cisco.



Hybrid Cloud Connectivity Deployment for Cisco NX-OS

First Published: 2023-01-31 Last Modified: 2023-03-21

Americas Headquarters

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883 © Cisco Systems, Inc. All rights reserved.



Trademarks

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

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

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

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

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

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

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

I



CONTENTS

P R E F A C E	Trademarks iii
CHAPTER 1	New and Changed Information 1
	New and Changed Information 1
PART I	Setting Up the Infra Configuration for Hybrid Cloud and Multi-Cloud Connectivity Deployment 3
CHAPTER 2	Overview 5
	Understanding Components of Hybrid Cloud Connectivity 5
	Building Hybrid Cloud Connectivity 7
	Terminology 9
	Prerequisites 12
	Guidelines and Limitations 12
	Related Documentation 12
CHAPTER 3	Supported Topologies 13
	Connection Options 13
	Supported Topologies with IPsec (Single-Cloud) 14
	Supported Topologies with IPsec (Multi-Cloud) 18
	Supported Topologies without IPsec (Single Cloud) 23
	Supported Topologies without IPsec (Multi-Cloud) 26
CHAPTER 4	Setting Up the Infra Configuration for Hybrid Cloud and Multi-Cloud Connectivity Deployment 31
	Example Topology of Infra Configuration for Hybrid Cloud and Multi-Cloud Connectivity Deployment 31
	Set Up the On-Premises NDFC Fabrics 32

Create an NDFC VXLAN Fabric 32 Create an NDFC VXLAN Fabric 33 Add Switches to the VXLAN Fabric 37 Configure an NDFC External Fabric 41 Create an NDFC External Fabric 42 Add the On-Premises Cisco Catalyst 8000V to the External Fabric 44 Deploy Cloud Network Controller on Cloud Sites 49 Deploy the Cloud Network Controller on the AWS Cloud Site 50 Configure the Necessary Parameters in Advanced Settings for AWS 50 Configure the Necessary Parameters in Region Management for AWS 52 Deploy the Cloud Network Controller on the Azure Cloud Site 56 Configure the Necessary Parameters in Advanced Settings for Azure 56 Configure the Necessary Parameters in Region Management for Azure 57 Onboard the NDFC and Cloud Sites into ND and NDO 62 Complete Site-to-Site Connectivity Between NDFC and Cloud Sites 69 Complete the Necessary Control Plane Configurations 69 Add the On-Premises IPsec Device and IPsec Tunnel Subnet Pools 71 Add Ports for the External Devices in the NDFC External Fabric 78 Define the Multi-Site VIP for the VXLAN Fabric Site 80 Map the IPsec Device to the VXLAN Fabric Site 81 Add the Port for the BGW Spine Device in the NDFC VXLAN Fabric 83 Connect the First Cloud Site to the NDFC VXLAN Fabric Site 85 Connect the First Cloud Site to the Second Cloud Site 88 Connect the Second Cloud Site to the NDFC VXLAN Fabric Site 90 Deploy the Configuration in Nexus Dashboard Orchestrator 92

PART II	Use Cases 97
CHAPTER 5	Deploying the Tenant 99
	Deploying the Tenant 99
CHAPTER 6	Stretched VRF Use Case 107
	About the Stretched VRF Use Case 107
	Configure the Stretched VRF Use Case 108

CHAPTER 7

Route Leaking Use Case 143

About the Route Leaking Use Case 143 Configure the Necessary Templates 145 Configure the On-Premises Site Template 145 Configure the Azure Site Template 153 Configure the AWS Site Template 158 Configure Route Leaking 163 Configure Route Leak from Azure VRF to NDFC VRF 163 Configure Route Leak from Azure VRF to AWS VRF 166 Configure Route Leak from AWS VRF to NDFC VRF 168 Configure Route Leak from AWS VRF to Azure VRF 170 Configure Route Leak from NDFC VRF to AWS VRF 172 Configure Route Leak from NDFC VRF to Azure VRF 173 Verify the Configurations 175

Contents

I



.

New and Changed Information

• New and Changed Information, on page 1

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
NDFC release 12.1.2e	Initial release of this use case document.	Initial release of this use case document.



PART

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

- Overview, on page 5
- Supported Topologies, on page 13
- Setting Up the Infra Configuration for Hybrid Cloud and Multi-Cloud Connectivity Deployment, on page 31



Overview

- Understanding Components of Hybrid Cloud Connectivity, on page 5
- Building Hybrid Cloud Connectivity, on page 7
- Terminology, on page 9
- Prerequisites, on page 12
- Guidelines and Limitations, on page 12
- Related Documentation, on page 12

Understanding Components of Hybrid Cloud Connectivity

This document describes deployment steps for the Cisco Hybrid Cloud Networking Solution powered by Cisco Nexus Dashboard Orchestrator (NDO) with a Cisco Nexus 9000 NX-OS based fabric managed by Nexus Dashboard Fabric Controller (NDFC) and public cloud sites managed by Cisco Cloud Network Controller (CNC).

The Cisco Nexus Dashboard Orchestrator (NDO) based Hybrid Cloud solution offers seamless connectivity between on-premises and cloud networks. This solution uses NDFC to manage on-premises VXLAN-based fabric and on-premises Cisco Catalyst 8000Vs, while cloud sites (AWS or Microsoft Azure) are managed by the Cisco Cloud Network Controller (CNC). NDO is used to orchestrate connectivity between on-premises and cloud sites, and between two or more cloud sites. VXLAN is used to build overlay tunnels between the sites.

The following figure shows an example topology for hybrid cloud connectivity using these components. See Supported Topologies, on page 13 for more information.



In this example topology, the on-premises site managed by NDFC has a secure connection setup to AWS and Azure cloud sites, where Cisco Catalyst 8000Vs sitting on the infra VPC/VNet serve as the cloud gateway for all traffic to and from the on-premises data centers.

On the on-premises site, Border Gateways (BGWs), which support seamless Layer-2/Layer-3 DCI extensions between different on-premises VXLAN EVPN sites, also support Layer-3 extension to the public cloud.

BGP-EVPN is used for the control plane between the BGWs and the Cisco Catalyst 8000Vs in the cloud, and VXLAN is used for the data plane.

As shown in the previous figure, the Cisco Hybrid Cloud Networking Solution consists of the following components:

- Cisco Nexus Dashboard Orchestrator (NDO): NDO acts as a central policy controller, managing policies across multiple on-premises fabrics managed by different NDFC instances, with each cloud site being abstracted by its own Cisco Cloud Network Controller. NDO runs as a service on top of Nexus Dashboard, where Nexus Dashboard can be deployed as a cluster of physical appliances or virtual machines running on VMware ESXi, Linux KVM, Amazon Web Services or Microsoft Azure. Inter-version support was introduced previously, so NDO can manage Cisco Cloud Network Controller running different software versions.
- Cisco Nexus Dashboard Fabric Controller (NDFC): NDFC is a network automation and orchestration tool for building LAN, VXLAN, SAN and Cisco IP Fabric for Media (IPFM) fabrics. NDFC runs as a service on top of Nexus Dashboard cluster that can be either a physical or a virtual cluster. For the Hybrid Cloud Networking Solution, NDFC manages the on-premises VXLAN fabric and on-premises Cisco Cloud Routers (Catalyst 8000V).
- **On-premises VXLAN fabric**: The on-premises VXLAN fabric is built with Nexus 90000/3000 switches managed by NDFC. The fabric should have one or more Border Gateway (BGW) devices that are responsible for originating and terminating VXLAN Multisite Overlay tunnels between on-premises and cloud sites. NDFC has pre-built templates for creating a VXLAN fabric; this document uses the External_Fabric template for the VXLAN fabric.

• On-premises Cisco Cloud Router (CCR): The CCR is used to provide reachability between the on-premises VXLAN fabric and the cloud sites. The CCR provides connectivity to the cloud sites using either public internet or private connections (such as AWS Direct Connect or Azure ExpressRoute). The on-premises CCRs are managed by NDFC using a pre-built External_Fabric template and need to be assigned the Core Router role.

The Cisco Catalyst 8000V is used as the on-premises CCR for the Cisco Hybrid Cloud Networking Solution.

- Cisco Cloud Network Controller (CNC): Cisco Cloud Network Controller runs as a virtual instance on a supported public cloud to provide automated connectivity, policy translation, and enhanced visibility of workloads in the public cloud. The Cisco Cloud Network Controller translates all the policies received from NDO and programs them into cloud-native constructs, such as VPCs and security groups on AWS, and VNets on Microsoft Azure. Cisco Cloud Network Controller is deployed through the public cloud Marketplace, such as AWS Marketplace and Azure Marketplace.
- Cisco Catalyst 8000V: The Cisco Catalyst 8000V is an important component in the public cloud platforms. Cisco Catalyst 8000Vs are used for inter-site communication to on-premises sites and the public cloud platforms. In addition, Cisco Catalyst 8000Vs are used for on-premises cloud connectivity and for connectivity between different cloud providers (for example, Azure to AWS).

Building Hybrid Cloud Connectivity

This section describes the process used to build hybrid cloud connectivity.

- Starting Point, on page 7
- Building the Underlay Layer, on page 8
- Building Overlay, on page 9

Starting Point

The following figure shows the starting point for the hybrid cloud connectivity, where we have the various pieces described in Understanding Components of Hybrid Cloud Connectivity, on page 5:

- Nexus Dashboard Fabric Controller (NDFC) fabrics:
 - On-premises VXLAN fabric
 - External fabric
- · Cloud sites (AWS and Azure) managed by Cloud Network Controller

Figure 2:



Building the Underlay Layer

Next, we will show how the underlay later is built:

- 1. First, a BGP connection is established between the border gateway spine switch in the VXLAN fabric and the Cisco Catalyst 8000V in the external fabric.
- 2. Then, BGP peering is used to establish the underlay connectivity between the on-premises Cisco Catalyst 8000V in the external fabric to each of the cloud routers in the cloud sites.
- 3. Finally, OSPF is used between the cloud sites for cloud-to-cloud underlay connectivity.

Figure 3:



Hybrid Cloud Connectivity Deployment for Cisco NX-OS

Building Overlay

Finally, we show how to establish the VXLAN Multisite Overlay on top of underlay connectivity established in previous step:

- 1. A VXLAN multi-site is established, which originates from the border gateway spine switch in the VXLAN fabric and terminates at the Cisco Catalyst 8000Vs in the cloud sites.
- 2. If you select Public Internet as the connection type, then IPsec and BGP are used to connect between the NDFC VXLAN fabric site and the cloud sites.

Figure 4:



Terminology

The following terms are used throughout this document.

Term	Acronym	Definition
Border Gateway	BGW	One of the supported switch roles in an NDFC Easy Fabric (for example, a VXLAN EVPN fabric). The BGW is used to extend Layer 2/Layer 3 DCI connectivity between on-premises fabrics and Layer 3 connectivity toward public cloud sites (for example, hybrid cloud connectivity).

Term	Acronym	Definition
Core Router		One of the supported roles in an NDFC external fabric.
		The core router is used to establish Layer 3 connectivity (Underlay) on one side with the VXLAN EVPN fabric, and on the other with the Catalyst 8000Vs in cloud sites.
Direct Connect		Used in the AWS cloud. AWS Direct Connect is a cloud service that links your network directly to AWS to deliver consistent, low-latency performance.
ExpressRoute		Used in the Azure cloud. You can use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on premises or in a co-location environment.
Inter-Site Network	ISN	The Layer 3 infrastructure used to interconnect on-premises VXLAN fabrics, between the on-premises VXLAN fabrics and with the public cloud (also referred to as the "underlay"). As such, the ISN could also include the Internet or the Direct Connect and ExpressRoute dedicated circuits.
IP Security Router	IPsec router	A router capable of Internet Protocol Security (IPsec) is required to establish IPsec connections between the on-premises site and the cloud sites Cisco Cloud Network Controller.

Term	Acronym	Definition
Route Server	RS	The control plane node used to facilitate the establishment of EVPN adjacencies between on-premises BGW devices, alleviating the need of creating full-mesh peering between all of them. The Route Server runs BGP protocol and is used to pass routes between two or more BGP peers.
		The Route Server function is the eBGP equivalent of the "Route Reflector" function traditionally used for iBGP sessions; it helps in reducing the number of BGP peering required.
Virtual Network	VNet	Used in the Azure cloud. Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VMs), to securely communicate with each other, the internet, and on-premises networks.
		As related to the Cloud Network Controller, the VRF in the Cloud Network Controller maps to a VNet in Azure.
Virtual Private Cloud	VPC	Used in the AWS cloud. Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
		As related to the Cloud Network Controller, the VRF in the Cloud Network Controller maps to a VPC in AWS.

Prerequisites

The following software versions are required:

- Cisco Nexus Dashboard (ND) version 2.3.1c or later (physical or virtual cluster)
- Cisco Nexus Dashboard Fabric Controller (NDFC) version 12.1.2e or later
- Cisco Nexus Dashboard Orchestrator (NDO) version 4.1(1) or later
- Cisco Cloud Network Controller (CNC) version 25.1(1e) or later for AWS site and Microsoft Azure site

Guidelines and Limitations

Following are certain guidelines and limitations that you should understand when deploying the hybrid cloud connectivity solution:

• Currently, each Cisco Cloud Network Controller can manage up to sixteen regions in AWS and Azure clouds. If you want to manage more than sixteen regions, you will have to deploy additional Cisco Cloud Network Controllers. For more information, see the "Understanding Limitations for Number of Sites, Regions and CCRs" section in the *Cisco Cloud Network Controller for AWS Installation Guide* or *Cisco Cloud Network Controller for Azure Installation Guide*, Release 25.1(x) or later.

Related Documentation

You can find documentation for the components that make up the Cisco Hybrid Cloud Networking Solution in the following locations:

- Cisco Nexus Dashboard Orchestrator (NDO) documentation
- Cisco Nexus Dashboard Fabric Controller (NDFC) documentation
- Cisco Cloud Network Controller (CNC) documentation
- Cisco Catalyst 8000V documentation
- Amazon Web Services (AWS) documentation
- Microsoft Azure documentation



Supported Topologies

- Connection Options, on page 13
- Supported Topologies with IPsec (Single-Cloud), on page 14
- Supported Topologies with IPsec (Multi-Cloud), on page 18
- Supported Topologies without IPsec (Single Cloud), on page 23
- Supported Topologies without IPsec (Multi-Cloud), on page 26

Connection Options

You can use these connection options for the Cisco Hybrid Cloud Networking Solution:

- With IPsec: If the connectivity from the on-premises data center to the cloud is over the public Internet, then an IPsec tunnel is required for establishing a secure channel. In this situation, the border gateway (BGW) will be connected to an on-premises IPsec-capable device, such as an ASR 1000 or a Cisco Catalyst 8000V. This device establishes IPsec tunnels with the Catalyst 8000Vs in the cloud. The on-premises BGWs can then leverage this "IPsec secured underlay" to build VXLAN tunnels with the Catalyst 8000Vs in the cloud.
- Without IPsec: If the BGWs are connected to the public cloud using Direct Connect (AWS) or ExpressRoute (Azure), then enabling IPsec is optional. In this case, a VXLAN connection is employed between the on-premises VXLAN EVPN data centers and the Cisco Catalyst 8000Vs on top of those dedicated circuits.

The following sections provide more detailed information on the supported topologies available using either of these connection options:

- Supported Topologies with IPsec (Single-Cloud), on page 14
- Supported Topologies with IPsec (Multi-Cloud), on page 18
- Supported Topologies without IPsec (Single Cloud), on page 23
- Supported Topologies without IPsec (Multi-Cloud), on page 26

Supported Topologies with IPsec (Single-Cloud)

The following table shows how BGP EVPN control plane adjacencies can be established between on-premises sites and on-premises to a cloud site, and how IPsec is leveraged to establish underlay connectivity between on-premises sites and a single cloud site.

Ŵ

Note

Each of the following figures show a simple example. In a real life scenario, there might be redundant devices deployed for each role.

BGP EVPN Between On-Premises Sites	BGP EVPN and IPsec to the	BGP EVPN and IPsec to the Cloud Site			
	Full-Mesh	Through Hub Site Only	 BGP EVPN to the Cloud Site: Full-Mesh IPsec to the Cloud Site: Through Shared IPsec Router Only 		
Full-Mesh	Option 1, on page 14	Option 3, on page 16	Option 5, on page 17		
With Route Server	Option 2, on page 15	Option 4, on page 17	N/A		

Option 1

- The BGW nodes on all the on-premises sites establish full-mesh BGP EVPN adjacencies between them.
- The Cisco Catalyst 8000V in the cloud site establishes IPsec tunnels with core routers deployed in each on-premises site and full-mesh BGP EVPN adjacencies with all the BGW devices on the on-premises sites.



Option 2

The following figure shows an example of a single-cloud connection using IPsec, where:

- The BGW nodes on all the on-premises sites establish BGP EVPN adjacencies with a Route Server (RS) control plane node.
- The Cisco Catalyst 8000V in the cloud site establishes full-mesh IPsec tunnels with core routers deployed in each on-premises site and BGP EVPN adjacencies with all the BGW devices on the on-premises sites.



Note It is currently not supported to peer the Cisco Catalyst 8000Vs with the Route Server control node.



The following figure shows an example of a single-cloud connection using IPsec, where:

- The BGW nodes on all the on-premises sites establish full-mesh BGP EVPN adjacencies between them.
- The Cisco Catalyst 8000V in the cloud site establishes an IPsec tunnel only with the core router deployed in a specific on-premises Hub Site and BGP EVPN adjacency only with the BGW device on the Hub Site.
- The BGW deployed in Site 2 (to which the Cisco Catalyst 8000V peers EVPN) cannot have a fabric behind it. It is only used to exchange prefixes between the on-premises and the cloud site.

Figure 7:



The following figure shows an example of a single-cloud connection using IPsec, where:

- The BGW nodes on all the on-premises sites establish BGP EVPN adjacencies with a Route Server control plane node.
- The Cisco Catalyst 8000V in the cloud site establishes an IPsec tunnel only with the core router deployed in a specific on-premises Hub Site and EVPN adjacency only with the BGW device on the Hub Site.
- The BGW deployed in Site 2 (to which the Cisco Catalyst 8000V peers EVPN) cannot have a fabric behind it. It is only used to exchange prefixes between the on-premises and the cloud site.

Figure 8:



Option 5

- The BGW nodes on all the on-premises sites establish full-mesh EVPN adjacencies between them.
- The Cisco Catalyst 8000V in the cloud site establishes full-mesh BGP EVPN adjacencies with all the BGW devices on the on-premises sites.
- The IPsec connection to the cloud site is through a shared IPsec router only.



Supported Topologies with IPsec (Multi-Cloud)

The following table shows how BGP EVPN control plane adjacencies can be established between on-premises sites and on-premises to cloud sites, and how IPsec is leveraged to establish underlay connectivity between on-premises sites and multiple cloud sites.

\$

Note

Each of the following figures show a simple example. In a real life scenario, there might be redundant devices deployed for each role.

BGP EVPN Between On-Premises Sites	n BGP EVPN and IPsec to the Cloud Sites			BGP EVPN and IPsec between Cloud Sites
	Full-Mesh	Through Hub Site Only	 BGP EVPN to the Cloud Site: Full-Mesh IPsec to the Cloud Site: Through Hub Site Only 	
Full-Mesh	Option 1, on page 19	Option 3, on page 20	Option 5, on page 22	Full-Mesh
With Route Server	Option 2, on page 19	Option 4, on page 21	N/A	

The following figure shows an example of a multi-cloud connection using IPsec, where:

- The BGW nodes on all the on-premises sites establish full-mesh BGP EVPN adjacencies between them.
- The Cisco Catalyst 8000Vs in the cloud sites establish IPsec tunnels with core routers deployed in each on-premises site and full-mesh EVPN adjacencies with all the BGW devices on the on-premises sites.
- The Cisco Catalyst 8000Vs in different cloud sites establish full-mesh IPsec tunnels and EVPN adjacencies between them.

Figure 10:



Option 2

- The BGW nodes on all the on-premises sites establish BGP EVPN adjacencies with a Route Server control plane node.
- The Cisco Catalyst 8000Vs in the cloud sites establish IPsec tunnels with core routers deployed in each on-premises site and full-mesh BGP EVPN adjacencies with all the BGW devices on the on-premises sites.
- The cloud routers peer BGP EVPN with the BGW on the Hub Site.



- The BGW nodes on all the on-premises sites establish full-mesh EVPN adjacencies between them.
- The Cisco Catalyst 8000Vs in the cloud sites establish IPsec tunnels only with the core router deployed in a specific on-premises Hub Site and EVPN adjacency only with the BGW device on the Hub Site.
- The Cisco Catalyst 8000Vs in different cloud sites establish full-mesh IPsec tunnels and EVPN adjacencies between them.
- The BGW deployed in Site 2 (to which the Cisco Catalyst 8000V peers EVPN) cannot have a fabric behind it. It is only used to exchange prefixes between the on-premises and cloud sites.



Option 4

- The BGW nodes on all the on-premises sites establish BGP EVPN adjacencies with a Route Server control plane node.
- The Cisco Catalyst 8000Vs in the cloud sites establish IPsec tunnels only with the core router deployed in a specific on-premises Hub Site and BGP EVPN adjacency only with the BGW device on the Hub Site.
- The cloud routers peer BGP EVPN with the BGW on the Hub Site.
- The BGW deployed in Site 2 (to which the Cisco Catalyst 8000V peers EVPN) cannot have a fabric behind it. It is only used to exchange prefixes between the on-premises and cloud sites.



- The BGW nodes on all the on-premises sites establish full-mesh EVPN adjacencies between them.
- The Cisco Catalyst 8000V in the cloud sites establishes full-mesh BGP EVPN adjacencies with all the BGW devices on the on-premises sites.
- The Cisco Catalyst 8000Vs in the cloud sites establish IPsec tunnels only with the core router deployed in a specific on-premises Hub Site.
- The Cisco Catalyst 8000Vs in different cloud sites establish full-mesh IPsec tunnels and EVPN adjacencies between them.

L



Supported Topologies without IPsec (Single Cloud)

The following table shows how BGP EVPN control plane adjacencies can be established between on-premises sites or on-premises to a cloud site.

BGP EVPN Between On-Premises Sites	BGP EVPN to the Cloud Site	
	Full-Mesh	Through Hub Site
Full-Mesh	Option 1, on page 23	Option 3, on page 24
With Route Server	Option 2, on page 24	Option 4, on page 25



Note Each of the following figures show a simple example. In a real life scenario, there might be redundant devices deployed for each role.

Option 1

The following figure shows an example of a single-cloud connection without IPsec, where:

- The BGW nodes on all the on-premises sites establish full-mesh BGP EVPN adjacencies between them.
- The Cisco Catalyst 8000V in the cloud site establishes full-mesh BGP EVPN adjacencies with all the BGW devices on the on-premises sites.



