

# 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(1ページ)
- •オンプレミス NDFC ファブリックを設定 (3 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 (21ページ)
- NDFC とクラウド サイトを ND と NDO に導入準備する (36 ページ)
- Complete サイト間の接続 NDFC と クラウド サイトの間 (44 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のオプション1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 **2**:



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3:

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.	
Select	

**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 4:

Fabric Name	
sydney	
Pick Template	
Easy_Fabric >	
General Parameters Replication VPC Protocols Adva	nced Resources Manageability Bootstrap Configuration Backup Flow Monitor
BGP ASN*	
65084	1-4294967295   1-65535(.0-65535) h 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 5:

Fabric Name sydney		VTEP HoldDown Time 180	NVE Source Inteface HoldDown Time (Min:1, Max:1500) in seconds
Pick Template Easy_Fabric >		Brownfield Overlay Network Name Format 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* Default_VRF_Universal	Default Overlay VRF Template For Leafs	Enable VXLAN OAM	Enable the Next Generation (NG) OAM feature for all switches in the fabric to aid in trouble-shooting VXLAN EVPN fabrics
Network Template* Default_Network_Universal	Default Overlay Network Template For Leafs	Enable Tenant DHCP	
VRF Extension Template* Default_VRF_Extension_Universal	Default Overlay VRF Template For Borders	Enable NX-API on HTTP port	Enable NX-API on port 443 Enable NX-API on port 80
Network Extension Template* Default_Network_Extension_Universal	Default Overlay Network Template For Borders	Enable Policy-Based Routing (PBR)	
Overlay Mode config-profile	VRF/Network configuration using config-profile or CLI, default is config-profile	Enable Strict Config Compliance	Enable bi-directional compliance checks to flag additional configs in the running config that are not in the intent/expected config
Site id	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* 9216	(Min:576, Max:9216). Must be an even number	Enable NDFC as Trap Host	Configure NDFC as a receiver for SNMP traps
Layer 2 Host Interface MTU* 9216	(Min:1500, Max:9216). Must be an even number	Anycast Border Gateway advertise-pip	To advertise Anycast Border Gateway PIP as VTEP. Effective on MSD fairs' 'Denatoriates Confin'

- **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6:

		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*	
General Parameters Replication VPC Protocols Adv	anced Resources Manageability Bootstrap	2-511	Per Border Dot1q Range For VRF Lite Connectivity (Min:2, Max:4093)
		VRF Lite Deployment*	
Manual Underlay IP Address Allocation		Manual V	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		created VRF Lite IFC links will have 'Auto Deploy Flag' enabled.
		VRF Lite Subnet IP Range*	
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	VRF Lite Subnet Mask*	
Underlay RP Loophack IP Range*		30	(Min:8, Max:31)
20.254.254.0/24	Anycast or Phantom RP IP Address Range	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(7 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 (4 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 7:

ney		172.16.0.67-68,172.16.0	.76	MD5	admin	
isword Set		Max Hops 2		Preserve config Disabled		
ck						
scovery Results						
iter 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	9600UQZJFTJ	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 V 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 **8**:

図9:

		Interfaces Interfac	e Groups Po	licies Networks \	/RFs Services E	vent Analytics His	tory Resources Vir	tual Infrastructure			
lter	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	FD02442051Z	In-Sync	Minor	• Ok	N9K-C9348GC-FXP	Secondary	ndfc-leaf2	Preview
	ndfc-leaf2	172.16.0.68	Leaf	FDO2442054U	In-Sync	O Minor	• Ok	N9K-C9348GC-FXP	Primary	ndfc-leaf1	Discovery
1	ndfc-spine1	172.16.0.76	Spine	FDO243503ZG	In-Sync	O Mir Spine	Ok	N9K-C9332C			Set Role
1											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	
s	elect

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 10:

Fabri	c Overview	- sydney								Actions A	0? -
Overvie	w Switches Links	s Interfaces Interfac	e Groups Pol	cies Networks	/RFs Services E	vent Analytics Hist	ory Resources Vir	tual Infrastructure	Edit	t Fabric d Switches	
Filte	r 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	Minor	Ok	N9K-C9348GC-FXP	Secondary	ndfc-leaf2	Normal
	ndfc-leaf2	172.16.0.68	Leaf	FDO2442054U	In-Sync	O Minor	• Ok	N9K-C9348GC-FXP	Primary	ndfc-leaf1	Normal
	ndlc-spine1	172.16.0.76	Border Gateway Spine	FDO243503ZG	• in-Sync	O 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11:

Fabr	ic Overview	r - sydney								Actions ~	• • • • • • • • • • • • • • • • • • •
Overvi	w Switches Lin	ks Interfaces Interface	Groups Polic	ies Networks V	RFs Services Ev	ent Analytics Histo	ry Resources Vir	tual Infrastructure			
Filt	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	FD0243503ZG	In-Sync	♥ Minor	• Ok	N9K-C9332C			Normal

#### 次のタスク

NDFC 外部ファブリックを構成(11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 (4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 13:

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 14:

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(15 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 (12 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 15:

Add Switches	? ×
Add Switches	? ×
	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 16:

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 17:

