

# Setting Up the Infra Configuration for Hybrid Cloud and Multi-Cloud Connectivity Deployment

- Example Topology of Infra Configuration for Hybrid Cloud and Multi-Cloud Connectivity Deployment, on page 1
- Set Up the On-Premises NDFC Fabrics, on page 2
- Deploy Cloud Network Controller on Cloud Sites, on page 19
- Onboard the NDFC and Cloud Sites into ND and NDO, on page 32
- Complete Site-to-Site Connectivity Between NDFC and Cloud Sites, on page 39

# Example Topology of Infra Configuration for Hybrid Cloud and Multi-Cloud Connectivity Deployment

The following figure shows one of the supported topologies that could be used for the infra configuration for hybrid cloud and multi-cloud connectivity deployment.

Figure 1:



The procedures in this document will use this topology as a specific use case, which is based on Option 1 in Supported Topologies with IPsec (Multi-Cloud), and will describe how to configure the hybrid cloud connectivity options specifically for this topology use case.

In this deployment procedure, you will configure multi-cloud connectivity with IPsec, where you will make certain configurations in each of these hybrid cloud connectivity areas. The overall configuration steps are as follows:

Installing NDFC

For more detailed information, see:

- Cisco Nexus Dashboard Fabric Controller Installation and Upgrade Guide, Release 12.1.2 or later
- Cisco NDFC-Fabric Controller Configuration Guide, Release 12.1.2 or later
- Cisco Nexus Dashboard Fabric Controller Deployment Guide, Release 12.1.2 or later
- Initial setup:
  - · Setting up the on-premises NDFC fabric
  - Installing Cisco Cloud Network Controller
  - Setting up cloud sites
  - Installing NDO
  - Setting up hybrid cloud connectivity using NDO
- Deploying the tenant and schema:
  - Use case 1: Stretched VRF (intra-VRF)
  - Use case 2: Route leaking (inter-VRF)

# Set Up the On-Premises NDFC Fabrics

In this section, you will set up the two on-premises NDFC fabrics:

- NDFC VXLAN fabric
- NDFC external fabric

Complete the procedures in the following sections to set up the two on-premises NDFC fabrics.

# **Create an NDFC VXLAN Fabric**

In this procedure, you will be configuring the part of the example topology highlighted below.



The VXLAN fabric must contain one or more Border Gateway (BGW) devices, which are used to build VXLAN Multi-Site connectivity between on-premises fabrics and the cloud sites.

Complete the procedures in the following sections to configure an NDFC VXLAN fabric.

# **Create an NDFC VXLAN Fabric**

Step 1 Log into the Nexus Dashboard where you have NDFC installed. Step 2 Log into your NDFC account. Step 3 Navigate to LAN > Fabrics. The LAN Fabrics window appears. Step 4 Click Actions > Create Fabric. The Create Fabric window appears. Step 5 Begin the process of creating an NDFC VXLAN fabric using the Easy Fabric template. a) In the Fabric Name field, enter a name for the NDFC VXLAN fabric. b) In the Pick a Template area, click Choose Template. The Select Fabric Template window appears. c) Locate and click the Easy Fabric template. d) Click Select.

#### Figure 3:



## **Step 6** Complete the necessary general VXLAN fabric parameter configurations.

The following parameter tabs in the Easy\_Fabric template must be completed, but they do not contain parameters that are specific to this hybrid cloud topology use case:

- General Parameters
- Replication
- VPC
- Protocols

Complete the VXLAN fabric configurations in those parameter tabs as you normally would. See *Cisco Nexus Dashboard Fabric Controller Deployment Guide*, Release 12.1.2 or later, for more information.

For example, using the information in the example topology, you would enter 65084 in the **BGP ASN** field in the **General Parameters** page.

#### Figure 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) 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*		
p2p	~	Numbered(Point-to-Point) or Unnumbered
Underlay Subnet IP Mask*		
.30	$\sim$	Mask for Underlay Subnet IP Range
Underlay Subnet IPv6 Mask		
Select an Option	$\sim$	Mask for Underlay Subnet IPv6 Range
Underlay Routing Protocol*		
ospf	$\sim$	Used for Spine-Leaf Connectivity
Route-Reflectors*		
2	~	Number of spines acting as Route-Reflectors

**Step 7** In the **Advanced** parameter tab, make the necessary configuration specifically for this hybrid cloud topology use case.

• Locate the **Anycast Border Gateway advertise-pip** field and check the box to enable this option. This advertises the Anycast Border Gateway PIP as VTEP.

This is required when Layer 3 only connectivity (for example, no Layer 2 extension) is established across sites, which is always the case for hybrid cloud and multi-cloud deployments.

• Complete the remaining configurations in the Advanced parameter tab as you normally would.

#### Figure 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 Advan	ced 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*	Data di Carda 1977 Tara las Facilitat		Enable NX-API on port 443
Network Extension Template*	Deraum Overlay vice template For borders	Enable NX-API on HTTP port	Enable NX-API on port 80
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
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* 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 fabric 'Recalculate Config'

**Step 8** Click the **Resources** parameter tab and enter the necessary values in this page.

- Enter the appropriate information in the following fields specifically for this hybrid cloud use case:
  - Underlay Routing Loopback IP Range: This is typically the loopback0 IP address range.
  - Underlay VTEP Loopback IP Range: This is typically the loopback1 IP address range.
  - Underlay RP Loopback IP Range: The Anycast or Phantom Rendezvous Point (RP) IP address range.
  - Underlay Subnet IP Range: The address range to assign numbered and peer link SVI IP addresses.
  - VRF Lite Subnet IP Range: The address range to assign P2P inter-fabric connections.

• Complete the remaining configurations in the **Resources** parameter tab as you normally would.

#### Figure 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*	
Constal Parameters - Poplication - VPC - Protocola - Adu	anad Resources Managaphility Restation	2-511	Per Border Dot1 q 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	
Hadaday Daviting Lagrahash ID Dagast			Whether to auto generate VRF LITE sub-interface and BGP
Underlay Routing Loopback IP Range"			peering configuration on managed neighbor devices. If set, auto created VRF Lite IFC links will have 'Auto Deploy Flag' enabled.
20.2.0.0/22	Typically Loopback0 IP Address Range	VRE 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 Loopback 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)

**Step 9** Complete the necessary general VXLAN fabric parameter configurations in the **Manageability** and **Bootstrap** parameter tabs.

The configurations in the **Manageability** and **Bootstrap** parameter tabs might need to be completed, but they do not contain parameters that are specific to this hybrid cloud topology use case.

**Step 10** Click the **Configuration Backup** parameter tab and check the box in the **Hourly Fabric Backup** field to enable that feature.

Complete the remaining configurations in the **Configuration Backup** parameter tab as you normally would.

**Step 11** Click **Save** when you have completed the necessary configurations in the **Create Fabric** window for the VXLAN fabric.

You are returned to the LAN Fabrics window, with the VXLAN fabric that you just created displayed.

#### What to do next

Add the switches to the VXLAN fabric and set the necessary role for the switches using the procedures provided in Add Switches to the VXLAN Fabric, on page 7.

# Add Switches to the VXLAN Fabric

In this procedure, you will add the switches to the VXLAN fabric and set the necessary role for the switches.

## Before you begin

Create an NDFC VXLAN fabric using the procedures provided in Create an NDFC VXLAN Fabric, on page 3.

Step 1 In the LAN Fabrics window, click the VXLAN fabric that you just created.

The **Overview** window for this fabric appears.

Note The following steps describe how to manually enter the necessary information to allow NDFC to discover switches. You could also use the Power On Auto Provisioning (POAP) feature in NDFC instead, which is useful if you do not already have certain parameters, such as the management IP address, default route, and start up configurations, already configured on the switches that need to be discovered. POAP automates the process of installing configuration files on devices that are deployed on the network for the first time and allows devices to be brought up without performing any manual configuration. See Inband POAP Management in External Fabrics and LAN Classic Fabrics and Zero-Touch Provisioning of VXLAN Fabrics using Inband POAP with NDFC for more information on POAP.

#### Step 2 Click Actions > Add Switches.

The Add Switches window appears.

- **Step 3** Add the necessary information to discover the switches.
  - Fill in the necessary information in this page to discover the switches, including the Seed IP, username, and password.
  - Determine if you want to preserve the existing configuration on the switches:
    - If this is a brownfield deployment where you want to keep the existing configurations on the switches, check the **Preserve Config** checkbox to preserve those existing configurations.
    - If this is a greenfield deployment, uncheck the **Preserve Config** checkbox to clean up the configurations on the switches.

#### Step 4 Click Discover Switches.

Click **Confirm** in the confirmation popup window that appears.

**Step 5** Once the switches have been discovered, add the switches to the NDFC VXLAN fabric.

In the **Discovery Results** area, choose the appropriate switches (click the box next to each of the appropriate switches).

As an example, the figure below shows two leaf switches and one spine switch being added to the fabric.

#### Figure 7:

ney		172.16.0.67-68,172.16.0	.76	MD5	admin	
sword Set		Max Hops 2		Preserve config Disabled		
:k						
covery Results						
ter 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 V Rows					Page 1	of 2 ≪ < 1-10 of 14 > 🚿

#### Step 6 Click Add Switches.

**Note** If the **Preserve Config** option is checked, the switches will go through a reboot after being added to the NDFC VXLAN fabric.

## **Step 7** Set the role for the appropriate switch to Border Gateway Spine.

In these example procedures, one spine switch plays the dual role of spine switch and border gateway spine switch, so we will be changing the role of the spine switch to border gateway spine switch in these example procedures. However, in your environment, you might have two separate switches, one with the role of spine switch and the other with the role of border gateway.

- a) Click the **Switches** tab in the NDFC VXLAN fabric overview window. The switches that have been added to this fabric are displayed.
- b) Click the box next to the spine switch to choose that switch, then click Actions > Set Role.

#### Figure 8:

or	by attributes										Actio
	Switch	IP Address	Role	Serial Number	Config Status	Oper Status	Discovery Status	Model	VPC Role	VPC Peer	Add Switche
	ndfc-leaf1	172.16.0.67	Leaf	FD02442051Z	In-Sync	O 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
I	ndfc-spine1	172.16.0.76	Spine	FDO243503ZG	In-Sync	O Mir Spine	• Ok	N9K-C9332C			Set Role vPC Pairing

c) Locate and select the Border Gateway spine role in the Select Role list, then click Select.

#### Figure 9:

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

**Step 8** Navigate to LAN > Fabrics and select the NDFC VXLAN fabric that you created.

The Overview page for this NDFC VXLAN fabric appears.

- **Step 9** Click the **Switches** tab to verify that the switches that you just added appear correctly.
- **Step 10** Click Actions > Recalculate and Deploy.

#### Figure 10:

Overview - sy	/dney								Actions A	O? —
Switches Links Int	erfaces Interface	e Groups Poli	cies Networks V	/RFs Services E	vent Analytics Hist	ory Resources Vir	tual Infrastructure	Edit Adv	l Fabric 5 Switches	
attributes								Rec	re >	Actions ~
witch	IP Address	Role	Serial Number	Config Status	Oper Status	Discovery Status	Model	VPC Role	VPC Peer	Mode
dfc-leaf1	172.16.0.67	Leaf	FDO2442051Z	In-Sync	O Minor	Ok	N9K-C9348GC-FXP	Secondary	ndfc-leaf2	Normal
dfc-leaf2	172.16.0.68	Leaf	FDO2442054U	In-Sync	O Minor	• Ok	N9K-C9348GC-FXP	Primary	ndfc-leaf1	Normal
dfc-spine1	172.16.0.76	Border Gateway Spine	FDO24350320	• In-Sync	O Minor	• Ok	N9K-C9332C			Normal
	Overview - sy Switches Links Int attributes witch Mc-harl1 Mc-spine1	Switches     Links     Interfaces     Interfaces       stributes     Interfaces     Interfaces       witch     IP Address       Mic-Half     172.16.0.67       Mic-Half     172.16.0.76       Mic-Half     172.16.0.76	Netroite     System     System     System     System       Switches     Links     Interfaces     Interface Groups     Politication       attributes     IP Address     Role       Micharl     172.16.0.67     Link       Micharl     172.16.0.68     Link       Micharl     172.16.0.76     Border       Micharl     172.16.0.76     Gateway	Switches         Links         Interfaces         Interface Groups         Policies         Networks         Networks           attributes         IP Address         Role         Serial Number           Mitches1         172.16.0.87         Leaf         FD02420512           Mitches2         172.16.0.88         Leaf         FD02420512           Mitches1         172.16.0.86         Leaf         FD024205020           Mitches1         172.16.0.76         Garler Spine         FD024350320	Switches         Links         Interfaces         Interface Groups         Policies         Networks         VRFs         Services         E           attributes         attributes         PAddress         Role         Serial Number         Config Status         Interface         Interface	Bit P Address         Role         Serial Number         Config Status         Oper Status           Mic-Nall         172.16.0.67         Leaf         FD024420512         In-Sync         0 Minor           Mic-spine1         172.16.0.76         Berder Spine         FD0244205322         In-Sync         0 Minor	Network         Switches         Links         Interfaces         Interface Groups         Policies         Networks         VRFs         Services         Event Analytics         History         Resources         Vir attributes           witch         IP Address         Role         Serial Number         Config Status         Oper Status         Discovery Status           Mc-Wal1         172.16.0.57         Leaf         FD02442051Z         In-Sync         ® Miroor         0 K           Mc-Wal1         172.16.0.68         Leaf         FD02442051Z         In-Sync         ® Miroor         0 K           Mc-spine1         172.16.0.76         Garder         FD02450312G         In-Sync         ® Miroor         0 K	Netrolice         Policies         Networks         VRFs         Services         Event Analytics         History         Resources         Virtual Infrastructure           stributes          PAddress         Role         Serial Number         Config Status         Oper Status         Discovery Status         Model           ntc-war1         172.16.0.67         Lasif         FD02442051Z         is tr-Sync         O Miroor         O K         N9K-C92480C-FXP           ntc-war2         172.16.0.68         Lasif         FD02442054Z         is tr-Sync         O Miroor         O K         N9K-C92380C-FXP           ntc-spine1         172.16.0.76         Berder Spine         FD0243503Z0         is tr-Sync         O Miroor         O K         N9K-C93332C	Switches       Links       Interfaces       Interfaces	Accome         Switches       Interface Groups       Policies       Networks       VRFs       Services       History       Resources       Virtual Infrastructure       Edit Fabric Add Switches       Add Switches       Edit Fabric       Add Switches       Real-       Real-