The following figure shows an example of a single-cloud connection without IPsec, where:

- The BGW nodes on all the on-premises sites establish BGP EVPN adjacencies with a Route Server (RS) control plane node.
- The Cisco Catalyst 8000V in the cloud site establishes full-mesh BGP EVPN adjacencies with all the BGW devices on the on-premises sites.

Figure 16:



Option 3

The following figure shows an example of a single-cloud connection without IPsec, where:

- The BGW nodes on all the on-premises sites establish full-mesh BGP EVPN adjacencies between them.
- The Cisco Catalyst 8000V in the cloud site establishes a BGP EVPN adjacency only with the BGW device on the Hub Site.
- The BGW deployed in Site 2 (to which the Cisco Catalyst 8000V peers EVPN) cannot have a fabric behind it. It is only used to exchange prefixes between the on-premises and the cloud site.

Figure 17:



Option 4

The following figure shows an example of a single-cloud connection without IPsec, where:

- The BGW nodes on all the on-premises sites establish BGP EVPN adjacencies with a Route Server control plane node.
- The Cisco Catalyst 8000V in the cloud site establishes a BGP EVPN adjacency only with the BGW device on the Hub Site.
- The BGW deployed in Site 2 (to which the Cisco Catalyst 8000V peers EVPN) cannot have a fabric behind it. It is only used to exchange prefixes between the on-premises and the cloud site.



Supported Topologies without IPsec (Multi-Cloud)

The following table shows how BGP EVPN control plane adjacencies can be established between on-premises sites or on-premises to cloud sites.

BGP EVPN Between On-Premises Sites	BGP EVPN to the Cloud S	BGP EVPN between Cloud Sites	
	Full-Mesh Through Hub Site		
Full-Mesh	Option 1, on page 26	Option 3, on page 28	Full-Mesh
Route Server	Option 2, on page 27	Option 4, on page 28	

Ŵ

Note Each of the following figures show a simple example. In a real life scenario, there might be redundant devices deployed for each role.

Option 1

- The BGW nodes on all the on-premises sites establish full-mesh BGP EVPN adjacencies between them.
- The Cisco Catalyst 8000Vs in the cloud sites establish full-mesh BGP EVPN adjacencies with all the BGW devices on the on-premises sites.
- The Cisco Catalyst 8000Vs in different cloud sites establish full-mesh BGP EVPN adjacencies between them.



The following figure shows an example of a multi-cloud connection without IPsec, where:

- The BGW nodes on all the on-premises sites establish BGP EVPN adjacencies with a Route Server control plane node.
- The Cisco Catalyst 8000Vs in the cloud sites establish full-mesh BGP EVPN adjacencies with all the BGW devices on the on-premises sites.
- The Cisco Catalyst 8000Vs in different cloud sites establish full-mesh BGP EVPN adjacencies between them.

Figure 20:



The following figure shows an example of a multi-cloud connection without IPsec, where:

- The BGW nodes on all the on-premises sites establish full-mesh BGP EVPN adjacencies between them.
- The Cisco Catalyst 8000Vs in the cloud sites establish BGP EVPN adjacencies only with the BGW device on the Hub Site.
- The Cisco Catalyst 8000Vs in different cloud sites establish full-mesh BGP EVPN adjacencies between them.
- The BGW deployed in Site 2 (to which the Cisco Catalyst 8000V peers EVPN) cannot have a fabric behind it. It is only used to exchange prefixes between the on-premises and cloud sites.

Figure 21:



Option 4

- The BGW nodes on all the on-premises sites establish BGP EVPN adjacencies with a Route Server control plane node.
- The Cisco Catalyst 8000Vs in the cloud sites establish BGP EVPN adjacencies only with the BGW device on the Hub Site.
- The Cisco Catalyst 8000Vs in different cloud sites establish full-mesh BGP EVPN adjacencies between them.
- The BGW deployed in Site 2 (to which the Cisco Catalyst 8000V peers EVPN) cannot have a fabric behind it. It is only used to exchange prefixes between the on-premises and cloud sites.




CHAPTER -

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 31
- Set Up the On-Premises NDFC Fabrics, on page 32
- Deploy Cloud Network Controller on Cloud Sites, on page 49
- Onboard the NDFC and Cloud Sites into ND and NDO, on page 62
- Complete Site-to-Site Connectivity Between NDFC and Cloud Sites, on page 69

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 23:



The procedures in this document will use this topology as a specific use case, which is based on Option 1, on page 19 in Supported Topologies with IPsec (Multi-Cloud), on page 18, 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 25:



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 26:

abric Name	
sydney	
Pick Template	
asy_Fabric >	
General Parameters Replication VPC Protocols A	dvanced 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	V Numbered(Point-to-Point) or Unnumbered
Underlay Subnet IP Mask*	
30	V Mask for Underlay Subnet IP Range
Underlay Subnet IPv6 Mask	
Select an Option	V Mask for Underlay Subnet IPv6 Range
Underlay Routing Protocol*	
ospf	Used for Spine-Leaf Connectivity
Route-Reflectors*	
2	V 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 27:

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\$\$VIAN\$\$VLAN_ID\$\$	Generated network name should be < 64 characters
General Parameters Replication VPC Protocols Adva	nced Resources Manageability Bootstrap	Enable CDP for Bootstrapped Switch	Enable CDP on management interface
VRF Template* Default_VRF_Universal	Default Overlay VRF Template For Leafs	Enable VXLAN OAM	Enable the Next Generation (NG) OAM feature for all switches in the fabric to aid in trouble-shooting VXLAN EVPN fabrics
Network Template* Default_Network_Universal	Default Overlay Network Template For Leafs	Enable Tenant DHCP	
VRF Extension Template* Default_VRF_Extension_Universal	Default Overlay VRF Template For Borders	Enable NX-API on HTTP port	Enable NX-API on port 443
Network Extension Template* Default_Network_Extension_Universal	Default Overlay Network Template For Borders	Enable Policy-Based Routing (PBR)	Enable NX-API on port 80
Overlay Mode	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 28:

		Layer 2 VXLAN VNI Range*	
		30000-49000	Overlay Network Identifier Range (Min:1, Max:16777214)
		Layer 3 VXLAN VNI Range*	
		50000-59000	Overlay VRF Identifier Range (Min:1, Max:16777214)
		Network VLAN Range*	
Fabric Name		2300-2999	Per Switch Overlay Network VLAN Range (Min:2, Max:4094)
sydney		VRF VLAN Range*	
Pick Template		2000-2299	Per Switch Overlay VRF VLAN Range (Min:2, Max:4094)
Easy_Fabric >		Subinterface Dot1q Range*	
General Parameters Denlication V/DC Protocols Ad	vanced Desources Manareability Bootstran	2-511	Per Border Dot1q Range For VRF Lite Connectivity (Min:2, Max:4093)
		VRF Lite Deployment*	
Manual Underlay IP Address Allocation		Manual ~	VRF Lite Inter-Fabric Connection Deployment Options
	Checking this will disable Dynamic Underlay IP Address Allocations	Auto Deploy Both	
Hadaday Davis I aankaali ID Davaat			Whether to auto generate VRF LITE sub-interface and BGP
			created VRF Lite IFC links will have 'Auto Deploy Flag' enabled.
20.2.0.0/22	Typically Loopback0 IP Address Hange	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	VIDE Line Outputs Marshit	
Useladas DD Lasarkask ID Dassat		VRF Lite Subnet Mask*	
		30	(Minos, MaxC31)
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 37.

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 33.

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 29:

Iney		172.16.0.67-68,172.16.0	0.76	MD5	admin			
sword Set		Max Hops 2		Preserve config Disabled				
ick								
covery Results								
ilter by attributes								
Switch Name	Serial Number	IP Address	Model	Version	Status	Progress		
10.18.1.2		10.18.1.2	cisco C8000V	17.7.1a,				
ndfc-spine1	FD0243503ZG	172.16.0.76	N9K-C9332C	9.3(9)	Manageable			
ndfc-leaf2	FD02442054U	172.16.0.68	N9K-C9348GC-FXP	9.3(9)	Manageable			
ndfc-leaf1	FD02442051Z	172.16.0.67	N9K-C9348GC-FXP	9.3(9)	Manageable			
leaf1	96O0UQZJFTJ	172.16.0.77	N9K-C9300v	9.3(9)	Already Managed In Vsite1			
leaf2	97UVLYWGPAN	172.16.0.78	N9K-C9300v	9.3(9)	Already Managed In Vsite1			
spine1	95INZNPCD1D	172.16.0.79	N9K-C9500v	9.3(9)	Already Managed In Vsite1			
ACI-TA-SW	FOC1752R19H	172.16.0.3	N6K-C6001-64P	7.1(4)N1(1)	Manageable			
bgw2	91P6JV6YK6U	172.16.0.83	N9K-C9300v	9.3(9)	Manageable			
aci-tme-lab-mgmt	SAL184436V9	172.16.0.50	N9K-C9372PX	9.3(9)	Manageable			
10 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 30:

Switch IP Address Role Serial Number Config Status Oper Status Discovery Status Model VPC Role VPC Peer Add Switch ndfc-leaf1 172.16.0.67 Leaf FD024420512 In-Sync O Minor O K N9K-C9348GC-FXP Secondary ndfc-leaf2 Discovery ndfc-leaf2 172.16.0.68 Leaf FD02442054U In-Sync O Minor O K N9K-C9348GC-FXP Primary ndfc-leaf1 Discovery ndfc-leaf2 172.16.0.68 Leaf FD02442054U In-Sync O Minor O K N9K-C9348GC-FXP Primary ndfc-leaf1 Discovery ndfc-leaf2 172.16.0.68 Leaf FD02442054U In-Sync O Minor O K N9K-C9348GC-FXP Primary ndfc-leaf1 Discovery ref Total Leaf FD02442054U In-Sync O Minor O K N9K-C9348GC-FXP Primary ndfc-leaf1 Discovery												
Switch IP Address Role Serial Number Config Status Oper Status Discovery Status Model VPC Role VPC Peer Add Switch ndfc-leaf1 172.16.0.67 Leaf FD024420512 In-Sync C Minor O K N9K-C9348GC-FXP Secondry ndfc-leaf2 Discovery Discovery Secondry ndfc-leaf2 Discovery N9K-C9348GC-FXP Private Deploy Discovery T22.16.0.68 Leaf FD024420512 In-Sync O Minor O O K N9K-C9348GC-FXP Private Discovery Discovery T22.16.0.68 Leaf FD02442054U In-Sync O Minor O O K N9K-C9348GC-FXP Private Discovery	er by	attributes										Action
ndic-leaf1 172.16.0.67 Leaf FD024420512 In-Sync © Minor O K N9K-C9348GC-FXP Secondary ndic-leaf2 Deploy ndic-leaf2 172.16.0.68 Leaf FD02442051U In-Sync © Minor O K N9K-C9348GC-FXP Primary ndic-leaf2 Deploy ndic-leaf2 172.16.0.68 Leaf FD0244205UU In-Sync © Minor O K N9K-C9348GC-FXP Primary ndic-leaf2 Discovery	s	Switch	IP Address	Role	Serial Number	Config Status	Oper Status	Discovery Status	Model	VPC Role	VPC Peer	Add Switche
Indic-teal2 172.16.0.68 Leaf FD02442054U In-Sync ID Minor ID X N9K-C93480C-FXP Primary Indic-teal1 Discovery Interview Set Discovery Discovery Set Role Set Role	n	dfc-leaf1	172.16.0.67	Leaf	FD02442051Z	In-Sync	O Minor	Ok	N9K-C9348GC-FXP	Secondary	ndfc-leaf2	Preview
Set Role] n	dfc-leaf2	172.16.0.68	Leaf	FDO2442054U	In-Sync	Minor	• Ok	N9K-C9348GC-FXP	Primary	ndfc-leaf1	Discovery
		dfc-enine1	172 16 0 76	Spine	ED024350376	In-Sync	C Mir Spine	O Ch	N9K-C9332C			Set Role

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

Figure 31:

Select Role	×
् 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 32:

Fab	ic Overview	- sydney								Actions A	0? -
Overv	ew Switches Links	s Interfaces Interfac	e Groups Poli	cies Networks \	/RFs Services E	vent Analytics His	tory Resources Vit	tual Infrastructure	Edit Adv	Fabric I Switches	
FB	er by attributes								Rec	e >	Actions ~
	Switch	IP Address	Role	Serial Number	Config Status	Oper Status	Discovery Status	Model	VPC Role	VPC Peer	Mode
	ndfc-leaf1	172.16.0.67	Leaf	FDO2442051Z	In-Sync	O Minor	• Ok	N9K-C9348GC-FXP	Secondary	ndfc-leaf2	Normal
	ndfc-leaf2	172.16.0.68	Leaf	FDO2442054U	In-Sync	O Minor	• Ok	N9K-C9348GC-FXP	Primary	ndfc-leaf1	Normal
	ndfc-spine1	172.16.0.76	Border Gaterway Spine	FDO2435032G	• in-Sync	O Minor	Ok	N9K-C9332C			Normal

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 33:

L

viev	w Switches Link	s Interfaces Interfac	e Groups Poli	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	FD02442054U	 In-Sync 	♥ Minor	Ok	N9K-C9348GC-FXP	Primary	ndfc-leaf1	Normal
	ndfc-spine1	172.16.0.76	Border Gateway Spine	FDO243503ZG	In-Sync	Minor	• Ok	N9K-C9332C			Normal
			-								

What to do next

Configure an NDFC external fabric using the procedures provided in Configure an NDFC External Fabric, on page 41.

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 34:



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 33 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 35:

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

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 36:

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 44.

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 42

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 37:

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 38:

dd Switches						?
Switch Addition Mechanism* O Discover O Move Neighbor	r Switches					
Seed Switch Details Fabric ext-fab-1		Switch 172.16.0.234		Authentication Protocol MD5	Username admin	9
Password Set		Max Hops 0		Preserve config Enabled		
E Back Discovery Results						
Filter by attributes						
C8K3-Fab2	Serial Number 98JE1U8CZ8M	IP Address 172.16.0.234	C8000V	Version 17.7.1a	Manageable	Progress

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

Figure 39:

Add S	Switches								? ×
Switch	Addition Mechanism* cover O Move Neighbor Sv	witches							
Seed Switch Details Fabric ext-fab-1			Switch 172.16.0.234		Authentication Protocol		Username admin		
Pass • S	word et	M	ax Hops	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 40:

oric	c Overview - e	ext-fab-1								Actions ~	ð?·
rview Switches Links Interfaces Policies Event Analytics History Resources Virtual Infrastructure											
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 41:

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 42:

Fabric Overview - ext-fab-1 CActions 🔿 🔿 ? -									● () ? - >		
verview Switches Links Interfaces Policies Event Analytics History Resources Virtual Infrastructure											
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	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 43:

≡ cisco Nexus Dashbo:	ard 🕴 🕀 One	View ~				Feedback 👤 (
F Fabric Controller										
n Dashboard		abrics				G				
in the second s		00103				e				
	Filter by	attributes				(Actions ~)				
Fabrics		Pakala Nama	Patrola Tanto a la su	Palada Tara	401	Tabala Usadh				
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 44:



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 45:

≡ cisco Nexus Dashboard	🔅 One Viev 🗸
Fabric Controller	
🎓 Dashboard	💿 Data Center / 🔿 Sydney
¥ Topology	View A Search by Attributes
I LAN ^	$(+ - 2 \circ \mathbb{R})$
Fabrics	Show Logical Links
Switches	Operation Configuration
Interfaces	Networks (0) VRFs (0) VM (3)
Services	Hierarchical
📥 Virtual Management 🗸 🗸	In-Sync
☆ Settings ∨	Pending
🖈 Operations 🗸	In Progress Out-of-Sunc
	 NA
	Multi-select O 0 selected
	ndtc-leat2 ndtc-leat1

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 49.

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 (²) 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 52.

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 50.

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 47:

ht				
Regions to Manage	2 General Co) nnectivity		
Eerun Claat Tetera Costrate Oro-Prentises ACI Site	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 (Sociholm) EU Sociholm) 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 48:

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 49:

Add Hub Network		×
Name *		
hub1		
BGP Autonomous System Number *		
65091		
TGW Connect		
Enable		
Changing the use of TGW Connect w	ill cause temporary traffic loss.	
CIDR		
Region *	CIDR *	
US West (Oregon)	176.16.11.0/24	/ 11
Add CIDR		
TGW Route Table Association Labels 🌒		
Name *		
Add TGW Route Table Association Label		
		Add

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 56.

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 50.

- **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 (²) 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 57.

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 56.

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 50:

Setup - Region N	lanagement		
	i Please note that CSR is now changed to Catalyst 8000	V.	
	Connectivity for Internal Network VNet Peering		
	Regions to Manage * 🕲		
	Region Name	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 India	centralindia	
	Central US	centralus	
	East Asia	eastasia	
	East US	eastus 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 51:

Setup - Region Management				
External Cloud Network Controller	ACI Site	Inter-Site Connectivity -		R Catalyst 8000V
Configure the fabric infra connection the configuration template used	ectivity for the Cloud S d for the Cloud Routers is now changed to Cat	ite. The Fabric Autonomous Sy in the Cloud Site. alyst 8000V.	stem Number is use	d for BGP peering insid
General				
Subnet Pools for Cloud Ro	outers 📵			
Subnet *	Regions	Created By		
10.90.0.0/24		System Internal	8	
10.90.1.0/24		User	8	
+ Add Subnet Pool for	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 52:

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 62.

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 33.
- Create the NDFC external fabric using the procedures provided in Create an NDFC External Fabric, on page 42.
- 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 50.
- 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 56.
- **Step 1** Log into the Nexus Dashboard (ND) cluster with Nexus Dashboard Orchestrator (NDO).
- Step 2 In Nexus Dashboard, click Sites > Add Site.

Figure 53:

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 _o	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 54:

≡ disco Nexus Dash	nboard 🤅) One View \vee				Feedback
Admin Console	C fab2no	d2				0 0 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 down Dasword * O unum Ensistent Direct Block Sites Bis Name Greets Block Sites Market Dasks Name Add Security Domains Name Add Security Domains Name Add Security Domains Name	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 55:

	O 1652nd2					0 (
a Overview	-					
S Sites						
		Site Type				
G Gystein Resources						۲
Coperations		ACI		Cloud Network Controller	NDFC	
iofrastructure			Select		×	
		Prescharting in scores Prescharting in scores Heatmannel® Address T216119 Username Pressent • ① Inter Login Domain ① Inter Itses	Control Contro	No teen solicited Select the For Crain		
					Cancel 200	
		O Select Sites				
		Add Security 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
Add Site page, then click Save.
- **Step 8** In Nexus Dashboard, click **Sites** > **Add Site** again to add the first cloud site.

Figure 56:

≡ cisco Nexus	Dashboa	ard 🛛 🗐 o Admin Console 🗸					Feed	back 1 O
= Admin Conso	le	G fab2nd2					0	00
G Overview		Sites						0
III Services		Filter by attributes						Add Site
E/ System Resources		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
C Infrastructure		A Minor	Sydney	NDFC	(O up	12.1.2.275	0	
\underline{x}° Administrative		Ø Healthy	ext-fab-1	NDFC	(qU (Q)	12.1.2.275	0	
		10 ~ Rows					Page 1 of 1 << < 1-2	l of 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 57:

≡ cisco Nexus Dashbo	oard 🛛 🍈 One View 🗸		
	G fab2nd2		01
Overview Sites	4 Sites		
III Services	Site Type		
 <i>⊕</i> System Resources ∨ □ Operations ∨ 	ACI	Cloud Network Controller	
◯ Infrastructure ~			
\underline{r}° Administrative \lor	General		
	Name *		
	Settings		
	Hostname/IP Address *		
	Username • ① admin Reserved • ①		
		•	
	Login Domain ⊙		
	Enable Proxy		
	Name		
	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 58:

≡ cisco Nexus Das	hboard	a Admin Console					Ŕ	iedzack 🛓 🛙
	G	fab2nd2					C	
Overview Sites		Sites						0
III Services		Filter by attributes						Add Site
 System Resources Descriptions 		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
C Infrastructure		<u>(А</u> марог)	AWS	Cloud Network aws	(@u@)	25.1(te)	0	
<u>1</u> ° Administrative		金 Minor	Sydney	NOFC	(@up)	12.1.2.275	0	
		Ø Healthy	ext-fab-1	NDFC	(Qup)	12.1.2.275	0	
		Tax shares						
		10 V Rows					Page 1 of 1 << <	1-3 of 3 2 22

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 59:

≡ cisco Nexus Dash	iboard 🕴 🕀	One View ~						Feed
	G fab2nd	2						0
Overview Sites	Sites							
III Services		Site Type						
System Resources				20128 N.B	۲			
El Operations		ACI	Cloud Ne	twork Controller		NDFC		
O Infrastructure								
1º Administrative		General						
		Name *						
		Azure						
		Settings						
		Hostname/IP Address *						
		Username • 🕢						
		admin						
		Password • 🕢						
		Logia Domain						
		Login bolilain ()						
		Enable Proxy						
		Security Domains						
		Name						
		Add Security Domains						
							ſ	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 60:

≡ diniji. Cisco Nexu	s Dashboar	d 🕼 🔒 Admin Console	×					Feedback 💄 📀
	ole	G fab2nd2						Ø 🖪 🖸
Overview Sites		Sites						٥
III Services		Filter by attributes						Add Site
 System Resources Operations 		Health Score	Name	Туре	Connectivity Status	Firmware Version	Services Used	
C Infrastructure		A Major	Azure	Cloud Network Controller	(⊘ Up	T 25.1(1e)	o	
<u>⊥</u> ⁰ 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 61:

Ξ	cisco Nexus Dashboard	🔅 One View 🔿	Feedback 💄 💿
	One view	Dne View	
	My Sites	Admin Console	Map Table
0		Onceased particular Some association of the service in one one Total association Total association Total association	+ _

Step 15 In NDO, click Sites.

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

Figure 62:

≡ disco Nexus Dashb	ioard 🔶 🌲 Orchestrator 🗸			일 기가 가 주요		Feedback 💄 🔊
 Dashboard Sites 	Sites					0 ()
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
 Infrastructure 	⊘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 63*:

Dashboard	Sites					
Sites						0 1
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
Operations Infrastructure	⊘ок	AWS	🥥 AWS	Unmanaged ~	25.1(1e)	
Integration	⊘ок	Azure	Azure	Managed ~	25.1(1e)	
	⊘ок	ext-fab-1	NDFC	Unmanaged 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 64:

≡ ^{•• ••• ••} Nexus Dasht	ooard 🔶 Orchestrator 🗸					Feedback 💄 🕐
a Dashboard	Sites					
Sites						
CE Application Management						
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
 O Infrastructure 	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 65:

≡ "cisco" Nexus Dashbo	oard 🏩 Orchestrator 🗸					Feedback 💄 ೨
Dashboard Sites	Sites					65 (0
Application Management	Filter by attributes					
Fabric Management	Controller Connectivity	Name	Туре	State	Version	
 Operations O Infrastructure 	⊘ок	AWS Site ID: 91	o aws	Managed	25.1(1e)	
Ø Integration	ØОК	Azure Site ID: 92	Azure	Managed	25.1(1e)	
	ØОК	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

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 69.

