

ステップ6 この VRF の [表示名 (Display Name)] フィールドに名前を入力します(例:azure10)。

図 180:

≡ -i[i:i]i. cisco Nexus Dashboard	Feedback
RF Route Leaking Schema	4 / 1000 Objects Save Schema の だ
/iew Azure Template ~	Add New Template VRF azure10
Azure Template Azure Jenson default-in	Other is conserved on the conserve
iemplate Properties ~	Actions - Description
VRFs ~	Add Vpr
azure10	VRFID ©
	Default_Ver_Universal X · · · · · · · · · · · · · · · · · ·
	Loopback Routing Tag 12345
	Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET
	Disable RT Auto-Generate

ステップ7 [テンプレート プロパティ(Template Properties)]エリア内で [アクション(Actions)]>[サイトの関連 付け(Sites Association)]をクリックします。

図 181 :

E CISCO Nexus Dashboard 🗠 Orchestrator			Feedback
VRF Route Leaking Schema		4 / 1000 Objects	ve Schema 🛈 📢
View Azure Template ~		Add New Template 2/07	
	Associated Sites	USED IN CURRENT SCHEMA 0	O EV OTHER ECHIMAE O
Tenant: dcnm-default-tn	In Sync 0 Out of Sync 0	Common Properties	
Template Properties V		Azure10 Deployed Name:	
Template Properties		Actions A Description	
Filter		Sites Association	
VRFs 🗸		Clone Template Apperties	
azure10			
azure10		VRF Profile * Default_VRF_Universal	
azure10		VRF Profile * DefauLV/RF_Universal VRF Extension Profile * DefauLV/RF_Extension.Driversal	
szure10		VRF Profile * Default_VRF_Universal VRF Extension Profile * Default_VRF_Extension_Universal Loopback Routing Tag	
82ue10		VIEP Profiles * Default_VIE_Universal VIEP Extension Profiles * Default_VIEP_Extension_Universal Loopback Routing Tay 12345 Extensions Prove Event Mon	
azure10		VIEP Profiles * Default_VIEP_Universal VIEP Extension Profiles * Default_VIEP_Extension_Universal Loopback Routing Tag 12345 Repetitional Direct Route Map FABRIC-RNAP-REDIST-SUBJECT	
azure10		VIFF Profile * URF Extension Profile * URF Extension Profile * Default_VRF_Extension_Universal Loopback Running Tag 12345 Redistribute Direct Route Map FARRO-RAW-REDIST-SUBJET Disability RT-Auto-Generate	

ステップ8 このテンプレートを Azure サイトのみに関連付け、[OK] をクリックします。

_	
্য	102 .
<u> </u>	102.

≡ cisco Nexus Dashboard . Orches	trator ~			Feedback
VRF Route Leaking Schema			4 / 1000 Objects Save	Schema 🕢 🏷
View Azure Template ~		Add New Template	VRF azure 10 carce in Control Control	
Acure Template Applied to 1 sites Tenant: donm-adfault-tn	Associated Sites Associated Sites Associated Sites Associated Sites	Explay to alter	Common Properties Objety Namo* ©	
Template Properties ~	Add Sites To Azure Template	×	azurerio Deployed Name: Delscription	
VRFs ~	■ Name ■ AWS = 2511ml		NDFC Properties	
	Ature		VRF Profile * Default, VRF_Universal	
	2112205		VRF Extension Profile * Default_VRF_Extension_Universal	
			Loopback Reating Tag 12345 Redditionate Direct Brone Man	
			FABRIC-RMAP-REDIST-SUBNET Disable RT Auto-Generate	

ステップ9 azure10 VRF をクリックし、[リージョンの追加(Add Region)]をクリックして、選択したリージョンに VNet を作成します。

[クラウドリージョン CIDRs を追加(Add Cloud Region CIDRs) ウィンドウ が表示されます。

- ステップ10 [リージョン(Region)]フィールド内で VNet を作成したいリージョンを選択します。
- **ステップ11** CIDRフィールド内で[CIDR を追加(Add CIDRs)]をクリックし、VNetの CIDR ブロックを定義します。
- ステップ12 サブネットを作成するために[サブネットを追加(Add Subnet)]をクリックし、[保存(Save)]をクリックします。

巡 183:

≡ dhaht cisco Nexus Dashboard . Corchestrator ∨			Feedback 🛓 🔿
VRF Route Leaking Schema			4/1000 Objects Save Schema の む X
			ver
Add Cloud Region CIDRs			×
Region *			•
eastus			× ~
Container Overlay			
CIDRs	To an a	105	
	туре	. VR	
CIDR *			
90.1.0.0/16			
CDR type () Primary			
Secondary Select Associated VDE			
Parent VRF Hosted VRF			
Add Subnets			
Subnet Name Private Link Labels Availability Zone			
90.1.1.0/24			
Add Subnet			
Cancel Save			
			·
and the second se			

ステップ13 [VNet ピアリング (VNet Peering)] フィールドの下にあるチェックボックスをオンにして、Azure 用の Cisco クラウド ネットワーク コントローラで作成されたハブ ネットワークを選択します。

図 184 :

≡ ^{•• ••• ••} Nexus Dashboard Orchestrat	or ~				Feedback 🛓 🌘
VRF Route Leaking Schema				:47	1000 Objects Save Schuma 🐵 🗘 🗙
Unable to get template Template2 from schema 63ch	r7d0c15e5a21ab89985f by name	×		VRF azore10	×
Add Cloud Region CIDRs					×
Region * eastus					× ~
Container Overlay Enabled					
CIDR	Type	VRF			
90.1.0.0/16	Primary	azure10			/=
Add CIDRs					
VPN Gateway Router					
VNet peering					
Hub Network					
Default					X 🗸
			1		

- ステップ14 [OK] をクリックします。 Azure テンプレート ウィンドウに戻ります。
- ステップ15 Azure サイトの横にある矢印をクリックし、ドロップダウンメニューから[テンプレートのプロパティ (Template Properties)]を選択します。
- ステップ16 [サイトに展開 (Deploy to Sites)]をクリックします。
- ステップ17 [Azure テンプレート (Azure Template)]をサイトに展開ます。

・追加認証のために[展開プラン(Deployment Plan)]をクリックします。

Azure サイトをクリックして、その特定のサイトの展開計画を表示します。

図 185 :

≡ ^{etholfs} Nexus Dashboard / ≛ Orchestrator ~				Feedback 👤 📀
VRF Route Leaking Schema				ets Destinent O () X
View Azure Template ~			Template Azure Template	
	Associated Sites		Template Settings	~
Deployment Plan				×
Ceneral Information Peroplate Azure Template	Schema VRF Route Leaking Schema	Tenant donm-default-tn		
Plan			Oreated Obeleted Modified	OExisting Shadow
O done-default-in O asure10 O route-target as2-m4-23456: O route-target as2-m4-23456:	95 ML			(View Payload)

•[展開(Deploy)]をクリックして、NDOがNDFCに構成をプッシュします。

構成が正しくプッシュされたことを確認するには、Azureに展開されたクラウドネットワークコントロー ラに接続し、クラウド技術情報の>仮想ネットワークに移動してから、azure10 VNet をクリックし、概 要ページの情報を使用して追加の確認を行います。

図 186:

💿 Virtual N	letwork az	zure10			Actions V 📕 🛋 🔿 🔿 — 🔿
Overview Topolog	gy Cloud Reso	ources Application	Management Event Analytics	Subnets for CIDR Block 90.1.0.0/16	90.1.2.0/24
General Account dcnm-default-tn Region eastus			Settings Cloud Access Privilege Inherited (Routing & Security) Cloud Context Profile azure10-eastus CIDRs	C 01.1.0/24	Settings Cloud Access Privilege Inherited (Routing & Security) Cloud CIDR*s Subnet 90.12.0/24 Name
Cloud Resources	0	2	CIDR Block Range 90.1.0.0/16	Pr ye	Poute Table Settings
Regions	Routers	Network Security Groups	Cloud Provider ID		Name azure10:egress
1 Application Security	0 Virtual Machines	0 Endpoints	A gase 1, paragraphic discord functionalities		Oper State configured
Groups					Cloud Provider ID
Application Manage	ement				ane'l apes
O Application Profiles	O EPGs	1 Cloud Context Profiles			Direction egress
1 VRFs	O Service Graphs				Entries Destination Address * Next Hop

次のタスク

AWS サイトテンプレートの構成 (172ページ) の手順を実行します。

AWS サイト テンプレートの構成

このセクションでは、AWS サイトに関連付けられる [AWS テンプレート (AWS Template)]を構成 します。

始める前に

Azure サイト テンプレートの構成 (166 ページ) の手順を実行します。

- ステップ1 [VRF ルート リーク スキーマ (VRF Route Leaking Schema)]スキーマの下で[新しいテンプレートを追加しま す (Add New Template)]をクリックします。
- ステップ2 NDFC テンプレートを選択します。
- **ステップ3** [表示名 (Display Name)] フィールドに名前を入力して、AWS サイトの NDFC タイプのテンプレートを 作成します (例: [AWS テンプレート (AWS Template)])。
- ステップ4 テナントにテンプレートをマップするために[テナントを選択(Select a Tenant)]フィールド内の dcnm-default-tn テナントを選択します。