As described earlier, for these procedures, one spine switch plays the dual role of spine switch and border gateway spine switch, so we changed the role of the spine switch to border gateway spine switch in these example procedures, as shown below. In these example procedures, a vPC pair has also been configured already for the two leaf switches, as shown in the figure below. For more information on configuring a vPC pair, see the *Cisco NDFC-Fabric Controller Configuration Guide*, release 12.1.2e or later.

#### Figure 11:

L

viev	w Switches Link	s Interfaces Interfac	e Groups Polic	cies Networks \	/RFs Services Ev	vent Analytics Hist	ory 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	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	FDO2442054U	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
			_								

# What to do next

Configure an NDFC external fabric using the procedures provided in Configure an NDFC External Fabric, on page 11.

# **Configure an NDFC External Fabric**

In this procedure, you will be configuring the part of the example topology highlighted below. In the example figure below and throughout the use case procedures, a Cisco Catalyst 8000V is used as the IPsec device in the external fabric, but there could be many different types of devices in the external fabric, as long as they support IPsec and can be managed by NDFC (for example, ASR 1000 and Catalyst 8000V).

#### Figure 12:



An NDFC-managed external fabric contains one or more IPsec devices. The IPsec devices have connectivity to cloud networks either via the internet (public) or by a private connection, such as Direct Connect (AWS) or ExpressRoute (Azure). If public internet is used to connect to the cloud sites, IPsec tunnels are established between on-premises IPsec devices and Catalyst 8000Vs in the cloud sites.

Complete the procedures in the following sections to configure an NDFC external fabric.

# **Create an NDFC External Fabric**

# Before you begin

Complete the procedures provided in Create an NDFC VXLAN Fabric, on page 3 before proceeding with these procedures.

- **Step 1** Log into your NDFC account, if you are not logged in already.
- Step 2 Navigate to LAN > Fabrics.
- Step 3Click Actions > Create Fabric.The Create Fabric window appears.
- **Step 4** Begin the process of creating an external fabric using the External\_Fabric template.

The External\_Fabric template is used to build traditional LAN fabrics using Nexus as well as non-Nexus devices, such as Catalyst 8000Vs.

- a) In the Fabric Name field, enter a name for the external fabric.
- b) In the **Pick a Template** area, click **Choose Template**. The **Select Fabric Template** window appears.
- c) Locate and click the External\_Fabric template.
- d) Click Select.

## Figure 13:

2	Search Fabric Template
E Fa	asy_Fabric abric Template for a VXLAN EVPN deployment with Nexus 9000 and 3000 witches.
E Fa	asy_Fabric_IOS_XE abric Template for a VXLAN EVPN deployment with CAT9000 switches.
E Fa	asy_Fabric_eBGP abric Template for an eBGP based Fabric with Nexus 9000 and 3000 switches.
E Fa	xternal_Fabric abric Template for support of Nexus and non Nexus devices.
F	abric_Group abric Template that can contain other LAN Classic fabrics
L Fa	AN_Classic abric Template to manage various switches and topologies
L	AN_Monitor his fabric template is used for NI in Monitor Mode Only.
	Select

**Step 5** In the **General Parameters** tab, make the necessary configuration specifically for this hybrid cloud topology use case.

• In the **BGP ASN** field, define the BGP ASN.

For example, using the information in the example topology, you would enter 65080 in the **BGP ASN** field for this use case.

- Determine if you want the external fabric to be monitored or not:
  - If the on-premises IPsec device is going to be managed by NDFC, uncheck the box next to the **Fabric Monitor Mode** field to unselect this option.
  - If the on-premises IPsec device is not going to be managed by NDFC (such as a non-Cisco, third-party firewall), check the box next to the **Fabric Monitor Mode** field if the fabric is going to be monitored only.

#### Figure 14:

Create Fabric		
	Fabric Name ext-fab-1 Pick Template External_Fabric > General Parameters Advanced Resources Configuration	n Backup Bootstrap Flow Monitor
	BGP AS #* 65080 Fabric Monitor Mode	1-4294967295   1-65535[.0-65535] It is a good practice to have a unique ASN for each Fabric. If enabled, fabric is only monitored. No configuration will be deployed
	Enable Performance Monitoring (For NX-OS Switches Only)	

**Step 6** Complete the necessary general external fabric parameter configurations.

The following parameter tabs in the External\_Fabric template must be completed, but they do not contain parameters that are specific to this hybrid cloud topology use case:

- Advanced
- Resources
- Configuration Backup
- Bootstrap
- Flow Monitor

For example, in the **Configuration Backup** parameter tab, you might check the box in the **Hourly Fabric Backup** field to enable that feature.

See Cisco Nexus Dashboard Fabric Controller Deployment Guide, Release 12.1.2 or later, for more information.

**Step 7** Click **Save** when you have completed the necessary configurations in the **Create Fabric** window for the external fabric. You are returned to the **LAN Fabrics** window, with the external fabric that you just created displayed.

# What to do next

Add the on-premises Cisco Catalyst 8000V to the external fabric and set the necessary role using the procedures provided in Add the On-Premises Cisco Catalyst 8000V to the External Fabric, on page 14.

# Add the On-Premises Cisco Catalyst 8000V to the External Fabric

Follow these procedures to add the on-premises Cisco Catalyst 8000V to the external fabric and set the necessary role for the Cisco Catalyst 8000V.

# Before you begin

Create the NDFC external fabric using the procedures provided in Create an NDFC External Fabric, on page 12

Step 1 In the LAN Fabrics window, click the external fabric that you just created.

The **Overview** window for this fabric appears.

Step 2Click Actions > Add Switches.

The **Add Switches** window appears.

- Step 3 Add the necessary information to discover the Cisco Catalyst 8000V, then click Discover Switches.
  - Enter the necessary information in the Seed IP field for the Cisco Catalyst 8000V.
  - In the Device Type field, choose IOS-XE.
  - Choose the CSR/C8000V option underneath the Device Type field when it appears.

Figure 15:

Add Switches	? ×
Add Switches	? ×
	Close Discover Switches

# Step 4 Click Discover Switches.

Click Confirm in the confirmation pop-up window that appears.

**Step 5** Once the Cisco Catalyst 8000V has been discovered, add the Cisco Catalyst 8000V to the external fabric.

In the **Discovery Results** area, choose the Cisco Catalyst 8000V (click the box next to the Cisco Catalyst 8000V) and click **Add Switches**.

Figure 16:

dd Switches						?	>
Switch Addition Mechania	ism* e Neighbor Switches						
Seed Switch Deta Fabric ext-fab-1	ills	Switch 172.16.0.234		Authentication Protocol MD5	Username admin		
Password Set		Max Hops 0		Preserve config Enabled			
← Back							
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 Add S	witche

The status will change to Switch Added. Click Close to close out of this window.

#### Figure 17:

Add S	Switches								? ×
Switch	Addition Mechanism* cover O Move Neighbor Sv	witches							
Seed Switch Details Fabric ext-fab-1			vitch '2.16.0.234		Authenticati MD5	on Protocol	Username admin		
Password Set		M	Max Hops P 0		Preserve co Enabled	Preserve config Enabled			
← Bac	k overy Results								
Filt	er 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		
								Close	Add Switches

**Step 6** Set the role for the Cisco Catalyst 8000V to Core Router.

a) Click the box next to the Cisco Catalyst 8000V to choose that router, then click Actions > Set Role.

## Figure 18:

bric	c Overview - e	ext-fab-1								Actions ~	ð? ·
view	/ Switches Links Ir	nterfaces Policies	Event Analytic	cs History Resou	rces Virtual Infrast	tructure					
Filter I	by attributes										Action
	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
											VPC Pairing
											TOR Pairing
											vPC Overview
											More

b) Locate and select the Core Router role in the Select Role list, then click Select.

All the Catalyst 8000Vs should be set to the Core Router role so that NDFC automatically enables BGP protocol.

#### Figure 19:

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

**Step 7** Navigate to LAN > Fabrics and select the external fabric that you created.

The Overview page for this external fabric appears.

Step 8Click the Switches tab to verify that the Cisco Catalyst 8000V that you just added appears correctly.Figure 20:

Fabric Overview - ext-fab-1									⊘Ŏ? – ×		
Overvie	Zverview Switches Links Interfaces Policies Event Analytics History Resources Virtual Infrastructure										
Filte	Filter 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	C8000V			Normal
											_

**Step 9** Click **Actions** > **Recalculate and Deploy**.

At this point in the process, the VXLAN and external fabrics are configured in NDFC, as shown when you navigate to **LAN** > **Fabrics**.

Figure 21:

$\equiv$ <b>cisco</b> Nexus Dashboar	d 🕴 🕀 One V	Лew ∨				Feedback 👤				
🗐 Fabric Controller										
n Dashboard		brice				G				
⊯ Topology	LANTC	101103				e				
≣ LAN ^	Filter by a	ttributes				(Actions ~ )				
Fabrics		Eshris Nama	Fabrie Technology	Fabrie Tume	ACN	Eshris Uselih				
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 🗸 🗸										

You can also use the Topology view to determine the following configurations at this point in the process:

• That there is no connectivity yet between the VXLAN and external fabrics:

Figure 22:



This NDFC has the VMM Visualizer feature enabled, so the vCenter icon with an IP address of 172.16.0.252 is displayed in the topology view. For more information on the VMM feature, see the Virtual Infrastructure Manager chapter in the *Cisco NDFC-Fabric Controller Configuration Guide*.

• That there are no networks or VRFs created yet in the VXLAN fabric:

#### Figure 23:

E cisco Nexus Dashboard	🔅 One View 🗸			
F Fabric Controller				
n Dashboard	Data Center / Sydney			
🗙 Topology	View A Se	earch by Attributes		
∎ LAN ^	(+ - / 0 🗎 X)			
Fabrics	Show Logical Links			
Switches	Operation Configuration		NET VRF	
Interfaces			Networks (0) VREs (0) VM (3)	
Services	Hierarchical			
📥 Virtual Management 🗸 🗸	In-Sync			
🔅 Settings 🗸 🗸	Pending			
<u>∎</u> ° Operations ∨	In Progress			
	NA			
	Multi-select 💿			
	Uselected		(B)	
			ndfc/spine1	
			ndfc-leaf2 ndfc-leaf1	

# What to do next

Deploy the Cloud Network Controller on the cloud sites using the procedures provided in Deploy Cloud Network Controller on Cloud Sites, on page 19.

# **Deploy Cloud Network Controller on Cloud Sites**

In this section, you will be configuring the part of the example topology highlighted below.



Based on the example hybrid cloud topology, these procedures assume that we will be setting up two cloud sites through the Cloud Network Controller (AWS and Azure cloud sites). We will therefore refer to the following documents throughout these procedures:

- Cisco Cloud Network Controller for AWS Installation Guide, Release 25.1(x) or later
- Cisco Cloud Network Controller for AWS User Guide, Release 25.1(x) or later
- Cisco Cloud Network Controller for Azure Installation Guide, Release 25.1(x) or later
- Cisco Cloud Network Controller for Azure User Guide, Release 25.1(x) or later

Complete the procedures in the following sections to deploy the Cloud Network Controller on the cloud sites.