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 62.

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

Figure 66:

≡ distlin cisco Nexus Dash	board 🔔 Orchestrator 🗸					Feedback 💄 💿
 Dashboard Sites 	Sites					0 83
Application Management Entric Management	Filter by attributes					
	Controller Connectivity	Name	Туре	State	Version	
 Infrastructure 	Infrastructure	AWS Site ID: 91	🤤 AWS	Managed	~ 25.1(1e)	
@ Integration	System Configuration	Azure Site ID: 92	Azure	Managed	~ 25.1(1e)	
	OUX.	ext-fab-1 Site ID: 80	NDFC	Managed	√ 12.1.2.275	
	⊘ок	Sydney Site ID: 82	NDFC	Managed	× 12.1.2.275	
	10 V Rows				Page 1] of 1 $\ll <1\text{-4 of }4\!>\!\gg$

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 67:

≡ داندان دisco Nexus Dashboar	d 🔄 👲 Orchestrator 🗸	Feedback 💄
 Dashboard Sites 	Site Connectivity	्रि 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 68:

— 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, on page 13 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, on page 19 topology in Supported Topologies with IPsec (Multi-Cloud), on page 18, 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 71.

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 69.

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

Figure 69:

≡ 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.

F :		70.
FIQ	ure	<i>IU</i> :

≡ disco 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 71:

≡ داندان داندوه Nexus Dasi	nboard Archestrator V
Site Connectivity	
	Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDFC Settings
	On Premises IPsec Devices
	Name Type IP Address Next Hop Address Add On Premises IPsec Device IPsec Device IPsec Device IPsec Device
• • Azure	Add On Premises IPsec Device ×
• • ext-fab-1	Type Unmanaged Managed
 Sydney 	Site * 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.

119410 72.

site connectivity		
	Control Diana Configuration On Bramileos (Base Devices	Externel Daviane - IDean Tunnel Subart Deale - NDEC Settings
	Control Plane Configuration Of Premises (Psec Devices	External Davices (rsec runner subner Pools NDPC settings
	On Premises IPsec Devices	
		Add On Premises IPsec Device ×
	Name Type IP Address	
	Add On Premises IPsec Device	Туре
 Azure 		Unmanaged Managed
		Site *
		extra0-1
👳 🌑 ext-fab-1		ASN
		00000
		Device *
🐐 🌒 Sydney		Cok3-Pa02
		Interface *
		GigabitEthernet2
		IP Address
		04.104.200.12
		Next Hop Address *
		04.104.200.1

- 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 73:

≡ "lisco" Nexus Dasht	ooard 🔔 Orchestrator 🗸
Site Connectivity	
SETTINGS	Control Plane Configuration On Premises IPsec Devices External Devices IPsec Tunnel Subnet Pools NDEC Settings
General Settings	
SITES	External Subnet Pool \odot
• O AWS disabled	IP Address 169.254.0.0/16
• Azure	Add IP Address
◦ ● ext-fab-1	Site Specific Subnet Pool Name IP Address
🔹 🌘 Sydney 🥥	Add Site Specific Subnet Pool

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 74:

≡ 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 75:*

SETTINGS				NDEO Osti
General Settings		Control Plane Configuration On Premises IPsec Devices External Devi	res insec lunnel Subnet Pools	NDFC Settings
SITES		External Subnet Pool 💿		
🔹 🤤 AWS		IP Address 🝈		
disabled	0	169.254.0.0/16		
💿 🙆 Azure		170.1.0.0/16	< 11 m	
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 76:

≡ divition Nexus Dashboard A Orchestrator ∨						
Site Connectivity						
SETTINGS	Control Diana Configuration On Dramicae IDeac Davicae External Davicae IDeac Tunnal Subnat Doole NDEC Sattinge					
General Settings						
SITES	NDFC Settings					
O AWS disabled	Layer 2 VXLAN VNI Range 130000-149000					
🔹 🔕 Azure	Layer 3 VXLAN VNI Range 150000-159000					
disabled	Multi-Site Routing Lookback IP Range 10.10.0.024					
◦ ● ext-fab-1	Anycast Gateway MAC 2020.0000.00aa					
🔹 🌢 Sydney 🥥	Auto Route Target Prefix * 23456 Mapped 1-PONDS					
	Advanced Settings V					

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 78.

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 71.

- **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 77:

L

≡ cisco Ne	xus Dashbo	ard 🙏 Orchestrator			Fe	edback 上 🧿
Site Connect	ivity				DEPLOY V) @ <i>t</i> } X
SETTINGS			0 (C8K3-Fab2		
General Settings		Site ext-fab-1				
SITES		Core Router C8K3-Fab2	critical	major	minor	warning
o O AWS	0		Ports	net Port ID		
o Azure disabled	Ø		O Ado	Port		
💿 🌘 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, on page 20 in Supported Topologies with IPsec (Multi-Cloud), on page 18, 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 83.

Figure 78:

Add Port		×
Ethernet Port ID *		
GigabitEthernet4	\times \checkmark	
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 () BGP Authentication None Simple Cisco		
Towards Cloud Router 🕢		
BFD Enabled		
		Ok
lick Ok 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 80.

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 78.

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 3** In 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 79:

≡ ^{••} li••li• cisco Nexus Dashboa	rd 🌲 Orchestrator 🗸	Feedback 1 🕑
Site Connectivity		DEPLOY V O() X
SETTINGS		Sydney Settings
General Settings	Refresh	C Sydney Security S
SITES	Switch_ndfe-spine1	Inter-Site Connectivity
🔹 🤤 AWS		General A
disabled		82 Multi-Site VID
💌 🔕 Azure		10.10.0.1 Auto Allocate
disabled		IPsec Device () Name Device ID IP Address
 ext-fab-1 		Add IPsec Device
 Sydney 		

What to do next

Follow the procedures provided in Map the IPsec Device to the VXLAN Fabric Site, on page 81.

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 80.

- 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 80:

≡ disco Nex	us Dashbo	ard 🛛 🙏 Orchestrator ->	Feedback 1 0
Site Connecti	vity		DEPLOY ~ O(1 X
SETTINGS			Sydney Settings
General Settings		Site Sydney Refresh	
SITES		Switch ndfc-spine1	Inter-Site Connectivity
g Gisabled	Ø		General A
disabled	Ø		Mutti-Site VIP 10.10.0 1 IPsec Device ①
💿 🌘 ext-fab-1	Ø		Name Device ID IP Address Add IPsec Device
😦 🌘 Sydney	0		

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

Figure 81:

≡ cisco Ne	xus Dashb	aard 🌐 🙏 Orchestrator 🗸	Feedba	ick 上 🛛
Site Connect	ivity		DEPLOY V	× €3€
SETTINGS			Svdnev Settings	0
General Settings		Site Sydney Refresh		0
SITES		Switch ndfc-spine1	Inter-Site Connectivity	
e 🤤 AWS	0		General Site ID 82	^
e O Azure	0		Multi-Site VIP 10.10.0.1 IPsec Device	to Allocate
🔹 🌒 ext-fab-1	0		Name Device ID IP Address	~ 1
Sydney	0		C8K3-Fab2	

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

Figure 82:

≡ cisco Ne	kus Dashboa	rd 🗶 Orchestrator 🗸	Feedback 🛓 🕐
Site Connect	ivity		DEPLOY V Oth X
SETTINGS General Settings		Sha Suday	• Sydney Settings ①
SITES	0	Switch ndfc-spine1	Inter-Site Connectivity General
disabled a Azure disabled	0		Ster ID 82 Multi-Site VIP 10.10.0.1 Auto Allocate IPsec Device ()
🧧 🌒 ext-fab-1	0		Name Device ID IP Address C8K3- 98JE1U8CZ8M 64.104.255.12
 Sydney 	Ø		Add IPee Device

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 83.

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 81.

- 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 83:

≡ cisco Ne	kus Dasht	pard 🗶 Orchestrator 👳			Fe	edback 上 📀
Site Connect	ivity				DEPLOY V	0€3 X
SETTINGS			⊽ n	dfc-spine1		
General Settings		Refresh Refresh	_			
SITES		Switch ndfc-spine1	critical	major	minor	warning
e 🤤 AlWS	0		BGP-EV 20.2.0	PN ROUTER-ID 3		
🔹 🔕 Azure			BGW PI	4		
disabled	0		Ports	- Part ID		
e ext-fab-1	0		Add	Port		
	~					
 Sydney 						

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

Figure 84:

≡ cisco Nexus Da	ishboard 🙏 Crohestrator 🗸						Feed	back 1 9
Site Connectivity						D	EPLOY V	× 13@
					o nd	fc-spine1		
	Site Sydney	Add Port	×	Refresh				- warning
	Switch ndfc-spine1	Ethernet Port ID • Ethernet1/32 × V			BGP-EVP 20.2.0.3			
e O Azure disabled		IP Address * 10.140.1.2/30 Description towards on-prem C8Ky Gi-4			BGW PIP 20.3.0.4 Ports			
🔹 🔮 ext-fab-1		Remote Address * 10.140.1.1 Remote ASN *			Add Po			
Sydney		65080 ‡ MTU * 9216						
		BOP Authentication Portantia Simple Towards Goud Router BFO Enabled						

- 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, on page 20 in Supported Topologies with IPsec (Multi-Cloud), on page 18.

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 85:

ite Connecti	vity					DEPLOY V) @t} ×
ETTINGS				⊕ n	dfc-spine1		
eneral Settings		Site Sydney	Refresh				
res		Switch ndfc-spine1		critical	major	minor	warning
AWS disabled	0			BGP-EV 20.2.0	PN ROUTER-ID		
Azure disabled	Ø			BGW PI 20.3.0 Ports	P .4		
ext-fab-1	0			Ethen Ethen	net Port ID net1/32 Port		/
Sydney	0						

What to do next

Follow the procedures provided in Connect the First Cloud Site to the NDFC VXLAN Fabric Site, on page 85.

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 83.

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 86:

Site Connecti	vity		DEPLOY V Oti
SETTINGS			AWS Settings
General Settings		Site AWS	Refresh
SITES		Region us-west-2	Inter-Site Connectivity External Connectivity
e O AWS	0	♥ ct_routerp_us- west-2_0 west-2_1	General Site ID 91
 Azure disabled 	0	CBAV CBAV	Multi-Site () BOP
• ext-fab-1	0		65991 Contract Based Bruilion
 Sydney 	Ø		Inter-Site Connectivity Protocol Site Protocol

The Add Site page appears.

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

Figure 87:

≡ cisco Nex	tus Dashboard 🔶 Orchestrate	or ~			Feedback 上 💿
Site Connecti	vity				DEPLOY V Ota X
					AWS Settings
	Site AW:	5		Refresh	· Arro octango · · ·
SITES					Inter-Site Connectivity External Connectivity
anates	Region Region ct_route west-2_	Add Site		×	General A
disabled	CERV	Connected to Site Select Site > Connection Type *			Natio Ster () BOP BOP Antononome Sustain Narenae
e 🔵 ext-fab-1		Protocol BGP-EVPN Hub Site C			
 Sydney 		IPsec			Inter-Site Conductivity Site Protocol Add Site
		On Premises IPsec Devices		_	
		C8K3-Fab2	IP Address 64104 25512		
			UNIUSADOLA		

The Select a Site page appears.

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

Figure 88:

≡ 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 Connecti	ivity				
General Settings		Site AWS	Add Site		
		Region us-wes	AWS -> Sydney		
			Avvo - Joydney		
		9 ct_routerp_us-	Sydney ×		
		west-2_0	Connection Type *		
e 🔕 Azure		C8kV	Public Internet		^
			Public Internet		~
a avt.(ab.1			Private Connection		
extriduri					
			IPsec		
Sydney			On Promises (Page Davies		
			On Premises iPsec Devices Device Name	IP Address	
			C8K3-Eab2	64.104.255.12	
			Sydney ● → AWS 🥯		
			Please check if C8kVs are configure	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 89:

- 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, on page 20 in Supported Topologies with IPsec (Multi-Cloud), on page 18.

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 88.

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 85.

- **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 90:

≡ cisco Nexu	s Dashboar	d 🔶 Orchestrator 🗸			Feedback 👤 🖲
Site Connectiv	ity				DEPLOY V Oth X
SETTINGS					AWS Settings
General Settings		Site AWS		Refresh	
SITES		Region us-west	-2		Inter-Site Connectivity External Connectivity
enabled	0	 ct_routerp_us- west-2_0 	ct_routerp_us- west-2_1		General A
Azure	Ø	C8kV	CBKV		Multi-Site () BGP
e ext-fab-1					BGP Autonomous System Number 65091
	0				Contract Based Routing
 Sydney 	Ø				Site Protocol Sydney Connection Trace 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 91:

≡ cisco Ne	xus Dashboar	d 🔶 🙏 Orchestrator 🗸				Feedba	ick 土 🖸
Site Connect	ivity					DEPLOY V	X IJG
						AWS Settings	
		Site AWS			Refresh	Inter-Site Connectivity External Connectivity	
		 Region us-wes ct_routerp_us- west-2.0 	Add Site		×	General Site ID 91	
esolio		CBIA	Select Site	S Site	×	Multi-Site () BCP BCP	
e ext-fat-1			Azure	Azure Site ID 92			
 Sydney 				Type Azure URL https://20.127.114.214:443	- 1	Inter-Site Connectivity Site Protocol Sydnoy Connection Type Public BGP-EVPN	/ 11
				4	, 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 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 92:

≡ "listo" Nexus Dashboard	. Orchestrator ~		Feedback 💄 💿
Site Connectivity			DEPLOY V Oti X
	Site AWS	Add Site ×	AWS Settings
	-	1	Inter-Site Connectivity External Connectivity
	Region us-wes	AWS ⊖ → Azure Q	General
	ct_routerp_us- west-2.0	Please check if C8kVs are configured with Public IPs for Public Underlay connection	
e 🔾 Azure	CEKV	Connected to Site	Muti-Ste
		Azure X	BOP
		Public Internet	
(e extribut)		Protocol	
Sydney			Site Protocol
		IPsec	Sydney BOP-EVPN X T
		Azure Q → AWS 😑	Add See
		Please check if C8kVs are configured with Public IPs for Public Underlay connection	
		Connected to Site	
		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 90.

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 85.
- Connected the first cloud site to the second cloud site in Connect the First Cloud Site to the Second Cloud Site, on page 88.

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 88, 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 88.

- **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 93:

Site Connect	ivity		DEPLOY V	t) X
SETTINGS			Azure Settings	
General Settings		Site Azure	Refresh	
sites		Region eastus	General External Connect	tivity
enabled	0	* ct_routep_eatus	Site ID 92 Multi-Site ①	
disabled	0		BCP BCP Autonomous System Number	^
o 🔵 ext-fab-1	0		65092 Contract Based Routing	
🔹 🌘 Sydney	0		Inter-Site Connectivity Protocol	
			Connection Type: Public BGP-EVPN	/ 1

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 94:

≡ disco Nexus Da	shboard 🔔 Orchestrator				Feedback 💄	Ð
Site Connectivity					DEPLOY V Ota X	
					A Arura Sattings	
	Site Azure	Add Site		×	• Azure Setungs	
				*	Inter-Site Connectivity External Connectivity	
	🔞 Region eastus	Azure ^O → Sydney [●]			General	
		Connected to Site				
		Connection Type *				
	CBKV	Public Internet		×	Mutrone ()	
		Protocol			BGP	
		BGP-EVPN				
je 🔮 ext-tap-1		Hub Site O				
		IPsec				
· Sydney		On Premises IPsec Devices			Inter-Site Connectivity	
		Device Name	IP Address		AWS DOG DIGN / 1	
		C8K3-Fab2	64.104.255.12			
					Add Site	
		Sydney ● → Azure O				
		Please check if C8kVs are configured v	with Public IPs for Public Underlay connection			
		Connected to Site				
		Auces				
				•		

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

The configured sites appear.

Figure 95:

≡ disco Nex	s Dashboard 🔹 🍨 Orchestrator 👳	Feedback 1
Site Connecti	ity	DEPLOY V Oth X
SETTINGS		A Ture Settings
General Settings	O Site Azure Bafrech	• Azure Settings 0
SITES		Inter-Site Connectivity External Connectivity
🔹 🤤 AWS	Region eastus	General
enabled	ct_routerp_eastus ct_routerp_eastus	Site ID 92
a Azure		Multi-Site ()
		BCP
		BGP Autonomous System Number
ext-fab-1	0	Contract Based Routing
 Sydney 	0	Site Protocol
		AWS BGP-EVPN Connection Type: Public
		Sydney BGP-EVPN / T
		AGI SIGE

What to do next

Follow the procedures provided in Deploy the Configuration in Nexus Dashboard Orchestrator, on page 92.

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 90.

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 71, 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 71, at the top right of the page, click **Deploy > Deploy Only**.

Figure 96:

≡ " 11 1. CISCO NO	exus Dashboar	rd 🙏 Orchestrator 🗸	Feedback	10
Site Connect	ivity		DEPLOY A Ot	5 ×
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 Devention	O
enabled Azure enabled	0	Region eastus C_routerp_eastus J casv casv casv	Download External Device Config files	^
ext-fab-1 Sydney	Ø		BDP Autonomous System Number 65002 Contract Based Routing Inter-Site Connectivity	
	Ø		site Protocol AVS BOP-EVPN Sydney BOP-EVPN Connection Type Public BOP-EVPN Add Site BOP-EVPN	/=

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 97:



• 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 98:

AWS O Regions A 2 O Inter-Site Connections	Ci Muti-Site N	Site ID 91	BOP ASN 65091		∽ Hide Connectivity Status ∧
Device	Device Status	Interface Status	Peering Status	BGP Peer	Destination
ct_routerp_us-west-2_1	↑ Up	tunn-7 🕇 Up	OSPF 🕈 Up	-	1 C
ct_routerp_us-west-2_1	↑ Up	tunn-6 🛧 Up	BGP ↑ Up	170.1.254.6	64.104.255.12
ct_routerp_us-west-2_1	↑ Up	tunn-8 🛧 Up	OSPF 🕈 Up		
ct_routerp_us-west-2_0	↑ Up	tunn-7 🕇 Up	OSPF 🕈 Up		
ct_routerp_us-west-2_0	↑ Up	tunn-8 🛧 Up	OSPF 🕈 Up		·
ct_routerp_us-west-2_0	↑ Up	tunn-6 🕇 Up	BGP ↑ Up	170.1.254.2	64.104.255.12

• 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 99:

Azure o					~
Regions 1	ACI Multi-Site On	Site ID 92	BGP ASN 65092		
Inter-Site Connections	us				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	97.0	
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
ct_routerp_eastus_1	TUP	tunn-i 个 Up	BON L OD	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 100*:

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	D					
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 101:



• 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).







PART

Use Cases

- Deploying the Tenant, on page 99
- Stretched VRF Use Case, on page 107
- Route Leaking Use Case, on page 143



Deploying the Tenant

• Deploying the Tenant, on page 99

Deploying the Tenant

Once the underlay and overlay connectivity is established between the sites, you must then deploy the endpoint network/VPC/VNet to establish communication between tenant endpoints deployed in the on-premises and in the cloud sites.

NDO uses the notions of schemas and templates for defining VRFs and networks. In the context of NDFC, VRFs are used to isolate one tenant from another. All the endpoint networks (subnets) of one tenant are mapped to the respective VRF. The same notion of VRFs can also be extended to the cloud, where a VRF corresponds to a VPC in AWS and a VNet in Azure.

The following procedures for deploying the tenant applies to all the topologies previously described and leverage the specific infra config deployed, and also applies for any of the following use cases.



Note NDO has a pre-built dcnm-default-tn tenant, which can be associated with on-premises sites as well as cloud sites. We recommend that you associate this pre-built dcnm-default-tn tenant with the NDFC and cloud sites when deploying hybrid cloud connectivity, but you can also create your own tenant from scratch, if necessary.

Step 1 In NDO, navigate to **Application Management** > **Tenants**.

Figure 103:

≡ disco Nexus Dast	nboard 🔶 Orchestrator 🗸	Feedback
Dashboard Sites Application Management	Site Connectivity	Configure
 Patric Management Infrastructure Infrastructure Integration 	Paperson management Tananta Schemas Tanant Rviceis L30xt Tempartas Cloud Peticles	Group Marters

The Tenants window appears.

Figure 104:

≡ cisco Nexus Dashbo	Dard 🙏 Orchestrator 🗸					Feedback 💄 📀
 Dashboard Sites 	Tenants					① 1) Add Tenant
Application Management	Filter by attributes					
Fabric Management	Name	Description	Assigned To Sites	Assigned To Users	Assigned to Templates	
Operations O Infrastructure	common	Common tenant for use with all other tenants	4	1	0	
Ø Integration	infra	Infra tenant for use with all other tenants	2	a	0	
	dcnm-default-tn	Default tenant for NDFC	1	1	o	
	10 × Rows				Page 1	f 1 ≪ (1-3 of 3) ≫

Step 2 Click the dcnm-default-tn tenant.

The Update Tenant page for the dcnm-default-tn tenant appears.
Figure 105:

≡ cisco Nexus Dasht	ooard 🔍 Orchestrator 🗸			Feedback 👤 📀
Update Tenant dcnn	n-default-tn			©t} ×
	General Settings			
	Display Name *			
	donm-default-tn			
	Description			
	Default tenant for NDFC			
	Associated Sites	Site Type		
	Sydney 12.1.2.275	NDFC		
	Azure 25.3(1e)	Azure		
	AWS 25.1(1e)	AWS		
	5 V Rows		Page 1 of 1 $\ll <1-3$ of 3 $>$ \gg	
	Associated Users			
	No user is available			
Cancel				Save

Step 3 Select the sites shown in the screen.

Note that the external fabric site does not appear in the list. The external site is only used to provide connectivity between the on-premises site to the cloud sites and there are no end hosts in the external fabric, so no tenant deployment required for the external fabric.

Figure 106:

≡ 'll'ill' Cisco Nexus Dasht	ooard 🔺 Orchestrator 🗸		
Update Tenant dcnm	n-default-tn		
	General Settings		
	Display Name *		
	dcnm-default-tn		
	Internal Name: dcnm-default-tn		
	Description Default tenant for NDEC		
	Associated Sites There are cloud site settings that need to be configured.		
	2 Sites selected		Unselect Items
	Site Name	Site Type	
	Sydney 12.1.2.275	NDFC	/
	Azure 25.1(10)	Azure	/
	AWS 25.1(1e)	AWS	
	5 ~ Rows		Page 1 of 1 $\ll <1-3$ of 3 $>$ \gg

Step 4 For the cloud sites, click the Edit button (the pencil icon) and provide the necessary information for each cloud account.