図 187:

≡ diulu cisco Nexus Dashboard A Orchestrator ~	Feedback 上 🕥
VRF Route Leaking Schema	4 / 1000 Objects (07) ×
View AWS Template ~	(Add New Template) Series (Add New Template) Add New Template
Applied to 1 sites Tenant: dcom-default-tn Applied to 1 sites	Last Deployes: Dec 4, 2022 09-40 pm Orgicy to stes Display Name* AWS Template
Template Properties ~	Actions - Deprove name: Actions - Deprove name:
Filter	IMPORT - SELECT CREATE OBJECT - Template Type NOFC
ee vRPs v aws10	Tenant Settings
N	Description Default tenant for NDFC sites
- **ステップ5** [テンプレート プロパティ (Template Properties)]で[オブジェクトの作成 (Create Object)]をクリックし、[VRF]を選択して、AWS サイトで使用される VRF を作成します。
- **ステップ6** この VRF の [表示名 (Display Name)] フィールドに名前を入力します(例: aws10)。

図 **188**:

≡ diadi. cisco Nexus Dashboard . Orchestrator ~	Feedback 上
VRF Route Leaking Schema	4/1000 Objects のたり 🗙
View AWS Template ~	Add New Template Gro VRF
AxvS Template Version 13 Applied to 1 sites 0 - our of Sync 1	Last Deployed: De: 4, 2022 09:40 p.m 2 0
Template Properties ~	Actions
Enter Control of Contr	IMPORT V SELECT C CREATE OBJECT V
O VRFs v	NDFC Properties
ews10	157172 VRF Profile *
	Default_VRF_Universal VFF Extension Profile Porture VRF Extension
	Loopback Routing Tag
	Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET

- ステップ7 [テンプレート プロパティ (Template Properties)]エリア内で [アクション (Actions)]>[サイトの関連 付け (Sites Association)]をクリックします。
- ステップ8 このテンプレートを AWS サイトのみに関連付け、[OK] をクリックします。

図 **189**:

≡ cisco Nexus Dashboard . Crchestrator ∨				Feedback 👤
VRF Route Leaking Schema			3 / 1000 Objects Sav	ve Schema 💿 🔃 🗙
View AWS Template ~		Add New Template	VRF aws10	×
AWS Template Texant: doom-default-tn	Associated Sites 0 • © Site 0 • © Site 0 • © Site 0		Common Properties Display Name*	
Template Properties ~	Add Sites To AWS Template	×	ama to Depolyed Name: Description	
VRPs v	Name Salves Salves Ang		NDFC Properties	
	23.51ke 3ydney 12.2.275		VRF Profile * Default_VRF_Universal VRF Extension Profile *	
		۲	Default_VRF_Extension_Universal Loopback Routing Tag 12345	
			Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET	

- **ステップ9** [テンプレートのプロパティ(Template Properties)]の横にある矢印をクリックし、ドロップダウンメ ニューから AWS クラウド サイト を選択します。
- ステップ10 aws10 VRF をクリックし、[リージョンの追加(Add Region)]をクリックして、選択したリージョンに VPC を作成します。

[クラウドリージョン CIDRs を追加(Add Cloud Region CIDRs) ウィンドウ が表示されます。

- ステップ11 [リージョン(Region)]フィールド内で VPC を作成したいリージョンを選択します。
- ステップ12 CIDRフィールド内で[CIDRを追加(Add CIDRs)]をクリックし、VPCのCIDRブロックを定義します。
- ステップ13 サブネットを作成するためと可用性ゾーンにマップするためにに[サブネットを追加(Add Subnet)]を クリックし、[保存(Save)]をクリックします。

図 190:

cisco Nexus Dashboard 🏩 Ord	hestrator ~			Feedback
RF Route Leaking Schema				3/1000 Objects Serve Schoma 🕘 🤃
				VOE
Add Cloud Pegion CIDPs				
Add Cloud Region CIDRS				
egion *				
us-west-2				×.~
Container Overlay				
:IDRs				
CIDR		Туре	VRF	
CIDR *				
10.220.0.0/16				
CIDR Type ()				
Secondary				
Add Subnets				
Subnet Name Private Lin	k Labels Availability Zone			
10.220.1.0/24	us-west-2a 🗸 🗙]		
10 000 0 0101				
10.220.2.0/24	us-west-zo V]		
Add Subnet				
	Cancel Save			

ステップ14 [ハブネットワーク(Hub Network)]フィールドの下にあるチェックボックスをオンにして、AWS用の Cisco クラウド ネットワーク コントローラで作成されたハブ ネットワークを選択します。

> Cisco クラウド ネットワーク コントローラがサブネットをトランジット ゲートウェイに付加することを 許可します。これは、トランジット ゲートウェイが既に接続のあるサブネットからクラウド上の Cisco Catalyst 8000Vsにトランジット ゲートウェイに接続を積み上げます。

ステップ15 [サブネット(Subnet)]フィールド内でトランジットゲートウェイに使われるサブネットをマップします。

トランジットゲートウェイに専用のサブネットを使用するのがベストプラクティスです。

図 191 :

≡ cisco Nexus Dashboard . Crchestrator ∨		والطاعير وساعين والمتعادي والمتارين	Feedback 🛓 🔿
VRF Route Leaking Schema			3 / 1000 Objects Save Schema 🕢 t 🕽 🗙
			VRF
Add Cloud Region CIDRs			×
Region *			
us-west-2			×v
Container Overlay Enabled			
CIDRS	Time	VDE	
10.220.0.0/16	Primary	aws10	/=
Add CIDRs			
VPH Gateway Router	ption and deploy the template first. Then re-enable the	option, select the new Hub Network, and redeploy the template.	
klub Network			
hub-1 - infra			×.*
Subnets			
10.2201.0/24 × 10.220.2.0/24 ×			X ~

- ステップ16 [OK] をクリックします。 AWS テンプレート ウィンドウに戻ります。
- ステップ17 AWS サイトの横にある矢印をクリックし、ドロップダウン メニューから [テンプレートのプロパティ (Template Properties)]を選択します。
- ステップ18 [サイトに展開 (Deploy to Sites)]をクリックします。

図 **192**:

≡ ^{attrade} Nexus Dashboard	Feedback 土 🕄
VRF Route Leaking Schema	3 / 1000 Objects Save Schema 🗿 🏷 🗙
View AWS Template ~	Template AWS Template X
AWS Template Applied to 1 alles female: dotsmicedule to Applied to 1 alles female: dotsmicedule to Could Systel Could Systel	Templato Settings AU Display Name* AWS Template Displayd Name: Dissolption
Filter MMORT - SELECT + Create Object	Template Type NDFC
VRFs V Add VRF	Tenant Settings
avis10	dcnm-default-tn \times \sim

ステップ19 [AWS テンプレート (AWS Template)]をサイトに展開ます。

追加認証のために[展開プラン(Deployment Plan)]をクリックします。
 AWS サイトをクリックして、その特定のサイトの展開プランを表示します。

図 193 :

≡ cisco Nexus Dashboard . • Orchest	trator ~		Feedback 上
VRF Route Leaking Schema			× () ⊙
View AWS Template ~		Add New Template Add New Template	×
	Associated Sites	Template Settings	~
Deployment Plan			×
General Information			
Template AWS Template	Schema VRF Route Leaking Schema	Tenant donm-default-tn	
Plan			
AWS		Created ODeleted Modified OExistin	ng 🜑 Shadow
		(View Payload
O dcnm-default-tn O aws10	O route-target as 2-m4 23456:158 O route-target as 2-m4 23456:316		

•[展開(Deploy)]をクリックして、NDOがNDFCに構成をプッシュします。

構成が正しくプッシュされたことを確認するには、AWSに展開されたクラウドネットワークコントロー ラに接続し、クラウド技術情報の>VPCに移動してから、aws10 VPCをクリックし、概要ページの情報 を使用して追加の確認を行います。

図 194 :

iew Topology	Cloud Resources	s Application Mana	gement Event Analytics	Subnets for CIDR Block 1	0.210.0.0/16	
eral bunt n-default-tn on reest-2			Settings Cloud Access Privilege Inherered (Routing Only) Cloud Provider ID CIDRs CIDR Block Range	10.210.1.0/24 10.210.2.0/24	Image: Strategy of the	
1 Regions 1 Security Groups	4 Cloud Availability Zones 0 Instances	0 Reuters 0 Endpoints	10.210.0.0/16	у	- Route Table Settings Name aws10 repress Oper State conformed	
lication Managem	ent				Cloud Provider ID	
0 Application Profiles 1 VRFs	0 EPGs 0 Service Graphs	1 Cloud Context Profiles			Direction egress Entries Destination Address * Nex	tt Hop

AWS のプロセスのこの時点で宛先アドレスが構成されていることに注意してください。ただし、これ は、この AWS サイトがそれ自体と通信できることのみを示しています。 AWS サイトは、プロセスのこ の時点ではまだ他のサイトと通信できません。AWS サイトが別のサイトと通信できるようにするために 必要な宛先アドレス構成は、ルート リーク手順が完了した後にプッシュされます。