# Deploy the Cloud Network Controller on the AWS Cloud Site

Follow the procedures in these sections to deploy the Cloud Network Controller on the AWS cloud site.

# Configure the Necessary Parameters in Advanced Settings for AWS

In this section, you will make the necessary configurations for the AWS cloud site in **Advanced Settings** area in the **Cloud Network Controller Setup** page specifically for this example hybrid cloud topology.

Use the procedures provided in the "Configuring Cisco Cloud Network Controller Using the Setup Wizard" chapter in the Cisco Cloud Network Controller for AWS Installation Guide, but note that there are two areas in the **Cloud Network Controller Setup** page that you will have to configure specifically for this example hybrid cloud topology:

- Contract-based routing: Cloud Network Controller supports two types of modes:
  - Contract-based routing
  - · Route map-based routing

Contract-based routing means that a contract between the EPGs will drive the routing between VRFs, but this type of contract-based routing is not available through NDFC, so for this specific example hybrid cloud topology, you will turn off contract-based routing and will use route map-based routing instead. For more information, see the "Routing Policies" and "Configuring the Global Inter-VRF Route Leak Policy" sections in the Cisco Cloud Network Controller for AWS User Guide, Release 25.1(x) or later.

- Cloud Network Controller Access Privilege: By default, the Cloud Network Controller has Routing & Security access privilege, which means that the Cloud Network Controller can automate not only networking, it can also automate and configure security groups on the cloud. If the Cloud Network Controller automates and configures the security groups, it also has to configure the EPGs and contracts; however, EPGs and contracts are not applicable to NDFC end users who only need routing automation. To integrate well with NDO and NDFC, you should set the Cloud Network Controller Access Privilege option to Routing Only.
- **Step 1** Log into your Cisco Cloud Network Controller for AWS.
- **Step 2** Begin the process of setting up the first cloud site, the AWS cloud site, for this example hybrid cloud topology.

The first few chapters in the Cisco Cloud Network Controller for AWS Installation Guide, Release 25.1(x) or later, contain generic information that is not specific to this hybrid cloud topology use case, so complete the procedures in these chapters in that document, then return here:

- Overview
- · Preparing for Installing the Cisco Cloud Network Controller
- Configuring the Cloud Formation Template Information for the Cisco Cloud Network Controller
- Step 3 In the Cisco Cloud Network Controller GUI, click the Intent icon (<sup>2</sup>) and select Cloud Network Controller Setup.
   The Let's Configure the Basics page appears.
- **Step 4** Locate the **Advanced Settings** area and click **Edit Configuration**.
- **Step 5** In the Advanced Settings page, set the following configurations:

• **Contract Based Routing**: Verify that the box is unchecked (that this feature is not enabled). This turns off contract-based routing and uses route map-based routing instead

· Cloud Network Controller Access Privilege: Choose the Routing Only option.

# Step 6 Click Save and Continue.

You are returned to the Let's Configure the Basics page.

## What to do next

Follow the procedures provided in Configure the Necessary Parameters in Region Management for AWS, on page 22.

# Configure the Necessary Parameters in Region Management for AWS

In this section, you will make the necessary configurations for the AWS cloud site in the **Region Management** area in the **Cloud Network Controller Setup** page specifically for this example hybrid cloud topology.

#### Before you begin

Complete the procedures provided in Configure the Necessary Parameters in Advanced Settings for AWS, on page 20.

#### **Step 1** Locate the **Region Management** area and click the appropriate button.

Click **Begin** if this is your first time setting up the Cloud Network Controller, or **Edit Configuration** if you had already configured region management in this Cloud Network Controller previously.

**Step 2** Enable AWS Transit Gateway.

You normally use Transit Gateway to avoid using VPN tunnels for connectivity within a region and across the regions where TGW peering is supported. For more information, see the *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway or AWS Transit Gateway Connect* document.

Specifically for this example hybrid cloud topology use case, in the **Use Transit Gateway** area, click the checkbox next to **Enable** to use AWS Transit Gateway. This will allow you to add a hub network later in these procedures, which is necessary to enable TGW Connect.

**Step 3** In the **Regions to Manage** area, verify that the Cisco Cloud Network Controller home region is selected.

The region that you selected when you first deployed the Cisco Cloud Network Controller in AWS is the home region and should be selected already in this page. This is the region where the Cisco Cloud Network Controller is deployed (the region that will be managed by Cisco Cloud Network Controller), and will be indicated with the text Cloud Network Controller deployed in the Region column.

**Step 4** Select additional regions if you want the Cisco Cloud Network Controller to manage additional regions, and to possibly deploy Cisco Catalyst 8000Vs to have inter-VPC communication and Hybrid-Cloud, Hybrid Multi-Cloud, or Multi-Cloud connectivity on those other regions.

The Cisco Catalyst 8000V can provide hybrid cloud and multi-cloud connectivity for up to four regions, including the home region where Cisco Cloud Network Controller is deployed.

**Step 5** To deploy cloud routers locally to a region, click to place a check mark in the **Catalyst 8000Vs** check box for that region.

You must have at least one region with Catalyst 8000Vs deployed. However, if you choose multiple regions in this page, you do not have to have Catalyst 8000Vs in every region that you choose.

**Step 6** If you want to use AWS Transit Gateway statistics, check the box in the **TGW Stats** column for one or more regions.

Checking the check box enables collection of AWS Transit Gateway traffic statistics for infra tenants for the specified regions.

**Note** You also need to create flow logs in order to collect AWS Transit Gateway statistics. See the section "Enabling VPC Flow Logs" in the chapter "Cisco Cloud APIC Statistics" of the *Cisco Cloud APIC for AWS User Guide*, release 25.1(x) or later.

Specifically for this example hybrid cloud topology use case:

- Place a check mark in the check boxes next to the US East (N. Virginia) and US West (N. California) regions (the us-east-1 and us-west-1 regions).
- Place a check mark in the check boxes in the **Catalyst 8000Vs** and **TGW Stats** columns for the Cisco Cloud Network Controller home region.

#### Figure 25:

ht				
Regions to Manage	2 General Co	) nnectivity		
Eerun Claat Tetera Costrate Oro-Prestase ACI Sta	Lase-Sile Consectivity -	Transf General Transf General B Catalyst BOODY	Inter-Region Connectivity	Regions
ect the regions to be managed by Cloud Ne ween VPCs in all managed regions.	twork Controller and which regions shore to Catalyst 8000V.	uld host Cloud Routers. Cloud Routers need to	be deployed in at least one region to enal	ble connectivity
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 Pacific (Mumbai)	ap-south-1			
Asia Pacific (Singapore)	ap-southeast-1			
Asia Pacific (Sydney)	ap-southeast-2			
Asia Pacific (Sydney)	ap-southeast-2 ap-southeast-3			
Asia Pacific (Sydney) Asia Pacific (Jakarta) Canada (Central)	ap-southeast-2 ap-southeast-3 ca-central-1			
Asia Pacific (Sydney) Asia Pacific (Jakarta) Canada (Central) EU (Frankfurt)	ap-southeast-3 ap-southeast-3 ca-central-1 eu-central-1			
Asia Pacific (Sydney) Asia Pacific (Jakarta) Canada (Central) EU (Frankfurt) EU (Stockholm)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-north-1			
Asia Pacific (Sydney) Asia Pacific (Jakarta) Canada (Central) EU (Frankfurt) EU (Stockholm) Europe (Mian)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-north-1 eu-south-1			
Asia Pacific (Systemy) Asia Pacific (Jakarta) Cansola (Central) EU (Frankfurt) EU (Stockholm) EU (Stockholm) EUrope (Man) EU (reland)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-north-1 eu-south-1 eu-south-1			
Asia Pacific (Systemy) Asia Pacific (Jakarta) Cansala (Central) EU (Frankfurt) EU (Stockholm) EU (Stockholm) EU (Stockholm) EU (veland) EU (veland) EU (veland)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-north-1 eu-south-1 eu-west-1 eu-west-2			
Asia Pacific (Systemy) Asia Pacific (Jakarta) Cansala (Central) EU (Frankfurt) EU (Stockholm) EU (Stockholm) EU (Stockholm) EU (veland) EU (veland) EU (veland) EU (veland) EU (veland)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-north-1 eu-south-1 eu-south-1 eu-west-1 eu-west-2 eu-west-3			
Asia Pacific (Systemy) Asia Pacific (Jakarta) Cansala (Central) EU (Frankfurt) EU (Stockholm) EU (Stockholm) EU (Stockholm) EU (veland) EU (veland) EU (veland) EU (veland) EU (veland) Middle East (Bahrain)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-south-1 eu-south-1 eu-west-1 eu-west-2 eu-west-3 me-south-1			
Asia Pacific (Systemy) Asia Pacific (Jakarta) Cansala (Central) EU (Frankfurt) EU (Stockholm) EU (Stockholm) EU (Stockholm) EU (Veland) EU (Veland) EU (Veland) EU (Lendon) EU (Paria) South America (Sao Paulo)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-south-1 eu-south-1 eu-west-1 eu-west-2 eu-west-3 me-south-1 sa-east-1			
Asia Pacific (Systemy) Asia Pacific (Jakarta) Cansala (Central) EU (Frankfurt) EU (Stockholm) EU (Stockholm) EU (Stockholm) EU (Lendon) EU (Lendon) EU (Lendon) EU (Lendon) US East (N. Vrognia)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-north-1 eu-south-1 eu-west-1 eu-west-2 eu-west-3 me-south-1 sa-east-1 us-east-1			
Asia Pacific (Systemy) Asia Pacific (Jakarta) Cansala (Central) EU (Frankfurt) EU (Stockholm) EU (Stockholm) EU (Stockholm) EU (Lendon) EU (Lendon) EU (Lendon) EU (Para) Middle East (Bahrain) US East (Na Vraginia) US East (Na Vraginia) US East (Na Vraginia)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-north-1 eu-south-1 eu-west-1 eu-west-2 eu-west-3 me-south-1 sa-east-1 us-east-2			
Asia Pacific (Systemy) Asia Pacific (Jakarta) Cansada (Central) EU (Frankfurt) EU (Stockholm) EU (Stockholm) EU (Stockholm) EU (Lendon) EU (Lendon) EU (Lendon) EU (Lendon) US East (Nu Vrogina)	ap-southeast-2 ap-southeast-3 ca-central-1 eu-central-1 eu-south-1 eu-south-1 eu-west-1 eu-west-3 mei-south-1 sa-east-1 us-east-1 us-east-2 us-west-1			

**Step 7** When you have selected all the appropriate regions, click **Next** at the bottom of the page.

The General Connectivity page appears.

**Step 8** Make the necessary configurations in the **General Connectivity** page.

See the "Configuring Cisco Cloud Network Controller Using the Setup Wizard" chapter in the *Cisco Cloud Network Controller for AWS Installation Guide*, Release 25.1(x) or later, for more information.

Specifically for this example hybrid cloud topology use case, add a hub network using the procedures in the following steps.

In Cisco Cloud Network Controller, a collection of two or more AWS Transit Gateways is called a **hub network**. A hub network provides network isolation for VRFs. A group of VRFs can be attached to a hub network to isolate the group of VRFs from other VRFs that are attached to other hub networks. A hub network creates at least two AWS Transit Gateways for each region.

## Step 9 In the Hub Network area, click Add Hub Network.

The Add Hub Network window appears.

- **Step 10** In the **Name** field, enter a name for the hub network.
- **Step 11** In the **BGP Autonomous System Number** field, enter a zero for AWS to choose a number, or enter a value between 64512 and 65534, inclusive, for each hub network, and then click the check mark next to the field.

For example, using the information in the example hybrid cloud topology, you would enter 65091 in this field.

**Step 12** In the **TGW Connect** field, click the checkbox next to **Enable** to enable the AWS Transit Gateway Connect feature.

You will enable the AWS Transit Gateway Connect feature for this example hybrid cloud topology use case. See *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway or AWS Transit Gateway Connect* for more information.

# **Step 13** In the **CIDRs** area, click **Add CIDR**.

This will be the AWS Transit Gateway Connect CIDR block, which will be used as the connect peer IP address (the GRE outer peer IP address) on the Transit Gateway side.

- a) In the Region field, click Select Region and select the appropriate region.
- b) In the **CIDR** field, enter the CIDR block that will be used as the connect peer IP address on the Transit Gateway side.

Figure 26:

CIDR		
Region *	CIDR *	
Select Region >		✓ ×

- c) Click the checkmark to accept these values for this CIDR block.
- d) For every managed region that will be using the AWS Transit Gateway Connect feature, repeat these steps to add CIDR blocks to be used for each of those managed regions.

#### Figure 27:

Add Hub Network		×
Name *		
hub1		
BGP Autonomous System Number *		
65091		
TGW Connect		
Enable		
Changing the use of TGW Connect will	cause temporary 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
		, au

## **Step 14** Complete the remaining configurations as you normally would.

- Complete the remaining configurations in the **General Connectivity** page as you normally would, then click **Save** and **Continue**.
- Complete the necessary configurations in the Smart Licensing page as you normally would.