You need an additional account for AWS for the user tenant, but for Azure, you can use the same subscription as the Azure infra tenant.

• For example, after clicking the Edit button for the AWS cloud site, in the AWS Account Setting area, you might click **Trusted** for the Access Type and enter the associated AWS account ID in that field.

Figure 107:

≡ cisco Nexus Dashboard / 🍨 Orchestrator 🤟	وتنهيه ومركات الترجز والمأته الم	
Update Tenant dcnm-default-tn		
General Settings		
Disptay Name * doom-default-tir:	Tenant Setting for AWS site ×	
	General Setting	
Default tenant for NDFC	Security Domains Select Security Domain(s)	
Associated Sites	AWS Account Settings AWS Account Id *	
There are cloud site settings that need	to bi	
3 Sites selected	Untrusted inusted Urganization	Unselect terms
Site Name	Cancel Save	
Sydney 1212.275	NDFC	/
Azure 25/(5e)	Azure	/
🕑 🌘 AWS (283(16)	AWS.	1
5 v Rows		Page 1 of 1 《<1-3 of 3 》

See the section "Setting Up the AWS Account for the User Tenant" in the *Cisco Cloud Network Controller for AWS Installation Guide*, Release 25.1(1) or later, for more information on the different access types for the tenants in AWS.

• Similarly, after clicking the Edit button for the Azure cloud site, you would enter the necessary information, depending on whether the tenant is managed or unmanaged.

Figure 108:

date Tenant	dcnm-default-tn		
	General Settings		
		Topont Satting for Azura sita	
	Internal Name: dcnm-default-tn	Tenant Setting for Azure site	
	Description Default tenant for NIDEC	General Settings	
	Default tenant for http://	Security Domains	
		Subert Secondy Somethings	
	Associated Sites	azureAccount Settings	
		Mode Create Own Select Shared	
	2 Sites selected		
	-	× ~	
	Site Name	Cancel Save	
	Sydney 1212.275		/
	Azure 25.1(1e)	Azure	/
	AWS 25.00er	aws	

See the section "Adding a Role Assignment" in the *Cisco Cloud Network Controller for Azure Installation Guide*, Release 25.1(1) or later, for more information on the different access types for the tenants in Azure.

Step 5 Verify the tenants were deployed correctly.

For example, in the figure below, the dcnm-default-tn tenant has three sites mapped (one on-premises NDFC site and the two cloud sites).

Figure 109:

≡ cisco Nexus Dashboa	ird 🌲 Orchestrator 🗸					Feedback 💄 🕐
Dashboard Sites	S Tenant dcnm-default-tr	has been successfully updated.				×
Application Management	Tenants					
Fabric Management						Add Tenant
Derations	Filter by attributes					
 Infrastructure 	Name	Description	Assigned To Sites	Assigned To Users	Assigned to Templates	
& Integration	common	Common tenant for use with all other tenants	4	1	0	
	infra	Infra tenant for use with all other tenants	2	1	0	
	dcnm-default-tn	Default tenant for NDFC	3	1	0	
	10 v Rows				Page 1 of 1	≪<1-3 of 3 > ≫

≡ cisco Nexus Dashb	ooard 🙏 Orchestrator 🗸					Fe	edback 💄 📀
a Darkhard	Tenants			Sites			×
 Dashboard Sites 	Tenanto			Q Search	Sites Sydney		
Application Management	Filter by attributes			Sydney	0 0	0	0 Î
Fabric Management	Name	Description	Assigned To Sites	Azure	critical majo	minor	warning
 Operations Operations 	common	Common tenant for use with all other tenants	4	dcnm-default-tn AWS	General Name		^
Ø Integration	infra	Infra tenant for use with all other tenants	2	dcnm-default-tn	Sydney		
	dcnm-default-tn	Default tenant for NDFC	3		Type on-premise		
					Cloudsec Encrypti Not Enabled Site ID 82	on	
					Site Controller URI URL	S	
					https://172.16.0.19	1:443	
	10 V Rows				Topology		^
					5	S	

You can also check the dcnm-default-tn tenant deployed in the Cisco Cloud Network Controllers for the cloud sites. *Figure 110*:

Ŧ	alı Cis	Cloud Network Controller (AWS) 🥶 🔍 🖓 🖓 🖓 🖓 🖓 🖓 🖓									
Dashboard	Ter	Tenants									Ø
Topology Cloud Resources											Actions ~
Application Management ^						Application	Management			Cloud Resources	
Tenants		Health	Name	Description	Application Profiles	EPGs	VRFs	AWS Account	Regions	VPCs	Endpoints
Application Profiles		Healthy	common		1	0	2		0	0	0
EPGs Contracts	Γ	Healthy	dcnm-default-tn	Default tenant for NDFC sites	0	0	0	11737874641 1	4	0	0
Filters VRFs		♥ Major	infra		1	15	2	25759168523 0	4	1	12
Services		Healthy	mgmt		0	0	2		0	0	0
External Networks	15	5 🗸 Rows							Page	1 ∨ of 1 4	4 1-4 of 4 ▶ ▶

Ŧ	al) Cis	·!/u!!· Cloud Network Controller (AZURE) 🗛 Aure									
Dashboard	Ter	nants									0
Topology	TO	lants									٩
Cloud Resources	Filter										Actions ~
Application Management ^						Application	Management			Cloud Resources	
Tenants		Health	Name	Description	Application Profiles	EPGs	VRFs	Azure Subscription	Regions	Virtual Networks	Endpoints
Application Profiles		• Healthy	common		1	0	2		0	0	0
EPGs			denor defende te	D. ()			0	01	0	0	
Contracts		Healthy	dcnm-default-tn	tenant for	0	0	0	shared from infra	0	0	0
Filters				NDFC SILES							
VRFs		Major	infra		1	12	2	74094178- 785d-	1	1	7
Services								468a-bf23- 41e85a1a3a			
Cloud Context Profiles								da			
External Networks		Healthy	mgmt		0	0	2		0	0	0
Operations	15	5 🗸 Rows							Page 1	✓ of 1 4 4	1-4 of 4 ▶ ▶
⊖ Infrastructure ∨											

What to do next

Configure one or both of the following use cases:

- Stretched VRF Use Case, on page 107
- Route Leaking Use Case, on page 143

Deploying the Tenant

I



Stretched VRF Use Case

- About the Stretched VRF Use Case, on page 107
- Configure the Stretched VRF Use Case, on page 108

About the Stretched VRF Use Case

Stretched VRF (intra-VRF) is a common use case where a single (common) VRF is defined in a template that is associated to all the sites (on-premises and cloud sites). A separate template is used to deploy networks for the on-premises site since it is not possible to stretch networks between on-premises and cloud sites.

Stretching the same VRF to all the sites enables the exchanging of prefixes between the sites without having the requirement of any additional routing configuration. CIDR blocks (used to provision subnets in cloud VPCs/VNets) are mapped to this stretched VRF.



Note Stretching a Layer 2 subnet across on-premises and cloud sites or between cloud sites is not supported.

The following figure shows two templates being created under the Demo schema:

- The stretched Template, which defines the VRF to be deployed to all three sites. For cloud sites, we define the regions and CIDR blocks under the VRF.
- The On_Prem Template, which contains the networks to be deployed to the on-premises VXLAN fabric.

Figure 111:



Configure the Stretched VRF Use Case

Step 1 In NDO, navigate to Application Management > Schemas and click Add Schema.

Figure 112:

Feedback 上 🕥
⊙ t} Add schma

Step 2 Provide the schema name and click **Add**.

For this use case, we will name the new schema Stretched Schema.

Figure 113:

E cisco Nexus Dashboard & Orchestrator			
View Overview ~ Overview			
General Name Description Untitled Schema	Audit Lo Created General	gs Deleted Upd o	ated Deploye O
Sites Type	Name * Stretched[Schema		
ABIC 0 * ADFC 0 * AWS 0 * AWS 0 * Aure 6 Google Cloud Partorm 0	Description	Sync 0 It of Sync 0	
Application Management			

You are returned to the Overview page for the new Stretched Schema schema.

Step 3 Click Add New Template.

Figure 114:

≡ cisco Nexus Da	shboard 🔶 Orchestrator	·						Feedback 🔔
Stretched Schema							0 / 100	0 Objects Save Schema tl X
View Overview ~ ^{Overview}								Add New Template
General Name Stretched Schema	Description		0	Audit Logs Created 0	Deleted 0	Updated 0	Deployed 0	Other 0
Sites Type 0	APIC 0 NDFC 0 Ature 0 Ocoge Cloud Platform 0			Templates Sync Status () 0	In Sync Out of Syni	0		
Application Managem • Application Profiles (0) • Filters (0)	• EPGs (0) • External EPGs (0)	 Contracts (0) L3Outs (0) 	VRFs (0) Service Graphs (0)	Bridge Don Networks (nains (0) (0)			0 Total Objects
Topology								

Step 4 Choose the NDFC template, then click **Add**.

You should use the NDFC template type for on-premises as well as cloud sites.

Figure 115:

≡ •IIIIII Nexus Dashboard Orche	trator ~		Feedback 👤 📀
Stretched Schema			0 / 1000 Objects Save Schema CL 🗙
View Overview ~			Add New Template
Overview	Select a Template type	x	
General Name Description Stretched Scheme Sites Type • APC 0 • NDC 0			Deployed Other O O
0 • Artic 0 • Could Partiers 0 • Could Partiers 0	ACI Multi-Cloud On-prem ACI site to site On-prem ACI site to cloud site Cloud to cloud site	C Cloud Local • Non-stretched template for cloud site local BGP-IPv4 connected site	-
Application Management		Add	
Application Profiles (0) EPOs (0) Estamat EPOs (0)	Commette (0) Contracte (0) Contracte (0) Contracte (0)	Endge/Domains (0) Pretworks (0)	0 Total Objects

Step 5 Enter a name in the **Display Name** field to create an NDFC-type template (for example, stretched Template) and select the dcnm-default-tn tenant in the **Select a Tenant** field to map the template to that tenant.

Figure 116:



Step 6 Under **Template Properties**, click **Create Object** and choose **VRF** to create a VRF that will be stretched to all the sites.

Figure 117:

≡ ^{•Ittutti} • cisco Nexus Dashboard . ♣ Orchestrator >				Feedback 💄 🔮
Stretched Schema			0 / 1000 Objects	Save Schema () X
View Stretched Template ~		Add New Template	Template Stretched Template	×
Stretched Template Tenant: dcnm-default-tn	Associated Sites In Sync 0 Out of Sync 0	Deploy in silon	Template Settings Display Name* Stretched Template Deployed Name:	
Template Properties 🗸		Actions 🗸	Description	
	IMPC	VRF	Template Type NDFC	
		Network	Tenant Settings	^
			dcnm-default-tn	× ~]
Click "Create O	Let's create an object bject" on template properties to create an o	bject		

NoteIf you have an on-premises VRF already created that you want to use instead of creating a new VRF, under
Template Properties, click Import, then import the already-created VRF.

Currently, we only support importing VRFs and networks from on-premises sites.

Step 7 Enter a name in the **Display Name** field for the stretched VRF (for example, stretched-vrf).

Figure 118:

≡ diviți. cisco Nexus Dashboard Orchestrator ∨	Feedback 💄 🕥
Stretched Schema	1/1000 Object Save Schema 💱 🗙
View Stretched Template \vee	(Add New Template) VRF ×
Stretched Template Tenant: donm-default-in	Sites 0 0 0 Sites 0 0 0 0 Sites 0 0 0 0 Sites 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Template Properties ~	Actions
VRFs U	Add VRF NDFC Properties
stretched-vrf	VRF Profile * Default_VRF_Universal × ✓
	VRF Extension Profile * Default_VRF_Extension_Universal X v
	Loopback Routing Tag 12345
	Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET
	Disable RT Auto-Generate

- **Step 8** Associate all the sites (on-premises and cloud sites) to Stretched Template for the stretched VRF use case.
 - a) In the **Template Properties** area, click **Actions** > **Sites Association**. *Figure 119:*

≡ ^{«I]+I +} Nexus Dashboard ≜ Orchestrator ∨				Feedback 💄
Stretched Schema			1 / 1000 Object	Same Scheme 🛈 th 🗙
View Stretched Template \vee		Add New Template	Template Stretched Template	×
Tenant: dcnm-default-tn	Associated Sites In Sync 0 Out of Sync 0	Deploy to sites	Template Settings Display Name* Stretched Template Deployed Name: Deployed Name:	^
Femplate Properties 🗸		Actions: ~		
Filter	IMPORT ~	SELECT + Create Object Clone Templa Delete Templa	te ate Type	
VRFs ~		History Rollback	t Settings	^
stretched-vrf		Sites Associa	default-tn	
		Tag	-default-tn	
			Description Default tenant for NDFC	

b) Select all the sites, then click **Ok**.

This also allows you to select each site individually to provision site-level configurations for the objects defined in this template (in this specific case, just the stretched VRF).

Figure 120:

≡ cisco Nexus Dashboard Oref	nestrator V			Feedback 上 🥐
Stretched Schema				0 t3 X
View Stretched Template \vee		Add New Template	Template Stretched Template	×
Stretched Template Version 1 Testant: dcrm-default-tn	Associated Sites ** Sync: 0 Out of Sync: 0	(Second second	Template Settings Display Name* d Template Arms:	
Template Properties ~	Add Sites To Stretched Template		x on	
	AWS 25.5(te)		Type	
stretched-vrf			ame fault-tn	
			en enant for NDFC	
			_	

Once the sites are associated with the template, they will appear under Template Properties.

Figure 121:

≡ ^{+ -} . Tisco Nexus Dashboard		Feedback 👤 🥑
Stretched Schema	1 / 1000 Object Saw	schema の たよ 🗙
View Stretched Template ~	Template Stretched Template	×
Stretched Template Version 1 Applied to 3 sites Tenant: doom-default-in Outplay to sites Outplay to sites Outplay to sites	Template Settings Display Name* Stretched Template Deployed Name:	^
Template Properties Actions - Average Av	Template Type NDFC	
Azure © do et Sync Sydney © Cot et Sync Stretched-wrf	Tenant Settings Display name dom-default-tn Name dom-default-tn Description Default tenant for NDFC	A.,

- **Step 9** Click **Template Properties** and select the first cloud site (the AWS site in this example use case), then associate the VRF to the appropriate regions to create the VPC.
 - a) Click the VRF, then click Add Region to create the VPC in the selected region.

Figure 122:

≡ ditel/- cisco Nexus Dashboard . ★ Orchestrator ~	Feedback
Stretched Schema	1/1000 Object Save Schema) ① たえ 🗙
View Stretched Template ~	Add New Template Stretched-vrf
AWS Version 1 Awsociated Sites Awsociated Sites Awsociated Sites Awsociated Sites Awsociated Sites Awsociated Sites	Denny to sole
Tenant: dcmi-default-tn AWS @ box at sync. Filter	Template Properties Display Name * stretched-vrt Description N/A VRF ID O 150555
Estretched-vrf	Site Local Properties Context Profiles Region Context Region Leak Routes
	Target VRF Routes

The Add Cloud Region CIDRs window appears.

b) In the **Region** field, choose the region where you want to create the VPC.

Figure 123:

Stretched Schema 1/1000 object	
	o Schema 💿 🞲 🗙
View Stretched Template ~ VRF stratched-wrf	×
Add Cloud Region CIDRs	×
Region* Select region uturente?	
us-east-1	
CICR Type VRF And CIORs	
VPN Gateway Router	
	•

- c) In the CIDR field, click Add CIDRs and define a CIDR block for the VPC.
- d) Click Add Subnet to create the subnets and map them to the availability zones, then click Save.

Figure 124:

						- Feedback
tched Schema						1/ 1000 Object Save Schema 🕢 🔃
dd Cloud Region CIDRs						
ion *						
-west-2						\times \sim
tainer Overlay						
Rs						
R				Туре	VRF	
URP Type () Primary Secondary dd Subnets ubnet Name Private Link Labels	Availability Zone					
0.230.1.0/24	us-west-2a	~	×			
0.230.2.0/24	us-west-2b	~	\times			
Add Subnet						

e) Check the box under the **Hub Network** field, then select the hub network that was created on the Cisco Cloud Network Controller for AWS.

This allows the Cisco Cloud Network Controller to attach the subnets onto the transit gateway, which builds the connectivity from those subnets to the transit gateway, where the transit gateway already has the connectivity to the Cisco Catalyst 8000Vs in the cloud.

f) In the **Subnets** field, map the subnets that will be used for the transit gateway.

It is best practice to have a dedicated subnet that will be used for the transit gateway.

Figure 125:

≡ cisco Nexus Dashboard Crchestrator ∨			Feedback 💄 🔮
Stretched Schema			1/1000 Object Seve Schema 🕢 th 🗙
Add Cloud Region CIDRs			×
Region *			
Container Overlay Enabled CDRs			
CIDR	Туре	VRF	
10.230.0.0/16	Primary	stretched-vrf	/=
🚯 Add CIDRs			
VPN Gateway Router Hub Network			
A To change the selected Hub Network, uncheck the Hub Network option	and deploy the template first. Then re-enable the option, select the new h	lub Network, and redeploy the template.	
Hub Network			
hub-1 - infra			× ~
Subnets			
10.230.1.0/24 × 10.230.2.0/24 ×			X ~
			OK

Note Alternatively, a dedicated /25 subnet per availability zone can be used for connectivity to a hub network (TGW). This will allow the entire end-point subnets to be used for end hosts.

g) Click Ok.

You are returned to the AWS template window.

When this configuration is deployed, a VPC with CIDR 10.230.0.0/16 will be created in the AWS cloud, stretching between the us-west-2a and us-west-2b availability zones, with the 10.230.1.0/24 and 10.230.2.0/24 subnets created respectively.

Figure 126:

≡ athuth Nexus Dashboard . Crchestrator ∨	Feedback 💄 🖬
Stretched Schema	1/1000 Object Save Schema の たし 🗙
View Stretched Template ~	Add New Template VRF ×
Aws vesos Stractad familia	Denny / studio
AWS @ out of spec] V	Actions Template Properties ^ Display Name * stretched-wrf Deployed Tame: stetched-wrf Deployed Tame: stetched-wrf Deployed Tame: stetched-wrf Deployed Tame: stetched-wrf VRF ID O 150555
stretched-vrf	Site Local Properties Context Profiles Region
	us-west-2 / 章 CIDR-10.2300.0/16
	Add Region Leak Routes Target VRF Routes
	💿 Add Leak Route

- **Step 10** Click **Template Properties** and select the second cloud site (the Azure site in this example use case), then associate the VRF to the appropriate region to create the VNet.
 - a) Click the VRF, then click Add Region to create the VNet in the selected region.

Figure 127:

≡ diudu cisco Nexus Dashboard . Orchestrator ~	Feedback: 🛓 9
Stretched Schema	1/1000 Object Save Schema ④ 代과 🗙
View Stretched Template \sim	Add New Template Stretched-vrf ×
Azure Version 1 Stretched Template	(seeby to kine)
Tenant: domi-default-in Azure @ out style: Filter	Actions A
VRFs ···	Site Local Properties Context Profiles Region
	Add Region Leak Route Add Leak Route

The Add Cloud Region CIDRs window appears.

- b) In the Region field, choose the region where you want to create the VNet.
- c) In the CIDR field, click Add CIDRs and define a CIDR block for the VNet.
- d) Click Add Subnet to create the subnets, then click Save.

Figure 128:

tched Schema			1 / 1000 Object Save Scheme 🕢
dd Cloud Region CIDRs			
on *			×
tainer Overlay Enabled			
R	Туре	VRF	
DR * 701.0.0/16 DR Type O Primary			
Secondary lect Associated VRF Parent VRF Hosted VRF			
d Subnets Ibnet Name Private Link Labels Availability Zone			
0.11.0/24 ✓ X			
Cancel Save]		

e) Check the box under the **VNet Peering** field, then select the Default hub network that was created on the Cisco Cloud Network Controller for Azure.

Figure 129:

≡ cisco Nexus Dashboard . Circhestrator ∨	فرحدا الأحجاز المالي والمتنا		Feedback 💄 📀
Stretched Schema		1/1000-0	oject Save Schema @ C3 ×
View Stratchad Template V		Add New Template	×
Add Cloud Region CIDRs			×
Region *			
eastus			× ~
Container Overlay Enabled			
CIDRs			
CIDR	Туре	VRF	
70.1.0.0/16	Primary	stretched-vrf	/=
🔂 Add CIDRs			
VPN Gateway Router ↓ Net peering			
Hub Network			
Default			× ~
			ОК

f) Click Ok.

When this configuration is deployed, the VNet that you configured (in this example, 70.1.0.0/16) will be created on the appropriate region in Azure (in this example, the eastus Azure region) and VNet peering is configured to the infra VNet in the infra tenant in Azure.

Figure 130:

≡ cisco Nexus Dashboard . Crchestrator ~	Feedback	10
Stretched Schema	1 / 1000 Object Save Schema ④ 1	es X
View Stretched Template ~	Add New Template Stretched-vrf	×
Associated Sites Associated Sites Sitetched Template	critical major minor warning	
Filter	Actions Template Properties Display Name * stoteched-wr Description N/A VPF IO (O) 150555 Site Local Properties	^
stretched-vrf	Context Profiles Region eastus come to access	/ =
	Add Region	
	Leak Routes Target VRF Routes	
	Add Leak Route	

- **Step 11** Click **Template Properties** and select the on-premises site (the Sydney site in this example use case), then select the stretched-vrf VRF.
- **Step 12** In the right pane, click **Add Static Leaf**.

L

Figure 131:

≡ disco Nexus Dashboard / ⋬. Orchestrator ∨	Feedback	10
Stretched Schema	1 / 1000 Object Ssre Schema 🕥	() ×
View Stretched Template ~	Add New Template Stretched-vrf	×
Sydney Version 1 Stretched Template		2
Tenart: dom-default-in Sydney O dat at the VB's VB's Stretched-vrf	Actional Template Properties Display Name * State Actional Description Description NAM Name VIP ID O Display Panece stretched-wif Description NAM Name NAM Name Display Panece stretched-wif Description NAM Name Display Panece stretched-wif Description NAM Name NAM Name Display Panece stretched-wif Description NAM Name Display Panece stretched-wif Description NAM Name NAM Name Display Panece stretched-wif Description NAM Name Display Panece stretched-wif Description NAM Name NAM Name Display Panece stretched-wif Description NAM Name NAM Name Display Panece stretched-wif Description NAM Name Display Panece stretched-wif Description NAM Name Display Panece stretched-wif Description Display Panece stretched-wif Description <t< td=""><td>^</td></t<>	^
	Add State Leaf	

The Add Static Leaf window appears.