次のタスク

ルートリークの設定(177ページ)で提供されている手順を使用して、ルートリークを設定します。

ルートリークの設定

ルートリーク ユース ケースの構成するために次のセクションの手順を使用します。

Azure VRF から NDFC VRF へのルート リークの構成

このセクションでは、Azure VRF (azure10) から NDFC VRF (v10) へのルート リークを構成 します。

始める前に

必要なテンプレートの構成(157ページ)で提供される手順を使用して、必要なテンプレート を構成します。

- ステップ1 これらの手順で前に構成した Azure テンプレートと、dcnm-default-tn テナントをクリックします。
- ステップ2 これらの手順で前に構成した azure10 VRF をクリックします。
- ステップ3 右のペインで、[リークルートを追加(Add Leak Route)]をクリックします。

図 **195**:

≡ tisco Nexus Dashboard . Crchestrator ∨					Feedback 1
VRF Route Leaking Schema			4 / 10	00 Objects Save Sat	× 63 @
View Azure Template ~		Add New Template	VRF azure10		×
Azure Version 3 Azure Template	Associated Sites In Sync 0 Out of Sync 1	Last Deployed: Jan 24, 2023 07:17 pm .		- minor	- warning
Filter	•	(Astorn	Template Properties Display Name * azure10 Desployed Name: azure10 Description N/A VIRF ID () 155847		^
azure10			Site Local Properties Context Profiles Region		^
			eastus CIDR: 90.1.0.0/76		/ =
			 Add Region Leak Routes Target VRF 	Routes	
			v10 Internal VBF Route Leaking Schema > On-Pre Template > dcnm-default-tn	m 90.1.1.0/24	/ =
			aws10 Internal WF Route Leaking Schema > AWS Templata > donm-default-tn	90.1.1.0/24	/ =

[リークルートを追加(Add Leak Routes)]ウィンドウが表示されます。

ステップ4 [リークルートを追加(Add Leak Routes)]ウィンドウ内で[ターゲット VRF を選択(Select a Target VRF)] をクリックします。 図 196 :

E cisco Nexus Dashboard . Orchestr	ator ~			4/1000.0	Volocte
Viti Noute Leaking Schema					
View Azure Template \sim		Add New Template	VRF azure10		
Azure Version 1	Associated Sites		- critical	- major	- minor
Tenant: dcnm-default-to	• Out at syne 0		Template Properti	ies	
Azure • man ~		Actions ~	Display Name * azure10 Deployed Name: azure		
VRFs ~	Add Leak Routes	×			
	Target VRF		Site Local Propert	ies	
	Select a Target VRF >		Context Profiles Region		
			eastus CIDR 9010.0/16		
			Add Region		
			Leak Routes Target VRF	R	loutes
			Add Leak Route		

[ターゲット VRF を選択(Select a Target VRF)] ウィンドウが表示されます。

ステップ5 [ターゲット VRF を選択(Select a Target VRF)]ページで、ルートをリークしたい NDFC VRF (v10) を 選択し、[選択(Select)]をクリックします。

図 197:

≡ ^{•1 •1 •} Nexus Dashboard . Crchestrator				
VRF Route Leaking Schema				
View Azure Template ~			VRF azure10	
Azure Version 1 Azure Templare	Associated Sites	Last Deployed: Jan 24, 2023 00:33 pm	- relical maj	
	Select a Target VRF	×	Template Properties Display Name *	
	Q. Search a Target VRF	V10		
VRPs	stretched-vrf Internal Stretched Schema > Stretched Template	Name v10		
	VRP. Route Leaking Schema > On-Prem Template aws10 Internal VRF Route Leaking Schema > AWS Template	Tenant donm-default-tn	Context Profiles Region	
	azure10 Internal VRF Route Leaking Schema > Azure Template	Description VRF Route Leaking Schema - On-Prem Template - dcnm-default-tn	eastus DIDR: 901.0.0/18	
		Setting Site Associations	Leak Rounes Target VRF	Routes
			Add Leak Route	

[リークルートの追加(Add Leak Routes)] ウィンドウに戻ります。

- ステップ6 [リーク ルートを追加(Add Leak Routes)] ウィンドウで [サブネット IP の追加(Add Subnet IP)] をク リックし、オンプレミス サイトに伝達する Azure クラウド サブネットを追加します。
 - (注) [サブネット IP を追加(Add Subnet IP)] オプションは、選択的サブネットのみのリークを許可します。または、全てのプレフィックスが接続先 VRFにリークされる必要のある場合、全てのサブネット IPs オプションを代わりに使用できます。

図 198 :

VRF Route Leaking Schema			
View Azure Template ~		Add New Tomplate	VRF azure10
Azure Version 1 Azure Template	Associated Size		- major
Azure • nov ·	Add Leak Routes Target VRF v10 × Routes to Target VRF () Type ()	×	Template Properties Display Name 4 azure10 Description NA VIRFID © 155847 Site Local Properties
	IP Address 90.1.1.0/24	~ 會	Context Profiles Region eastus
	Add Subnet IP		CIDR-903.00/18
			Leak Routes Target VRF Ro
		•	Add Leak Route

このユースケースの場合、90.1.1.0/24 サブネットを使用します。

ステップ7 [OK] をクリックします。

Azure テンプレートページに戻り、Azure VRF から NDFC VRF へのこのルート リークの構成を確認できます。

次のタスク

Azure VRF から AWS VRF へのルート リークの構成 (179ページ) の手順を実行します。

Azure VRF から AWS VRF へのルート リークの構成

このセクションでは、Azure VRF (azure10) から AWS VRF (aws10) へのルート リークを構成します。

この手順は、Azure VRFからNDFC VRFへのルートリークの構成(177ページ)と全く同じ手 順を行います、しかしこれらの手順では、違うターゲット VRF(この手順の AWS ターゲット VRF)を選択します。

始める前に

Azure VRF から NDFC VRF へのルート リークの構成 (177 ページ) の手順を実行します。

ステップ1 [ターゲット VRF の選択(Select a Target VRF)] ページで、ルートをリークする AWS VRF (aws10)を選 択し、[**選択(Select)]** をクリックします。

図 199:

≡ •1 •1 • cisco Nexus Dashboard Archestrator →					dback 🔟 🤇
VRF Route Leaking Schema				000 Objects Save Schema	× () ©
View Azure Template ~			VRF azure10		
Azure version 1	• Associated Sites		• • • • • • • • • • • • • • • • • • •		
Tenunt, ocnm-default-to	Select a Target VRF	×	Template Properties Display Name *		
Filter	Q. Search a Target VRF	aws10			
VRFs ~	stretched-vrf Internal Stretched Schema > Stretched Template	Name aws10			
Pazute10	VRF Route Leaking Schema > On-Prem Template aws10 Internal	General A	Site Local Properties Context Profiles Region		
	Azure10 Internal VRF Route Leaking Schema > Azure Template	Description VRF Route Leaking Schema - AWS Template - dcnm-default-tn	eastus case seconde		× 8
		Setting Site Associations	Add Region Leafk Routes Targot VRF	Routes	
		Select			/ 11
			Add Leak Route		

[リーク ルートの追加(Add Leak Routes)] ウィンドウに戻ります。

ステップ2 [リークルートの追加(Add Leak Routes)] ウィンドウ内で AWS クラウドへ伝達したいサブネットを追加 します。

> このユース ケースの場合、90.1.1.0/24 サブネットを使用します。したがって、ドロップダウン メニュー をクリックして、90.1.1.0/24 サブネットを選択します。

図 *200* :

≡ difutiti Nexus Dashboard Orchestrator					Feedback 💄 💿
VRF Route Leaking Schema			-4/1	000 Objects Save S	choma 🛈 tà 🗙
View Azure Template ~			VRF azure10		×
Azure version 1 Azura Tempiaze	Associated Sites in Sync 1 Out of Sync 0		eritical major	- minor	- warning
Azure •= two v	Add Leak Routes Target VRF aws10 × Routes to Target VRF ()	×	Template Properties Display Name * azure10 Description N/A VRF ID () 155847		
VRPs Pazure10	Type ① Subnet IP All Subnet IPs IP Address		Site Local Properties Context Profiles Region		
	90.11.0/24 Add Subnet IP		eastus catel 9010076 Add Region Litak Routes Target VRF	Routes	/ #
			Internal ordefined s undefined s dener- ortauts in		/ 8
			Add Leak Route		

ステップ3 [OK] をクリックします。

[Azure テンプレート (Azure Template)] ページに戻ります。ここでは、Azure VRF から AWS VRF へのこの ルート リークの構成と前のステップのセットで構成した Azure VRF から NDFC VRF へのルート リークを 確認できます。

- ステップ4 Azure サイトの横にある矢印をクリックし、ドロップダウンメニューから[テンプレートのプロパティ (Template Properties)]を選択します。
- ステップ5 [サイトへ展開(Deploy to sites)]をクリックします。

図 **201** :