See the "Configuring Cisco Cloud Network Controller Using the Setup Wizard" chapter in the Cisco Cloud Network Controller for AWS Installation Guide, Release 25.1(x) or later, for more information.

At this point in the process, you have completed the basic configurations for the first cloud site for the Cisco Cloud Network Controller (in this example hybrid cloud topology, the AWS cloud site). Proceed with the following steps to complete the basic configurations for the second cloud site for the Cisco Cloud Network Controller (in this example hybrid cloud site).

**Step 15** Configure Direct Connect for AWS, if necessary.

Configure Direct Connect if you want private connections for the connectivity for the Catalyst 8000V routers to the cloud networks. For information on configuring Direct Connect for AWS, see the Cisco Cloud Network Controller for AWS User Guide, release 25.1(x) or later.

#### What to do next

Deploy the Cloud Network Controller on the second cloud site (the Azure cloud site) using the procedures provided in Deploy the Cloud Network Controller on the Azure Cloud Site, on page 26.

# Deploy the Cloud Network Controller on the Azure Cloud Site

Follow the procedures in these sections to deploy the Cloud Network Controller on the Azure cloud site.

# **Configure the Necessary Parameters in Advanced Settings for Azure**

In this section, you will make the necessary configurations for the Azure cloud site in **Advanced Settings** area in the **Cloud Network Controller Setup** page specifically for this example hybrid cloud topology.

Make the same configurations for the Azure cloud site as you did for the AWS cloud site.

Use the procedures provided in the "Configuring Cisco Cloud Network Controller Using the Setup Wizard" chapter in the Cisco Cloud Network Controller for Azure Installation Guide, but note that there are two areas in the **Cloud Network Controller Setup** page that you will have to configure specifically for this example hybrid cloud topology:

- Contract-based routing: Cloud Network Controller supports two types of modes:
  - Contract-based routing
  - Route map-based routing

Contract-based routing means that a contract between the EPGs will drive the routing between VRFs, but this type of contract-based routing is not available through NDFC, so for this specific example hybrid cloud topology, you will turn off contract-based routing and will use route map-based routing instead. For more information, see the "Routing Policies" and "Configuring the Global Inter-VRF Route Leak Policy" sections in the Cisco Cloud Network Controller for AWS User Guide, Release 25.1(x) or later.

• Cloud Network Controller Access Privilege: By default, the Cloud Network Controller has Routing & Security access privilege, which means that the Cloud Network Controller can automate not only networking, it can also automate and configure security groups on the cloud. If the Cloud Network Controller automates and configures the security groups, it also has to configure the EPGs and contracts; however, EPGs and contracts are not applicable to NDFC end users who only need routing automation. To integrate well with NDO and NDFC, you should set the Cloud Network Controller Access Privilege option to Routing Only.

#### Before you begin

Deploy the Cloud Network Controller on the first cloud site (the AWS cloud site) using the procedures provided in Deploy the Cloud Network Controller on the AWS Cloud Site, on page 20.

- **Step 1** Log into your Cisco Cloud Network Controller for Azure.
- **Step 2** Begin the process of setting up the second cloud site, the Azure cloud site, for this example hybrid cloud topology.

The first few chapters in the Cisco Cloud Network Controller for Azure Installation Guide, Release 25.1(x) or later, contain generic information that is not specific to this hybrid cloud topology use case, so complete the procedures in these chapters in that document, then return here:

• Overview

- · Preparing for Installing the Cisco Cloud Network Controller
- Deploying the Cisco Cloud Network Controller in Azure
- Step 3 In the Cisco Cloud Network Controller GUI, click the Intent icon (<sup>2</sup>) and select Cloud Network Controller Setup.
   The Let's Configure the Basics page appears.
- **Step 4** Locate the **Advanced Settings** area and click **Edit Configuration**.
- **Step 5** In the Advanced Settings page, set the following configurations:
  - Contract Based Routing: Verify that the box is unchecked (that this feature is not enabled). This turns off contract-based routing and uses route map-based routing instead
  - · Cloud Network Controller Access Privilege: Choose the Routing Only option.

## Step 6 Click Save and Continue.

You are returned to the Let's Configure the Basics page.

## What to do next

Follow the procedures provided in Configure the Necessary Parameters in Region Management for Azure, on page 27.

# **Configure the Necessary Parameters in Region Management for Azure**

In this section, you will make the necessary configurations for the Azure cloud site in the **Region Management** area in the **Cloud Network Controller Setup** page specifically for this example hybrid cloud topology.

## Before you begin

Follow the procedures provided in Configure the Necessary Parameters in Advanced Settings for Azure, on page 26.

**Step 1** Locate the **Region Management** area and click the appropriate button.

Click **Begin** if this is your first time setting up the Cloud Network Controller, or **Edit Configuration** if you had already configured region management in this Cloud Network Controller previously.

**Step 2** Verify that the **Virtual Network Peering** in the **Connectivity for Internal Network** area is automatically enabled.

VNet peering at the global level is set in the **Connectivity for Internal Network** area, which enables VNet peering at the Cisco Cloud Network Controller level, deploying NLBs in all the regions with a CCR. For release 5.1(2) and later, VNet peering at the global level is enabled by default and cannot be disabled. See *Configuring VNet Peering for Cloud APIC for Azure* for more information.

**Step 3** In the **Regions to Manage** area, verify that the Cisco Cloud Network Controller home region is selected.

The region that you selected when you first deployed the Cisco Cloud Network Controller in AWS is the home region and should be selected already in this page. This is the region where the Cisco Cloud Network Controller is deployed (the region that will be managed by Cisco Cloud Network Controller), and will be indicated with the text Cloud Network Controller deployed in the Region column.

- **Note** Because Azure VNet peering is enabled automatically, you must also check the box in the **Catalyst 8000Vs** column for the Cisco Cloud Network Controller home region, if it is not checked already.
- **Step 4** Select additional regions if you want the Cisco Cloud Network Controller to manage additional regions, and to possibly deploy Cisco Catalyst 8000Vs to have inter-VNet communication and Hybrid-Cloud, Hybrid Multi-Cloud, or Multi-Cloud connectivity on those other regions.

The Cisco Catalyst 8000V can provide hybrid cloud and multi-cloud connectivity for up to four regions, including the home region where Cisco Cloud Network Controller is deployed.

**Step 5** To deploy cloud routers locally to a region, click to place a check mark in the **Catalyst 8000Vs** check box for that region.

You must have at least one region with Catalyst 8000Vs deployed. However, if you choose multiple regions in this page, you do not have to have Catalyst 8000Vs in every region that you choose.

Specifically for this example hybrid cloud topology use case, place a check mark in the check box in the **Catalyst 8000Vs** column for the Cisco Cloud Network Controller home region.

Figure 28:

Setup - Region M	lanagement		
	Please note that CSR is now changed to Catalyst 8000	ν.	
	Connectivity for Internal Network  VNet Peering		
	Regions to Manage *	Region	Catalyst 8000Vs @
	Australia Central	australiacentral	
	Australia Central 2	australiacentral2	
	Australia East	australiaeast	
	Australia Southeast	australiasoutheast	
	Brazil South	brazilsouth	
	Canada Central	canadacentral	
	Canada East	canadaeast	
	Central IIS	centralindia	
	East Asia	eastasia	
	East US	Bastus Cloud Network Controller Deployed	

Step 6When you have selected all the appropriate regions, click Next at the bottom of the page.The General Connectivity page appears.

**Step 7** Make the necessary configurations in the **General Connectivity** page.

See the "Configuring Cisco Cloud Network Controller Using the Setup Wizard" chapter in the *Cisco Cloud Network Controller for Azure Installation Guide*, Release 25.1(x) or later, for more information.

Specifically for this example hybrid cloud topology use case, make the following configurations for the Cisco Catalyst 8000Vs using the procedures in the following steps.

**Step 8** Under the **General** area, in the **Subnet Pools for Cloud Routers** field, click **Add Subnet Pool for Cloud Routers** to add additional subnets for the Catalyst 8000Vs.

The first subnet pool is automatically populated (shown as System Internal). Addresses from this subnet pool will be used for inter-region connectivity for any additional regions that are added that need to be managed by the Cisco Cloud Network Controller. Subnet pools added in this field must be a valid IPv4 subnet with mask /24.

Add additional subnets for Catalyst 8000Vs in this step in these situations:

- If you have a Catalyst 8000V deployed in the Cisco Cloud Network Controller home region, add one additional subnet pool in addition to the System Internal subnet pool that is automatically generated.
- If you selected additional regions to be managed by Cisco Cloud Network Controller in the previous page:
  - Add *one* additional subnet pool for every managed region with 2-4 Catalyst 8000Vs per managed region (if you enter **2**, **3**, or **4** in the **Number of Routers Per Region** field in this page)
  - Add *two* additional subnet pools for every managed region with five or more Catalyst 8000Vs per managed region (if you enter between **5** and **8** in the **Number of Routers Per Region** field in this page)

Specifically for this example hybrid cloud topology use case, add one additional subnet pool using 10.90.1.0/24 as the subnet entry.

#### Figure 29:

Setup - Region Management				
External Cloud Network Controller	ernal Router	Inter-Site Connectivity -		R Catalyst 8000V
Configure the fabric infra cor the configuration template us i Please note that CS	nnectivity for the Cloud Si sed for the Cloud Routers R is now changed to Cata	te. The Fabric Autonomous Sy in the Cloud Site. alyst 8000V.	stem Number is used	l for BGP peering insid
General				
Subnet Pools for Cloud	Routers 🗊			
Subnet *	Regions	Created By		
10.90.0.0/24		System Internal	8	
10.90.1.0/24		User	8	
+ Add Subnet Pool fo	or Cloud Routers			

**Step 9** Under the **Catalyst 8000Vs** area, in the **BGP Autonomous System Number for C8kVs** field, enter the BGP autonomous system number (ASN) that is unique to this site.

The BGP autonomous system number can be in the range of 1 - 65534. See the "Configuring Cisco Cloud Network Controller Using the Setup Wizard" chapter in the *Cisco Cloud Network Controller for Azure Installation Guide*, Release 25.1(x) or later, for additional restrictions.

Specifically for this example hybrid cloud topology use case, you would enter 65092 in the **BGP Autonomous System Number for C8kVs** field.

#### Figure 30:

Setup - Region Management	
Catalyst 8000Vs	
BGP Autonomous System Number for C8kVs *  65092 Assign Public IP to C8kV Interface  Cashie	
Changing C8kV connectivity from private to public (or vice versa) may cause disruption in your network.	
Number of Routers Per Region 2 V	
Username * cisco	
Paesword	
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  Tier1 (up to 100M throughput)	
TCP MSS *  1300	
License Token  Back to Overview Previous	Next Save :

**Step 10** Click **Next**, then complete the remaining configurations as you normally would.

- Complete the remaining configurations in the **General Connectivity** page as you normally would, then click **Save** and **Continue**.
- Complete the necessary configurations in the Smart Licensing page as you normally would.

See the "Configuring Cisco Cloud Network Controller Using the Setup Wizard" chapter in the *Cisco Cloud Network Controller for Azure Installation Guide*, Release 25.1(x) or later, for more information.

# **Step 11** Configure ExpressRoute for Azure, if necessary.

Configure ExpressRoute if you want private connections for the connectivity for the Catalyst 8000V routers to the cloud networks. For information on configuring ExpressRoute for Azure, see the *Cisco Cloud Network Controller for Azure User Guide*, release 25.1(x) or later.

# What to do next

Onboard the NDFC-managed sites (VXLAN fabric, external fabric, and cloud sites) into Nexus Dashboard (ND) and Nexus Dashboard Orchestrator (NDO) using the procedures provided in Onboard the NDFC and Cloud Sites into ND and NDO, on page 32.

# **Onboard the NDFC and Cloud Sites into ND and NDO**

# Before you begin

- Create the NDFC VXLAN fabric using the procedures provided in Create an NDFC VXLAN Fabric, on page 3.
- Create the NDFC external fabric using the procedures provided in Create an NDFC External Fabric, on page 12.
- Deploy the Network Cloud Controller on the first cloud site using the procedures provided in Deploy the Cloud Network Controller on the AWS Cloud Site, on page 20.
- Deploy the Network Cloud Controller on the second cloud site using the procedures provided in Deploy the Cloud Network Controller on the Azure Cloud Site, on page 26.
- **Step 1** Log into the Nexus Dashboard (ND) cluster with Nexus Dashboard Orchestrator (NDO).
- Step 2 In Nexus Dashboard, click Sites > Add Site.