Step 13In the Leaf field, select the leaf/border/border gateway device where this VRF is to be deployed and click Ok.Figure 132:

Stretched Schema					0 Object Save S	Schema 🕥
View Stretched Template ~		Add New Template	VRF			
Sydney Version 1 Stretched Template	Associated Sites		- critical	- major	= minor	- warnin
Sydney Court see. ~	Add Static Leaf	× Actions ~	Template Pr Display Nam stretched-v Deployed Nam Description N/A VRF ID ()	operties io * if e: stretched-wrf		
VRFs ~	VLAN		150555 Site Local P Tehant Rout	roperties ed Multicast		
			Static Leaf t Node/Swit	lodes tch : Leaf		

You are returned to the Stretched Template page.

Step 14 Click **Add Static Leaf** again to add additional leaf/border/border gateway devices where this VRF is to be deployed.

In this example, you need to deploy the VRF on the leaf nodes (where the endpoints part of the network mapped to the VRF will be connected) and on the BGW spine node to be able to extend the Layer 3 connectivity for the VRF towards the cloud sites.

I

Figure 133:

≡ ^{•(• • •} Nexus Dashboard .					Feedback 💄 🔮
Stretched Schema			1 / 100	0 Object Save S	chema 💿 🕄 🗙
View Stretched Template \sim		Add New Template	VRF stretched-vrf		×
Sydney Version 1	Associated Sites		major	- minor	- wanning
Sydney Part of type Filter VRFs Stretched-wrt	Add Static Leaf	x Actors ~	Template Properties Display Nams * attestification Description N/A: WFID () 150555 Stel Local Properties Temark Rooted Municest PR External District Leaf Nodes Noted Works		
			ndfc-leaf1 ~ ndfc-leaf2 VLAM: N/A		× ±
			Add Static Leaf		

When you have added all of the leaf/border/border gateway devices where this VRF is to be deployed, they will appear in the **Stretched Template** page.

Figure 134:

≡ athtatha cisco Nexus Dashboard . ♠ Orchestrator ~		Feedback 💄 🧿
Stretched Schema	1 / 1000 Object	Save Schema 🛈 🛟 🗙
View Stretched Template \sim	Add New Template VRF stretched-vrf	×
Sydney Version 1 Statistical States		- warning
Tenant: dcnm-default-in Sydney • Got of Spec Filter VRFs stretched-vrf	Actions Template Properties Copyon Name ** Display Name ** Actions Display Name ** NA VRF ID VRF ID State State Leaf Nodes State Leaf Nodes	^
	Node/Switch	
	VLAN: N/A	/ =
	ndfc-spine1 VLAN: N/A	/ =
	Add Static Leaf	

- Step 15 Click the arrow next to the Sydney site, and from the drop-down menu, select Template Properties.
- Step 16 Click Deploy to sites.

Figure 135:

E cisco Nexus Dashboard . ♠ Orchestrator ~	Feedback	10
Stretched Schema	1/1000 Object Save Schema 🛈 🏌	γX
View Stretched Template ~	Template Stretched Template	×
Stretched Template Version 1 Applied to 3 sites Temant: doom-default-in Copy of the site of the s	Template Settings Display Name* Stetch-d Template Deployer Name: Description	
Filter MMPORT > SELECT + Create Object	Template Type NDFC	
VRFs ~ Add VRF stretched-wf	Tenant Settings Display name dcnm-default-tn mame dcnm-default-tn Description Default tenant for NDFC	~

The **Deploy to Sites** window appears, showing the three sites where the stretched template will be deployed. *Figure 136*:



Step 17 Click **Deployment Plan** for additional verification, then click on each site to see the deployment plan for that specific site.

I

Figure 137:

etched Schema ew Stretched Template ~			X 57 0
ew Stretched Template ~			
		Add New Template Add New Template Stretched Template	×
Deployment Plan			×
General Information			
Template Stretched Template	Schema Stretched Schema	Tenant dcnm-default-tn	
Pian			
AWS Azure Sydney		Ocreated Obeleted OModified OExisti	ing Shadow
			View Payload
O doom-default-the O stratetbackurf	nn4:23456:150		
O route-target:as2-	nn4:23456:301		

Figure 138:

≡ disco Nexus Dashboard Ore	hestrator V	Feedback 上 💿
Stretched Schema		1/ 1000 Object. To Change & Ch X
View Stretched Template ~		Add New Template Stretched Template X
Deployment Plan		×
General Information Template Stretched Template	Schema Stretched Schema	C Tenant dcnm-default-in
Plan AWS Azero Sydney O donm-default-tn O stretchäd-vrf	O route-targetas2-nn4:23456:150	O Created O Deleted O Modified O Existing @ Shadow

Figure 139:

≡ cisco Nexus Dashboard	shestrator \vee	Feedback 👗 🕄
Stretched Schema		1/ 1000 Object: 100 00 th X
Deployment Plan		×
General Information		
Template Stretched Template	Schema Stretched Schema	Tenant dcnm-default-tn
Plan		
AWS Azure Sydney		Created Obeleted OModified OExisting Shadow
		(View Payload)
	route-target:as2-nn4:23456:301	
O dcnm-default-tn Stretched-vrf	oroute-target:as2-nn4:23456:150	
	Indiceal - Indiceal	

Step 18Click Deploy to have NDO push the configurations to the site specific controllers (NDFC and Cloud Network Controller).Figure 140:

	kus Dashboard 📃 🙏 o	rchestrator \sim					Feedback 💄 💿
Stretched Sche	ema						× 63 ©
View Stretch	ed Template ~				Add New Templaté	Template Stretched Template	×
G Stretche	ed Template Version 2		O Associat	ed Sites in Sync 0 Out of Sync 3	Doploy to sites	Template Settings Display Name*	^
Deploy to s	ites						×
Modifications						View Version I	History Deployment Plan
- Created	🔽 🗹 Modified 🔽 👕	Deleted 🧧 🏾 Config Drift	Migrated				
Object Type	Name	O AWS 25.1(1e)	Azure 25.1(1e)	Sydney 12.1.2.275			
VRF	stretched-vrf	+ Created	+ Created	+ Created			
							Deploy

- **Step 19** Verify that the configurations were deployed successfully.
 - To view the VRF deployment on NDFC, go to the **Topology** view, select the on-premises fabric **Sydney** > **VRFs**, then select stretched-vrf.

Figure 141:

n dudu Nexus Dashb	poard
Fabric Controller	
☆ Dashboard	Data Center / default / Sydney / VRFs (1) / stretched_vrf
s≮ Topology	View A Search by Attributes
≣ LAN ∨	
🔅 Settings 🗸 🗸	Operation Configuration
	Operation Configuration Hierarchical In-Sync Pending In Progress Out-of-Sync NA Multi-select O In Selected
	ndfc-leaf2 ndfc-leaf1

• Connect to the Cloud Network Controller deployed on AWS to verify that the configurations for the first cloud site (AWS) were deployed successfully.

Go to Application Management > VRFs, locate stretched-vrf and click under the column VPCs, then go to the Overview page and click under Subnets.

• Connect to the Cloud Network Controller deployed on Azure to verify that the configurations for the second cloud site (Azure) were deployed successfully.

Go to Application Management > VRFs, locate stretched-vrf and click under the column Virtual Networks, then go to the Overview page and click under Subnets.

Step 20 Create another template under Demo Schema for deploying networks on the on-premises site.

- a) Under the Demo Schema template, click Add New Template.
- b) Choose the NDFC template.
- c) Enter a name in the **Display Name** field to create an NDFC-type template (for example, On-Prem Template) and select the dcnm-default-tn tenant in the **Select a Tenant** field to map the template to that tenant.

Figure 142:

Figure 143:

≡ ^{•1 •1 •} Nexus Dashboard Orche	istrator ~	Feedback 💄 💿
Stretched Schema		1 / 1000 Object Save Schema ④ たよ 🗙
View On-Prem Template \vee	[Add	New Template On-Prem. Template X
On-Prem Template	Associated Sites • Sync 0 • Out of Sync 0	Template Settings
Template Properties ~		Actions ~
	IMPORT SELECT + Create Obje	Template Type NDFC
		Tenant Settings
		Select a Tenant *
(i)	Let's create an object Click "Create Object" on template properties to create an object	

- **Step 21** Create the net20 network under the VRF on On-Prem Template.
 - **Note** If you have a network already created that you want to use instead of creating a new network, under **Template Properties**, click **Import**, then import the already-created network.
 - a) Under Template Properties, click Create Object and choose Network to create a network.

≡ cisco Nexus Dashboard Orchest	trator v			Feedback 💄 📀
Stretched Schema			1 / 1000 Object	ave Schema 🛈 🗘 🗙
View On-Prem Template \vee		Add New Template	Template On-Prem Template	×
On-Prem Template Tenant: dcnm-default-tn	Associated Sites In Symc 0 Out at Symc 0	Deploy to sitila	Template Settings Display Name* On-Pren Template Deployed Name: Description	^
Template Properties V	BMPORT ~ SELECT	Actions ~	Template Type NDFC	
		Network	Tenant Settings Select a Tenant *	^
i	Let's create an object Click "Create Object" on template properties to create an object		dcnm-default-tn	XV

- b) Enter a name in the Display Name field for the network (for example, net20).
- c) In the Virtual Routing & Forwarding field, choose the stretched-vrf VRF to map net20 to that VRF.

Figure 144:

≡ cisco Nexus Dashboard Orchestrator ∞	Feedback 🗶 🖉
Stretched Schema	2/1000 Objects (1000 to the test of te
View On-Prem Template ~	Add New Template Network © ×
On-Prem Template Tenart: down-default to	tele transmission
Template Properties ~	Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions Actions A
Networks ~	Add Network NDFC Properties
	Liyer 2 only Virsul Routing & Forwarding R* stretched-vir
	Network Profile * Default_Network_Universal X </td
	Network Extension Profile * Default_Vetwork_Extension_Universal VIII
	VLAN Name
	Gateway IP Add Sabert Surpress Add

d) In the Gateway IP field, click Add Subnet.

The Add Subnet window appears.

e) Click **Add Gateway IP** and provide the gateway IP address, then click the checkmark to accept the value and click **Add**.

Figure 145:

≡ direle Nexus Dashboard . Crchestrator ~				Feedback 1
Stretched Schema			2 / 1000 Objects	0 t) ×
View On-Prem Template ~		(Add New Template)	Network net20	©×
On-Prem Template Tonurc doom-default in	Associated Sites • 0 binc • 0 binc • 0 binc		Common Properties Display Name*	
Template Properties ~				
	Add Subnet ×	+ Create Object		
Networks 🤟	Gateway IP Type 77216.20.1/24 primary V 11 Add Gateway IP	Add Network	NDFC Properties Network (D ©	
		1	Virtual Routing & Forwarding	
	Aar	<u> </u>		
			Default_Network_Universal	
			Default_Network_Extension_Universal	
			* Gateway IP	
			Suppress ARP	

The gateway IP address is now displayed in the Gateway IP field.

Figure 146:

≡ ^{cificit} Nexus Dashboard . Orchestrator ~	Feedback 1
Stretched Schema	2 / 1000 Objects Stree Schema 🛈 🗘 🗙
View On-Prem Template 🗸	Add New Template net20
On-Prem Template Premat: source-default-in On-Prem Template On-Prem Template	0 0 0 0 0 0 0 0 0 0 0 0 0 0
Template Properties ~	Actions ~ Description ButGet ~ SELECT + Create Coper
Networks 😤	Add Network NDFC Properties
net20	Layer2 Only
	stretched-wrf \times \sim
	Network Profile *
	Default_Network_Universal
	Network Extension Profile *
	Default_Network_Extension_Universal X 🗸
	VLAN ID
	VLAN Name
	* Gateway IP

f) Define other optional parameters for this network, if necessary.

Step 22 In the Template Properties area, click Actions > Sites Association. Figure 147:

≡ •i[i:i]i. cisco Nexus Dashboard . Orchestrator ∨				Feedback
Stretched Schema			2 / 1000 Objects Save So	chema 🛈 tì X
View On-Prem Template ~		Add New Template	Network net20	© ×
On-Prem Template Tenant: dcnm-default-tin	Associated Sites In Sync 0 Out of Sync 0	Topplay to sales	O Common Properties	0
Femplate Properties ~	0	(Actions ~)	Display Name* net20 Deployed Name: Description	
Filter		IMPORT	plate	
Networks 😪		Add	Network ID 💿	^
net20			Layer2 Only	
			Virtual Houting & Forwarding # *	
			Network Profile *	
			Default_Network_Universal	×v
			Network Extension Profile *	
			Default_Network_Extension_Universal	×v
			VLAN ID	
			VLAN Name	
			* Gateway IP	
			172.16.20.1/24 Type: primary	/ 11

Step 23 Associate this template only to the on-premises site (the Sydney site in this example use case), then click **Ok**.

Figure 148:

≡ ^{•1]•1]•} Nexus Dashboard				Feedback 1
Stretched Schema			2/3000 Objects Save	Schema 💿 🔃 🗙
View On-Prem Template ~		(Add New Terriplate)	Network met20	© ×
On-Prem Template	Associated Sites • Spec 0 • Got at Spec 0		Common Properties	
Template Properties ~	Add Sites To On-Prem Template	×	nezo Deployed Name: Description	
	Name			
Networks	AWS 25.5(Te)		NDFC Properties	
	C Azure Sither Sydney			
	12.1.2.275		Virtual Routing & Forwarding 🗮 * stretched-vrf	
			Default_Network_Universal	
			Default_Network_Extension_Universal	

You are returned to the On-Prem Template window.

Step 24From the Template Properties drop-down, select the on-premises site (the sydney site in this example use case), click
the net20 network, then click Add Static Port to add the ports where you want to deploy this network.
The Add Static Port window appears.

Figure 149:

Stretched Schema		2/100) Objects Save S	Schema 🕘 tù 🗙
View On-Prem Template ~	Add New Template	Network		3
Sydney On Prum Template	Depubly to white	- tical major	- minor	- warning
Sydney @ Guard Save V	Actors	mmon Properties pipy Name * 20 Single Name: 20		
	DF	ICP Servers erver Address		
	Su Pa L	Add DHCP Server atic Ports th eaf VLAN	Ports	

- Step 25 In the Add Static Port window, click Add Path.
- The Add Static Port window appears.
- **Step 26** In the **Leaf** field, select the device where you want to deploy this network.
- **Step 27** (Optional) Enter the necessary information in the VLAN field.

Step 28 In the **Ports** field, select the ports where you want to deploy this network.

Step 29

Step 30

Figure 150:

Click Save.

≡ diudi. cisco Nexus Dashboard	hestrator ->	Feedback 上 🖸
Stretched Schema	1 States and a state	2/1000 Objects Save Schema 🕢 Cl 🗙
View On-Prem Template ~	(Add New Temptate)	Network X
Sydney	Add Static Port	×
On-Prom Template Tenant: dcnm-default-tn	Harding Nextus Dashboard I rookestrator Inded Schema 2 / 1000 deprets On-Prem Template ~ Add Static Port Static administration Inded Static Port Path Leaf VLAN Ports Index Static Ports Path Leaf VLAN Ports Index Static Ports Index Static Ports Vitable Ports Index Static Ports	orts Properties
Sydney @ Dut of Sync. V	Leaf ndrc-leaf1 ~ ndrc-leaf2	ame -
	VLAN 2320	00
Networks	VPC48 X VPC51 X VPC52 X 👌	Il Properties
	Add Puth	3 Geteway Border
		optiack ID
		Server Address
		Static Ports Path
		Add Static Port

You are returned to the Add Static Port window.

In the Add Static Port window, click Submit.

Figure 151:

≡ disco Nexus Dashboard Orchestrator					Feed
Stretched Schema					
View On-Prem Template ~				Add New Template	Network net20
Sydney Version 3 On-Priem Temptate	Associated Sites				major entical minor and
Tenan; donm-default-in Sydney @ out at sym				(Section or section)	Common Properties Display Name * net20 Depoyed Name: ret20
	Add Static Port	VIAN	Boste	×	
Networks Pret20	ndfc-leaf1 ~ ndfc-leaf2	2320	VPC49 VPC51 VPC52	/1	Site Local Properties Tenant Routed Multicast
	Add Path				
				Submit	DHCP Servers Server Address
					Add DBCP Server Static Ports Path
					Leaf VLAN Ports

You are returned to the **On-Prem Template** window.

- Step 31 Click the arrow next to the on-premises site (the sydney site in this example use case), and from the drop-down menu, select Template Properties.
- Step 32 Click Deploy to Sites.

Figure 152:



The Deploy to Sites window appears, showing the site where the template will be deployed.

Figure 153:

≡ cisco Nexus Dashboard	Feedback 💄 📀
Stretched Schema	2 / 1000 Objects 🛛 😨 الله 🗙
View On-Prem Template ~	mplate Con-Prem Template
Associated Sites	Template Settings
Deploy to sites Modifications	X View Version History Deployment Plan
✓ + Greated ✓ Modified ✓ III Deleted ✓ Econig Drift ✓ Migrated Object Time Name	
Network Net20 + Created	
	Deploy

Step 33 Click **Deployment Plan** for additional verification, then click on the on-premises site to see the deployment plan for that specific site.

L

Figure 154:

≡ cisco Nexus Dashboard . Orchestrator ∨			Feedback 💄 🕘
Stretched Schema			as 🚺 🕘 () 🗙
View On-Prem Template ~		Add New Template	×
Deployment Plan			×
General Information Template On-Prem Template	Schema Stretched Schema	Tenant donm-default-in	
Plan		Oreated Objetered OModified	OExisting @Shadow
O dom-default-tn ener20 O stretched	• vPC49 - ndro-teat2 • vPC51 vrf • vPC52		(View Payload)

Step 34 C

Click **Deploy** to have NDO push the configurations to NDFC.

Figure 155:

≡ cisco Nexus Dashboard Orchestrator ->	Feedback
Stretched Schema	2 / 1000 Objects State Science 🕢
View On-Prem Template ~	Add New Template On-Prem Template
On-Prem Template Version 6 Applied to 1 sites Tenunt: dcnm-default-tn	Last Deployed: Jan 24, 2023 09:22 pm Deploy to allow Deploy Name* On-Prem Template Deploy Name Deploy Name Deploy Name Deploy Name
Template Properties ~	Actions -
Filter	IMPORT - SELECT + Create Object - Template Type NDFC
Networks ×	Add Network Tenant Settings Display name domm of adult to Name Common Seturation
	Description Default tenant for NDFC

Step 35 Verify that the configurations were deployed successfully.

Note that for each of these verification steps, the exact command that would be used specifically for the configurations in this use case are shown. Replace the appropriate variables in each command based on your configuration.

- a) In NDO, verify that the configurations were deployed successfully.
 - Verify that the Stretched Template was deployed successfully.

Figure 156:

able and	Schemas			Templates	
es	Schemas			Q. Search	Template Stretched Template
plication Management	Filter by attributes			Stretched Template	General
ric Management	Name	Templates	Tenants	Stretched Schema On-Prem Template	Change Control Status
arations	Stretched Schema	2 02	1	Stretched Schema	Tenant Name dcnm-default-tn
egration					Sites By Type
					APIC AVIS
					3 Azure NDFC
					Googe Could
					Application Management
	10				0 0
	10 V Rows				ANPS BRIDGE DOMAIN
					0 0
					CONTRACT EXTERNAL EPG
					0 0
					HOLEY LOOT
					0 0
					MELYNUNGS SERVICE GRAPHS

• Verify that the On-Prem Template was deployed successfully.

Figure 157:

	ooard 🖉 🙏 Orchestrator 🗸			Templates	Feedback 上
Dashboard Sites	Schemas			Q. Search	Template On-Prem Template
Application Management	Filter by attributes			Stretched Template Stretched Schema	General A
Fabric Management Operations Infrastructure Integration	Name Stretched Schema	Name Templates Bretched Schema 2 02	Tenants 1	On-Prem Template Stretched Scheins	Control Galaxies Displayment Successful Tenant Name dorm-offall: fin Sites By Type
	10 v Rows				Application Management

• Verify that the dcn-default-tn tenant was deployed successfully.

Figure 158:

Sashboard	Schemas		Tena	ints		
Sites	oononido		Q. 9	earch	Tenants dcnm-default-tn	0
Application Management	Filter by attributes		dcnm	-default-tn	General	^
abric Management	Name	Templates	Tenants	ed Schema.	Name dcnm-default-tn	
operations	Stretched Schema	2 02	1		Description Default tenant for NDFC	
ntegration					Associated Sites	
					• Sites (3)	- 3 of 4
					Associated Users	
					Users (1)	of 1
					Assigned Schemas	
					Schemas (2)	2 of 1
	10 ~ Rows				Topology	^
	- Andrews					
					6	
					6	
					S S.	

- b) In NDFC, verify that the following were done successfully:
 - Verify that one vrf and one network has been created.

Figure 159:

≡ cisco Nexus Dashboard	🔅 One View 🗸		Feedback 👤
F Fabric Controller			. (
 ☆ Dashboard ☆ Topology ⇒ LAN ~ 	Data Center / default / Sydney View + - 2 0 20 20 Search by Attributes		Actions ~
Virtual Management Virtual Management Settings Virtual Management Virt	Show Logical Links	NET VRF C1 Meta-fatzand2-Azure VM (3)	
	Muti-select O	es ntt-hapen ntt-kear1 ntt-kear1	

• Verify that the VRF was deployed successfully.

Figure 160:



• Verify that the network was deployed successfully.