Switch 172.16.0.234	A N	Muthentication Protocol MD5	Username admin			
Max Hops 0	P	Preserve config Enabled				
r IP Address	Model	Version	Status	Progress		
A 172.16.0.234	C8000V	17.7.1a	Switch Added			
en	Switch 172.16.0.234 Max Hops 0 Provide the second	Switch 172.16.0.234  Max Hops 0  P  172.16.0.234  P  172.16.0.234  Model  172.16.0.234  Model  172.16.0.234  172.16.0.24  172.16	Switch 172.16.0.234     Authenication Protocol MD5       Max Hops 0     Preserve config <ul> <li>Preserve config</li> <li>Enabled</li> </ul> er     IP Adress     Model     Version           Max         172.16.0.234         G8000V         Version           Max         172.16.0.234         G8000V         Image: Configuration of the second of the seco	Authentication Protocol MDS       Username admin         MDS       Preserve config         0       Preserve config       Enabled         Preserve config       Enabled       Username admin         Preserve config       Enabled       Username admin         Preserve config       Enabled       Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Username admin         Preserve config       Enabled       Image: Colspan="2">Image: Colspan="2"       Image: Colspan="2"       Image: Colspan="2"       Image: Colspan="2"        Image: Colspan="2" <th <<="" colspan="2" td=""></th>		

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 18:

Fab	ric Overviev	v - ext-fab-1								Actions ~	O? –
Overv	Verview Switches Links Interfaces Policies Event Analytics History Resources Virtual Infrastructure										
Fi	er by attributes										Actions A
C	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 >
											থম vPC Pairing
											TOR 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。

**巡 19**:

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

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 **20** :

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 **21** :

≡ داندان دانده Nexus Dashboard	d 🕴 🕀 One V	iew ~				Feedback 💄			
E Fabric Controller									
n Dashboard	I AN Fa	brics				6			
∺ Topology	LANTO	01105				e			
≡ LAN ^	Filter by at	tributes				Actions ~			
Fabrics									
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 22:



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 23 :

≡	🔅 One View 🗸			
F Fabric Controller				
🏫 Dashboard	Data Center / Sydney			
% Topology	View A Searc	h by Attributes		
	(+ - 2 0 <b>B</b> X)			
Fabrics	Show Logical Links			
Switches	Operation Configuration		NET	
Interfaces				
Services	Hierarchical		INCLINITIES (U) VRFS (U)	VIVI (3)
📥 Virtual Management 🔍	In-Sync			
🔅 Settings 🗸 🗸	Pending			
_r⁰ Operations ∨	<ul> <li>In Progress</li> </ul>			
	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 (21 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(<sup>2</sup>) 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(24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(23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 25:

Setup - Region Mar	nagement				>
	0	2			
	Regions to Manage	General Connec	tivity		
	Derma Ceval Reterior Controller Der-Prentises AC Site	kter-Six Consciony	Tardi Garey Tardi Garey Casiyet Soory	Inter-Regios Connectivity	
	between VPCs in all managed regions.	for controller and which regions about it	ust Global Robers, Global Robers need to	pe deployed in acleast one region to enable connectivity	
	Please note that CSR is now changed to	Catalyst 8000V.			
	Use Transit Gateway ● ✓ 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 Pacific (Mumbai)	ap-south-1			
	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		×	
	US East (Ohio)	us-east-2		$\checkmark$	
	US West (N. California)	us-west-1			
	US West (Oregon)	US-WeSt-2 Cloud Network Controller De	ployed	<ul> <li>Image: A set of the set of the</li></ul>	
				Back to Overvi	ew Previous Next Save and Continu

**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 **26** :

CIDR *	
	✓ ×
	CIDR *

- 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 27:

Add Hub Network		×
Name *		
hub1		
BGP Autonomous System Number *		
65091		
TGW Connect		
Chapter Enable		
Changing the use of TGW Connect will cause temporal	ry 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 (29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 (22 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(31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(29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 **28** :

Setup - Region Management							
0	Please note that CSR is now changed to Catalyst 8000V.						
Con	nectivity for Internal Network 🐠						
	VNet Peering						
Reg	ions to Manage * 💿						
	Region Name	Region	Catalyst 8000Vs 🚳				
	Australia Central	australiacentral					
	Australia Central 2	australiacentral2					
	Australia East	australiaeast					
0	Australia Southeast	australiasoutheast					
	Brazil South	brazilsouth					
	Canada Central	canadacentral					
	Canada East	canadaeast					
C	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 **29** :

Setup - Region Management			
External Cloud Network Controller Con-Premises ACI Site		Inter-Site Connectivity ——	R © © Catalyst 8000V
Configure the fabric infra connectivity the configuration template used for the i Please note that CSR is now	for the Cloud Site. The Cloud Routers in the Cloud Routers in the changed to Catalyst	ne Fabric Autonomous System e Cloud Site. 8000V.	Number is used for BGP peering insid
General			
Subnet Pools for Cloud Routers	Ð		
Subnet * R	Regions	Created By	
10.90.0.0/24		System Internal	0
10.90.1.0/24		User	8
	Routers		

**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。

30	
	30

Setup - Region Management	
Catalyst 8000Vs	
BGP Autonomous System Number for C8kVs * 65092	
Assign Public IP to CSkV Interface 🖗	
Changing CBKV connectivity from private to public (or vice versa) may cause disruption in your network.	
Number of Routers Per Region 2 V	
Username * cisco	
Password	
Confirm 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	
TCP MSS *	
1300	
License Token  Back to Overview Previou Previou	Is Next Save .