# Figure 31:

Ξ	E cisco Nexu	is Dashbo	ard and Admin Console						Feedback 👤 🕐
Ξ	Admin Cons	ole	G fab2nd2						
6	Overview Sites		Sites						٥
=	Services		Filter by attributes						Add Site
0	System Resources		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
0	Infrastructure								
T <sub>o</sub>	Administrative								
						No rows found			
			10 v Rows					Page 1 of 1 4	≪<0 to 0-0>≫

The Add Site page appears.

- Step 3 Click the NDFC box in the Add Site page.
- **Step 4** Enter the necessary information to add the NDFC site.
  - In the Hostname/IP Address field, enter the data interface IP address for your NDFC.
  - In the Username and Password field, enter the username and password login information for your NDFC.
- Step 5 Click Select Sites.

#### Figure 32:

≡ disco Nexus Dash	nboard 🤅	) One View $\vee$				Feedback
Admin Console	6 fab2nc	d2				0 🛛 🕻
© Sites	a sines					
III Services		Site Type			10 <u>4</u>	
System Resources			0			۲
Operations		ACI		Cloud Network Controller	NDFC	
O Infrastructure						
<u>4</u> Administrative		Preschality is required between Nexus Dask network. Use the DCNMNDFC Iseans if address Hostname(IP Address * 172 161 191 Username * O done adone Desavord * O unume * O done Desavord * O unume * O done done Company O Ense Bes Name Greets Block Stres The Name Greets Block Stres Manume * O Add Security Donales Name Add Security Donales	eard data network and DCMMND/FC site is for onboarding DCMM/ND/FC site	C Intend 5.	ля.	

Step 6 Click the boxes next to the two NDFC sites that you added previously (the VXLAN fabric and external fabric sites), then click Select.

# Figure 33:

Ouerstand     Ouerstand	NDFC O	
And     Shore     Shore     Could Network Controller     Prestaurunte     Prestaurunte	NDFC O	
	NDFC O	
	NDFC O	
Active Controller      Active Controller	NDFC .	
Select X		
Adventuative     Practicative is reacted between     recurs. Use the DEDMONDET laws     ended-     recurs. Use the DEDMONDET laws     ended-     recurs. Use the DEDMONDET laws     ended-     recurs. Use the DEDMONDET laws     recurs. Use the DEDMONDET laws		
Stel		
Site Name		
© Sever Sites		
Add Sectory Domains		

You are returned to the Add Site page.

- Step 7Verify that the two NDFC sites (VXLAN fabric and external fabric sites) appear correctly in the Nexus Dashboard<br/>Add Site page, then click Save.
- **Step 8** In Nexus Dashboard, click **Sites > Add Site** again to add the first cloud site.

#### Figure 34:

≡ cisco Nexus	Dashboa	rd 🛛 🗐 admin Console 🗸					Feedback	10
Admin Consol	le	C fab2nd2					0 0	) 🖸
Overview     Sites		Sites						0
III Services		Filter by attributes					•	idd Site
System Resources		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
C Infrastructure		A Minor	Sydney	NDFC	(Ø Up )	12.1.2.275	0	
$\underline{x}^{\circ}$ Administrative		Ø Heatthy	ext-fab-1	NDFC	( QU Up	12.1.2.275	0	
		10 ~ Rows					Page 1 of 1 << 1-2 of 2	2>>>

The Add Site page appears.

- **Step 9** Click the **Cloud Network Controller** box in the **Add Site** page, then enter the necessary information to add the first cloud site (the AWS site in this example topology).
  - In the Hostname/IP Address field, enter the IP address of the Cloud Network Controller (CNC) for the first cloud site.
  - In the **Username** and **Password** field, enter the username and password login information of the Cloud Network Controller (CNC) for the first cloud site.
  - For Cloud Network Controller (CNC), Enable Proxy if the CNC is reachable via a proxy. Proxy must be already configured in your Nexus Dashboard's cluster settings. If the proxy is reachable via management network, a static management network route must also be added for the proxy IP address. For more information about proxy and route configuration, see *Nexus Dashboard User Guide* for your release.

#### Figure 35:

≡ cisco Nexus Dashb	oard 🛛 🕀 One View 🗠	والتعديد والتقافي المتواط والمتعادي والمتعاد	Feedb
	C fab2nd2		0
<ul><li>Overview</li><li>Sites</li></ul>	Sites		
III Services	Site Type		
<ul> <li>System Resources</li> <li>Operations</li> </ul>	aci	Cloud Network Controller	
$\odot$ Infrastructure $\lor$			
$\underline{x}^{\rm o}$ . Administrative $\qquad \qquad \qquad$	General		
	Name*		
	Settings		
	Hostname//P Address *		
	Username+ ① admin Password+ ①		
	Login Domain ⊙		
	Enable Proxy Security Domains		
	Namo		
	Add Security Domains		
			Cancel

- **Step 10** Click **Save** to add the first cloud site.
- **Step 11** In Nexus Dashboard, click **Sites** > **Add Site** again to add the second cloud site.

#### Figure 36:

≡ cisco Nexus	Dashboar	d 🛛 🌡 o Admin Console 🗸					r.	nedback 1 G
	le (	G fab2nd2					(	
© Overview		Sites						Ó
III Services		Filter by attributes						Add Site
<ul> <li>System Resources</li> <li>Descriptions</li> </ul>		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
C Infrastructure		(A Major	AWS	Cloud Network avs	(Øup)	25.1(te)	0	
1° Administrative		A Minor	Sydney	NDFC	(O Up)	12.1.2.275	0	
		() Healthy	ext-fab-1	NDFC	(O Up	12.1.2.275	0	
		10 v Rows					Page 1 of 1 《 <	1-3 of 3 > >>

The Add Site page appears.

**Step 12** Click the **Cloud Network Controller** box in the **Add Site** page, then enter the necessary information to add the Cloud Network Controller (CNC) for the second cloud site (the Azure site in this example topology).

Repeat the previous set of steps, this time entering the necessary information in the **Hostname/IP Address**, **Username**, and **Password** fields for the Cloud Network Controller (CNC) for the second cloud site, and clicking **Enable Proxy** if the CNC for the second cloud site is reachable via a proxy.

Figure 37:

≡ cisco Nexus Dash	board 🕴 🕀	One View 🐱			التواجي الم			Feed
	G fab2nd2	2						0
Co Overview	d Sitos							
© Sites								
III Services		Site Type		-				
System Resources			0			•		
El Operations		ACI		Cloud Networ	k Controller		NDFC	
O Infrastructure			1					
<u>1</u> ° Administrative		General						
		Name =						
		Azure						
		Settings						
		Hostname/IP Address •						
		Username * 🛈						
		admin						
		Password • ①						
		•						
		Login Domain 🕢						
		Enable Proxy						
		Security Domains						
		Name						
		Add Security Domains						
								Cancel Save

- **Step 13** In Nexus Dashboard, click **Sites** and verify that the four sites appear correctly:
  - The two sites from NDFC (the VXLAN fabric and external fabric sites)
  - The cloud sites with Cloud Network Controller deployed (for this example hybrid cloud topology, the AWS and Azure cloud sites)

#### Figure 38:

≡ diniji. Cisco Nexu	s Dashboar	d 🕼 🔒 Admin Console	×					Feedback 💄 📀
	ole	G fab2nd2						Ø 🖪 🖸
Overview           Sites		Sites						0
III Services		Filter by attributes						Add Site
<ul> <li>System Resources</li> <li>Operations</li> </ul>		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
C Infrastructure		A Major	Azure	Cloud Network Controller	(⊘ Up	<b>T</b> 25.1(1e)	o	
<u>⊥</u> <sup>0</sup> Administrative		🛆 Major	AWS	Cloud Network aws Controller	Ø Up	25.1(1e)	a	
		A Minor	Sydney	NDFC	Ø Up	12.1.2.275	0	
		Healthy	ext-fab-1	NDFC	ØUp	12.1.2.275	0	
		10 V Rows					Page 1 of 1 <	≪<1-4 of 4>≫

**Step 14** Access the Nexus Dashboard Orchestrator (NDO).

In Nexus Dashboard, at the top of the window, click **One View > Orchestrator**.

## Figure 39:

Ξ	cisco Nexus Dashboard	🔆 One View 🔿	Feedback 💄 🕐
	One view	One View	
6	My Sites	Admin Console	Map Table
0		Version To reaction of the survice in one of the reaction of the survice in one of the reaction of	+

# Step 15 In NDO, click Sites.

The four sites that you added in ND appear but are shown in the Unmanaged state.

#### Figure 40:

≡ disco Nexus Dashb	ioard 🔶 🌲 Orchestrator 🗸			일 기가 가 주요		Feedback 💄 🔊
<ul> <li>Dashboard</li> <li>Sites</li> </ul>	Sites					0 ()
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
<ul> <li>Infrastructure</li> </ul>	⊘ок	AWS	e aws	Unmanaged ~	25.1(1e)	22772
@ Integration	⊘ок	Azure	Azure	Unmanaged	25.1(1e)	2000
	⊘ок	ext-fab-1	NDFC	Unmanaged ~	12.1.2.275	
	⊘ок	Sydney	NDFC	Unmanaged 🗸	12.1.2.275	2000
	10 V Rows				Page 1	of 1 $\ll$ (1-4 of 4 ) $\gg$

**Step 16** From NDO, manage the four sites.

Perform the following steps for each site in NDO:

a) For the first site listed in NDO, under the **State** column, change the state from **Unmanaged** to **Managed**. *Figure 41*:

95						12
						-C
plication Management	Filter by attributes					
aric Management	Controller Connectivity	Name	Туре	State	Version	
rastructure	⊘ок	AWS	😑 AWS	Unmanaged ~	25.1(1e)	
egration	ØОК	Azure	Azure	Managed ~	25.1(1e)	
	© ОК	ext-fab-1	NDFC	Unmanaged V Ommanageu V	12.1.2.275	
	⊘ок	Sydney	NDFC	Unmanaged ~	12.1.2.275	

b) Provide a site ID that is unique to this particular site (a site ID that does not conflict with site IDs for any other site being managed through this NDO), then click Add.

#### Figure 42:

≡ <sup>•• ••• ••</sup> Nexus Dasht	ooard 🔶 Orchestrator 🗸					Feedback 💄 🕐
a Dashboard	Sites					
Sites						
CE Application Management						
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
<ul> <li>O Infrastructure</li> </ul>	Øок		AWS	Unmanaged		
	©ок	Azure	Azure	Unmanaged		
	©ок	ext-		Unmanaged		
	⊘ок	Syd	d Configuration	× Unmanaged		
		Site ID *	•			
				Add		
	10 V Rows				Page 1	of 1 << 1-4 of 4 >>

c) Repeat these steps for the remaining sites in NDO to change each site to the **Managed** state and provide a unique site ID for each site.

The following figure shows an example of all four sites (the two NDFC sites and the two cloud sites) with their states changed to **Managed** and a unique site ID provided for each site.

## Figure 43:

≡ cisco Nexus Dashb	oard 💄 Orchestrator 🗸		i di Lini Mi			Feedback 👤 🤭
Dashboard     Sites	Sites					65 ©
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
<ul> <li>O Infrastructure</li> </ul>	⊘ок	AWS Site ID: 91	aws	Managed	25.1(1e)	
Ø Integration	⊘ок	Azure Site ID: 92	Azure	Managed	25.1(1e)	
	⊘ок	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 $\ll$ $\!\!\!\!<$ 1-4 of 4 $\!\!\!>$ $\!\!\!\!\!>$

# What to do next

Complete the site-to-site connectivity between the NDFC and the cloud sites using the procedures provided in Complete Site-to-Site Connectivity Between NDFC and Cloud Sites, on page 39.

# Complete Site-to-Site Connectivity Between NDFC and Cloud Sites

Follow the procedures in the following sections to complete the site-to-site connectivity between the NDFC and cloud sites.

# **Complete the Necessary Control Plane Configurations**

## Before you begin

Onboard the NDFC and cloud sites in ND and NDO using the procedures provided in Onboard the NDFC and Cloud Sites into ND and NDO, on page 32.

**Step 1** In NDO, navigate to **Infrastructure** > **Site Connectivity**.

#### Figure 44:

≡ cisco Nexus Dash	nboard 🔔 Orchestrator 🗸					Feedback 💄 📀
<ul> <li>Dashboard</li> <li>Sites</li> </ul>	Sites					() ()
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
<ul> <li>Infrastructure</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 $\ll <$ 1-4 of 4 $> \gg$

At this point, you will see the sites on the world map but they will not have any links in between, which means that there is no connectivity between the sites at this point.

#### Figure 45:

≡ cisco Nexus Dashboar	d 🗶 Orchestrator 🗸	Feedback 💄
<ul> <li>Dashboard</li> <li>Sites</li> </ul>	Site Connectivity	t Configure
Application Management  Application Management  Application Management  Application  Applicatio	Connectivity Settings	Croup Markers

- Step 2In the upper right area in the Site Connectivity window, click Configure.The General Settings area of the Site Connectivity window appears.
- **Step 3** In the **General Settings** area, click the **Control Plane Configuration** tab, then make the necessary configurations in this page.