Figure 161:



c) Enter sh ip route vrf stretched-vrf on the on-premises Border Gateway Spine device:

m drfc-leaf1 - SecureCRT		-	×
File Edit View Options Transfer Script Tools Window Help			
- ● ● □ ● □ ● ● ● ● ● ● ● ● ● ● ● ● ● ●			
0) Ondfc-ext-c8k Ocat8K-AWS V Cat8K-AZURE V ndfc-leaft × Ondfc-spine Ocat8K-AWS (1) Cat8K-AWS-2			0 Þ
Certain components of this software are licensed under Certain components of this software are licensed under thus General Public License (GPL) version 3.0 or the GNU Lesser General Public License (LGPL) version 2.1 or A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/gpl-2.1.php and http://www.opensource.org/licenses/gpl-2.1.php and http://www.opensource.org/licenses/gpl-2.1.php and http://www.opensource.org/licenses/library.txt. ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# ndfc-leafl# 10.230.0.0/16, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 00:16:32, bgp-65084, internal, tag 65091, segid: 150555 tunnelid: 0xa0a0001 encap: V2 70.1.0.0/16, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 00:17:37, bgp-65084, internal, tag 65092, segid: 150555 tunnelid: 0xa0a0001 encap: V2 72.16.20.0/24, ubest/mbest: 1/0, attached *via 172.16.20.1, vlan2320, [0/0], 00:04:48, direct, tag 12345 *via 12.16.20.1, vlan2320, [0/0], 00:04:48, local, tag 12345 *via 12.2.16.20.1, vlan2320, [0/0], 00:04:48, local, tag 123	XLAN		~
Default			

For this use case, using the routing table, you can verify that the NDFC leaf switch can reach out to the following subnets:

- AWS: 10.230.0.0/16
- Azure: 70.1.0.0/16
- d) Connect to the Cloud Network Controller deployed on AWS and make the following verifications:
 - Verify that the donm-default-tn tenant is created and one VPC is deployed:

← → C ▲ Not secure https:// Ø DMZ2-VCenter ● fab2vnd226 ● ND	44.238.203.132/#/application-mai	nagement/tenants -AWS @ cAPIC-Azure 🍅 AWS Inf	ira 🛕 Azure 🎯 Images						년 ☆	Update 👔
Ŧ	cisco Cloud Ne	etwork Controller (A	WS) aws						000	
Dashboard	Tenants									O
Topology Cloud Resources	Fitter by attributes									(Actions ~)
Application Management					Applica	ation Management			Cloud Resource	ces
Tenants	Health	Name	Description	Application Profiles	EPGs	VRFs	AWS Account	Regions	VPCs	Endpoints
Application Profiles	Healthy	common		1	0	2		0	0	0
EPGs Contracts	Healthy	dcnm-default-tn	Default tenant for	0	0	1	117378746 411	2	1	1
Filters VRFs	🗆 🔉 Major	infra	NDPC	1	15	2	257591685 230	2	1	12
Services	Healthy	mgmt		0	0	2		0	0	0
External Networks	15 🗸 Rows							Page 1	✓ of 1	< 1-4 of 4 ▶ ▶
Deperations V										
C Infrastructure V										

• Verify that the VPC is deployed:

← → C ▲ Not secure https://4	4.238.203 0-231	NDFC-224 @ cAPI	anagement/tenants C-AWS @ cAPIC-Azure 😑 AWS	Infra 👗 Azure 🛞 Images		Ê	🖈 🔲 🛓 Update 🚦	
Ŧ	alla Ci	cloud N	etwork Controller (Q 🧕	000		
Dashboard	Tenants			dcnm-default-tn : VPCs			×	
Topology	101	Indi ito			VPC			
Cloud Resources				Q Search	stretched-vrf		Ľ	
Application Management				stretched-vrf 10.230.0.0/16		V Healthy		
Tenants		Health	Name	dcnm-default-tn > us-west-2	General		~	
Application Profiles		• Healthy	common		Account			
EPGs			dama defeute te		dcnm-default-tn			
Contracts		Healthy	NDO		Region			
Filters					us-west-2			
VRFs		Major	inira		Cloud Resources		~	
Services		Healthy	mgmt					
Cloud Context Profiles					1	4	0	
External Networks	1:	5 V Rows			Regiona	Cloud Availability Zones	Routers	
Operations					1	0	1	
⊖ Infrastructure ∨					Security Groups	Instances	Endpoints	
1º Administrative V					Application Manageme	int	^	
					0	0	1	
					Application Profiles	EPGs	Cloud Context Profiles	
					1	0		
					VBFa	Service Graphs		
					Cattinge			

- Using the routing table view from the Cloud Network Controller deployed on AWS, verify that the reachable subnets are:
 - NDFC: 172.16.20.0/24
 - Azure: 70.1.0.0/16
| VPC stretched-vrf | | | Actions | ✓ ■ ● O − × |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Oveniew Topology Cloud Resources Application | Management Event Analytics | Subnets for CIDR Block 10.230.0.0/16 | | × |
| General
Account
dcm-oefault-tn
Region
us-west-2 | Settings
Cloud Access Privilege
Inherited (Routing & Security)
Cloud Provider ID
vpc-057/c951679a0971d | 10.230.1.0/24
10.230.2.0/24 | Settings
Cloud Access Privilege
Inherited (Routing & Security)
Cloud CIDR*s Subnet
10.230.1.0/24
Name | |
| Cloud Resources 1 4 0 Territory Conges Cond Analability Zames Descens 1 0 2 Descript Conges Descens Exposes | vpc-057/c951679a0971d
CIDRs
CIDR Block Range
10 230 0.0/16 | | Route Table Settings
Name
stretched-vrt-egress
Oper State
configured
Cloud Provider ID
rtb-04d472959543ce393
Direction
egress
Entries
Destination Address *
172_16_20_1/24
70.1_0_0/16 | Next Hop
Hub Network
tgw-034a97d05ed64b877
Hub Network |
| SVPC stretched-vrf | | | Actions | ✓ ■ ○ - × |
| Overview Topology Cloud Resources Application
General
Account
dcmm-default-in
Region
us-west-2
Cloud Resources | Management Event Analytics Settings Cloud Access Privilege Inherited (Routing & Security) Cloud Provider ID vpc-057/695157940971d CIDRs CIDR Block Range | Subnets for CIDR Block 10.230.0.0/16 | Settings
Cloud Access Privilege
Inherited (Routing & Security)
Cloud DDR'S Subnet
10.230.2.0/2.4
Name
-
-
Boute Table Santione | |
| 1 4 0 Import Cloud Australity Zone Boolers 1 0 2 | 10.230.0.0/16 | , | Notice Table Sectings
Name
stretched-vrf:egress
Oper State
configured
Cloud Provider ID
rtb-04d472959543ce393 | ^ |

- e) In the AWS console, verify the following:
 - Verify that you see one VPC and two subnets.



				[MIC+3]						6				
VPC dashboard X	Subne	ets (2) Info									C Actions	•	Create subr	iet
EC2 Global View 🖸 New Filter by VPC:	Q Fi	iter subnets											< 1 >	0
Select a VPC 🛛 🔻		Name	⊽	Subnet ID	∇	State	∇	VPC V	IPv4 CIDR	∇	IPv6 CIDR	∇	Available	Pv4 addr
Virtual private cloud		subnet-[10.230.1.0/24]		subnet-02e03f2bc17ffc9da		⊘ Available		vpc-057fc951679a0971d con	10.230.1.0/24		-		250	
Your VPCs		subnet-[10.230.2.0/24]		subnet-0318aa2d5634350d1		⊘ Available		vpc-057fc951679a0971d con	10.230.2.0/24		-		250	
Subnets	•													,
Route tables														
Internet gateways														
Egress-only internet gateways														
Carrier gateways														
DHCP option sets														
Elastic IPs														
Managed prefix lists														
Endpoints														
Endpoint services														
NAT gateways	Select a	subnet												

• Verify that you see the routing table.

aws 🔛 s	ervices Q Search		[Alt+S]		D 4 0	Oregon 🔻 demo @ 1173-7874-641
VPC dashboar EC2 Global Vi Filter by VPC: Select a VPC	rd X iew 🔁 tere :	$\label{eq:VPC} \begin{array}{l} \text{VPC} \end{tables} \end{tables} \end{tables} \end{tables} \end{tables} \end{tables} \text{ rb-04d472959543ce393} \\ \hline \textbf{rb-04d472959543ce393} \end{tables} \\ \hline \textbf{@} \end{tables} \end{tables} \begin{array}{l} \text{VPC} \end{tables} t$	routetable-[stretched	l-vrf:egress]	Run Reacl	Actions 🔻
Your VPCs Subnets		Details Info				
Route tables Internet gate Egress-only ir gateways Carrier gatew DHCP option Flastic IPs	ways nternet rays sets	Route table ID G rtb-046472859543ce395 VPC vpc-057fc951679a0971d context-[stretched- vrf]-addr-[10.230.0.0/16]	Main D No Owner ID D 117378746411	Explicit subnet-o318aa2d5634350d1 subnet-02e03f2bc17ffc9da / t	Edea stractisticat / subnet-[10.230.2.0/24] X ubnet-[10.230.1.0/24]	
Managed pret Endpoints	fix lists	Routes Subnet associations Edge asso	ciations Route propagation Ta	igs		
Endpoint serv NAT gateway: Peering conne	vices s ections	Routes (3)		Both		Edit routes
▼ Security						
Network ACL	s	Destination ∇	Target			∇
Security grou	ips	10.230.0.0/16	local	⊘ Active	No	
▼ Network Ana	lysis	70.1.0.0/16	tgw-034a97dd5ed64b877	⊘ Active	No	
Reachability /	Analyzer	172.16.20.0/24	tgw-034a97dd5ed64b877	⊘ Active	No	
Network Acce	ess Analyzer					

- f) Connect to the Cloud Network Controller deployed on Azure and make the following verifications
 - \bullet Verify that the <code>dcnm-default-tn</code> tenant is created:

Ŧ	cisco Cloud	Network Controller (Azu	re) 🔥 Azure						Q 🔊 🖸	000
Dashboard	Tenants									O
Topology										
Cloud Resources										Actions
Application Management				Application	Applic	cation Management			Cloud Resources	
Application Dration	Health	Name	Description	Profiles	EPGs	VRFs	Subscription	Regions	Virtual Networks	Endpoints
EPGs	Healthy	common		1	0	2		0	0	0
Contracts	Healthy	dcnm-default-tn	Default tenant for NDFC	0	0	1	Shared from infra	1	1	0
Filters	C Major	infra		1	12	2	74094178-	1	1	10
VRFs							bf23- 41e85a1a3ada			
Services	C Healthy	mgmt		0	0	2		0	0	0
Cloud Context Profiles	C V Healthy									
External Networks	15 V Rows								Page 1 v of 1	≪ ≪ 1-4 of 4 ⇒ ⇒
Infrastructure										
t ^o Administrative										
=	ababe Cloud	Network Controller (Azı	Ire) Aarra						00	308 8 🗊
	cisco Cloud	Network Controller (Azı	ITE) Azure						® 0	0000
E a Datbard i Toology	Cloud Tenants	Network Controller (Azı	ure) 🔥 Azure dcnm-	-default-tn : V	firtual Netwo	rks			@ 0 (>000 ×
E ■ Dastboard ● Topology ▲ Cloud Resurces ∨	-diale Cloud Tenants Terra anotae	Network Controller (Azu	Jre) Azure	-default-tn : V	firtual Netwo	orks	Stretch	¥etavork 9ed−vrf	® o (>0 © 0 • ×
Dasboard Topology Cool Resurces Cool Resurces Cool Resurces Cool Resurces Cool Resurces	-thete Cloud Tenants	Network Controller (Azu	ure) Azure donm-	-default-tn : \	'irtual Netwo	vrks	Stretch	¥etwork ed∼vrf	C Healthy) () () () × ··· :
Darboard Topology Cloud Resources Cool Resources Cool Resources Cool Resources Cool Resources Cool Resources	Heatth	Network Controller (Azu	Jre) Acure dcnm- c stratcher be	-default-tn : \ -default-tn : \ a-wr701.0.0/16 efault-tn > eastus	firtual Netwo	rks	Stretch	ietaork ed-vrf	Image: Second state Image: Second st	>0 © @ • × c
Dearboard Topolegy Cloud Resources V Application Management Application Profiles	Initial Cloud Tenants Prim to enterior	Network Controller (Azu Name common	Jre) Azure dcnm- Q be	-default-tn : \ 	'irtual Netwo	rks	General Account	letnork nod-vrf	Image: Second state Image: Second st	x
Dearboard Topology Cloud Resources Cad Resources	-II-II-Cloud Cisco Cloud Tenants Tens Is an Anti- Heath O Heathy	Network Controller (Azu Name common	Jre) Acure dcnm- De	-default-tn : \ == d-wt701.0.0/16 afault-tn > eastus	'irtual Netwo	rks	Ceneral Account dom-defau	ietwork ed-vrf	S S C	x
	-Internet Cloud -Internet Clo	Network Controller (Azu Name common dcom-default-in	Jre) Acure dcnm- De be for	-default-tn : \ -default-tn : \ -d-vrt70.1.0.0/16 afwalt-tn > eastus	'irtual Netwo	rks	General Account dom-defau Ropon	tetmork led-vrf	Sector Control Con	x
	-(iso Cloud -(iso	Network Controller (Azu Name common dcom-default-in infra	Jre) Acure dcnm- De be	-default-tn : \ -default-tn : \ a-wt 70 1.0.0/16 efault-tn > eastus	firtual Netwo	orks	Ceneral Account dorm-defau Region eastus	ietwork ied-vrf R-In	C Healthy	x
E Topoboard Topoboard	- Cloud - Clo	Network Controller (Azu Name common dcom-dafaat-in intra	Jre) Acure dcnm- De ber for	-default-tn : \ -default-tn : \ -d-wf 70.1.0.0/16 efault-tn > eastur	firtual Netwo	orks	Ceneral Account dorm-data Region estus Cloud Reso	ketwork ked-wf R-tn	C Healthy	x
E Topology C Topology	- (Inc) - Cloud - Clo	Network Controller (Azu Name common dcom-dafauf-in intra	Jre) Acure dcnm- De be for	-default-tn : \ -default-tn : \ a-wt 70.1.0.0/16 efault-tn > eastus	firtual Netwo	rks	Ceneral Account docum-datu Region estus Cloud Reso	eteork ed-vrf ft-tn urces	C Healthy	×
Deshboard Deshboard Tookky Ooud Resources V Application Management Application Profiles Filters Vitr's Bennices Senicides Cloud Characters Profiles Cloud Characters Profiles Cloud Characters Profiles	- cloud creater - cloud - creater - cloud - creater - cloud -	Network Controller (Azu Name common dcmm-dafauft-in intra	Jre) Acure dcnm- De ber for	-default-tn : \ -default-tn : \ -wt 70 1.0.0/16 efault-tn > eastus	Ĩirtual Netwo	rks	Ceneral Account Region estus Cloud Reso	setwork led-orf ft-tn urces 1	Healthy	1 1 1 1 1 1 1 1 1
Danhboard Danhboard Topology Topology Coold Resources Contract Polis Contracts Filers Viti's Services Contract Profiles External Networks Contract Profiles	Cloud Creating For the product For t	Network Controller (Azu Name common doxm-dafault-in infta mgmt	Jre) Acure dcnm- Q e be for	-default-tn : \ os d-wr70.1.0.0/16 d-wr70.1.0.0/16	Ĩirtual Netwo	rks	Ceneral General Account derom-data Region eastus Cloud Reso	ietuurk ied-vrf R-in urces	C Healthy	1 North States (1997)
	Cloud Creants For the pathode Health Health Health Health Health Health Health Health Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kaper Kap	Network Controller (Azu Name common doxm-dafauft-in infta mgmt	Jre) Acure dcnm- Q e be for	-default-tn : \ on d-wr70.10.0/16 d-wr70.10.0/16	Ĩirtual Netwo	rks	Ceneral Account Region eastus Cloud Reso	ieteorik ied-vrf R-in urces 1 npus 1 Sentry Group	C Healthy	1 Mark Starty Starty Company New Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Starty Sta
	Cloud Creating For the setting O Healthy O Healthy O Healthy O Healthy O Healthy Ts Nove	Network Controller (Azu Name common domr-dafault-in infta mgmt	Jre) Acare denm- e stetche for	-default-tn : \ on d-wr 70.1.0.0/16 draut-tn > eastua	firtual Netwo	rks	Ceneral Account dcm-adfau Region estus Cloud Reso	tehaork and-vrf R-tn urces 1 ngwm 1	C Healthy Healthy C	1 1 1 1 1 1 1 1 1 1 1 1 1 1
	- Interference Cloud Cl	Network Controller (Azu Name common domr-dafault-in infta mgmt	Jre) Anne denm- e steetste for	-default-tn : \ on d-wr 70.1.0.0/16 afault-tn > eastua	firtual Netwo	rks	General Account dcem-adfau Region eastus Cloud Reso Loud Reso Application	etanok ed-vrf R-tn arces 1 gum 1 Secrity Singet	C Healthy C Healthy Barren O Uncertification	1 1 1 1 1 1 1 1 1 1 1 1 1 1
	Instruction Classified Sector Classified Sector	Network Controller (Azu Name common doom-default-in infia infia	Jre) Acure dcnm- Q istectes be for	-default-tn : \ th fault-tn > eastus	firtual Netwo	rks	Ceneral Account dom-defau Region eastus Cloud Reso Cloud Reso	At-In At-In Ar-In Ar-In Arrows 1 Secury Grayat Management 0	C Healthy C Heal	1 1 1 1 1 1 1 1 1 1 1 1 1
Daabboard Topology Topology Could Resources Could Resources Could Resources Could Cou		Network Controller (Azu and Common Common doem-default-in infla infla ingent	Jre) Acure dcnm- o stretche for	-default-tn : \ ch de-wf 70.1.0.0/16 afault-tn > eastus	firtual Netwo	orks	Centeral Account dcmr-defac Region eastus Cloud Reso Cloud Reso Application Application	Interacrit arces 1 Secury Groups 1 Secury Groups Management 0 exce Parlins	C Healthy C Heal	
Dashboard Topology Topology Topology Cloud Resurces You Acplication Profiles Folia Contracts Folia Contracts Folia Contracts Folia Contracts Folia Contract Profiles UNF's Services Contract Profiles Con		Network Controller (Azu Name common docm-default-bn infta infta mgmt	Jre) Acure dcnm- Q isteration De for	-default-tn : \ a-wt 70.1.0.0/16 afault-tn > eastus	firtual Netwo	orks	Central Account dominant domin	Interaction Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna Alterna	C Healthy C Heal	Construction

• Verify that the VRF is deployed:

	cis	Cloud Netv	vork Controller (Azure) 🔥 Azure					9	00000 💶
Dashboard	VR	Fs							0
Topology	VIX								0
🐽 Cloud Resources 🔍	VRFs	Leak Routes							
Application Management	Eller								(Actions ~)
Tenants	-			Ap	plication Management		Clou	d Resources	
Application Profiles		Health	Name	EPGs	Cloud Context Profiles	Regions	Virtual Networks	Routers	Endpoints
EPGs							-		Lingonito
Contracts		 Healthy 	ave-ctri infra	0	0	0	0	0	0
Filters		Healthy	сору	0	0	0	0	0	0
VRFs			common						
Services		· Healthy	default common	0	0	0	0	0	0
Cloud Context Profiles		C Healthy	inb	0	0	0	0	0	0
External Networks			mgmt						
EI Operations V		Healthy	oob mgmt	0	0	0	0	0	0
O Infrastructure ~		· Healthy	overlay-1 Internal	12	1	1	1	2	10
1º Administrative \lor			infra						
		♥ Healthy	stretched-wrf internal	0	1	1	1	0	0
	15	✓ Rows						Page 1 🗸	of 1 4 4 1-7 of 7 ⊨ ⊨

- Using the routing table view from the Cloud Network Controller deployed on AWS, verify that the reachable subnets are:
 - NDFC: 172.16.20.0/24
 - AWS: 10.230.0.0/16

o Virtual Ne	twork stret	ched-vrf				∎ => o - ×
Overview Topology	Cloud Resource	es Application Manag	gement Event Analytics	Subnets for CIDR Block 70.1.0.0/16	1 30 110/04	×
General Account dcnm-default-tn Region eastus			Settings Cloud Access Privilege Inherited (Routing & Security) Cloud Context Profile Statched-off-eastus CIDRs CIDRs	70.1.1.0/24	Settings Cloud Access Privilege Inherited (Roding & Security) Cloud CIDR's Subnet 70.1.1.0/24 Name	
Cloud Resources	0 Routers 0 Virtual Machines	1 Network Security Groups 0 Endpoints	Cloud Provider ID //ubbcriptions/14094178-7856-468a-bf23-41e85a1s3ada/resourceGr //ubbcriptions/14094178-7856-468a-bf23-41e85a1s3ada/resourceGr //t_eastbs/providers/Microsoft/Network/virtualNetworks/atteched-virt		Route Table Settings Name stretchedvrt agress Oper State configured Cloud Provider ID Subacristicat (2004 178,-7855-468,-947	^
Application Manageme	ent				41e85a1a3ada/resourceGroups/CAPIC_do tn_stretched- vrf_eastus/providers/Microsoft.Network/rc	.nm-default- outeTables/rt-stretched-
0 Application Profiles	O EPGs O	1 Cloud Context Profiles			vrf_egress Direction egress Entries	
1071	Service Graphs				Destination Address • 10.230.0.0/16	Next Hop 10.90.1.36 Hub Network
					172.16.20.1/24	Hub Network
					172.16.20.0/24 Copied	10.90.1.36

g) In the Azure console, verify that you can see the subnets:

Home > Virtual networks > stretched-vrf						6		CISCO-INSBU	мкт
Virtual networks «	stretched-vrf Subne	ets ☆ …							\times
+ Create 🔕 Manage view 🗸 … 👂 Sea	earch «	+ Subnet + Gatev	ay subnet 🕚 Refres	h 🥄 🦓 Manage users	🖲 Delete				
Filter for any field	verview	P Search subnets							
Name T. S. AO	ccess control (IAM)	Name \uparrow_{\downarrow}	IPv4 ↑↓	IPv6 ↑↓	Available IPs 1+	Delegated to ↑↓	Security group †	Route table 14	
6-> stratcharlourf • Tag	igs	subnet-70.1.1.0_24	70.1.1.0/24		251		subnet-70.1.1.0_24	rt-stretched-vrf_egress	
/ Dia	agnose and solve problems								
Setting	gs								
↔ Ad	ddress space								
ø co	onnected devices								
<a> Sui	ubnets								
× Bat	astion								
0 00	DoS protection								



Route Leaking Use Case

- About the Route Leaking Use Case, on page 143
- Configure the Necessary Templates, on page 145
- Configure Route Leaking, on page 163

About the Route Leaking Use Case

This route leaking use case uses separate templates for each site, which contains VRF and network definitions for the on-premises site, whereas for cloud sites these templates only contain the VRF definition. Unlike the stretched VRF (intra-VRF) use case described in Stretched VRF Use Case, on page 107, which does not require any configurations for exchanging prefixes between the sites because the same VRF is stretched to all sites, you must configure VRF leaking for this use case because each site uses a different VRF.

To propagate the prefixes between the sites (on-premises as well as cloud sites), you must explicitly configure route leaking on the respective templates associated with the sites.

Figure 162:



As shown in the figure above, each site has a separate associated template, which contains VRF/network definitions specific to that site only. On-Prem Template is associated to the NDFC managed on-premises site, whereas AWS Template and Azure Template are associated to the AWS and Azure cloud sites, respectively. Inter-VRF route leaking is configured explicitly between different VRFs to allow communication between the sites.

L

Configure the Necessary Templates

Use the procedures in the following sections to configure the templates that you will need for the route leaking use case.

Configure the On-Premises Site Template

In this section, you will configure the On-Prem Template that will be associated to the NDFC managed on-premises site.