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 (36 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(4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 (12 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 (22 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(29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 31:

≡ cisco Nexus Dasht	ooard lo Admin Console						back 上 🤨
	G fab2nd2					0	
C Overview	Sites						٥
III Services	Filter by attributes						Add Site
System Resources  Operations	Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
⊖ Infrastructure ∨							
<u>k</u> <sup>e</sup> Administrative ~	10 V Rows			No rows found		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。

図 **32** :

≡ disco Nexus D	lashboard 🕴 🕀	One View $\sim$				Feedback 💄
F Admin Console	e 📀 fab2nd:	2				0 🖸 🕻
Overview	d Sites					
© Sites						
III Services		Site Type				
System Resources			0		0	۲
Operations		ACI	(W)	Cloud Network Controller	MDFC	
C Infrastructure						
£ Administrative			Jabased data antanà and DOMANDITO sites datas far antanà dia	istand	L	

**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。

図 33:

≡ 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 form      Societ Table      So	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 34:

Admin Console	e 🤇	6 fab2nd2						000
verview		Sites						
ervices		Filter by attributes						Add Si
vstem Resources		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
frastructure		A Minor	Sydney	NDFC	(O up	12.1.2.275	o	
Iministrative		() Healthy	ext-fab-1	NDFC	(Q) Up	12.1.2.275	0	
		10 ~ Rows					Page 1 of 1	< < 1-2 of 2

[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 **35** :

≡ cisco Nexus D	ashboard	One View ~			Fead
<ul> <li>Admin Console</li> <li>overview</li> <li>Sites</li> </ul>	e 🕝 fat Sites	2nd2			٥
Services System Resources Operations		Site Type	Cloud Network Controller	NDFC	
2 Administrative		General Name* Settings Username/P Address* Username* address* Username* address* Login Demain o Login Demain o			
		Chable Prov Security Domains Name Add Security Domains			
					Cancel

- 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。

図 36:

≡ cisco Nexus Dashboa	rd 🛛 🌡 o Admin Console 🗸						Feedback 1 9
	G fab2nd2						000
Overview	Sites						٥
III Services	Filter by attributes						Add Site
System Resources	Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
C Infrastructure	(A major)	AWS	Cloud Network Controller	aws 💿 up	25.1(Te)	0	
⊥° Administrative ∨	A Minor	Sydney	NDFC	(Ø up	12.1.2.275	0	
	() Healthy	ext-fab-1	NDFC	(d) (O)	12.1.2.275	0	
	10 v Roes					Page 1 of 1 🔇	<1-3 of 3>>>

[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 37:

≡ cisco Nexus Da	shboard 🕴 🔶	One View 🗸				Feed
	C fab2nd2	1				0
© Overview © Sites	d Sitos					
Surtem Resources		Site Type				
Departions		ACI	Cloud Network Controller	۲ 🌑 📲	NDFC	
O Infrastructure						
⊥° Administrative		General Name * Azure				
		Settings				
		Hostname/IP Address •				
		Username * 🛈 admin				
		Password * ()				
		Enable Proxy				
		Security Domains Name				
		Add Security Domains				
						Cancel Save

- **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 **38**:

≡ cisco Nexus	Dashboa	rd 🛛 🔒 o Admin Console	•					Feedback 💄 🕐
= Admin Consc	ole	G fab2nd2					9	0 🖪 🖾
Overview     Sites		Sites						Ó
III Services		Filter by attributes						Add Site
System Resources		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
Infrastructure		A Major	Azure	Cloud Network Controller	(⊘ Up	<b>T</b> 25.1(1e)	o	
_£° Administrative		🛆 Major	AWS	Cloud Network aws Controller	( Ø Up )	25.1(1e)	0	
		A Minor	Sydney	NDFC	[⊘ Up]	12.1.2.275	0	
		Ø Healthy	ext-fab-1	NDFC	(Ø 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。

図 **39** :



# 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 40:

≡ <sup>•• •• ••</sup> cisco Nexus Dashl	board 单 Orchestrator 🗸					Feedback 💄 📀		
Dashboard	Sites							
Sites						0 t)		
<ul> <li>Application Management</li> <li>Fabric Management</li> </ul>	Filter by attributes							
	Controller Connectivity	Name	Туре	State	Version			
Operations     Infrastructure	⊘ок	AWS	e aws	Unmanaged ~	25.1(1e)			
Integration	⊘ок	Azure	Azure	Unmanaged ~	25.1(1e)			
	⊘ок	ext-fab-1	NDFC	Unmanaged ~	12.1.2.275	5		
	⊘ок	Sydney	NDFC	Unmanaged V	12.1.2.275			
	10 V Rows				Page 1	of 1 $\ll$ 1-4 of 4 $>$ $\gg$		

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 41 :

≡ disco Nexus Dashbo	oard 🏩 Orchestrator 🗸					Feedback 👤 🌚
Dashboard     Sites	Sites					(† ©
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
<ul> <li>Operations</li> <li>Operations</li> </ul>	ØОК	AWS	😑 AWS	Unmanaged ~	25.1(1e)	
@ Integration	⊘ок	Azure	Azure	Managed ~	25.1(1e)	
	⊘ок	ext-fab-1	NDFC	Unmanaged V	12.1.2.275	
	⊘ок	Sydney	NDFC	Unmanaged ~	12.1.2.275	
	10 v Rows				Page 1	of 1 $\ll\!\!<\!\!1\text{-4}$ of 4 $\!>\!\!\gg$