∃ = diratit. cisco Nexus Dashboard Orchestrator ∨	Feedback 上
VRF Route Leaking Schema	4/1000 Objects Science documents 😨 the X
View On-Prem Template On-Prem Template Union 1 On-Prem Template Union	Add New Template NDFC Properties vpst. Jan 24, 2023 06:25 pm 155/12
Applied to 1 sites Tenant: down-default-tn	VRF Profile * VRF Lenversal X V
Filer SELECT	Loopback Routing Tag Loopback Rout
VRFs 0	Add VIP FARIC RNAP REDIst Subset
Networks net10	Add Network Select
convected	Import EVPN () Select V Export EVPN ()
	Select V Lesk Routes O Target VRF Routes
	Add Laak Route External Prefixes Subnet
	Add External Prefix

[サイトへ展開(Deploy to sites)]ウィンドウが表示され、テンプレートが展開される場所を表示します。

- **ステップ6 [展開プラン (Deployment Plan)**]を追加認証のためにクリックします。そして、その特定のサイトの展開 プランを表示するためにそのサイトをクリックします。
- ステップ7 [展開(Deploy)]を NDO が構成をサイト固有のコントローラにプッシュするためにクリックします。

図 202 :

VRF Route Leaking Schema 471000 obje	
	cts Oll X
View Azure Template V	×
Deploy to sites	×
The current template has a dependency on 2 other templates. Please make sure all these templates are successfully deployed in the order to have a successfull deployment. Show Details	
View Version History	Deployment Plan
♥ + Created ♥ ▲ Modified ♥ ■ Poleted ♥ # Config Drift	
VRF azure10 Z Modified	
	Deploy

次のタスク

AWS VRF から NDFC VRF へのルート リークの構成 (182ページ) の手順を実行します。

AWS VRF から NDFC VRF へのルート リークの構成

このセクションでは、AWS VRF (aws10)から NDFC VRF (v10) へのルート リークを構成します。

始める前に

Azure VRF から AWS VRF へのルート リークの構成 (179 ページ) の手順を実行します。

- ステップ1 これらの手順で前に構成した AWS テンプレートと、dcnm-default-tn テナントをクリックします。
- **ステップ2** これらの手順で前に構成した aws10 VRF をクリックします。
- ステップ3 右のペインで、[リークルートを追加(Add Leak Route)]をクリックします。

义	203	:
---	-----	---

≡ cisco Nexus Dashboard Orchestrator -					Feedback 🛓 📀
VRF Route Leaking Schema			4 / 1000	Objects	× fj @ man
View AWS Template \sim	Add New Template	VRF aws10			×
AWS Westors AWS Transition AWS Transition AWS Transition	Last Deployed: Jan 24, 2023 06-30 pm	- critical	- major	- minor	- warning
Tenant: dom-default-to	Posey a units	Template Prope Display Name * aws10 Deployed Name at Description N/A VRF ID ① 158134	rties vs10		^
Faves10		Site Local Prop Context Profiles Region	arties		^
		us-west-2 CIDR: 10.220.0.0	116		/ =
		Add Region Leak Routes Target VRF Add Leak Rou	te	Routes	

[リークルートを追加(Add Leak Routes)]ウィンドウが表示されます。

ステップ4 [リーク ルートを追加(Add Leak Routes)]ウィンドウ内で[ターゲット VRF を選択(Select a Target VRF)] をクリックします。

[ターゲット VRF を選択(Select a Target VRF)] ウィンドウが表示されます。

- ステップ5 [ターゲット VRF を選択(Select a Target VRF)] ウィンドウで、ルートをリークしたい NDFC VRF (v10) を選択し、[選択(Select)] をクリックします。
 - [リークルートの追加(Add Leak Routes)] ウィンドウに戻ります。
- ステップ6 [リーク ルートを追加(Add Leak Routes)] ウィンドウで [サブネット IP の追加(Add Subnet IP)] をク リックし、オンプレミス サイトに伝達する AWS クラウド サブネットを追加します。
 - (注) [サブネット IP を追加(Add Subnet IP)] オプションは、選択的サブネットのみのリークを許可します。または、全てのプレフィックスが接続先 VRFにリークされる必要のある場合、全てのサブネット IPs オプションを代わりに使用できます。

図 204 :

≡ ^{•IIIIIII} • Nexus Dashboard . Crchestrator →					Feedback 👤
VRF Route Leaking Schema				4 / 1000 Objects	0 () X
View AWS Template ~		Add Nevi Template	VRF aws10		×
AWS Version 1	Associated Sites in Sync 0		eritical rag	se minor	- erarning
Treaser: open-openalities	Add Leak Routes Target VRF v10 × Routes to Target VRF © Type © All Subnet IPs	×	Template Properties Display Name 1 Beneyes Name avest0 Description N/A VRP ID © 198134 Site Local Properties		
aws10.	10.2201.0/24 10.2202.0/24	< 営< 営	Context Profiles Region us-west-2 ODR-102200.078		/ 1
			Leak Routrs Target VRF	Routes	

このユースケースには、次のサブネットを使用します:

- 10.220.1.0/24
- 10.220.2.0/24
- ステップ7 [OK] をクリックします。

aws テンプレートページに戻り、AWS VRF から NDFC VRF へのこのルート リークの構成を確認できます。

次のタスク

AWS VRF から Azure VRF へのルート リークの構成 (184 ページ) の手順を実行します。

AWS VRF から Azure VRF へのルート リークの構成

このセクションでは、AWS VRF (aws10) から Azure VRF (azure10) へのルート リークを構成します。

この手順は、AWS VRF から NDFC VRF へのルート リークの構成 (182 ページ) と全く同じ手 順を行います、しかしこれらの手順では、違うターゲット VRF (この手順の Azure ターゲット VRF)を選択します。

始める前に

AWS VRF から NDFC VRF へのルート リークの構成 (182ページ) の手順を実行します。

ステップ1 [ターゲット VRF の選択(Select a Target VRF)]ページで、ルートをリークする Azure VRF(azure10)を 選択し、[**選択(Select)**] をクリックします。

[リーク ルートの追加(Add Leak Routes)] ウィンドウに戻ります。

ステップ2 [リークルートの追加(Add Leak Routes)] ウィンドウ内で Azure クラウドへ伝達したいサブネットを追加 します。

このユースケースには、次のサブネットを使用します:

- 10.220.1.0/24
- 10.220.2.0/24

したがって、ドロップダウンメニューをクリックして、それらのサブネットを選択します。

図 **205**:

≡ ^{•1} [•1]• cisco Nexus Dashboard Orchestrator ~					Feedback 💄 🕥
VRF Route Leaking Schema				000 Objects Save Sc	thomas 🕑 🕄 🗙
View AWS Template ~		Add Key's Template	VRF aws10		×
AWS Version 1	Associated Sites in Sync 0		- critical - mojar		- warning
Tenant, down dafaal in AWS © contract v	Add Leak Routes × Target VBF azure10 × Routes to Target VBF © Type © Subure (P) All Subure (Ps)	Template Properties Display Name * and D Cappants time: exercit Description NA VMP (ID (C) Tol 134			
ans10	IP Address 10.2201.0/24 10.220.2.0/24	< 書	Context Profiles Region us-west-2 cole 10 220/07/16		/ 8
	Add Sutnet IP		Add Region	Routes	
			Internal sudafinad sundafinad subme- datud-to		/ 8
			Add Leek Route		

ステップ3 [OK] をクリックします。

[AWS テンプレート (AWS Template)] ページに戻ります。ここでは、AWS VRF から Azure VRF へのこのルート リークの構成と前のステップのセットで構成した AWS VRF から NDFC VRF へのルート リークを確認 できます。

図 206 :

≡ disco Nexus Dashboard Orchestrator ∨					Feedback 1 0
VRF Route Leaking Schema			4 /	1000 Objects Save S	× €9 ⊕ ∎ened
View AWS Template ~		Add New Template	VRF aws10		×
AWS Version 2	Associated Sites In Sync 1	Last Deployed: Jan 24, 2023 07:17 pm		- minor	- warning
Tenant: dcnm-default-tn	U Wordphub	Deploy to alter-	Template Properties Display Name *		^
AWS • In Synce V		Actions ~	aws10 Deployed Name: aws10 Description		
VRPs V			VRF ID () 158134		
aws10			Site Local Properties Context Profiles Region		^
			us-west-2 CIDR: 10.220.0.0/16		/ =
			Add Region		
			Leak Routes	D	
			v10 Internal VRF Route Leaking Schema > On Template > dorm-default-in	10.220.1.0/24 10.220.2.0/24	/ =
			azure10 Internal VRF Route Leaking Schema > Azu Template > docen-default-tn	10.220.1.0/24 10.220.2.0/24	/ =
			Add Leak Route		

- ステップ4 AWS サイトの横にある矢印をクリックし、ドロップダウン メニューから [テンプレートのプロパティ (Template Properties)]を選択します。
- ステップ5 [サイトへ展開(Deploy to sites)]をクリックします。

[サイトへ展開(Deploy to sites)]ウィンドウが表示され、テンプレートが展開される場所を表示します。

- **ステップ6 [展開プラン (Deployment Plan)**]を追加認証のためにクリックします。そして、その特定のサイトの展開 プランを表示するためにそのサイトをクリックします。
- ステップ7 [展開(Deploy)]をNDOが構成をサイト固有のコントローラ(NDFCとクラウドネットワークコントロー ラ)にプッシュするためにクリックします。