Step 1 In NDO, navigate to Application Management > Schemas and click Add Schema.

Step 2 Provide the schema name and click **Add**.

For this use case, we will name the new schema VRF Route Leaking Schema.

Figure 163:

≡ elseb Nexus Dashboard Orchestrator ∨						Feedback 💄 🌘
Untitled Schema						1000 Objects Save Schema 🏷 🗙
View Overview ~						(Add New Template)
Overview						
General		Audit Logs				
Name Description		Created 0	Deleted 0	Updated 0	Deployed 0	
Sites	General		×			
Type APIC 0	Name *		Sync 0			
* NDFC 0 • AWS 0	VRF Route Leaking Schema		it of Sync. 0			
Atri Coopia Doud Ration 9	Description		Add			
Application Management						
deplocation Profiles (0)	• VIS's (0) •		• Fitara (0)			

You are returned to the Overview page for the new VRF Route Leaking Schema schema.

- Step 3 Under the VRF Route Leaking Schema schema, click Add New Template.
- **Step 4** Choose the NDFC template.
- **Step 5** Enter a name in the **Display Name** field to create an NDFC-type template (for example, On-Prem Template).
- **Step 6** Select the dcnm-default-tn tenant in the **Select a Tenant** field to map the template to that tenant.

Figure 164:

= dhulu				Foodback I O
				Teeuback 2
VRF Route Leaking Schema				4/1000 Objects ⊕₹1 X
View On-Prem Template	-	Add New Template Save	On-Prem Template	×
On-Prem Template Version 8 Applied to 1 stres Template Com-default-tn Template Properties	Associated Sites In Sync 1 Out of Sync 0	Last Deployed: Dec 3, 2022 12:53 pm Orpitry to sales Actions ~	Template Settings Display Name* On-Prem Template Description	
Filter		IMPORT - SELECT 🔁 CREATE OBJECT -	Template Type NDFC	
♥ VRFs ∨ 			Tenant Settings Display name dcnm-default-tn Name dcnm-default-tn Description	^
Networks v net10			Default tenant for NDFC sites	

- **Step 7** Under **Template Properties**, click **Create Object** and choose **VRF** to create a VRF that will be used with the NDFC managed on-premises site.
 - **Note** If you have an on-premises VRF already created that you want to use instead of creating a new VRF, under **Template Properties**, click **Import**, then import the already-created VRF.

Currently, support is only available for importing VRFs and networks from on-premises sites.

Step 8 Enter a name in the **Display Name** field for this VRF (for example, v10).

Figure 165:

≡ ^{••[]••]•} Nexus Dashboard . Orchestrator ∨				Feedback 💄 🔮
VRF Route Leaking Schema			1 / 1000 Obje	NCL Save Schema 🏷 🗙
View On-Prem Template \vee		Add New Template	VRF v10	×
On-Prem Template Tenant: dom-default-to	Associated Sites In Sync 0 Out of Sync 0	Bripfury to union	Common Properties	0
Template Properties V		Actions	Deptryvel Name: Description	
VRFs ~		Add VR#	NDFC Properties	^
VID			VRF Profile * Default_VRF_Universal	××
			VRF Extension Profile * Default_VRF_Extension_Universal	×v
			Loopback Routing Tag 12345	
			Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET	
			Disable RT Auto-Generate	
			Select	
			Export O	

- **Step 9** Under **Template Properties**, click **Create Object** and choose **Network** to create a network.
 - **Note** If you have a network already created that you want to use instead of creating a new network, under **Template Properties**, click **Import**, then import the already-created network.

Step 10 Enter a name in the **Display Name** field for the network (for example, net10).

Step 11In the Virtual Routing & Forwarding field, choose the v10 VRF to map the net10 network to that VRF.Figure 166:



Step 12In the Gateway IP field, click Add Subnet and provide the gateway IP address, then click Add.Figure 167:

≡ diudio cisco Nexus Dashboard Orchestrator ∨			Feet	inack 🛓 💿
VRF Route Leaking Schema				× is
View On-Prem Template ~		Add New Template	Network net10 data ar classor t science a	© ×
On-Prem Template Tenent: donn-default-tri	Associated Sites * tipe 0 * dzid Spec 0		0 0 Common Properties Display Name*	
Template Properties ~		Actions		
	Add Subnet ×	+ Create Daject	NDFC Properties	
	172.16.10.1/24 primary V			
S Networks ~		Add Network		
			Network Extension Profile * Default_Network_Extension_Universal	
			* Gateway IP	
			Add Swinet Suppress ARP	

The gateway IP address is now displayed in the Gateway IP field.

Figure 168:

≡ disco Nexus Dashboard Crohestrator ~		Feedback 上 🤋
VRF Route Leaking Schema		2/1000 Objects Save Schema ti X
View On-Prem Template ~	Add New Tremplate	Network O ×
On-Prem Template Tenaric dones default in	ssociated Sites • Day 0 • Out of Syme 0 • Day 1 Syme 0	UNED IN COMMENT OF COMMAN UNIC IN COMMENT OF COMMAN O O Company Name* sate
Template Properties > Filter	Actions -	Description
VRFs ~	Add VRF	NDFC Properties
v19	Add Network	Layer2 Only
net10		v10 × ~ Network Profile * Default,Network,Universal × ~
		Network Extension Profile * Default_Network_Extension_Universal X V
		VLAN ID VLAN Name
		* Gateway IP 172:16:10:1/24
		Type: primary Add Subnet

- **Step 13** Define other optional parameters for this network, if necessary.
- Step 14In the Template Properties area, click Actions > Sites Association.

Figure 169:

E cisco Nexus Dashboard 2 Crohestrator -			Feedback 1
/RF Route Leaking Schema		2 / 1000 Objects Save	Schema 🤃 🗙
/iew On-Prem Template ~	dd New Template	Network	0
On-Prom Template On-Prom Template		USED IN CURRENT SCHEMA USED BY OT	0
Transft: dcnm-default-in	Deploy to sides	Common Properties Display Name*	
emplate Properties ~	Actions	Deployed Name:	
IMPORT - SELECT + Create C	Delete Templ Sites Associa	tion	
VRFs \vee	Clone Templa	Network ID G	
vio		Laver2 Only	
🕲 Networks 😒	Add Network	Virtual Routing & Forwarding *	
ner10		v10 Network Profile *	×
		Default_Network_Universal	×
		Default_Network_Extension_Universal	×
		VLAN ID	
		VLAN Name	
		* Gateway IP 172:16:10:1/24	/
		Type: primary	
		Add Subnet	

Step 15 Associate this template only to the on-premises site (the sydney site in this example use case), then click Ok.

L

Figure 170:

≡ dindin cisco Nexus Dashboard . ♠ orei	estrator ~				Feedback	10
VRF Route Leaking Schema					4 / 1000 Objects - ①てえ	×
View On-Prem Template ~	Add N	New Template	0	Template On-Prem Template		×
On-Prem Template Version 8 Applied to 1 sites Tenant: dcnm-defauit-tn	Add Sites To On-Prem Template	Der 2. 2022 12:52 em	×	• Settings lame* n Template		
Template Properties 🗸	Name			vame: on		
	▲ AZURE 25.1(te)			Туре		
IVRFs ∨ 10	Sydney 12,2,2,275			ettings ame fault-tn		
			Ok Default	fault-tn Lion t tenant for NDFC sites		
neti0						

- **Step 16** Click **Template Properties** and select the on-premises site (the sydney site in this example use case), then select the v10 VRF.
- **Step 17** In the right pane, click **Add Static Leaf**.

Figure 171:

E disco Nexus Dashboard A Orchestrator ∞	Feedback
VRF Route Leaking Schema	2/1000 Objects Sever Schema 12 X
View On-Prem Template \sim	Add New Template v10
Sydney Sydney Arbon Template	Critical major minor warning
Sydney Condige V	Template Properties
Fitter	Deskyption
VRFs	Vie tu U NA Site Local Properties ∧
V 10	Tenant Routed Multicast PP External PP External
Networks	Static Leaf Nodes Node/Switch
Prietto	ndfc-spine1 🗸 🕿
	ndfc-leaf1 ~ ndfc-leaf2 / =
	Add Static Leaf

The Add Static Leaf window appears.

Step 18 In the **Leaf** field, select the leaf/border/border gateway device where this VRF is to be deployed and click **Ok**.

In this example, you need to deploy the VRF on the leaf nodes (where the endpoints part of the network mapped to the VRF will be connected) and on the BGW spine node to be able to extend the Layer 3 connectivity for the VRF towards the cloud sites.

Step 19 To attach the network to the leaf switches, click the net10 network, then click **Add Static Port** to add the ports where you want to deploy this network.

The Add Static Port window appears.

- Step 20In the Add Static Port window, click Add Path.
- The **Add Static Port** window appears.
- **Step 21** In the **Leaf** field, select the device where you want to deploy this network.
- **Step 22** (Optional) Enter the necessary information in the VLAN field.
- **Step 23** In the **Ports** field, select the ports where you want to deploy this network.
 - Click Save.

Step 24

Figure 172:

≡ ditutiti cisco Nexus Dashboard Orchestrator ∽				Feedback 💄
VRF Route Leaking Schema			2/1000 0	bjects Save Schemar () 🗙
View On-Prem Template ~		Add New Template	Network	
Sydney	Associated Sites Associated Sites Associated Sites		major	evinor warring
	Add Static Port	×	Common Properties	
Sydney Count Synce V	Path Leaf	VLAN Ports	net10 Deployed Name Description N/A	
Viers V	ndfc-leaf1 - ndfc-leaf2 VLAN 2310	~	Network ID (c) N/A Site Local Properties Tenant Routed Multicast	
Networks	Ports vPoda x VPost x VPost x V Cancel	Save		
InetID	Add Puth		DHCP Servers Server Address	
		Submit	Static Ports Path Lenf VLAN P	orts
			Add Stalic Port	

You are returned to the Add Static Port window.

Step 25 In the Add Static Port window, click Submit.

Figure 173:

≡ cisco Nexus Dashboard Orchestrator	~						Feedback 上 🤇
VRF Route Leaking Schema						2 / 1000 Objects	Save Scheme CL X
View On-Prem Template ~					Network		×
Sydney On Prom Template	Associated				eritical	jai - minor	- warning
Film	Add Static Port Path Leaf ndfc-leaf1 - ndfc-leaf2	VLAN 2310	Ports vPC49 vPC52	×	Common Properties Display Name * nat10 Description NVA Network ID () NVA Site Local Properties		
Networks	Add Path		Hide All∨				
				Sutent	DHCP Servers Server Address		
					Path Leaf	VLAN Ports	

You are returned to the on-premises template window.

Figure 174:

≡ ^{d]tu]n} Nexus Dashboard A Orchestrator ∨		eedback 上 📀
VRF Route Leaking Schema	2 / 1000 Objects Save	Schema () X
View On-Prem Template ~	Template net10	×
Sydney On Prem template On Prem templa	critical major minor	- warning
Sydney • On at See	Common Properties Display Name * net10 Display Name: Display Name: Description N/A Network ID Q	~
Vers ~	Site Local Properties Tenant Routed Multicast Enable L3 Gateway Border	^
Networks Metro	DHCP Loopback ID	
	DHCP Servers Server Address	
	Add DHCP Server Static Ports Path	
	Leaf VLAN Ports	
	vPC49 ndfc-leaf1 ~ ndfc- leaf2 vPC51 vPC52 Hide All√	<i>·</i> •
	Add Static Port	

- **Step 26** Click the arrow next to the on-premises site, and from the drop-down menu, select **Template Properties**.
- Step 27 Click Deploy to Sites.

Figure 175:

≡ ^{-ifficiti} . Nexus Dashboard Orchestrator -		Feedback 上 📀
VRF Route Leaking Schema	2 / 1000 Object	s Save Schema () X
View On-Prem Template ~	On-Prem Template	×
On-Prem Template Applied to 1 sites Template Properties On disubiting	Template Settings Display Name* On-Prem Template Deployed Name: Description	^
Filter Buffolt - SELECT + Create Coged	Template Type NDFC	
VRFe Add VRF V10	Tenant Settings Select a Tenant * dcnm-default-tn	^ × ~
Networks Add Network exetto		

- **Step 28** Deploy On-Prem Template to the sites.
 - Click **Deployment Plan** for additional verification.

Click on the on-premises site to see the deployment plan for that specific site.

Figure 176:

cisco Nexus Dashboard . Orchestrator		Feedback 🛓 🖉
RF Route Leaking Schema		2/1000 Objects
		Template
Deployment Plan		×
Template On-Prem Template	Schema VRF Route Leaking Schema	fenant dcnm-default-tn
Plan		
Sydney		○Created OPeleted OModified OExisting @Shadow
		(View Payload)
e vio	c-spine i	
O donim-default-tn	2.16.10.3/24 ••• vPC49	
@ net10 @ nd	ic-leaf1~ndfc-leaf2+@ vPC51	
O vit	• vPC52	

- Click **Deploy** to have NDO push the configurations to NDFC. This pushes the NDO configurations to NDFC.
- **Step 29** In NDFC, verify that the VRF was deployed successfully.

L

Figure 177:

Ŧ	Fabric Controller		
Â	Dashboard	💿 Data Center / 🔘 default / 💭 VRFs (2) / 💭 v10	
×	Topology	View A Search by Attributes	
=	LAN V	$(+ - 2 \circ \mathbb{I} \times)$	
•	Virtual Management 🗸 🗸	Operation Configuration	
۵	Settings ~	Hierarchical	
£	Operations v	 In-Sync Pending In Progress Out-of-Sync NA Muti-select O O selected	
		B ndtc-leat2 ndtc-leat1	

What to do next

Follow the procedures provided in Configure the Azure Site Template, on page 153.

Configure the Azure Site Template

In this section, you will configure the Azure Template that will be associated to the Azure site.

Before you begin

Follow the procedures provided in Configure the On-Premises Site Template, on page 145.

- Step 1 Under the VRF Route Leaking Schema schema, click Add New Template.
- **Step 2** Choose the NDFC template.
- **Step 3** Enter a name in the **Display Name** field to create an NDFC-type template for the Azure site (for example, Azure Template).
- **Step 4** Select the dcnm-default-tn tenant in the Select a Tenant field to map the template to that tenant.

Figure 178:

≡ dialio cisco Nexus Dashboard . Crehestrator ~			Feedback 👤 🕐
VRF Route Leaking Schema			4/1000 Objects のたえ 🗙
View Azure Template ~	Add New Template Save	Template Azure Template	×
Acure Template Version 17 Appled to 1 sites Template to 1 sites Template to 1 sites Template to 1 sites	Last Deployed: Dec 4, 2022 09:40 pm Deploy to sites	Template Settings Display Name* Azure Template	^
Template Properties ~	Actions ~	Deployed Name: Description	
Filter	IMPORT SELECT 🔀 CREATE OBJECT	Template Type NDFC	
VRFs V szure10	Add VRF	Tenant Settings Display name dcmdefault-In Name dcmdefault-In Description Default tenant for NDFC sites	^

Step 5 Under **Template Properties**, click **Create Object** and choose **VRF** to create a VRF that will be used with the Azure site.

Figure 179:

≡ disco Nexus Dashboard			Feedback 💄
/RF Route Leaking Schema		3 / 1000 Objects	Save Schema の たよう
View Azure Template >	Add New Template	Template Azure Template	
Azure Template Associated Sites O · Sign: 0 · Sign: 0	(Stabley linear)	Template Settings Display Name* Azure Template Deployed Name:	,
emplate Properties V	Actions	Description Template Type NDFC	
	Network	Tenant Settings Select a Tenant * dcnm-default-tn	××
Let's create an object Click "Create Object" on template properties to create an object			

Step 6 Enter a name in the **Display Name** field for this VRF (for example, azure10).

Figure 180:

E cisco Nexus Dashboard A Orchestrator	Feedback
VRF Route Leaking Schema	4/1000 Objects Save Schema の たみ X
View Azure Template ~	(Add New Temptate) Szurs10
Azure Template Fenant: dozen-default in	Operation unce to receive a contract 0 0 0 0 Common Properties ∧ Display Name* ⊙ >
Template Properties V	Actions ~ MMPORT ~ SELECT + Create Object - BMPORT ~ SELECT + Create Object -
VRFs V	Add Vier NDFC Properties
azure10	VRF Profile * Default_VRF_Universal × V
	VRF Extension Profile * Default_VRF_Extension_Universal ×
	Loopback Routing Tag 12345
	Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET
	Disade KI Auto-Generate

Step 7 In the **Template Properties** area, click **Actions** > **Sites Association**.

Figure 181:

		Feedback
VRF Route Leaking Schema		4 / 1000 Objects Save Schema の た
View Azure Template ~		Add New Template azure 10
Azure Template Tenant: come-default-tn	Associated Sites Asociated Sites Asoci	Units occessor for contain Units occessor for contain 0 0 0 Common Properties Display Name* 0
Template Properties ~		Actions Activity Dephysic Martini
Filter		IMPORT - SELECT + Create Object Template Sites Association
VRFs ~		Clove Template Appenties VRF ID O
azure10		VRF Profile *
		VRF Extension Profile *
		Default_VRF_Extension_Universal >>
		Loopback Routing Tag
		12345
		FABRIC-RMAP-REDIST-SUBNET
		Disable RT Auto-Generate

Step 8 Associate this template only to the Azure site, then click **Ok**.

Figure 182:

≡ cisco Nexus Dashboard Orche	strator ~			Feedback
VRF Route Leaking Schema			4 / 1000 Objects Save	Schema 🕕 🦚
View Azure Template ~		Add New Template	VRF azure10	
Azure Template Appled to 1 Sites Tenant: donm-default-tri	Associated Sites * a Spec * a Spec * do at draws	(Deploy to altern	Common Properties	
Template Properties ~	Add Sites To Azure Template	×	azureno Deployed Name: Description	
VRFs ~	Name AWS ASSIST		NDFC Properties	
	C Azure zs.trai Sydney: Sydney:		VRF Profile * Default_VRF_Universal	
			VRF Extension Profile * Default_VRF_Extension_Universal	
	-		Loopback Routing Tag 12345 Redistribute Direct Route Map	

- Step 9Click the azure10 VRF, then click Add Region to create the VNet in a selected region.
The Add Cloud Region CIDRs window appears.
- **Step 10** In the **Region** field, choose the region where you want to create the VNet.
- Step 11 In the CIDR field, click Add CIDRs and define a CIDR block for the VNet.
- **Step 12** Click **Add Subnet** to create the subnets, then click **Save**.

Figure 183:

cisco Nexus Dashboard . Orchestrator			Feedback
F Route Leaking Schema			00 Objects Save Scheme 🕢 🥲
		VDF	
dd Cloud Region CIDRs			
ion *			
talene Ousstau			X Y.
Enabled			
Rs	Turne	VDE	
5	13340		
DR *			
0.1.0.0/16			
DR Type ① Primary			
Secondary			
ect Associated VRF			
Parent VICP Prosted VICP			
ubouners ubnet Name Private Link Labels Availability Zone			
0.11.0/24 V X			
And Subar			
Print Administ			
Cancel	1		
	1		

Step 13 Check the box under the **VNet Peering** field, then select the hub network that was created on the Cisco Cloud Network Controller for Azure.

Figure 184:

≡ disco Nexus Dashboard ★ Orchestrator -					Feedback 🛓 🕻
VRF Route Leaking Schema					4/1000 Objects Sever Schema @ ti X
Unable to get template Template2 from schema 63c/87d0c15e	Sa21ab89985f by name		×	VRF azore10	×
Add Cloud Region CIDRs					×
Region *					
eastus					\times \sim
Container Overlay Enabled					
CIDRs					
CIDR	Туре	VRF			
90.1.0.0/16	Primary	azure10			/=
Add CIDRs					
VPN Gateway Router					
VNet peering					
Else Metrovela					
Default					× v

Step 14 Click Ok.

You are returned to the Azure template window.

Step 15 Click the arrow next to the Azure site, and from the drop-down menu, select Template Properties.

Step 16 Click Deploy to Sites.

- **Step 17** Deploy Azure Template to the sites.
 - Click Deployment Plan for additional verification.

Click on the Azure site to see the deployment plan for that specific site.

Figure 185:

≡ cisco Nexus Dashboard Orchestrator ∨			Feedback	10
VRF Route Leaking Schema				τ×
View Azure Template ~			Template Azure Template	
	Associated Sites		Template Settings	~
Deployment Plan				×
General Information Template Azure Template	Schema VWF Route Leaking Schema	Tenant dcnm-default-tn		
Plan			Created ODeleted Modified Existing Shadow	
O route-target.as2-rnx423456:155_ O done-default-tn O azuer02 O route-target.as2-rnx423456:311_			(View Payload)

• Click **Deploy** to have NDO push the configurations to NDFC.

To verify that the configurations were pushed out correctly, connect to the Cloud Network Controller deployed on Azure and navigate to **Cloud Resources** > **Virtual Networks**, then click the azure10 VNet and use the information in the Overview page for additional verifications:

Figure 186:

Virtual Network azure10			Actions 🗸 🗖 🖚 🔿 — 🗙
Overview Topology Cloud Resources Application General Account dcnm-default-tn Region eastus Cloud Resources 1 0	Management Event Analytics Settings Cloud Access Privilege (Cloud Access Privilege Cloud Context Profile azure10-eastus ClDRs ClDRs DIDR Block Range Pl 90.1.0.0/16 ye	Subnets for CIDR Block 90.1.0.0/16	Actions I III Constraints Actions IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
1 0 2 Brown Brown Hences Growny Orace 1 0 0 Application Security Orace Vital Machines 0 Application Management 0 1 Application Management Etrois 1 0 0 1 1 0 Security 1 0 Security 1 0 Security	Cloud Provider ID		Name azure 10-egress Oper State configured Cloud Provider ID Direction egress Entries Destination Address * Next Hop

Note that there is no destination address configured at this point in the process, so the Azure site cannot talk to any other site yet at this point in the process. This destination address configuration will be pushed out after you have completed the route leaking procedure.

What to do next

Follow the procedures provided in Configure the AWS Site Template, on page 158.

Configure the AWS Site Template

In this section, you will configure the AWS Template that will be associated to the AWS site.

.

Before you begin

Follow the procedures provided in Configure the Azure Site Template, on page 153.

Step 1	Un Un	ider the	VRF	Route	Leaking	Schema SC	hema, (click	Add .	New	Template.	

Step 2 Choose the NDFC template.

__ _ _

- Step 3 Enter a name in the Display Name field to create an NDFC-type template for the AWS site (for example, AWS Template).
- Step 4 Select the dcnm-default-tn tenant in the Select a Tenant field to map the template to that tenant.