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 42:

	Siles									
Sites										
	Controller Connectivity	Name	Туре	State	Vers	sion				
	Øок		🥥 AWS	Unmanaged						
	Оок	Azure	Azure	Unmanaged						
	ØOK	ext-		Unmanaged						
	Оок	Syo	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 43:

Dashboard	Siles							
Sites						0		
Application Management     Fabric Management     Operations     Infrastructure     Infrastructure	Filter by attributes							
	Controller Connectivity	Name	Туре	State	Version			
	ØОК	AWS Site ID: 91	AWS	Managed	25.1(1e)			
	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 (44 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 (36 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 44:

≡ cisco Nexus Dash	nboard 🔔 Orchestrator 🗸					Feedback 💄 📀
<ul> <li>Dashboard</li> <li>Sites</li> <li>Application Management</li> </ul>	Sites					€5 ©
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
<ul> <li>Operations</li> <li>Operations</li> </ul>	Infrastructure	AWS Site ID: 91	e aws	Managed	~ 25.1(1e)	
@ Integration	System Configuration	Azure Site ID: 92	Azure	Managed	~ 25.1(1e)	
	Site Connectivity	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 $\ll\!\!<\!\!1\text{-4 of }4\!>\!\!\gg$

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 45 :

≡ cisco Nexus Dashboar	rd 🙏 Orchestrator 🗸	Feedback 💄 🔮
Dashboard     Sites	Site Connectivity	₹↓ Configure
Application Management  Fabric Management  Genations  Infrastructure  Infrastructure  Infrastructure  Infrastructure  Infrastructure Infrast	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46:

≡ cisco Nex	xus Dash	board to destant -	Feedback 1 9
Site Connecti	ivity		DEPLOY V Oti X
SETTINGS		Control Bios Configuration On Dramines Bios Devices Enternal Devices Inter Transl School NUEC Settions	
General Settings			
SITES		BGP	^
a 🤤 AWS		00P Preving Type	
disabled	0	Ad-mah v	
• O Azure		Keep-Alve Internal (Seconds) ()	
disabled	0	80 Matteria (Barren) ()	
e est-fab-1		190 x	
	0	State instruct Second ( )	
🔹 🌒 Sydney	0	Cased/Histort	
		0	
		00 TTL bitseen Paers	
		OSPF	~
		DDF Anno O	
		CloudSec Control	^
		NNA Augred Prin D	
		Data Path	^
		VILAY USD descenation port charge will cause traffic disruption for existing flows. Charge with cautor.	
		Orcepsionen Type NEAN ANIAN	

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 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 の オプション 1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(46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(44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 47:

[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。

2	48	
	τu	٠

≡ disco Ne	xus Dashb	oard 📃 🚖 Orchestrator 🗸
Site Connect	ivity	
		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         ×
e Azure		Type Unmanaged Managed
o 🔮 ext-fab-1		Name *
Sydney		ASN *
		Next Hop Address *

 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 49:

	ivity	
		Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDFC Settings
		On Premises IPsec Devices
		Name         Type         IP Address         Next Hop Address           Add On Premises IPace Device         IPAction         IPAction         IPAction         IPAction
disabled		Add On Premises IPsec Device ×
ext-fab-1		Type Unmanaged Managed
		Site *
Sydney		•

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	50	:
---	----	---

Site Connectivity		
	Control Diana Configuration - On Devalues (Dava Devices	Distant Davies, 1944 Transfer to the Destin
	Control Plane Configuration On Premises IPSec Devices	External Devices (Psec runnel Subnet Pools NUPC Setting
	On Premises IPsec Devices	
		Add On Premises IPsec Device ×
	Name Type IP Address	
	Add On Premises IPsec Device	Туре
Azure		Unmanaged Managed
0		Site *
		ext-fab-1
avtsfab-1		ASN
Ø OKTOD I		65080
		Device *
Surdaou		C8K3-Fab2
() Syuney		Interface *
		GigabitEthernet2 ~
		IP Address
		64.104.255.12
		Next Hop Address *
		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 51:

≡ داندان دانده Nexus Dasht	ioard 🌐 🙏 Orchestrator 👳	
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	IP Address 🕲	
disabled	169.254.0.0/16	
disabled		
◦ ● ext-fab-1	Site Specific Subnet Pool $\odot$	
	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 52:

≡ <sup>••  ••  •</sup> cisco Nexus Dasht	Doard 🏩 Orchestrator 🗸
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	IP Address 🔘
disabled	169.254.0.0/16
o 🔕 Azure	170.1.0.0/16
disabled	Add IP Address
🔊 🕒 ext-fab-1	
0	Site Specific Subnet Pool 💿
🔹 🌑 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 53:

TTINGS	Control Plane Configuration On Promises (Peee Paulace Este	rnal Devices - IPpee Tunnel Subnet Boole - NDEC Cattings
eneral Settings	Control Plane Computation On Premises iPsec Devices Exte	mai bevices insectiumer subnet Pools word settings
TES	External Subnet Pool 💿	
e 🤤 aws	IP Address D	
disabled	169.254.0.0/16	
Azure	170.1.0.0/16	~ <b>m</b>
disabled	Add IP Address	
ext-fab-1		
(c)	Site Specific Subnet Pool 💿	
Sydney	Name IP Address	
Ø	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 54:

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 (53 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 (46 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 55 :

≡ <sup>(1),1),</sup> cisco Nex	us Dashb	ard 🌐 🙏 Orchestrator 🗸			Fe	edback 上 😶
Site Connecti	vity			(	DEPLOY V	X €3©
SETTINGS			⊽ C	8K3-Fab2		
General Settings		P Site ext-fab-1 Refresh				
SITES		Core Router C8K3-Fab2	- critical	major	- minor	warning
o Oisabled	Ø		Ports Ethern	et Port ID		
💌 🔿 Azure			🔂 Add I	Port		
disabled	Ø					
o ext-fab-1	0					
🐑 🌒 Sydney	Ø					

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のオプション3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 (58 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 56 :

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 ○   Sep P Authentication   ● None ○ Simple ○ Cisco   Towards Cloud Router ○   BFD Enabled	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  Simple ○ Cisco  Towards Cloud Router ① BFD Enabled	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 ()   Import BGP Authentication   Inherit BGP Authentication   Import Simple () Cisco   Towards Cloud Router ()   BFD Enabled	IP 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  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   BGP Authentication  Simple Cisco  Towards Cloud Router   BFD Enabled	towards on-prem Spine BGW E1/32		
10.140.1.2   Remote ASN *   65084   MTU *   9216   Inherit BGP Authentication and BFD ①   Image: Second Se	Remote Address *		
Remote ASN * 65084 MTU * 9216 Inherit BGP Authentication and BFD ① Generation Oeneration	10.140.1.2		
65084         MTU ★         9216         Inherit BGP Authentication and BFD ③         SGP Authentication         Image: Simple Original Cisco         Towards Cloud Router ③         BFD Enabled	Remote ASN *		
MTU * 9216 Inherit BGP Authentication and BFD ① General Simple Cisco Towards Cloud Router ① BFD Enabled	65084		
9216 Inherit BGP Authentication and BFD ①  BGP Authentication  None Simple Cisco Towards Cloud Router ① BFD Enabled	MTU *		
Inherit BGP Authentication and BFD  BGP Authentication Simple Cisco Towards Cloud Router  BFD Enabled	9216		
BFD Enabled	Inherit BGP Authentication and BFD () BGP Authentication None Simple Cisco		
BFD Enabled	Towards Cloud Router 🕢		
	Towards Cloud Router 🕢		

**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。 (55 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 (53 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 57:

≡ <sup>•• ••• ••</sup> Nexus Dasht	oard A. Orchestrator ~	Feedback 上 🥥
Site Connectivity		DEPLOY V Oth X
SETTINGS		Sydney Settings
General Settings	Site Sydney	
SITES	Switch ndfc-spine1	Inter-Site Connectivity
disabled		General A
<ul> <li>Azure</li> <li>disabled</li> </ul>		Multi-Site VIP 10.10.0 1 IPsec Device ()
• • ext-fab-1		Name Device ID IP Address Add IPaec Device
<ul> <li>Sydney</li> </ul>		
	-	

#### 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 (56 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。 (55 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 58:

Site Connecti	vity		DEPLOY V Otl X
SETTINGS General Settings			Sydney Settings
attes	Ø	stre sydney     series	Inter-Site Connectivity General
a Azure	0		Multi-Site VIP 10.10.0.1 IPsec Device ①
ext-fab-1	Ø		Name Device ID IP Address
Sydney	ø		

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 **59** :

	xus Dashbo	ard 2. Orchestrator ~	Feedback 1 3
Site Connect	ivity		DEPLOY V OTIX
SETTINGS			Sydney Settings
General Settings		P Site Sydney Refresh	R
SITES		Switch ndfc-spine1	Inter-Site Connectivity
<ul> <li>AWS</li> <li>disabled</li> </ul>	Ø		General A Site ID 82
🔹 💿 Azure disabled	Ø		Multi-Site VIP 10.10.0.1 Auto Allocate IPsec Device ③
🔹 🌘 ext-fab-1	ø		Name Device ID IP Address
💌 🕒 Sydney	ø		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 60:

≡ disco Ne	xus Dashb	oard   🔔 Orchestrator	Feedback 💄 💿
Site Connect	ivity		DEPLOY V Otl X
SETTINGS			Sydney Settings
General Settings		Refresh	• Sydney Sectings
SITES		Cutter adda and	Inter-Site Connectivity
🤹 😑 AWS	0	Sauce une-shiner	General
disabled	0		Site ID 82
a Azure			Multi-Site VIP
disabled	0		IPsec Device ()
• ext-fab-1			Name Device ID IP Address
	0		C8K3- Fab2 98JE1U8CZ8M 64.104.255.12 🗸 💼
-			Add IPsec Device
Syuney	0		

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 (58 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 (56 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 **61** :

	kus Dasht			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					
<ul> <li>Sydney</li> </ul>						