次のタスク

NDFC VRF から AWS VRF へのルート リークの構成 (186 ページ) の手順を実行します。

NDFC VRF から AWS VRF へのルート リークの構成

このセクションでは、NDFC VRF (v10)から AWS VRF (aws10) へのルート リークを構成します。

始める前に

AWS VRF から Azure VRF へのルート リークの構成 (184 ページ) の手順を実行します。

- ステップ1 これらの手順で前に構成した[オンプレミス テンプレート (On-Prem Template)]と dcnm-default-tn テナントをクリックします。
- ステップ2 これらの手順で前に構成した v10 VRF をクリックします。

ステップ3 右のペインで、[リーク ルートを追加(Add Leak Route)]をクリックします。

図 **207**:

≡ ^{al}} tisco Nexus Dashboard . Crchestrator ∽	Feedback
VRF Route Leaking Schema	4/1000 Objects Save Schema の け) X
	153412
View On-Prem Template ~	Add New Template VRF Profile *
Characteristic Charac	Default_VRF_Universal X ~
On-Prem Template Version 1	Last Deployed: Jan 24, 2023 06:25 pm VRF Extension Profile *
Applied to 1 sites 1 Out of Sync 4	Default_VRF_Extension_Universal X v
	Loopback Routing Tag
Template Properties x	12345
Template Properties *	Actions Redistribute Direct Route Map
Filter	IMPORT SELECT + Create Object FABRIC-RMAP-REDIST-SUBNET
	Disable RT Auto-Generate
	Add Voe
VRPs -	select
v10	
	Export ()
	3000L. V
Networks 😪	Add Network Import EVPN ③
	Senect
net10	Export EVPN ()
	Select
	Leak Routes ③ Target VRF Routes
	awst0 internal Wif more samp down a very Timplar video works to
	Accurate Definitional Accurate
	S Add Leak Route
	External Prefixes 🕥

[リークルートを追加(Add Leak Routes)]ウィンドウが表示されます。

ステップ4 [リーク ルートを追加(Add Leak Routes)]ウィンドウ内で[ターゲット VRF を選択(Select a Target VRF)] をクリックします。

[ターゲット VRF を選択(Select a Target VRF)] ウィンドウが表示されます。

- **ステップ5 [ターゲット VRF を選択(Select a Target VRF)]** ウィンドウで、ルートをリークする AWS クラウド サイト VRF (aws10) を選択し、[選択(Select)] をクリックします。
 - [リークルートの追加(Add Leak Routes)] ウィンドウに戻ります。
- ステップ6 [リーク ルートを追加(Add Leak Routes)] ウィンドウで [サブネット IP の追加(Add Subnet IP)] をク リックし、オンプレミス サイトに伝達する AWS クラウド サブネットを追加します。
 - (注) [サブネット IP を追加(Add Subnet IP)] オプションは、選択的サブネットのみのリークを許可します。または、全てのプレフィックスが接続先 VRFにリークされる必要のある場合、全てのサブネット IPs オプションを代わりに使用できます。

このユース ケースでは、172.16.10.0/24 サブネットを使用します。

図 208 :

≡ disco Nexus Dashboard Orchestrate	x Ý	Føedback 1
VRF Route Leaking Schema		4/1000 Objects の な X
View On-Prem Template ~		NDFC Properties
On-Prem Template Version 1 Applied to 1 after Tement: doolm-default-to	Anopare Stee Earl Depart and A 502 dott on Out there 3	Ver Brig) 155412 VRF Profile * Default VRF.Universal
Template Properties ~	Add Leak Routes × Target V8F	VRF-Extension Profile * Default_VRF_Extension_Universal × <-
	aws10 \times Routes to Target VRF \odot	Looptask Routing Tag 12345 Redistribute Direct Route Man
	Type () Subare (P) IP Address	FABRIC-RMAP-REDIST-SUBNET Disable RT Auto-Generate
Networks ~	172:16:00;74 2 12	Import © Select
neri0 convected		Select
		Export EVPN Q Select
		Leak Routes Target VRF Routes Ad Leak Route
		External Profixes ③ Subnet
		Add External Prefix

ステップ7 [OK] をクリックします。

[オンプレミス テンプレート (On-Prem Template)] ページに戻り、NDFC VRF から AWS VRF へのこのルート リークの構成を確認できます。

次のタスク

NDFC VRF から Azure VRF へのルート リークの構成 (188 ページ) の手順を実行します。

NDFC VRF から Azure VRF へのルート リークの構成

このセクションでは、NDFC VRF (v10) から Azure VRF (azure10) へのルート リークを構成 します。

この手順は、NDFC VRF から AWS VRF へのルートリークの構成(186ページ)と全く同じ手順を行います、しかしこれらの手順では、違うターゲット VRF(この手順の Azure ターゲット VRF)を選択します。

始める前に

NDFC VRF から AWS VRF へのルート リークの構成 (186ページ) の手順を実行します。

ステップ1 [ターゲットVRFの選択(Select a Target VRF)]ウィンドウで、ルートをリークする Azure VRF (azure10) を選択し、[選択(Select)]をクリックします。

[リーク ルートの追加(Add Leak Routes)] ウィンドウに戻ります。

ステップ2 [リークルートの追加(Add Leak Routes)]ウィンドウ内でAzure クラウドへ伝達したいサブネットを追加 します。

> このユースケースでは、172.16.10.0/24サブネットを使用します。したがって、ドロップダウンメニュー をクリックして、172.16.10.0/24サブネットを選択します。

図 **209**:

≡ "littlit Nexus Dashboard Orchestrato		Feedback
VRF Route Leaking Schema		4 / 1000 Objects Save Schema の でよう
View On-Prem Template ~	Accounted Sites • Accounted Sites	NDFC Properties
Femplate Properties ~	Add Leak Routes ×	Default_VRF_Universal K V VRF_Extension Profile * Default_VRF_Extension_Universal K V
VRFs ~	asure10 × Routes to Target VRF () Type ()	Loophack Routing Tag 12345 Reclassification Direct Route Map FARRIC, BAAR-REDICT Output
V10	Subort IP All Subort IPs IP Address 1723630.0/24	
netto	Ant Subort P	
		Lesix Routes () Target VRF Routes aws10 Internal Vit fram Lasans denses - Aut
		Templan - accum-solead- on Add Leak Roade

ステップ3 [OK] をクリックします。

[オンプレミス テンプレート (On-Prem Template)] ページに戻ります。ここでは、NDFC VRF から Azure VRF へのこのルート リークの構成と前のステップのセットで構成した NDFC VRF から AWS VRF へのルート リークを確認できます。

- ステップ4 オンプレミス サイトの横にある矢印をクリックし、ドロップダウン メニューから [テンプレートのプロパ ティ(Template Properties)]を選択します。
- ステップ5 [サイトへ展開 (Deploy to sites)]をクリックします。

図 210:

≡ ^{•(]•(]•} Nexus Dashboard . Contestrator ~	Feedback
VRF Route Leaking Schema	4/1000 Objects Seve Schema の たえ 🗙
View On-Prem Template ~	Add New Template
Areacistad Sitar	Default_VRF_Universal X ~
On-Prem Template Version 1 Appled to 1 alter Tempt Count of Bulk-In	Last Desloyed: Jan 24, 2023 06/25 pm Default_VRF Extension Profile * Default_VRF_Extension_Universal × >
Template Properties ~	Actions - Reditivity Tag
[Ref.	IMPORT
V#rs ~	Add VRP Import Select
¥10	Export O Select
Networks \vee	Add Network Import EVPN Select
net10 connected	Export EVPN O Select_
	Leak Routes 🔿 Target VRF Routes
	aws10 Internal Wiff Annue Lasking Solama - Jang Timplate - down advant in
	azure10 Internal V 11 Wir Annet seinig stormer - Xanne 172:16:10.0/24 Templare - anno-Kant no
	Add Leak Route External Prefixes ()

[サイトへ展開(Deploy to sites)]ウィンドウが表示され、テンプレートが展開される場所を表示します。

ステップ6 [展開プラン (Deployment Plan)]を追加認証のためにクリックします。そして、その特定のサイトの展開 プランを表示するためにそのサイトをクリックします。

図 211:

≡ ditalit. cisco Nexus Dashboard Orchestrator ∨				Feedback 👤 🔮
VRF Route Leaking Schema			4 / 1000 Objects	× £1 ⊕ material
View On-Prem Template ~			Template On-Prem Template	
	Associated Sites	Last Destinant: Inc. 24, 2012 OR 28 apr	Template Settings	~
Deployment Plan				×
General Information Template On-Prem Template	Schema VKF Route Leaking Schema	Tenant donn-default-th		
Plan			Ocreated ODeleted Modified OEx	cisting Shadow
O dome defauit in VII Instant and 23456-355.				(View Payload)

ステップ7 [展開(Deploy)]をNDOが構成をサイト固有のコントローラ(NDFCとクラウドネットワークコントロー ラ)にプッシュするためにクリックします。

次のタスク

構成の確認(191ページ)で提供された手順を使用して構成の展開が成功したことを検証します。

構成の確認

このセクションでは、構成が正常に展開されたことを確認します。これらの各検証ステップでは、表示されているこのユースケースの構成のために特定のコマンドが使用されることにご注意ください。構成に基づいて各コマンドの適切な変数を入れ替えます。