#### Figure 46:

— cisco Nexus Dashi		Feedback 🛓 🕚
Site Connectivity		DEPLOY V Ot X
SETTINGS	Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDFC Settings	
Ceneral Settings		
sites	BGP	~
• O AWS disabled	ppP hereng Type Ad mean v	
• • Azure	Keep-Alex Intered Decemblo Q	
e est-fab-1	10 Selentaria Sectori U a seconda Contra Seconda S	
• • Sydney ⊘	Concold Network Concold Networ	
	OSPF           0007 Area 0           5886	^
	CloudSec Control	^
	Data Path	~
	YELAN LOP destinator port hunge will cause hulling designed for activity flows. Change with caudion.      Programmer Type     TRLAN     TRLAN	

Note that BGP is used for underlay connectivity between on-premises and cloud sites, whereas OSPF is used for cloud-to-cloud underlay connectivity.

**Note** These general BGP settings apply to the use of BGP for both underlay and overlay connectivity and normally should not be changed, with the exception of the **BGP Peering Type** option in the next step that only applies to overlay peering.

**Step 4** For overlay connectivity between on-premises and cloud sites, in the **BGP Peering Type** field in the **BGP** area, choose either **full-mesh** or **route-server**.

See Supported Topologies to see the topologies that use full mesh or route server connectivity.

For this specific use case, we are configuring a deployment based on the Option 1 topology in Supported Topologies with IPsec (Multi-Cloud), so we would choose **full-mesh** for this use case.

- **Step 5** Define any remaining parameters in the **BGP** area, if necessary.
- **Step 6** For cloud-to-cloud underlay connectivity, in the **OSPF** area, enter the appropriate value in the **OSPF** Area **ID** field.

This configuration is necessary for cloud-to-cloud connectivity because the underlay routing between two cloud sites use OSPF. For this example, enter OSFP Area ID 0.0.0.0 in this field.

# Step 7 Under Data Path, locate the Encapsulation Type area and select VXLAN.

By default, NDO uses standard VXLAN in data-plane for Hybrid Cloud for NDFC based on-premises fabrics. The other option is iVXLAN, which should be used when building Hybrid Cloud connectivity for ACI sites (since ACI uses iVXLAN).

# What to do next

Follow the procedures provided in Add the On-Premises IPsec Device and IPsec Tunnel Subnet Pools, on page 41.

# Add the On-Premises IPsec Device and IPsec Tunnel Subnet Pools

In this section, you will add the on-premises IPsec device (the Cisco Catalyst 8000V in the NDFC external fabric site) and configure the IPsec tunnel pool.

# Before you begin

Follow the procedures provided in Complete the Necessary Control Plane Configurations, on page 39.

- **Step 1** In the same **General Settings** page, click the **On Premises IPsec Devices** tab.
- Step 2 Click Add On Premises IPsec Device.

#### Figure 47:

≡ cisco Nexus Dashb	Doard 🏩 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
🔹 🔕 Azure	And on Hemises Hade Device
disabled	
▼ ● ext-fab-1	
🔹 🌘 Sydney 🥥	

The Add On Premises IPsec Device page appears.

## **Step 3** In the **Type** field, choose either **Unmanaged** or **Managed**.

Both the Unmanaged and Managed options are supported for the on-premises IPsec device.

If you choose the Unmanaged option for the on-premises IPsec device, you must enter the necessary information
for this unmanaged on-premises IPsec device, such as the Name, IP Address, and Next Hop Address. Use the
Unmanaged when the on-premies IPsec device is not being managed by NDFC (either that device is not supported
by NDFC or it's a third-party device). NDO then generates the required configuration for the unmanaged IPsec
device, which can be downloaded and applied on the on-premises IPsec devices manually.

110010 40.
------------

≡ <sup>•( ••  •</sup> cisco Nexus D	ashboard A Orchestrator V
Site Connectivity	
SETTINGS	Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDEC Settings
General Sattings	
SITES	On Premises IPsec Devices
e 🤤 AWS disabled	Add On Premises IPsec Device ×
disabled	Type Unmanaged Managed
e 🔮 ext-fab-1	Name *
Sydney	ASN*
	Next Hop Address * 1.1.1.1

• If you choose the **Managed** option for the on-premises IPsec device, the **Site** field becomes available below the **Managed** option. The sites available in the **Site** field is based on information that NDO pulls from NDFC for the external fabrics configured in NDFC.

#### Figure 49:

	xus Dasht	board 📄 🏩 Orchestrator 🗸
Site Connect	ivity	
		Control Plane Configuration On Premises (Psec Devices External Devices (Psec Tunnel Subnet Pools NDEC Settings
		On Premises IPsec Devices
		Name Type IP Address Next Hop Address
		Add On Premises IPsec Device
Azure		
		Add On Premises IPsec Device ×
ext-fab-1		Туре
		Unmanaged Managed
Sydney		Select
		ext-fab-1

Choose the NDFC external fabric with the managed on-premises IPsec device. The **ASN** field is automatically populated in this case based on the site that you chose.

For this use case example, we will choose **Managed** for the type for the on-premises IPsec device.

a) In the **Device** field, select the on-premises IPsec device that you want to use for this deployment.

The devices available in the **Device** field is based on information that NDO pulls from NDFC for the on-premises IPsec devices configured in the NDFC site that you selected above. The **ASN** field is then automatically populated based on the on-premises IPsec device that you selected in the **Device** field.

b) In the **Interface** field, select the appropriate interface that you want to use for the on-premises IPsec device.

The **IP Address** field for this interface is then automatically populated based on the interface that you selected in the **Interface** field.

c) In the **Next Hop Address** field, enter the address to be used for the route that you want to be configured on IPsec.

Figure	50:
119010	

	Control Plane Configuration On Premises IPsec Devices	External Devices IPsec Tunnel Subnet Pools NDFC Settings
	On Premises IPsec Devices	
		Add On Premises iPsec Device ×
	Name Type IP Address	
	Add On Premises IPaec Device	Type Managed
• 🔿 Azure		Site *
		ext-fab-1
		ASN
🔹 🌑 ext-fab-1		65080
		Device *
		C8K3-Fab2
Sydney		Interface *
		GigabitEthernet2
		IP Address
		64.104.255.12
		Next Hop Address *
		64.104.255.1

- Step 4When you have finished entering the necessary information in the Add On Premises IPsec Device page, click Ok.You are returned to the On Premises IPsec Devices page, which now shows the configured on-premises IPsec device.
- Step 5Click the IPsec Tunnel Subnet Pools tab to configure the IPsec tunnel subnet pools.The IPsec Tunnel Subnet Pools information is required for the cloud tunnel IP assignment.
- Step 6 In the External Subnet Pool area, click Add IP Address.

Figure 51:

≡ <sup>•</sup> ·II··II·· 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	External Subnet Pool 💿	
• 🤤 AWS disabled	IP Address	
• • Azure	Add IP Address	
◦ ● ext-fab-1	Site Specific Subnet Pool	
💿 🌘 Sydney	Add Site Specific Subnet Pool	

**Step 7** Enter the IP subnet pool that you will use for the IPsec tunnels.

Define the IP subnet pool, using public or private IP addresses, for the IPsec tunnels. This is the pool of IP addresses for the IPsec tunnel addressing between the on-premises external device to the Cisco Catalyst 8000V, and between the Cisco Catalyst 8000Vs deployed in the cloud sites.

- A /30 subnet is required for each IPsec tunnel.
- The pool size should be able to accommodate all the IPsec tunnels.
- The minimum allowed pool size is of 512 addresses (/23 subnet).
- Use a range of IP addresses (public or private) that does not overlap with other IP addresses in your environment.

Figure 52:

≡ cisco Nexus Da	shboard 🖉 🔔 Orchestrator 🗸
Site Connectivity	
SETTINGS	Control Plane Configuration On Premises (Psec 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	170.10.0/16
disabled	Add IP Address
👳 🌘 ext-fab-1	
	Site Specific Subnet Pool 💿
o Sydney	Name IP Address
C	Add Site Specific Subnet Pool

**Step 8** Click the checkbox to accept the IP subnet pool that you entered.

The IP subnet pool appears under the **External Subnet Pool** area. *Figure 53:* 

ETTINGS		Control Plana Configuration On Pramises (Deer Davises External Davise	e IPsec Tunnel Subnet Poole	NDEC Settings
eneral Settings		Control France Configuration On Frences Free Devices External Device		Horo settings
ITES		External Subnet Pool 💿		
• 🤤 AWS	0	IP Address 🜒		
disabled	0	169.254.0.0/16		
• 🛆 Azure		170.1.0.0/16	< 🗇	
disabled	$\odot$	Add IP Address		
🔹 🌘 ext-fab-1				
	$\odot$	Site Specific Subnet Pool 💿		
🔹 🌘 Sydney		Name IP Address		
	$\odot$	Add Site Specific Subnet Pool		

Step 9 Click the NDFC Settings tab and enter the necessary information in the Auto Route Target Prefix, if necessary.

#### Figure 54:

≡ cisco Nexus	shboard 🖉 🙏 Orchestrator 🗸	
Site Connectivit		
SETTINGS	Control Diano Configuration On Bramicos (Baco Daviago External Daviago IBaco Tunnal Subnat Baco	NDEC Settings
General Settings	Control Plane Configuration. On Prennses inset Devices. External Devices. Inset fulniel Subnet Por	
SITES	NDFC Settings	
💌 🤤 AWS disabled	Layer 2 VXLAN VNI Range 130000-149000	
🔹 🔕 Azure	Layer 3 VXLAN VNI Range 150000-159000	
disabled	Muti-Site Routing Lookback IP Range 10.10.0.0/24	
♥ ● ext-fab-1	Anycast Gateway MAC 2020.0000.00aa	
• Sydney	Auto Route Target Prefix * 23456 Manage 1-955	
	Advanced Settings	wa ∀

Under NDFC settings in NDO, the Route Target Prefix for the Route Target generation is set with a default value of 23456 for NDFC (Cloud Network Controller has different values for this setting), so you can change this value in the **Auto Route Target Prefix** field if required to avoid any possible duplication. Setting the value in this field allows NDO to push this value out to NDFC by NDO.

# What to do next

Follow the procedures provided in Add Ports for the External Devices in the NDFC External Fabric, on page 48.

# Add Ports for the External Devices in the NDFC External Fabric

In this section, you will add and configure the necessary ports for the external devices in the NDFC external fabric. These are the interfaces connecting the core router to the BGW nodes.

#### Before you begin

Follow the procedures provided in Add the On-Premises IPsec Device and IPsec Tunnel Subnet Pools, on page 41.

Step 1	I In the left pane under	General Settings: Sites	click the NDFC external fal	bric (the ext-fab-1 site in this	example).
--------	--------------------------	-------------------------	-----------------------------	----------------------------------	-----------

- **Step 2** In the middle pane, click on the first external device in the NDFC external fabric.
- **Step 3** In the right pane, click **Add Port**.

Figure 55:

≡ cisco Ne	xus Dashboard	j 🙏 Orchestrator 🗸					edback 上 💿
Site Connect	ivity				(	DEPLOY V	) @t} X
SETTINGS				⊽ C	8K3-Fab2		
General Settings		Site ext-fab-1	Refresh				
SITES		Core Router C8K3-Fab2		critical	major	minor	warning
<ul> <li>AWS</li> <li>disabled</li> </ul>	Ø			Ports	et Port ID		
e O Azure disabled	0			C Add F	ort		
😇 🕒 ext-fab-1	Ø						
🔹 🌒 Sydney	0						

- **Step 4** Enter the necessary information for the port configuration, including the IP address, remote IP address, and remote ASN.
  - **Note** The **Towards Cloud Router** option is only applicable for border gateways in a hub site. You will not enable this option in this window for the following reasons:
    - Because the topology that we're using for this example use case does not use a hub site, you will not enable the **Towards Cloud Router** for this example use case.
    - Even if we were configuring for a topology that uses a hub site, such as Option 3 in Supported Topologies with IPsec (Multi-Cloud), we would not enable this option in this page for the external device in the NDFC external fabric for that hub site topology; instead, we would enable this option in the page for the BGW spine device in the NDFC VXLAN fabric, as described in Add the Port for the BGW Spine Device in the NDFC VXLAN Fabric, on page 53.

#### Figure 56:

Add Port				
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 BGP Authentication None Simple Cisco Towards Cloud Router ①				
BFD Enabled				
ick <b>Ok</b> when you are finished				

**Step 6** Repeat these steps for the remaining external devices.

## What to do next

Follow the procedures provided in Define the Multi-Site VIP for the VXLAN Fabric Site, on page 50.

# **Define the Multi-Site VIP for the VXLAN Fabric Site**

In this section, you will define the Multi-Site VIP for the VXLAN fabric site.