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。

义	62	;
凶	ΟZ	

≡ <sup>•1 •• ••</sup> Nexus Dashboard	单 Orchestrator ~						Feed	back 👤 😏
Site Connectivity						D	EPLOY V	× (30
					o ndi	fc-spine1		
	Site Sydney			Defresh				
		Add Port	×		- critical	- major	minor	- warning
	Switch ndfc-spine1	Ethernet Port ID * Ethernet1/32 × ~						
e 💿 Azure		IP Address * 10.140.1.2/30			BGW PIP 20.3.0.4			
		Description towards on-prem C8Kv Gi-4						
<ul> <li>ext-fab-1</li> </ul>		Remote Address • 10.140.1.1 Remote Address •			O Add Po			
<ul> <li>Sydney</li> </ul>		65000 \$						
		BGP Authentication None Simple						
		Towards Cloud Router ③ BFD Enabled						
			<u>ok</u>					

- •[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のオプション3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 **63**:

≡ disco Nex	kus Dashboa	d 📜 🙏 Orchestrator 🗸			Fe	edback 1 9
Site Connecti	ivity				DEPLOY V	× €7@ [
SETTINGS			♡ 1	dfc-spine1		
General Settings		Refresh				
SITES		Switch ndfc-spine1	critical	major	minor	warning
disabled	0		BGP-EV	PN ROUTER-ID		
💌 🔕 Azure			BGW P	р 4		
disabled	0		Ports	net Port ID		
🔹 🌒 ext-fab-1	0		Ether	net1/32		/ =
			🔁 Add	Port		
<ul> <li>Sydney</li> </ul>	ø					

# 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 (60 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 (58 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 64:

Site Connect	ivity		DEPLOY V Otl
ETTINGS			AWS Settings
eneral Settings		Site AWS	Refresh Inter-Site Connectivity External Connectivit
AWS     disabled     o    Azure     disabled     o    Azure     disabled     o    ext-fab-1	0	Region us-west-2      Casy     Casy     Casy     Casy	General Site D 91 Nam-Site O B0P B0P Jonomous System Number 8091
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 **65**:

	exus Dashboard					
Site Connect	tivity					DEPLOY V Ota >
						AWS Settings
		Site AWS			Refresh	
						Inter-Site Connectivity External Connectivity
		Region us-wes	Add Site			General
		et_routerp_us-	Add Site			
0.45945			Connected to Site			
- ALUIG			Select Site >			BGP
					~	
e ext-fab-1			Protocol			
			BGP-EVPN			
Sydney						Inter-Site Connectivity
			IPsec			Site Protocol
			On Premises IPsec Devices			
			Device Name	IP Address		
			C8K3-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 66 :

図 67:

≡ داندان دانده Nexus Dashbo	oard 🌲 Orchestrator 🗸				
Site Connectivity					
SETTINGS					AWS Set
General Settings	Site AWS			Refresh	-
SITES	Region us-wes				Inter-Site Conne
(Q)	<pre>ct_routerp_us- west-2_0</pre>	Add Site		×	
e 🔕 Azure	C8KV	Select Site		×	Multi-Site ()
disabled	A	Q. Search Site	S Site Sydney		BGP Autonomous S
a 🌒 ext-fab-1		Azure	Site ID 82		
🝵 🖲 Sydney 💿			Type N/A		Inter-Site Connectiv
			URL https://172.16.0.191:443		Add Site
				Select	
				_	

[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。

ne connect	ivity				
neral Settings		Site AWS	Add Site		×
		Region us-wes			
			AWS - > Sydney		
		ct_routerp_us-	Connected to Site Sydney ×		
		west-2_0	Connection Type *		
🔕 Azure		C8kV	Public Internet		~
			Public Internet		~
			Private Connection		
ext-fab-1			hee one ty		
			IPsec		
Sydney			On Premises IPsec Devices		
			Device Name	IP Address	
			C8K3-Fab2	64.104.255.12	

[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のオプション3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

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 (63 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 (60 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 **68**:

≡ disco Ne:	xus Dashboar	rd 🗶 Orchestrator 🗸		Feedback 上 😋
Site Connect	ivity			DEPLOY V Oth X
SETTINGS				AWS Settings
General Settings		Site AWS	Refresh	
SITES	_	Boolog us-wast-2		Inter-Site Connectivity External Connectivity
AWS	0	Region us-west-2		General
enabled		ct_routerp_us-     west-2_0     west-2_1		Site ID 91
o 🔕 Azure	-	CBAV CBAV		Multi-Site 🕥
disabled	0			BCP
🔹 🌒 ext-fab-1				65091
	0			Contract Based Routing
<ul> <li>Sydney</li> </ul>				Inter-Site Connectivity
	0			Sydney RGP-EVPN 1
				Connection Type: Public
				And 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 **69**:

≡ disco Nexu	us Dashboai	rd 🔶 🙏 Orchestrator 🗸				Feedback 🛓 🤮
Site Connectiv	vity					DEPLOY V OCL X
						AWS Settings
		Site AWS			Refresh	
BITES		Region us-wes				Inter-Site Connectivity External Connectivity
		<ul> <li>ct_routerp_us- west-2.0</li> </ul>	Add Site		×	General A
a 🔘 Azute		CBKV	Select Site		×	MuttriSite @
			Q. Search Site	S Site Azure		BGP Autonomous System Number
is 🕘 ext-fab-1			Azure	Site ID 92		
🔹 🌘 Sydney				Type Azure	_	Inter-Site Connectivity  Protocol
				URL https://20.127.114.214:443		Sydnoy BGP-EVPN Z 11
				¢	Select	Add line