始める前に

NDFC VRF から Azure VRF へのルート リークの構成 (188 ページ) の手順を実行します。

ステップ1 NDO の構成を確認します。

≡ ^{•• ••• ••} Nexus Dashboar	d 🙏 Orchestrator 🗸				Feedback 🛓 🕐
Dashboard	Schemas			Tenants	×
Sites				Q. Search	Tenants C
Application Management	Filter by attributes			dcnm-default-tn	General
(@) Fabric Management	Name	Templates	Tenants	VRF Route Leaking Schema	Name dcom-default-to
Derations	Stretched Schema	2 22	1	-	Description
O Infrastructure	VRF Route Leaking Schema	3 @3	1		Default tenant for NDFC
₽ Integration					Associated Sites
					• Sites (3) 0f 4
					Associated Users
					• Users (1) of 1
					Assigned Schemas
					Schemas (5) 5 of 2
	10 ~ Rows				Topology
					6
					3
					G S
					and day
≡ cisco Nexus Dashboar	rd 🙏 Orchestrator 🗸				Feedback 👤 🕙
@ Dashboard	Schemas			Templates	>
Sites				Q. Search	Template
Application Management	Filter by attributes			On-Prem Template	General
Fabric Management	Name	Templates	Tenants	VRF Route Leaking Schema	Change Control Status
Derations	Stretched Schema	2 22	1	AWS Template VRF Route Leaking Schema	Tenant Name
O Infrastructure	VRF Route Leaking Schema	3 @3	1	Azure Template	donm-default-tn
Integration				The House Learning scrittering	Sites By Type
					APIC 1 AWS 0
					1 NDFC 0 Total General Claud Blatform 0
					Application Management
	10 V Press				
					0 0
					CONTRACT EXTERNAL ERG
					CONTRACT EXTERNAL EPO
					CONTINUET DITEMUL IPG 0 0
					OVITARY D PUTEN CADUT
					Oormac Dittemak B0 0 0 Nates 0 1 0
					CONTRACT DITEMUL (PO 0 0 PLTER LOUT 1 0 HETHORE BEDREC COMPARE
					CONTINUEY DITEMUL (PO) 0 0 1 0 1 0



ステップ2 オンプレミスのボーダー ゲートウェイ スパイン デバイスで sh ip route vrf v10 を入力します。

a	ndrc-leaf1 - SecureCRT	-	×
-	ile Edit View Options Transfer Script Tools Window Help		
	€∮⊑₽₽₽₿₿₩₽₽₽₽₽₽₩		
S	✓ ndfc-ext-c8k ✓ Cat8K-AWS ✓ Cat8K-AZURE ✓ andfc-leaft × ✓ Cat8K-AWS(1) Cat8K-AWS-2		4 Þ
ession Manager Command Manager	<pre>[A copy of each such license is available at http://opensource.org/licenses/gpl-3.0.html and http://oww.opensource.org/licenses/gpl-3.0.html and http://www.opensource.org/licenses/lgl-2.1.php and http://www.opensource.org/licenses/lgl-2.1.php and http://www.opensource.org/licenses/lgl-2.1.php and http://www.opensource.org/licenses/lgl-2.1.php ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# sh ip route vrf v10 IF Route rable for VRF "v10" "*" denotes best ucast next-hop 's" tenotes best ucast next-hop '[X/y]' denotes [preference/metric] '%strings' in via output denotes VRF <string></string></pre>		~
	10.220.1.0/24, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 03:01:42, bgp-65084, internal, tag 65091, segid: 153412 tunnelid: 0xa0a0001 encap: VXLAN		
	10.220.2.0/24, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 03:01:42, bgp-65084, internal, tag 65091, segid: 153412 tunnelid: 0xa0a0001 encap: VXLAN		
	90.1.1.0/24, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 03:06:33, bgp-65084, internal, tag 65092, segid: 153412 tunnelid: 0xa0a0001 encap: VXLAN		
	172.16.10.0/24, ubest/mbest: 1/0, attached *via 172.16.10.1, v1an2310, [0/0], 03:23:02, direct, tag 12345 172.16.10.1732, ubest/mbest: 1/0, attached *via 172.16.10.1, v1an2310, [0/0], 03:23:02, local, tag 12345 172.16.10.11/32, ubest/mbest: 1/0, attached *via 172.16.10.11, v1an2310, [190/0], 03:20:45, hmm		
	ndfc-leaf1#		~
	Default 🖂		

オンプレミスのリーフスイッチのルーティングテーブルは、到達可能なサブネットが次のことを示してい ます。

- AWS : 10.220.0.0/16
- Azure : 10.220.0.0/16
- **ステップ3** AWS に展開されたクラウドネットワーク コントローラに接続し、アプリケーション管理 > VRFに移動して、Azure および NDFC VRF が表示されることを確認します。

Ŧ	cisco	Cloud Network C	Controller (AWS) 👞						Q 0	0000 😐
Dashboard Topology Cloud Resources	VRFs	S Leak Routes								٥
Application Management	-									(Actions v
Tenants									0	
Application Profiles		Health	Name		EDGe	Cloud Context Profiles	Regions	VPCs	Routers	Endnointe
EPGs		an Line Mary	ave-ctrl		0	0	0	0	0	0
Contracts		e Healthy	infra							
VRFs		Healthy	dcnm-default-tn		0	1	1	1	1	2
Services		• Healthy	azure10 Internal		0	1	1	1	1	0
Cloud Context Profiles			MSC-SHADOW CONTE-default-th		2					
External Networks		• Healthy	common		0	0	0	0	0	0
E Operations V		O Healthy	default common		0	0	0	0	0	0
Infrastructure		• Healthy	inb		0	0	0	0	0	0
r Administrative			ngmt		0	0	0	0	0	0
		Healthy	mgmt							
		Healthy	overlay-1 Internal infra		15	1	1	1	3	12
		• Healthy	stretched-vrf internal kpp dcnm-default-tn		0	1	1	1	1	2
		Healthy	v10 Internal MSC-SHADOW dcnm-default-tn		0	1	1	1	1	0
	15	∼ Rows							Page 1 v of 1	≪ < 1-10 of 10
Ŧ	cisco	Cloud Network C	Controller (AWS) 📷						Q (2)	0000 😐
- Dashboard	VRF	Cloud Network C	Controller (AWS) 📷	aws10 : 1	VPCs				Q (9)	••••••
Dashboard Topology	VRF	Cloud Network C	Controller (AWS)	aws10 : Y	VPCs			VPC	80	•000 •
Dashboard Topology Could Resources	VRFs	Cloud Network C S Lesk Routes	Controller (AWS) 📷	aws10 : \ Q _ Seen	VPCs			aws10	Q ()	•••••
	VRFs	Cloud Network C S Leak Routes	Controller (AWS) 📷	aws10 : ¹ Q Seen	VPCs 0.0.0/16 t-th > us-west-2			e VPC avvs10	Healthy	••• •
Daitboard Daitboard Topokoy Topokoy Conditionation Conditionationation Conditionation Conditionationation Conditionationation Conditionationation Conditionationationation Conditionationationation Conditionationationation Conditionationationationation Conditionationationation Conditionationationationation Conditionationationationationation Conditionationationationationation Conditionationationationationation Conditionationationationationationationation	VRFs	Cloud Network C S Leak Routes	Controller (AWS) 🚥	aws10 : 1 Q Seen dcnm-default	VPCs 0.0.0/16 1-m > us-west-2			General		••••••••••••••••••••••••••••••••••••••
E Cashboard Cash	VRFs	Leak Routes	Controller (AWS) 2005	aws10 : 1 Q. Second dcnm-default	VPCs 0.0.0/16 1-tn > us-west-2			Ceneral Account dcm-default-tn	② ②	• • • • • • • • • • • • • • • • • • •
E Topiboard Topiboard	VRFs	Cloud Network C S Leak Routes methods Heatth @ Heatthy	Controller (AWS) and Name ave-cifi Inform	aws10 : 1 Q Seen aws10 10.22 dcnm-default	VPCs 0.0.0/16 1-th > us-west-2			Ceneral Account dcm-default-th Region	C Healthy	• • • • • • • • • • • • • • • • • • •
E Topiboard Topiboard	VRFs	Cloud Network C S Leak Routes	Controller (AWS) and Name ave-citi into assi 0 intornal assi 10 intornal assi 10 intornal	aws10 : 1 Q Seen aws10 10.22 dcnm-default	VPCs 0.0.0/16 0.0.9/16			Ceneral Account dcm-default-th Region us-west-2	Healthy	••• • •
E Coology C Cool Resources C C C C C C C C C C C C C C C C C C C	VRFs	Cloud Network C S Leak Routes Heatth Heatth Heatthy Heatthy	Controller (AWS) and Name ave-citi inta avesto internal com-detauth-in	aws10 : 1 Q seet aws10 10.22 dcnm-default	0.0.0/16 0.0.9/16 0.0.9/16			Ceneral Account dcm-default-tn Region us-west-2 Cloud Resources	Healthy	• • • • • • • • • • • • • • • • • • •
E Coshoard C C C C C C C C C C C C C C C C C C C	VRFs	Cloud Network C S Leak Routes	Controller (AWS)	aws10:1	0.0.0/16 0.0.0/16			Ceneral Account dcm-default-th Region us-west-2 Cloud Resources	Healthy	
E Cool Resources Cool Resourc		Cloud Network C S Leak Routes Heatth	Controller (AWS)	aws10 : 1	0.0.0/16 0.0.0/16 0.0.9/16			Ceneral Account Account Account Account Account Cloud Resources	C Healthy	0 0 0 0 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1
E Contracts Contract Profiles Contracts Contract Profiles Contracts View Contracts View Contracts Contract		Cloud Network C S Leak Routes Heatth	Controller (AWS) Controller (AWS) Contr	aws10 : 1	0.0.0/16 0.0.0/16 0.0.0/16			Ceneral Account dcm-default-th Region us-west-2 Cloud Resources	e	0 0 0 0 1 2
E Contractor Profiles Contractor Profiles Farsis Fa	VRFs VRFs	Cloud Network C S Leak Routes Heatth	Controller (AWS)	aws10 : 1	0.0.0/16 0.0.0/16			Ceneral Account dom-default-th Region us-west-2 Cloud Resources 1 Repuis Linguis 1 Secury down	Contractivity Down	0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1
Image: second		Cloud Network C Leak Routes Heatthy	Controller (AWS)	aws10 : 1	0.0.0/16 0.0.0/16			Ceneral Account dem-default-th Region us-west-2 Cloud Resources 1 Region 1 Security Groups	Contractive Sources	0 0 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
Image: Set in the set in		Cloud Network C S Leak Routes Heatth Heatth Heatthy H	Controller (AWS)	aws10 : 1	0.0.0/16 			Ceneral Account dcom-default-tn Region us-west-2 Ctoud Resources 1 Buoynes 1 Serviry Groups Application Management 0	Cuert Avsidering Dates	© © © © © © © ~ ~ © ~ ~ © 0 1
Image: Set in the set i	VRFS	Cloud Network C S Leak Routes Meattry Heattry Heatt	Controller (AWS)	aws10 : 1	0.0.0/16 			Ceneral Account dorm-default-tn Region us-west-2 Ctoud Resources 1 Buyers 1 Serviry Groups Application Management 0 Application Parlas	Contractions Co	© • • • • • • • • • • • • • • • • • • •
■ Darbbard ■ Topology ■ Topology ■ Cold Resources ~ ■ Cold Coltacts ~ Plans ~ ~ Cold Contact Profiles ~ ~ Extrant Networks ~ ~ ■ Operations ~ ● Intrastructure ~ ~ € Administructure ~ ~		Cloud Network C S Leak Routes Heattry Heatt	Controller (AWS)	aws10 : 1	0.0.0/16 0.0.0/16 0.0.9/16			VPC avs10 Ceneral Account Account accm-defauit-tn Region us-vest-2 Cloud Resources 1 Beyony 1 Serviry Group Application Management 0 Application Parkins 1 US-	Contracting Tores	C C C C C C C C C C C C C C C C C C C
Image: Service		Cloud Network C S Leak Routes Meatty Heatty Heatt	Controller (AWS)	aws10 : 1	0.0.0/16 			Conversion	Contractions Co	© • • • • • • • • • • • • • • • • • • •