# Before you begin

Follow the procedures provided in Add Ports for the External Devices in the NDFC External Fabric, on page 48.

Step 5

- Step 1 In the left pane under General Settings: Sites, click the NDFC VXLAN fabric site.
- **Step 2** In the middle pane, click on the spine device.
- Step 3In the right pane, under Inter-Site Connectivity, define the Multi-Site VIP in the Multi-Site VIP field.You can click Auto Allocate or you can explicitly define the IP address for the Multi-Site VIP.

Figure 57:

≡ "listo" Nexus	s Dashboar	d 🏩 Orchestrator 🗸	Feedback 🛓 📀
Site Connectivit	ity		DEPLOY V Otl X
SETTINGS			Sydney Settings
General Settings		Site Sydney Refresh	• Sydney Settings
SITES		Switch _nffceepine1	Inter-Site Connectivity
💌 😑 AWS	0		General
disabled			Site ID 82
<ul> <li>Azure</li> </ul>	0		Multi-Site VIP 10.10.0.1 Auto Allocate
disabled			IPsec Device ③
• ext-fab-1	0		Name Device ID IP Address
<ul> <li>Sydney</li> </ul>	0		

# What to do next

Follow the procedures provided in Map the IPsec Device to the VXLAN Fabric Site, on page 51.

# Map the IPsec Device to the VXLAN Fabric Site

In this section, you will map the IPsec device to the VXLAN fabric site.

# Before you begin

Follow the procedures provided in Define the Multi-Site VIP for the VXLAN Fabric Site, on page 50.

- Step 1 In the left pane under General Settings: Sites, click the NDFC VXLAN fabric site.
- **Step 2** In the middle pane, click the spine device.
- **Step 3** In the right pane, under **Inter-Site Connectivity**, click **Add IPsec Device**.

#### Figure 58:

≡ disco Nex	us Dashbo	ard to Onchestrator >	Feedback 1 0
Site Connecti	vity		DEPLOY V Oth X
SETTINGS			Svdnev Settings 0
General Settings		Site Sydney     Refresh	
SITES		Switch ndfc-spine1	Inter-Site Connectivity
disabled	Ø		Site ID 82
o Azure	Ø		Mutti-Site VIP 10.10.0 1 IPsec Device ()
💿 🌘 ext-fab-1	Ø		Name Device ID IP Address
💌 🛢 Sydney	0		

**Step 4** Click **Select**, then choose the appropriate IPsec device.

# Figure 59:

≡ cisco Ne	kus Dashbo	ard 🌐 🙏 Orchestrator 🗟	Feedback 💄 💿
Site Connect	ivity		DEPLOY V Oth X
SETTINGS			Sydney Settings
General Settings		Site Sydney     Refresh	
SITES  C C AWS  disabled  C Azure	Ø	Switch ndfc-spine1	Inter-Site Connectivity General Site ID 82 Multi-Site VIP
disabled	Ø		10.10.0.1 Auto Allocate
o 🔵 ext-fab-1	Ø		Name Device ID IP Address
<ul> <li>Sydney</li> </ul>	0		CBK3 HBC

The on-premises IPsec device is now mapped to the VXLAN fabric site.

#### Figure 60:

Site Connect	ivity		DEPLOY V Oti X
SETTINGS General Settings			Sydney Settings
SITES	Ø	Switch ndfe-spine1	Inter-Site Connectivity General Site ID 82
• Azure	0		Multi-Site VIP 10.10.0.1 IPsec Device O Name Device ID ID Address
ext-fab-1     Sydney	Ø		CBK3-     BBJE1UBCZ9M 64.104.255.12     C     Add IPsec Device
	Ø		

**Step 5** Repeat this step for each on-premises IPsec device (Cisco Catalyst 8000V) that will be used to connect the NDFC VXLAN site to the cloud sites.

# What to do next

Configure the ports on the BGW spine device connecting to the core router (Cisco Catalyst 8000V) using the procedures provided in Add the Port for the BGW Spine Device in the NDFC VXLAN Fabric, on page 53.

# Add the Port for the BGW Spine Device in the NDFC VXLAN Fabric

In this section, you will add and configure the necessary port for the BGW spine device in the NDFC VXLAN fabric facing towards the on-premises IPsec device.

#### Before you begin

Follow the procedures provided in Map the IPsec Device to the VXLAN Fabric Site, on page 51.

- Step 1 In the left pane under General Settings: Sites, click the NDFC VXLAN fabric site.
- **Step 2** In the middle pane, click on the spine device.
- **Step 3** In the right pane, click **Add Port**.

## Figure 61:

	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					
<ul> <li>Sydney</li> </ul>						

Step 4Enter the necessary information in this page.Define the port parameters in this page.

#### Figure 62:

≡ disco Nexus Dasht	ooard 🔔 Orchestrator 🗸				Feedback 🛓 🧕
Site Connectivity					DEPLOY V Oth X
					o ndfc-spine1
	Site Sydney			Refresh	
	Cuitch adfa.colos1	Add Port	×		critical major minor warning
	Shire Hurespirer	Ethernet Port ID * Ethernet1/32 × ~			BOP-EVPN ROUTER-ID 20.2.0.3
e 🖸 Azure		IP Address * 10.140.1.2/30 Description			BGW PIP 20.3.0.4 Ports
e ext-fab-1		towards on-prem CBKv Gi-4 Remote Address *			Ethernet Port ID
		10.140.1.1 Remote ASN *			
• Sydney		MTU * 9216			
		BGP Authentication  None Simple			
		Towards Cloud Router ③ BFD Enabled			
			Ok		

- In the Ethernet Port ID field, select the interface that is facing toward the on-premises Cisco Catalyst 8000V.
- In the IP Address field, enter the IP address for this interface. Later in these procedures, Nexus Dashboard Orchestrator
  will configure this IP address for this interface on the BGW spine switch residing in the VXLAN fabric.
- In the **Remote Address** field, enter the IP address of the gigabit 4 interface of the on-premises IPsec device.
- In the **Remote ASN** field, enter the ASN for the on-premises IPsec device. For example, for this example use case, we would enter 65080 as the ASN for the on-premises IPsec device.
- **Note** The **Towards Cloud Router** option is only applicable for border gateways in an on-premises hub site. This option would need to be enabled in topologies where you are using a hub site, such as Option 3 in Supported Topologies with IPsec (Multi-Cloud).

Because the topology that we're using for this example use case does not use a hub site, you will not enable the **Towards Cloud Router** for this example use case.

# Step 5 Click Ok.

The port for the BGW spine device is now added in the NDFC VXLAN fabric

Figure 63:

Site Connecti	vity				DEPLOY V	] 012 ×
ETTINGS			0	dfc-spine1		
eneral Settings		Site Sydney				
TES		Switch ndfc-spine1	critical	major	minor	warning
disabled	Ø		BGP-EV 20.2.0	/PN ROUTER-ID		
Azure			BGW P 20.3.0	р .4		
disabled	0		Ports	net Port ID		
ext-fab-1	0		Ether	net1/32		/ 1
			🕤 Add	Port		
Sydney	Ø					

# What to do next

Follow the procedures provided in Connect the First Cloud Site to the NDFC VXLAN Fabric Site, on page 55.

# **Connect the First Cloud Site to the NDFC VXLAN Fabric Site**

In this section, you will connect the first cloud site to the NDFC VXLAN fabric site.

## Before you begin

Follow the procedures provided in Add the Port for the BGW Spine Device in the NDFC VXLAN Fabric, on page 53.

- Step 1 In the left pane under General Settings: Sites, click the first cloud site (for example, the AWS site).
- Step 2In the right pane, click Inter-Site Connectivity, then check the box under Multi-Site to enable that feature.This feature is required for building VXLAN Multisite overlay tunnels between the sites.

**Step 3** In the right pane, click **Add Site**.

#### Figure 64:

Site Connecti	vity			DEPLOY	× 610 ~
SETTINGS				AWS Settings	
General Settings		Site AWS		Refresh	
		8 Region us-west	2	Inter-Site Connectivity External	Connectivity
disabled	0	ct_routerp_us- west-2_0	<ul> <li>ct_routerp_us- west-2_1</li> </ul>	General Site D 91	^
Azure	Ø	C8kV	CBxV	Mutti-Site	~
• • ext-fab-1				BGP Autonomous System Number 65991	
	0			Contract Based Routing	
<ul> <li>Sydney</li> </ul>	Ø			Inter-Site Connectivity  Site Protocol  Add Site	

The Add Site page appears.

**Step 4** In the **Add Site** page, click **Select a Site**.

# Figure 65:

≡ cisco Ne	kus Dashboard	, Orchestrator ~			Feedback 上 💿
Site Connecti	ivity				DEPLOY ~ Ota X
SHETTINGS					AM/C Cattings
	0	Site AWS		Refresh	Aws settings
SITES				- Contrain	Inter-Site Connectivity External Connectivity
Cartasher	0	Add Site		×	General A
Azure Cisabled		CRIAN Connected to Site Select Site > Connection Type *			Math Ste () BOP DDP Antroporter Stretum Mumber
★ ● ext-fab-1		Protocol BGP-EVPN Hub Site O			
a 🕒 Sydney		Psec			Inter-Site Consectivity  Site  Protocol  Add Site
		On Premises IPsec Devices			
		C8K3-Fab2	64.104.255.12		

The Select a Site page appears.

**Step 5** Select the NDFC VXLAN fabric (the Sydney site in this example), then click **Select**.

#### Figure 66:

≡ cisco Nexu	ıs Dashboa	rd 🕴 🙏 Orchestrator 🗸				
Site Connectiv	vity					
						AWS Set
		Site AWS			Refresh	
SITES		Region us-wes				Inter-Site Connec
		e ct_routerp_us-	Add Site		×	General Site ID 91
e 🔕 Azure		C8ky	Select Site		×	Multi-Site ()
			Q. Search Site	S Site Sydney		BGP BGP Autonomous Sy
a 🌒 ext-fab-1			Azure Sydney	Site ID 82		
🝵 🌘 Sydney				Type N/A	_	Inter-Site Connectiv
				URL https://172.16.0.191:443		Add Site
					Select	
					_	

You are returned to the Add Site page.

**Step 6** In the **Add Site** page, in the **Connection Type** field, choose the type of connection that you will use from the first cloud site to the NDFC VXLAN fabric site.

Site Connectivity				
eneral Settings	Site AWS	Add Site		
	Region us-wes	AWS 😑 → Sydney 🛡		
		Connected to Site		
	ct_routerp_us- west-2_0	Sydney $ imes$		
Azure		Connection Type *		
(		Functimet.		
		Public Internet		
ext-fab-1		Private Connection		
		IPsec		
<ul> <li>Sydney</li> </ul>		On Premises IPsec Devices		
		Device Name	IP Address	
		C8K3-Fab2	64.104.255.12	
		Sydney ● → AWS 😑		
		Please check if C8kVs are configured	with Public IPs for Public Underlay connection	
		Connected to Site		

You can select **Public Internet**, or you can select a **Private Connection** if you are using Direct Connect with AWS or ExpressRoute with Azure.

# Figure 67:

- Both **Public Internet** and **Private Connection** options are available for the on-premises site, whereas only the **Public Internet** connection option is available for the cloud sites.
- IPsec is mandatory for the **Public Internet** connection type and is automatically enabled for that connection type, whereas IPsec is optional for the **Private Connection** type.
- **Note** The **Hub Site** option would need to be enabled in topologies where you are using a hub site, such as Option 3 in Supported Topologies with IPsec (Multi-Cloud).

Because the topology that we're using for this example use case does not use a hub site, you will not enable the **Hub Site** option for this example use case.

**Step 7** When you have finished the configurations in this page, click **OK**.

#### What to do next

Follow the procedures provided in Connect the First Cloud Site to the Second Cloud Site, on page 58.

# **Connect the First Cloud Site to the Second Cloud Site**

In this section, you will connect the first cloud site to the second cloud site.

## Before you begin

Follow the procedures provided in Connect the First Cloud Site to the NDFC VXLAN Fabric Site, on page 55.

- **Step 1** In the left pane under **General Settings: Sites**, click the first cloud site (for example, the AWS site).
- **Step 2** In the right pane, click **Inter-Site Connectivity**.
- **Step 3** In the right pane, click **Add Site**.

#### Figure 68:

Site Connectivi	ity			DEPLOY 🗸	× £3⊙ [
SETTINGS				AWS Settings	
General Settings		Site AWS		Refresh	
SITES	_	Region us-west	-2	Inter-Site Connectivity External Co	onnectivity
<ul> <li>AWS</li> </ul>	0			General	~
enabled		ct_routerp_us- west-2_0	<ul> <li>ct_routerp_us- west-2_1</li> </ul>	Site ID 91	
👳 🔕 Azure	0	CSKV	C8kV	Multi-Site 🔿	
disabled	0			BCP BCP Autonomous System Number	^
🔹 🔵 ext-fab-1				65091	
	0			Contract Based Routing	
<ul> <li>Sydney</li> </ul>				Inter-Site Connectivity	
	Ø			Sydney Connection Type: Public BGP-EVPN	/ =
				Add Site	

The **Add Site** page appears.