[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 70:

= cisco Ne:	kus Dashboan	d X Orchestrator			Headback 1
Site Connect	vity				DEPLOY V OTX X
					AWS Settings
		Site AWS	Add Site	×	· Ano settings
		Region us-wes	AWS ⊖ → Azure Ø	Ť.	Inter-Site Connectivity External Connectivity
		* ct_routerp_us- west-2_0	Please check if CBkVs are configured with Public IPs for Public Underlay connection		
e O Azure disabled		CBKV	Connected to Site Azure × Connection Tune *		Muta-Site () BOP
e 🔵 ext-fab-1			Public Internet		
			Protocol BGP-EVPN		
· Sydney			Hub Site 📀		Inter-Site Connectivity  Protocol
			Psec 2		Sydney BOP-EVPN X =
			Azure		Add 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 (65 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 (60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 (63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(63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 (63 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 71:

≡ cisco Nexus	Dashboard	1. Orchestrator -	Feedback 1 O
Site Connectivit	ty		DEPLOY V Oth X
SETTINGS			• Azure Settings •
General Settings		Site Azure     Refresh	Inter-Site Connectivity External Connectivity
<ul> <li>AWS</li> <li>enabled</li> </ul>	0	Region eastus     C.routerp_seatus     C.routerp_seatus     C.routerp_seatus	General A
Azure disabled	Ø	CRAV CRAV	Mutti-Site © BOP BOP Autonomous System Number
o 🌒 ext-fab-1	0		65992 Contract Based Routing
<ul> <li>Sydney</li> </ul>	0		Inter-Site Connectivity  Protocol  AWS Connection Type: Public BOP-EVPN
			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 72:

	xus Dashboar	d 🕴 🏩 Orchestrator 🤟				Feedback	10
Site Connect	ivity					DEPLOY V	s ×
						Azure Settings	
		Site Azure	Add Site		×	- Addie eestinge	
					*	Inter-Site Connectivity External Connect	
a 🥥 AWS		eastus	Azure <sup>O</sup> → Sydney ●			General	
		<ul> <li>ct_routerp_eastur</li> <li>J</li> </ul>	Connected to Site Sydney × Connection Type 1				
		CBKV	Public Internet		~	Multi-Site ()	
			Protocol			BGP	
a 🔘 ext-fab-1			BOP-EVPN				
			IPsec				
Sydney			On Premises IPsec Devices			Site Protocol	
			Device Name	IP Address		AWS BOP-EVPN	/ =
			C8K3-Fab2	64.104.255.12		Consuction Type Public	
			Sydney ● → Azure O				
			Please check if C8kVs are configure	d with Public IPs for Public Underlay connection			
			Connected to Site				

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 73:

Site Connectivity SETTINGS. Oeneral Settings		DEPLOY V Oth X
SETTINOS General Settings		
General Settings		Azure Settings
	Site Azure     Refresh	
SITES		Inter-Site Connectivity External Connectivity
🔹 🥥 AWS	kegion eastus	General
enabled	e ct_routerp_eastus 1 0	Site ID 92
• Azure	CBKV CBKV	Multi-Site 🕢
enabled		BGP
👳 🌑 ext-fab-1		BGP Autonomous System Number 65092
0		Contract Based Routing
Cuttore		Inter-Site Connectivity
( Sydney		Site Protocol
		AWS BGP-EVPN Connection Type: Public
		Sydney BGP-EVPN / 1
		C Add Site

#### 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 (68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 (65 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 (46 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(46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 74:

≡ cisco Ne	xus Dashboard 📃 🗴	Orchestrator v	Fee	dback 上 📀
Site Connect	ivity		DEPLOY A	013 X
SETTINGS			Deploy Only Deploy & Download On Premises IPsec Device Config files	O
General Settings	e	Site Azure Refresh	Deploy & Download External Device Config files Download On Premises IPsec Device Config files	inectivity
enabled	0	Region eastus ct_routerp_eastus 	Download External Device Config files	^
enabled	0		BGP BGP Autonomous System Number	^
♥ ● ext-fab-1	0		Contract Based Routing	
9 🔮 Sydney	0		Site Protocol AWS Connection Type: Public BGP-EVPN 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 75:

≡ <sup>•1 ••1 •</sup> Nexus Dashboa	rd 🗶 Orchestrator 🗸	Feedback 💄 🤇
Dashboard     Sites	Site Connectivity	t Configure
Application Management Fabric Management Operations Infrastructure Infrastructure Infrastructure Information	Connectivity Settings	Croup 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 76:

AWS 😑					^
Regions	ACI Multi-Site On	Site ID 91	8GP ASN 65091		
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	a	
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 77:

Azure  Regions 1 Inter-Site Connections Overlay State Underlay State Underlay State	ACI Muti-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	222	
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 78:

Sydney •						^
Nodes 1	Site ID 32	Multi-Site VIP 10.10.0.1	BGP ASN 65084		Fabric Type VXLAN Fabric	
Inter-Site Connections Overlay Status Underlay Status						Hide Connectivity Status $ \wedge $
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 **79**:

AWS 😑								
2	ACI Multi-Site On		580 ID 91		8509 ASN 85091			
ter-Site Connections								Hide Connectivity Status A
Deerby Status Underby	Status	Devisionment Statum		Overational Status		NOR EVEN Status	Turned Status	
21/2		© OK		© OK		41 1 4 4 0 0 0K	41 * 4 + 0	
ydney		⊘ ок		© ok		21 + 2 4 0 © OK	<b>21</b> + 2 ÷ 0	
ture o								
legions 1	ACI Multi-Site On		Site ID 92		80P ASN 65092			
								Hide Connectivity Status
er-Site Connections								Hide Connectivity Status
er-Site Connections	Status							Hide Connectivity Status
er-Site Connections Nextsy Status Underlay Be Name	Status	Deployment Status 🔿		Operational Status 🔿		BOP EVPN Status	Tunnel Status	Hide Connectivity Status /
er-Site Connections werkey Status Underlay Ite Name	Datus	Deployment Status 🔿		Operational Status O		60P EVPN Status 41 ↑ 4 → 0 ② 0K	Tunnet Status 41 + 4 + 4	Hide Connectivity Status
er-Site Connections wetay Status Underlay Is Name VS Droy	500m	Depleyment Status () () OK () OK		Operational Status () () CK () CK		EOP EVMI Status 41 ↑ 4 ↓ 0 © 0K 21 ↑ 2 ↓ 0 © 0K	Tunnel Status 41 ↑ 4 ↓ 0 21 ↑ 2 ↓ 0	Hide Connectivity Status -
er-Site Connections weekly Intern Underlay Its Name VS Only Vdney I	Rea.	Deployment Status O OK O OK		Operational Status () () OK () OK		B07EVM Bunes 41 ↑ 4 + 0 0 00 21 + 2 + 0 0 00	Tennet Status 41 ↑ 4 ÷ 0 21 ↑ 2 ÷ 0	Hide Connectivity Status
er-Site Connections Nextry Status Underlay AS AS AS AS AS AS AS AS AS AS AS AS AS	Sterio 62	Deployment Status () () OX () OX	Multi-Sate V/P 1030.0.1	Operational Blackss O O OK O OK	60P A39	B0P EV/N Balus 41 + 4 ÷ 0 ⊙ ∞ 21 + 2 ÷ 0 ⊙ ∞	Teaned Status 41 + 4 + 0 21 + 2 + 0 False Type VEANTHING	Nide Connectively Status A
er-Site Connections Nortry Italian Its Rame Its Its Rame Its Its Its Its Its Its Its Its Its Its	90mm 50m 0 82	Deployment Status ○ ○ OC ○ OC	Multi-Sae V/P 10150.0	Operational Status () () Or () Or	80P AD 60084	BOP DYN Slava           41 17 4 4 9 0 0 000           21 17 2 4 9 0 0 000	Tennel Selve           41 ± 4 ± 0           31 ± 2 ± 0           Faller, Type           VGLAN Falme	Hide Connectivity Bates
er-Sile Connections hwithy Balani Underlay to Anne Michael Connections Natives 1 Service Sile Connections	50m	Bigitypest Same ○ ○ or ○ or	Multi-See VP 1635.01	Operational Status  O O C C C C C C C C C C C C C C C C C	50P A29 60984	607 DVN Slava 41 ↑ 4 ÷ 0 © 00 21 † 2 ÷ 0 © 00	Normal Tassa 41 + 1 + 2 + 0 31 + 2 + 0 7	Nide Connectivity Status -
er Site Connections werk Material I thereby et Annue et Site Connections Notes 1 er Site Connections bereitigen I thereby the Name	50x 0 62 90xx	Dephysest Bana ()	0.000 526 107 10155.01	Operational Distan () () OK () OK	SOP AD 65924	607 01% 5uns 41 ± 4 ÷ 0 ⊕ 0r 11 ± 2 ÷ 0 ⊕ 0r	Tennel Talvat           41 + 4 + 6           21 + 2 + 6           / ratio	Nide Connectivity Earlie
ser-Sis Connections Sindly Back III to the Ary Ard Sindly Variables Participation of the Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary Ary	Ster D E2 Toma	Diployment Status  O O O O O O O O O O O O O O O O O O O	0000-004 10 <sup>0</sup> 10550 1	Operational Status O	BOP AD 65084 Operational Status O	Bart trive lases           41 ↑ 4 ÷ 0 ⊕ ∞           21 ↑ 2 ÷ 0 ⊕ ∞	Total factor           41 + 1 + 0           31 + 1 + 0           Factor from VELAN Factor           Factor from VELAN Factor           Overlap Meeting Bacteria           11 + 2 + 0         0	Hide 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 80:

$\equiv \begin{array}{c} \text{clisto} \\ \text{cisco} \\ \text{Nexus Dashboard} \\ \end{array} \oplus \text{o}$	Our View v	Feedback 👤 📀
= Fabric Controller		
<ul> <li>▶ Destboard</li> <li>▶ Topology</li> <li>■ LAN</li> <li>&gt; Vrhual Management</li> <li>&gt; Settings</li> <li>&gt; Operations</li> <li>&gt; Operations</li> </ul>	a Center Secho by Attributes Secho by Attributes Secho by Attributes Fabric: default Meta-lab2nd2-AWS Meta-lab2nd2-Azure Sycnoy 172.16.0.252	Actions >
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。