ステップ4 AWS に展開された Cloud Network Controller に残ったまま、ルート テーブル表示で検証を実行します。

verview Topology Cloud Resources Application M	anagement Event Analytics	Subnets for CIDR Block 10.22	0.0.0/16
	angement contraction	L	S subnet
General Account domm-default-to Region us-west-2	Settings Cloud Access Phylinge Inherine (Routing Cety) Cloud Provider ID	10.2202.0,024	Settings Cloud Access Privilege Internet (Routing Only) Cloud COR* Subset I 2202 0/04
Cloud Resources	CIDRS CIDR Block Range	р	Name
1 4 0 Topole Could Availability Zaves Routers 1 0 2 Security Groups Instances Endpoints	10.220.0.0/16	4	Route Table Settings Narre any 10 ogress Oper State configured
Application Management 0 0 1 Application Polities 0% 1 Coard Control Polities 1 0 Service Graphs Service Graphs			Cloud Provider ID rm-d8c3124e554097tcf Direction egress Entries Destination Address * Next Hop
			90.1.1.0/24 tgw-C Hub Network 10.220.0.0/16 [Deeest] local
VPC aws10			Actions V 🔋 = O -
VPC aws10	anagement Event Analytics	Subnets for CIDR Block 10.220	Actions → ▲ → ◇ -
VPC aws10 Verview Topology Cloud Resources Application M General Account domn-default-tn Region us-west-2	Inagement Event Analytics Settings Cloud Access Phylioge Inherited (Routing Only) Cloud Provider ID CDRs	Subnets for CIDR Block 10.220 10 220 2 0/24 10 220 1 0/24	Actions Image: Classical Access Privilege 0.0.0/16 Image: Classical Access Privilege Settings Classical Access Privilege Classical Access Privilege Image: Classical Access Privilege
VPC aws10 Nerview Topology Cloud Resources Application Million General Account domm-default-ts Region domm-default-ts Region account-default-ts Region twwest-2 Cloud Resources D Boars 1 0 Region Boars 1 0 2 Dotester	Inagement Event Analytics Settings Cloud Access Privilege Inherited (Routing Only) Cloud Provider ID CDRs CDR Block Range 10.220.8.0/16	Subnets for CIDR Block 10.220	Color Image: Color
VPC aws10 Verview Topology Cloud Resources Application M General Account Application M Account domm-default-in Region us-west-2 Used Resources D Cloud Resources D D Topology Outer Austability Zeres D Strong Grass D D Application Management D D Upps O 1 Upps D D	anagement Event Analytics Settings Could Access Phylioge Internet (Bouling Only) Cloud Provider ID CORs CDR Block Range 10.220 0.0/18	Subnets for CIDR Block 10.224	Coord COPY's Subort 10:2001.074 Setting Cloud Access Phylings Internet Ricksong Only Cloud COPY's Subort 10:220.1074 Name - Recte Table Settings Name and Toperss Oper State Oper State Cloud Access Phylings Internet Ricksong Phylings Intern
VPC aws10 Verview Topology Cloud Resources Application Mi General Account dom:indefault-in Region usurvest-2 Cloud Resources I I General Cloud Resources I I General Cloud Resources I General Cloud Re	Integrine Event Analytics	Subnets for CIDR Block 10.224	Coton V I V Constant Concord I V Constant Concord Constant Cons

ステップ5 AWS コンソールで、ルートテーブル表示で検証を実行します。

Services Q Search		[Alt+S]		D 4	Oregon •	demo @ 1173-7
'C dashboard X 2 Global View I New ter by VPC:	VPC > Route tables > rtb-(outetable-[aws10:egre	ess]			Actions 🔻
elect a VPC 🔹						
rtual private cloud	You can now check network connectivity with Re	achability Analyzer			Run Reachability Ar	halyzer X
ur VPCs						
nets	Details Info					
u <mark>te tables</mark> ernet gateways	Route table ID	Main 🗗 No	Explicit subnet accorditions 2 subnets subnet-	Edos areacisti	one.	
ass-only internet aways	VPC vpc	Owner ID	subnet-	/ subnet-[10.220.2.0/24]		
P option sets	[10.220.0.0/16]					
itic IPs naged prefix lists Ipoints	Routes Subnet associations Edge assoc	iations Route propagation Tag	js			
point services	Decider (7)				-	
gateways	Routes (5)					Edit routes
	Q Filter routes		Both 🔻		<	1 > @
ring connections						
ring connections						
ring connections urity work ACLs	Destination 🗢	Target	⊽ Status	♥ Propagat	ted	~
ring connections arity work ACLs urity groups	Destination v	Target			ted	\$
ring connections urity work ACLs urity groups work Analysis	Destination	Target local tgw-i	✓ Status ⊘ Active ⊘ Active	♥ Propagat No No	ted	V

ステップ6 Azure に展開されたクラウドネットワーク コントローラに接続し、アプリケーション管理 > VRFに移動して、AWS および NDFC VRF が表示されることを確認します。