Step 4 In the Add Site page, click Select a Site.

The **Select Site** page appears.

**Step 5** Select the second cloud site (for example, the Azure cloud site), then click **Select**.

#### Figure 69:

≡ cisco Ne	xus Dashboard	d 🔶 🙏 Orchestrator 🗸				Feedback	10
Site Connect	ivity					DEPLOY V	es ×
						AWS Settings	
		Site AWS			Refresh	Inter-Site Connectivity External Connect	livity
		<ul> <li>ct_routerp_us- west-2_0</li> </ul>	Add Site		×	General Site ID 91	
disabled		CBKV	Select Site	s Site	×	Mutth-Site () ECP BCP BCP Autonomous System Number	
s 🕘 ext-fab-1			Azure	Site ID 92			
<ul> <li>Sydney</li> </ul>				Type Azure URL https://20.127.114.214:443		Inter-Site Connectivity  Site Protocol Sydnoy Connection Type Public BGP-EVPN Connection	1
					Salaci Salaci		

You are returned to the Add Site page.

**Step 6** In the Add Site page, in the Connection Type field, choose the type of connection that you will use from the first cloud site to the second cloud site.

For some types of cloud-to-cloud connectivity, you might these options:

- Public Internet
- Cloud Backbone

**Cloud Backbone** can be used to establish connectivity between cloud sites of the same provider (for example, an AWS site 1 managed by one Cloud Network Controller, and an AWS site 2 managed by a second Cloud Network Controller). However, between sites of different cloud providers (for example, AWS to Azure), **Public Internet** is the only option, as shown in the following figure.

#### Figure 70:

≡ <sup>•1 •1 •</sup> Nexus Dashboard	. Orchestrator ~		Feedback 上 📀
Site Connectivity			DEPLOY V Ota X
			-
	Site AWS	Add Site ×	VVS Settings
		÷	Inter-Site Connectivity External Connectivity
	Region us-wes	AWS 🗢 → Azure 🛇	General
	ct_routerp_us-     west-2 0	Please check if C8kVs are configured with Public IPs for Public Underlay connection	
a 🔘 Azure	CBKV	Connected to Site	Musi-Site ()
		Azure × Connection Type *	BOP
e extriat-1		Public Internet	
		Protocol BGP-EVPN	
		Hub Sike 🕥	Inter-Site Connectivity
<ul> <li>Shaueh</li> </ul>		Desc.	Site Protocol
		er anv	Sydney BOP-EVPN × = Connection Type: Public
		Azure ◎ → AWS 😑	Add Site
		Please check if CBkVs are configured with Public IPs for Public Underlay connection	
		Connected to Site AWS	
		Connection Type *	

When the **Public Internet** connection type is selected, the **IPsec** option is mandatory and is automatically enabled for that connection type, whereas IPsec is optional for the **Cloud Backbone** type.

**Note** You will not enable the **Hub Site** option for cloud-to-cloud connectivity, even if the topology uses a hub site (you would enable the **Hub Site** option when configuring connectivity between the cloud site and the NDFC VXLAN fabric site in that case).

**Step 7** When you have finished the configurations in this page, click **Ok**.

# What to do next

Follow the procedures provided in Connect the Second Cloud Site to the NDFC VXLAN Fabric Site, on page 60.

# **Connect the Second Cloud Site to the NDFC VXLAN Fabric Site**

In this section, you will connect the second cloud site to the NDFC VXLAN fabric site.

The procedures in this section are essentially the same steps that you performed in the previous sections, where you:

- Connected the first cloud site to the NDFC VXLAN fabric site in Connect the First Cloud Site to the NDFC VXLAN Fabric Site, on page 55.
- Connected the first cloud site to the second cloud site in Connect the First Cloud Site to the Second Cloud Site, on page 58.

For this section, you will be connecting the second cloud site to the NDFC VXLAN fabric site. Note that because you had already configured connectivity between AWS and Azure in Connect the First Cloud Site to the Second Cloud Site, on page 58, you do not have to configure connectivity from the second cloud site (Azure) back to AWS because that connectivity was already configured in that previous section.

# Before you begin

Follow the procedures provided in Connect the First Cloud Site to the Second Cloud Site, on page 58.

- **Step 1** In the left pane under **General Settings: Sites**, click the second cloud site (for example, the Azure site).
- Step 2 In the right pane, click Inter-Site Connectivity, then check the box under Multi-Site to enable that feature.
- **Step 3** In the right pane, click **Add Site**.

Figure 71:

Site Connectiv	ty	DEPLOY V Oth X
SETTINOS General Settings	Site Azure	Azure Settings
SITES  AWS  enabled  Azure  disabled  ext.fab-1	Cev	Inter-Site Connectivity External Connectivity General Site O S S O D S O D D D D D D D D D D D D D
<ul> <li>exc18D1</li> <li>Sydney</li> </ul>	0	Contract Based Routing Contract Based Routing Biter-State Connectivity @ Perfoced AVS Connection Type Parker @ AMI State

The Add Site page appears.

- Step 4In the Add Site page, click Select a Site.The Select a Site page appears.
- **Step 5** Select the NDFC VXLAN fabric (the Sydney site in this example), then click **Select**.

You are returned to the Add Site page.

**Step 6** In the Add Site page, in the Connection Type field, choose the type of connection that you will use from the second cloud site to the NDFC VXLAN fabric site.

#### Figure 72:

≡ cisco Nexus Dashboar	rd 🏩 Orchestrator 🗸				Feedback 上 🕥
Site Connectivity					DEPLOY V Ota X
					Azura Sattinge
	Site Azure	Add Site		×	• Azure settings 0
				×	Inter-Site Connectivity External Connectivity
	Region eastus	Azure <sup>O</sup> → Sydney ●			General
	ct_routero_eastur	Connected to Site Sydney X			
	3	Connection Type *			
	CBKV	Public Internet			
		Protocol			BGP
a ext-fab-1		Line City O			
0					
		IPsec			
n Sydney		On Premises IPsec Devices			Site Protocol
		Device Name	IP Address		AWS BOP-EVPN / #
		C8K3-Fab2	64.104.255.12		Carstaction Type Public
					0 A00 548
		Sydney ● → Azure O			
		Please check if C8kVs are configured	d with Public IPs for Public Underlay connection	_	
		Connected to Site			
		Autor .			
				<u>•</u>	

**Step 7** When you have finished the configurations in this page, click **OK**.

The configured sites appear.

# Figure 73:

≡ disco Nexus Dashboar	d 🌐 🖈 Orchestrator 🗸	Føedback 🛓 💽
Site Connectivity		DEPLOY V Ot X
SETTINGS		
General Settings	Site Azure	Befresh
SITES		Inter-Site Connectivity External Connectivity
🔹 🤤 AWS	C Region eastus	General
enabled	CLrouterp_eastus J	Site ID 92
<ul> <li>Azure</li> </ul>	CSKV CSKV	Multi-Site 🔘
enabled		BOP A treemain System Number
👳 🌒 ext-fab-1		65092
0		Contract Based Routing
🔹 🌘 Sydney		Inter-Site Connectivity
0		AWS Connection Type: Public BGP-EVPN / =
		Sydney BGP-EVPN * 章
		The Add Site

# What to do next

Follow the procedures provided in Deploy the Configuration in Nexus Dashboard Orchestrator, on page 62.

# **Deploy the Configuration in Nexus Dashboard Orchestrator**

In this section, you will deploy the configuration in Nexus Dashboard Orchestrator (NDO).

#### Before you begin

Follow the procedures provided in Connect the Second Cloud Site to the NDFC VXLAN Fabric Site, on page 60.

**Step 1** Deploy the configuration in NDO.

• If you chose the **Unmanaged** option for the on-premises IPsec device in Add the On-Premises IPsec Device and IPsec Tunnel Subnet Pools, on page 41, at the top right of the page, click **Deploy > Deploy & Download External Device Config files**.

This option downloads a zip file that contains the necessary configuration information that you will use to configure the on-premises IPsec device. A followup screen appears that allows you to select all or some of the configuration files to download.

• If you chose the **Managed** option for the on-premises IPsec device in Add the On-Premises IPsec Device and IPsec Tunnel Subnet Pools, on page 41, at the top right of the page, click **Deploy > Deploy Only**.

#### Figure 74:

≡ "  11  1. CISCO NO	xus Dashboa	rd   🙏 Orchestrator 🗸	Feedback 🛓 🤇
Site Connect	ivity		DEPLOY ~ Oth X
SETTINGS General Settings		Site Azure     Refresh	Deploy Only Deploy & Download On Premises IPsec Device Config files Deploy & Download External Device Config files Download On Premises IPsec Device Config files Download On Premises IPsec Device Config files Download On Premises IPsec Device Config files Device Device Device Device Config files Device
enabled     Azure     enabled	0	Region eastus     C_routerp_eastus     J     casv     casv     casv	Download External Device Config files
ext-fab-1     Sydney	Ø		BCP Autonomous System Number 65002 Contract Based Routing Inter-Site Connectivity
	0		site         Protocol           Avis         BOP-EVIPN         * 10           Sydney         BOP-EVIPN         * 10           Sydney         BOP-EVIPN         * 10           Add Site         BOP-EVIPN         * 10

**Step 2** Click **Yes** in the **Confirmation** window.

NDO does the following things at this point:

- Initiates communication with NDFC and the cloud sites (AWS and Azure) through the Cloud Network Controller to automate the IPsec tunnels.
- Configures OSPF between the Azure Catalyst 8000V and the AWS Catalyst 8000V.
- Configures eBGP between the BGW spine switch, the on-premises IPsec device, and the Azure Catalyst 8000V and the AWS Catalyst 8000V.
- Establishes BGP-EVPN peering sessions between the sites.
- **Step 3** Verify that the configurations were done correctly in NDO.
  - In the left nav bar, click **Infrastructure** > **Site Connectivity** and verify the connectivity between sites in the **Connectivity Settings** area.

Figure	75·
riguio	15.



• In the same page, scroll down to the area for the first cloud site (for example, the AWS site), click **Show Connectivity Status**, then click **Underlay Status** in the **Inter-Site Connections** area to verify the underlay status.

In this example, there are six IPsec tunnels because there are two Cisco Catalyst 8000Vs on the first cloud site (AWS) that have IPsec tunnels to two Cisco Catalyst 8000Vs on the second cloud site (Azure), and to one Cisco Catalyst 8000V for the on-premises external fabric.

Figure 76:

AWS e Regions 2	ACI Multi-Site On	Site ID 91	809 ASH 65091		A Hide Connectivity Status A
Overlay Status Underlay Status 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	0	
ct_routerp_us-west-2_0	↑ Up	tunn-6 ↑ Up	BGP 🛧 Up	170.1.254.2	64.104.255.12

• Scroll down to the area for the second cloud site (for example, the Azure site), click **Show Connectivity Status**, then click **Underlay Status** in the **Inter-Site Connections** area to verify the underlay status.

In this example, there are six IPsec tunnels because there are two Cisco Catalyst 8000Vs on the second cloud site (Azure) that have IPsec tunnels to two Cisco Catalyst 8000Vs on the first cloud site (AWS), and to one Cisco Catalyst 8000V for the on-premises external fabric.

#### Figure 77:

Azure Regions 1	ACI Multi-Site On	Site ID 92	BGP ASN 65092		^
Inter-Site Connections Overlay Status Underlay Status	15				Hide Connectivity Status $\wedge$
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		÷
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

• Scroll down to the area for the NDFC external fabric site, click **Show Connectivity Status**, then click **Underlay Status** in the **Inter-Site Connections** area to verify the underlay status.

The external fabric's function is to provide underlay reachability from the on-premises IPsec devices to the VXLAN fabric and the cloud sites. The underlay protocol uses eBGP.

• Scroll down to the area for the NDFC VXLAN fabric site, click **Show Connectivity Status**, then click **Underlay Status** in the **Inter-Site Connections** area to verify the underlay status.

The underlay status shows the eBGP session status between the BGW spine switch and the on-premises IPsec device. *Figure 78:* 

Sydney •						^		
Nodes 1	Site ID 82	Multi-Site VIP 10.10.0.1	BGP ASN 65084		Fabric Type VXLAN Fabric			
Inter-Site Connections						Hide Connectivity Status $\wedge$		
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				

• In each of those screens, click **Overlay Status** to verify the overlay status for each.

#### Figure 79:



• Return to the NDFC screen and verify the hybrid cloud connectivity in the **Topology** screen. In the following example, you can see the NDFC VXLAN fabric site (the Sydney site) connected to the first and second cloud sites (the AWS and Azure cloud sites).