Ŧ	-1)1- CIS	Cloud Network C	Controller (Azure) 🔥	zure					Q 0	0000
Dashboard Topology Glourd Resources	VRF VRFs	-S Leak Routes								۲
Application Management	Enert									(Actions ~)
Tenants					Application	Management		Cloud	Resources	
Application Profiles		Health	Name		EPGs	Cloud Context Profiles	Regions	Virtual Networks	Routers	Endpoints
EPGs		• Healthy	ave-ctrl		0	0	0	0	0	0
Filters			infra		0				0	0
VRFs		Healthy	MSC-SHADOW dcnm-default-tn						•	
Services Cloud Context Profiles		Healthy	azure10 Internal koo dcnm-default-tn		0	1	1	1	0	0
External Networks		🗢 Healthy	copy common		0	0	0	0	0	0
Operations		♥ Healthy	default common		0	0	0	0	0	0
Infrastructure		C Healthy	inb		0	0	0	0	0	0
		• Healthy	oob		0	0	0	0	0	0
		Healthy	overlay-1 Internal		12	1	1	1	2	10
		O Healthy	stretched-vrf Internal keo dcnm-default-tn		0	1	1	1	0	0
		• Healthy	v10 Internal MSC-SRADOW dcnm-default-tn		0	1	1	1	0	0
	15	Rows							Page 1 v of 1	≪ ≪ 1-10 of 10
=		Cloud Network	Controller (Azure)	171070					00	00000
=	cis	Cloud Network	Controller (Azure) 🔥	Azure					8 0	0000 😐
Dashboard Topology	viti cis	Cloud Network (Controller (Azure) 🔥	azure	: Virtual Network	<s< th=""><th></th><th></th><th>Q 3</th><th>0000</th></s<>			Q 3	0000
Dashboard Topology Cloud Resources	VRFs	Cloud Network (S Leak Routes	Controller (Azure) 🔥	azure10	: Virtual Network	KS		Virtual Network azure 10	@ 0	••• c
Dashboard Topology Cloud Resources Application Management A		ES Leak Routes	Controller (Azure) 🔥	azure10	: Virtual Network	KS		Virtual Network azure10	Q ⊘ ♥ Healthy	••••••
Dashbowd Deshbowd Topology Actional Resources Application Management Application Management Actional Concluses	VRFs	ES Leak Routes	Controller (Azure) 🗛	Azure azure10 Q Sector dcnm-defaul	: Virtual Network	<s< th=""><th></th><th>Virtual Network azure 10 General</th><th>Healthy</th><th>••••••••••••••••••••••••••••••••••••••</th></s<>		Virtual Network azure 10 General	Healthy	••••••••••••••••••••••••••••••••••••••
Dashboard Dashboard Topology Coud Resources Coud Resources Application Management Application PNMes EPGs	VRFs	Cloud Network (Controller (Azure)	Azure azure10 Q Secon dcmm-defaul	: Virtual Network	<5		Wintual Network azure 10 General Account domm-default-tn	Q ⊘ ♥ Healthy	••••••••••••••••••••••••••••••••••••••
Dashboard Dashboard Topology Coud Resources Apsilication Management Application Profiles EPGs Contracts	VRFs	Cloud Network (Controller (Azure)	Azure azure 10 Q. Seess azure 10 90.1 donm-defaul	: Virtual Network			Virtual Network azure 10 General Account Gener-default-in Region	Image: Control of the end	••••••••••••••••••••••••••••••••••••••
Deshboard Deshboard Topokoy Topokoy Coud Resources Coud Resources Application Protites EPGs Contracts Fitters		Cloud Network (S Leak Routes Health • Healthy • Healthy • Healthy	Controller (Azure)	Azure azure10 Q Second dom-defaul	: Virtual Network			Virtual Network acure 10 General Account dom-default-tn Region eastus	C S	
	VRFs	Cloud Network (S Leak Routes reath reath reath reathy reathy	Controller (Azure)	azure10 Q. Seen azure10 90.1 dcnm-defaul	: Virtual Network			Virtual Network acure 10 General Account dorm-default-tn Region eastus Cloud Resources	C S	
		Cloud Network (S Leak Routes reaction rea	Controller (Azure)	Azure 10	: Virtual Network			Virtual Network acure 10 General Account dorm-default-tin Region eastus Cloud Resources	C C	
		Cloud Network (CS Leak Routes reactions Healthy e Healthy e Healthy e Healthy e Healthy e Healthy	Controller (Azure)	Azure 10 Q Been azure 10 90.1 dccm-defad	: Virtual Network			Virtual Network acure 10 General Account domn-default-tin Region eastus Cloud Resources	C Pealthy	C C C C C C
		Cloud Network (CS Cloud Network (CS Cloud Network (CS CS Cloud Network (CS	Controller (Azure)	Azure 10 Q Second dccm-defaul	: Virtual Network	< <u>.</u>		Virtual Network acure 10 General Account Gorm-default-tn Region eastus Cloud Resources	C Pealthy	C C C C C C
		Cloud Network (CS Cloud Network (CS Cloud Network (CS CS Cloud Network (CS	Controller (Azure)	Azure 10 Q. Territoria dictore-default	: Virtual Network	< <u>.</u>		Virtual Network acure 10 Ceneral Account corm-default-tn Region eastus Cloud Resources I network Agricume Security Orange	C C C C C C C C C C C C C C C C C C C	
		Cloud Network (CS Cloud Network (CS Cloud Network (CS CS Cloud Network (CS	Controller (Azure)	Azure 10 Q. Torrest discurred to 00.1 discurred to 00.1	: Virtual Network	(S		Virtual Network acure 10 Ceneral Account dcmr-default-tn Region eastus Cloud Resources Cloud Resources I ngues Application Management	C C C C C C C C C C C C C C C C C C C	C C C C C
		Cloud Network (Cloud Network	Controller (Azure)	Azure 10 Q. azure 10 00.1 dcm-defaul	: Virtual Network	(S		Virbual Network acure 10 Ceneral Account dcom-default-to Region eastus Cloud Resources Cloud Resources I nguess Application Management O	C C C C C C C C C C C C C C C C C C C	C C C C C
Control Resources		Cloud Network (CS Leak Routes Amathematical Heatth Heatth Heatth Heatthy Heatth	Controller (Azure)	Azure 2 azure 10 azure 10 et. 1 azure 10 et. 1	: Virtual Network	(S		Control Network Control Contr	C C C C C C C C C C C C C C C C C C C	Cover Frederic
E Derbboard Derbboard Torokoy Torokoy Codebearces Code		Cloud Network (Cloud	Controller (Azure)	Azure 10 Q. asure 10 90.1 d.crm-defaul	: Virtual Network	< <u>s</u>		Virtual Network acure 10 Ceneral Account dorm-default-tin Region eastus Cloud Resources I gradients beionly Group 1 Againatic beionly Group 2 Application Management O Application Management I Uses	© Healthy © Healthy 0 10	C C
Danbbard Danbbard Danbbard Topokoy Topokoy Topokoy Contracts Contra		Cloud Network (CS Leak Routes Aeath Aea	Controller (Azure)	Azure 10 Q = 100 d current of etail	: Virtual Network	(S		Coneral Account Accou	C C C C C C C C C C C C C C C C C C C	

ステップ7 Azure に展開されたクラウドネットワーク コントローラーに残ったまま、[クラウド 情報技術(Cloud Resources)]>[仮想ネットワーク(Virtual Networks)]に移動し、azure10 VNet をクリックし、概要ページの情報を使用して追加の検証を行います。

Verview Topolog	verview Topology Cloud Resources Application Management Event Analytics		Subnets for CIDR Block 90.1.0.0/16					
			00110/24					
General Account dcnm-default-tn Region eastus			Settings Cloud Access Privilege Inherited (Routing & Security) Cloud Context Profile azure10-eastus CIDRs		Settings Cloud Access Privlege Inherited (Roding & Security) Cloud CIDR's Subnet 90.1.1.0/24			
Cloud Resources			CIDR Block Range	р	Name -			
1 Regions	0 Routers	1 Network Security Groups	90.1.0.0/16 Cloud Provider ID	2	Route Table Settings	~		
1 Application Security Groups	0 Virtual Machines	O Endpoints			Name azure10.egress Oper State configured			
Application Manager	nent				Cloud Provider ID			
0 Application Profiles	O EPGs	1 Cloud Content Profiles			Direction			
1 ver-	O Service Graphs				egress Entries Destination Address * Next Hop			
					172.16.10.0/24 10.90.1.36			

ステップ8 Azure コンソールで、追加の検証を実行します。

	${\cal P}$. Search resources, services, and docs (G+/)		📃 🗉 🕞 🖉 🖉 🤉 C	₽	ambsingh@cisco cisco-inse	D.com
Home >						
Virtual networks ∞ … Cisco-INSBU-MKT						×
🕂 Create 🐵 Manage view 🗸 🖒 Refresh 🞍 Export to	CSV 😚 Open query 🛛 🕅 Assign tags					
Filter for any field Subscription equals all Re	isource group equals all $ imes$ Location equals all $ imes$ $^{ extsf{hg}}$ Add filter					
			No grouping	\vee	E≣ List view	~
Name †.	Resource group 14	Location †4	Subscription †↓			
□ <→ azure10	CAPIC_dcnm-default-tn_azure10_eastus	East US	huyeduon-Demo05			
everlay-1	azurendfc	East US	huyeduon-Demo05			
Stretched-vrf	CAPIC_dcnm-default-tn_stretched-vrf_eastus	East US	huyeduon-Demo05			

	P Search n	esources, services, and docs (G+/)				🛱 🖉 🍥 🕐	R ambsingh@cisc	o.com 🕘
Home > Virtual networks > azure10 Virtual networks Cisco-INSBU-MKT + Create @ Manage view ∨ …	Azure10 Subnets Virtual network	☆ … + Subnet + Gate	way subnet 💍 Refre	와 ⁸ 옷 Manage users	Delete				×
Filter for any field Name †:	Overview Activity log Access control (IAM)		IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group 14	Route table ↑↓	
 Active to Active to	Tags Diagnose and solve problems	subnet-90.1.1.0_24	90.1.1.0/24	2	251	2	subnet-90.1.1.0_24	rt-azure10_egress	
	Settings								

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。