Figure 187:

≡ cisco Nexus Dashboard . ♣ Orchestrator ~				Feedback 上 🤊
VRF Route Leaking Schema				4/1000 Objects のひと 🗙
View AWS Template ~		Add New Template Sive	Template AWS Template	×
Applied to 1 sites fenant: dcnm-default-tn	Associated Sites In Sync Out of Sync 1	Last Deployed: Dec 4, 2022 09:40 pm Deploy to sites	Template Settings Display Name* AWS Template	^
Template Properties 🗸		Actions ~	Description	
Filter		IMPORT	Template Type NDFC	
ws10			Tenant Settings Display name dcnm-default-tn Name dcnm-default-tn	^
X			Description Default tenant for NDFC sites	

- **Step 5** Under **Template Properties**, click **Create Object** and choose **VRF** to create a VRF that will be used with the AWS site.
- **Step 6** Enter a name in the **Display Name** field for this VRF (for example, aws10).

Figure 188:

≡ ditulu cisco Nexus Dashboard . Crchestrator ~	Feedback 🛓 🕄
VRF Route Leaking Schema	4/1000 Objects のたり 🗙
View AWS Template Associated Sites Associated Sites	Add New Template Ser VRF Ser
Avv3 Terriplate version is Avv3 Terriplate version is Tennot: dcrm-default-tn Template Properties ~	0 Common Properties Common Prop
Filter	Description Descri
aws10	VRF ID () 157172 VRF Profile *
	Default_VRF_Universal X v VRF_Extension Profile * Vertex (VRF_Extension_Universal) Default_VRF_Extension_Universal X v
	Loopback Routing Tag Redistribute Direct Route Map
	FABRIC-RMAP-REDIST-SUBNET

- **Step 7** In the **Template Properties** area, click **Actions** > **Sites Association**.
- **Step 8** Associate this template only to the AWS site, then click **Ok**.

Figure 189:

≡ ^{•1} ••1 • cisco Nexus Dashboard	strator v		Feedback 👤
VRF Route Leaking Schema		3 / 1000 Objects Save S	thema 🛈 💱 🗙
View AWS Template \sim		Add New Template ows 10	×
AWS Template Terrant: dcnm:-default-tn	Associated Sites ** Box 0 ** Out of Syste 0	Common Properties Display Name*	
Template Properties ~	Add Sites To AWS Template	xens to Debugged Name: Description	
VRFs ~	AWS	NDFC Properties	
	State State Sydney 12.12.275	VNP Profile * Default/VNP_Universal VPP Encansion Profile *	
		Control Default, VRF_Extension, Universal Loopback Routing Tag 12345	
		Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET	

- Step 9 Click the arrow next to Template Properties, and from the drop-down menu, select the AWS cloud site.
- Step 10Click the aws10 VRF, then click Add Region to create the VPC in a selected region.
The Add Cloud Region CIDRs window appears.
- **Step 11** In the **Region** field, choose the region where you want to create the VPC.
- **Step 12** In the **CIDR** field, click **Add CIDRs** and define a CIDR block for the VPC.
- Step 13Click Add Subnet to create the subnets and map them to the availability zones, then click Save.Figure 190:

cisco Nexus Dashboard	Orchestrator ~			Feedback
Route Leaking Schema				3/1000 Objects Save Schema 🕢 🤱
				VDF
dd Cloud Region CIDRs				
n *				
west-2				Xx
ainer Overlay Fnabled				
s				
1		Туре	VRF	
a thr	100 M			
DR *				
10.220.0.0/16				
DR Type ①				
Primary Secondary				
/ Secondary				
ibnet Name Priva	ate Link Labels Availability Zone			
0004.0/04		1		
.220.1.0/24	us-west-za 🗸 🗙	-		
.220.2.0/24	us-west-2b 🗸 🗙			
Add Polyant		4		
Aug Subriet				
	Cancel Save			

Step 14 Check the box under the **Hub Network** field, then select the hub network that was created on the Cisco Cloud Network Controller for AWS.

This allows the Cisco Cloud Network Controller to attach the subnets onto the transit gateway, which builds the connectivity from those subnets to the transit gateway, where the transit gateway already has the connectivity to the Cisco Catalyst 8000Vs in the cloud.

Step 15 In the **Subnets** field, map the subnets that will be used for the transit gateway.

It is best practice to have a dedicated subnet that will be used for the transit gateway.

Figure 191:

cisco Nexus Dashboard	Orchestrator ~		Feedback
RF Route Leaking Schema			3 / 1000 Objects Save Schema 🕢 🏷
			VRF
Add Cloud Region CIDRs			,
egion *			
us-west-2			×
intainer Overlay) Enabled			
DRs	Type	VRF	
.220.0.0/16	Primary	aws10	/=
Add CIDRs			
N Gateway Router	ck the Hub Network option and deploy the template first. Then re-enable the opti	on, select the new Hub Network, and redeploy the template.	×
bnets			
0.2201.0/24 × 10.220.2.0/24 ×			>
			F

Step 16 Click Ok.

You are returned to the AWS template window.

- Step 17 Click the arrow next to the AWS site, and from the drop-down menu, select Template Properties.
- Step 18 Click Deploy to Sites.

Figure 192:

≡ disco Nexus Dashboard / I I Orchestrator ~	Feedback 1 0
VRF Route Leaking Schema	3 / 1000 Objects Save Schema 🕢 🕅 🗙
View AWS Template ~	Template AWS Template
AWS Template Appled in 1 state Template Properties Template Properties	Template Settings Uppay kane* AND Template Dispryso Name Description
Fitter NetFort - SELECT + Create Object -	Template Type NDFC
VRFs v Add VRF	Tenant Settings ^ Select a Tenant *

Step 19 Deploy AWS Template to the sites.

• Click Deployment Plan for additional verification.

Click on the AWS site to see the deployment plan for that specific site.

Figure 193:

≡ ditulu cisco Nexus Dashboard Orchestrator ∨		وجهارها ويعار والعادي		Feedback 👤 🔿
VRF Route Leaking Schema				× <i>t</i>) © (2 × 1
View AWS Template ~			Template AWS Template	×
	Associated Sites		Template Settings	~
Deployment Plan				×
General Information © Template AVS Template	Schema VRF Route Leaking Schema	Tenant dom-default-tn		
Plan			Ocreated ODeleted OModified (DExisting Shadow
				View Payload
O donm-default-tn O aws10 O route-targettas2-m4/23456-158_ O route-targettas2-m4/23456-318_				

• Click Deploy to have NDO push the configurations to NDFC.

To verify that the configurations were pushed out correctly, connect to the Cloud Network Controller deployed on AWS and navigate to **Cloud Resources** > **VPCs**, then click the aws10 VPC and use the information in the Overview page for additional verifications:

Figure 194:

leo VPC aws10			Actions 🗸 🔲 🔿 — 🗙
Overview Topology Cloud Resources Application Manage	ement Event Analytics	Subnets for CIDR Block 10.210.0.0/16	×
General	Settings	10.210.1.0/24	Subnet
Account dcnm-default-tn	Cloud Access Privilege Inherited (Routing Only)	10.210.2.0/24	Settings Cloud Access Privilege
Region us-west-2	Cloud Provider ID		Cloud CIDR's Subnet 10.210.1.0/24
Cloud Resources	CIDR Block Range P		Name -
1 4 O Regions Cloud Availability Zones Routers	10.210.0.0/16 y		Route Table Settings
1 0 0			Name aws10:egress
Security Groups Instances Endpoints			Oper State configured
Application Management			Cidd Provider iD
0 0 1 Application Profiles EPGs Cloud Context Profiles			Direction egress
1 O			Entries Destination Address * Next Hop
			10.210.0.0/16 Copied local

Note that there is a destination address configured at this point in the process for AWS, but this shows only that this AWS site can talk to itself; the AWS site cannot talk to any other site yet at this point in the process. The necessary destination address configuration that will allow the AWS site to talk to another site will be pushed out after you have completed the route leaking procedure.

What to do next

Configure route leaking using the procedures provided in Configure Route Leaking, on page 163.

Configure Route Leaking

Use the procedures in the following sections to configure the route leaking use case.

Configure Route Leak from Azure VRF to NDFC VRF

In this section, you will configure the route leak from the Azure VRF (azure10) to the NDFC VRF (v10).

Before you begin

Configure the necessary templates using the procedures provided in Configure the Necessary Templates, on page 145.

- **Step 1** Click the Azure Template that you configured earlier in these procedures and the dcnm-default-tn tenant.
- **Step 2** Click the azure10 VRF that you configured earlier in these procedures.
- **Step 3** In the right pane, click **Add Leak Route**.

Figure 195:

≡ distin Nexus Dashboard Orchestrator ~						Feedback 上 💿
VRF Route Leaking Schema					4 / 1000 Objects	× €7 ⊕ mentana
View Azure Template ~			Add New Template	VRF azure10		×
Azure Version 3	Associated Sites In Sync 0	Last Deployed: Ja	n 24, 2023 07:17 pm .	 critical m	ajor minor	- warning
Tenant: doim-default-in Azure @ ourritipe: Filter			Actions >	Template Propertie Display Name * azure10 Description N/A VRF ID O 155847 Site Local Propertie Context Profiles	s D	^
				eastus CIDR: 90.10.0/76 Add Region Leak Routes		/ =
				VIO Internal VIF Route Leaking Schema Template > donm-default-1	Routes	/ 1
				aws10 Internal VBF Route Leaking Schem Template > dcnm-default-1	s>AWS 90.1.1.0/24 m	/ =

The Add Leak Routes window appears.

Step 4 In the Add Leak Routes window, click Select a Target VRF.

Figure 196:

≡ disco Nexus Dashboard . Crchestrator			
VRF Route Leaking Schema			4 / 1000 Objects
View Azure Template ~		Add New Template	VRF azure10
Azure Version 1 Azuro Temptate	Associated Sites		eriticat major minor
	U		Template Properties Display Name *
Azure • Inspec •		Actions	azure10 Deployed Name: azure10 Description
	Add Leak Routes	×	
VRFs V	Target VRF		Site Local Properties
	Select a Target VRF >		Context Profiles Region
			eastus CIDR: 9010.0/18
			Add Region Litak Routes Target VRF Routes
			Add Leak Route

The Select a Target VRF window appears.

Step 5 In the Select a Target VRF page, select the NDFC VRF (v10) that you want to leak routes to, then click Select.

Figure 197:

Figure 198:

RF Route Leaking Schema				
/iew Azure Template ~			VRF azure10	
Azure Version 1	Associated Sites • Bype 1 • Dard Sync 0	Last Displayed: Jan 24, 2023 06:33 pm	- critical	
Zure • in two: V	Select a Target VRF	×	Template Propert Display Name * azure10	lies
	Q. Search a Target VRF	v10	Deployed Name; azur Description N/A	
VRFs ~	stretched-vrf Internal Stretched Schema > Stretched Template	Name v10	VRF ID () 155847	
	VRF Route Leaking Schema > On-Prem Template aws10 Internal	General Antonia Contraction Co	Site Local Propert Context Profiles Region	des .
	VKH- Koute Leaking Schema > AWS Template azure10 Internal VRF Route Leaking Schema > Azure Template	Description VRF Route Leaking Schema - On-Prem Template - dcnm-default-tn	eastus cicre servicio/re	
		Setting Site Associations	Add Region	Routes
		Select	Add Leak Route	

You are returned to the Add Leak Routes window.

- **Step 6** In the Add Leak Routes window, click Add Subnet IP, then add the Azure cloud subnets that you want to propagate to the on-premises site.
 - **Note** The **Add Subnet IP** option allows leaking of only selective subnets. Alternatively, you can use the **All Subnet IPs** option instead in the case where all the prefixes need to be leaked into a destination VRF.

/RF Route Leaking Schema			
View Azure Template ~		Add New Template	VRF azure10
Azure Version 1 Azure Template	Associated Size		major
Azure • nove v	Add Leak Routes Target VRF vt0 × Routes to Target VRF () Type () Subnet IP All Subnet IPs	×	Template Properties Display Name 1 azure10 Description N/A VRF ID (0 155647 Site Local Properties
	IP Address 90.11.0/24 Add Subnet IP	~ 8	Context Profiles Region eastus cone soloonte O Add Region
			Leak Routes Target VRF C Add Leak Route

For this use case, you will use the 90.1.1.0/24 subnet.

Step 7 Click Ok.

You are returned to the Azure Template page, where you can see the configuration for this route leak from the Azure VRF to the NDFC VRF.

What to do next

Follow the procedures provided in Configure Route Leak from Azure VRF to AWS VRF, on page 166.

Configure Route Leak from Azure VRF to AWS VRF

In this section, you will configure the route leak from the Azure VRF (azure10) to the AWS VRF (aws10).

For these procedures, you will be going through the exact same procedures that you performed in Configure Route Leak from Azure VRF to NDFC VRF, on page 163, except in these procedures, you will be selecting a different target VRF (the AWS target VRF in these procedures).

Before you begin

Follow the procedures provided in Configure Route Leak from Azure VRF to NDFC VRF, on page 163.

 Step 1
 In the Select a Target VRF page, select the AWS VRF (aws10) that you want to leak routes to, then click Select.

 Figure 199:

VRF Route Leaking Schema				000 Objects Sive S	ichema 🛈 tì 🗙
View Azure Template ~			VRF ozure10		
Azure version 1	Associated Sites		• • critical roaper		
	Select a Target VRF	×	Template Properties Display Name 1		
Azure • steel ···	Q. Search a Target VRF	aws10			
	stretched-vrf Internal Stretched Schema > Stretched Template	Name aws10			
Fazure10	VID Internal VRF Route Leaking Schema > On-Prem Template aws10 Internal	General Tenant dcnm-default-tn	Site Local Properties Context Profiles Region		
	azure10 Internal VRF Route Leaking Schema > Azure Template	Description VRF Route Leaking Schema - AWS Template - dcnm-default-tn	eastus core sociolité		× 11
		Setting Site Associations	Leak Routes Target VRF	Routes	
		Select			/ 1
			Add Lesk Route		

You are returned to the Add Leak Routes window.

Step 2 In the Add Leak Routes window, add the subnets that you want to propagate to the AWS cloud.

For this use case, you will use the 90.1.1.0/24 subnet. Therefore, you will click the dropdown menu and choose the 90.1.1.0/24 subnet.

Figure 200:

/RF Route Leaking Schema			4/3	000 Objects	chema 🕘 (1)
View Azure Template ~			VRF azure10		
Azure Version 1 Azure Template	Associated Sites • April 1 • April 1 • April 1		eritical major	- minor	warning
Azure • nov	Add Leak Routes Target VRF aws10 × Routes to Target VRF ()	×	Template Properties Display Name * azure10 Deskyed Name asure10 Description N/A VRR ID (0) 1955847		
VRFs Fazure10	Type O Subnet IP All Subnet IPs IP Address		Site Local Properties Context Profiles Region		
	90110/24 Add Submet IP		eastus click: 90:502/16 Add Region Leak Routes Target VRF	Routes	1
			Internal ordefined subdefined s dene- distuds in		1
			Add Leak Route		

Step 3 Click Ok.

You are returned to the Azure Template page, where you can see the configuration for this route leak from the Azure VRF to the AWS VRF, as well as the route leak from the Azure VRF to the NDFC VRF that you configured in the previous set of steps.

Step 4 Click the arrow next to the Azure site, and from the drop-down menu, select Template Properties.

Step 5 Click Deploy to sites.

Figure 201:

≡ ^{ciloulo} Nexus Dashboard ★ Orchestrator ∨	Feedback
VRF Route Leaking Schema	4/1000 Objects Sive common 🏵 🕄
View On-Prem Template ~	Add New Template
	NDFC Properties
On-Prem Template Version 1 Cast Deployed	d: Jan 24, 2023 06:25 pm 153412
Appled to 1 sites	VRF Profile *
	Default_VRF_Universal ×
Template Properties ~	VRF Extension Profile *
- compared a very second	Default_VRF_Extension_Universal ×
Filter BUPORT - SELECT	Create Object Loopback Routing Tag
	12345
VRFs \vee	Add VRF Redistribute Direct Route Map
	FABRIC-RMAP-REDIST-SUBNET
V10	Disable RT Auto-Generate
	Import ()
🕥 Networks 🖂	Add Network Select
	Export 🕥
netl0	Select
connected	Import EVPN ()
	Select
	Export EVPN ()
	Select
	Leak Routes 🛈
	Target VRF Routes
	Add Leak Route
	External Pretixes () Subnet
	Add Potentia
	Vou External Pretix

The Deploy to sites window appears, showing where the template will be deployed.

- **Step 6** Click **Deployment Plan** for additional verification, then click on a site to see the deployment plan for that specific site.
- **Step 7** Click **Deploy** to have NDO push the configurations to the site specific controllers.

Figure 202:

E diradin Nexus Dashboard A Orchestrator ∽		Feedback 💄 😗
VRF Route Leaking Schema		4/1000 Objects のたえ 🗙
View Azure Template ~	Add New Template	×
Deploy to sites		×
The current template has a dependency on 2 other templates. Please make sure all these templates are successfully deployed in the order t	to have a successfull deployment.Show Details	
Modifications		View Version History Deployment Plan
Created Z Modified Z 🏦 Deleted Z Z Config Drift		
Object Type Name Attraction VRF azure10 Zmodified		
		Deploy

What to do next

Follow the procedures provided in Configure Route Leak from AWS VRF to NDFC VRF, on page 168.

Configure Route Leak from AWS VRF to NDFC VRF

In this section, you will configure the route leak from the AWS VRF (aws10) to the NDFC VRF (v10).

Before you begin

Follow the procedures provided in Configure Route Leak from Azure VRF to AWS VRF, on page 166.

- **Step 1** Click the AWS Template that you configured earlier in these procedures and the dcnm-default-tn tenant.
- **Step 2** Click the aws10 VRF that you configured earlier in these procedures.
- **Step 3** In the right pane, click **Add Leak Route**.

Figure 203:

= st[tst]v. cisco Nexus Dashboard Orchestrator ↔				Feedback 💄 📀
VRF Route Leaking Schema		4 / 10	100 Objects	× {} 0 0
View AWS Template ~	Add New Template	/RF /ws10		×
AWS Version 1 AWS Tomolate	Last Deployed: Jan 24, 2023 06:30 pm	ical major	- minor	- warning
AWS © count spectrum Filter	County is with a set of the set o	nplate Properties play Name * s10 koyed Name: aws10 scription A F ID 3134		•
aws10	an Co R	ntext Profiles legion		^
		s-west-2 IDR: 10.220.0.0/16		/ =
		Add Region ik Routes arget VRF Add Leak Route	Routes	

The Add Leak Routes window appears.

- Step 4In the Add Leak Routes window, click Select a Target VRF.The Select a Target VRF window appears.
- **Step 5** In the Select a Target VRF window, select the NDFC VRF (v10) that you want to leak routes to, then click Select. You are returned to the Add Leak Routes window.
- **Step 6** In the Add Leak Routes window, click Add Subnet IP, then add the AWS cloud subnets that you want to propagate to the on-premises site.
 - **Note** The **Add Subnet IP** option allows leaking of only selective subnets. Alternatively, you can use the **All Subnet IPs** option instead in the case where all the prefixes need to be leaked into a destination VRF.

Figure 204:

≡ disco Nexus Dashboard • Orchestrator -					Feedback 1	•
VRF Route Leaking Schema			4/	000 Objects	0 () ×	
View AWS Template ~		[Add Rev Template]	VRF aws10			c
AWS Version 1	Associated Sites In Sync 0		major	- minor	warning	
Filter	Add Leak Routes Target VRF VIO × Routes to Target VRF () Type () Subert IP All Subert IPs	×	Template Properties Display Name 4 avts10 Destroto Name avts10 Dissorption N/A VRF 10 0 158134 Site Local Properties			
	10.2201.0/24 10.2202.0/24 ♥ Add Sabet (₽	く (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	Context Protes Region us-west-2 CORR 10/200,018 Add Region Lassk Routins Target VRF	Routes	/ 1	
			Add Leek Route			

For this use case, you will use the following subnets:

- 10.220.1.0/24
- 10.220.2.0/24

Step 7 Click Ok.

You are returned to the AWS Template page, where you can see the configuration for this route leak from the AWS VRF to the NDFC VRF.

What to do next

Follow the procedures provided in Configure Route Leak from AWS VRF to Azure VRF, on page 170.

Configure Route Leak from AWS VRF to Azure VRF

In this section, you will configure the route leak from the AWS VRF (aws10) to the Azure VRF (azure10).

For these procedures, you will be going through the exact same procedures that you performed in Configure Route Leak from AWS VRF to NDFC VRF, on page 168, except in these procedures, you will be selecting a different target VRF (the Azure target VRF in these procedures).

Before you begin

Follow the procedures provided in Configure Route Leak from AWS VRF to NDFC VRF, on page 168.

Step 1 In the Select a Target VRF page, select the Azure VRF (azure10) that you want to leak routes to, then click Select. You are returned to the Add Leak Routes window.

Step 2 In the Add Leak Routes window, add the subnets that you want to propagate to the Azure cloud.

For this use case, you will use the following subnets:

- 10.220.1.0/24
- 10.220.2.0/24

Therefore, you will click the dropdown menu and choose those subnets.

Figure 205:

VRF Route Leaking Schema			:473	000 Objects Save Sc	hima 🕢 Cl 🗙
View AWS Template ~		Add New Template	VRF aws10		5
AWS Version 1	Adsociated Sites in Sync 0	Last Dentryner: Jan 24, 2028 08:30 pm	mojor		warning
AWS Decord from two	Add Leak Routes Target VRF acuret 0 × Routes to Target VRF () 7ype () Type () Submet IP All Submet IPs	x	Template Properties Display Name * aver 10 Opticycol Hame, swcN0 Discol philon NVA VRF ID (O 15813.4 Sito Local Properties		
aws10	IP Address 10.220.1.0/24 10.220.2.0/24		Context Profiles Region us-west-2 citize 40.220.00/16		× 1
	Add Subnet IP		Add Region Litak Routes Target VRF	Routes	
			Internal settement - pedational - denom- detauti-on		/ 8
			Add Leak Route		

Step 3 Click Ok.

You are returned to the AWS Template page, where you can see the configuration for this route leak from the AWS VRF to the AZURE VRF, as well as the route leak from the AWS VRF to the NDFC VRF that you configured in the previous set of steps.

Figure 206:

≡ distance Nexus Dashboard Orchestrator					Feedback 💄 🤇
VRF Route Leaking Schema			4/10	000 Objects Save S	chema 🛈 () X
View AWS Template ~		(Add New Template)	VRF aws10		×
AWS Version 2	Associated Sites	Last Deployed: Jan 24, 2023 07:17 pm	major	= minor	- warning
AWS Template Tenant: dcnm-default-tn	Out of Sync 0	Breditoy to alter-	Template Properties		^
AWS • In Sync V		Actions ~	Display Name * aws10 Deployed Name: aws10		
Filter			Description N/A		
VRFs ~			158134		
Faws10			Site Local Properties Context Profiles Region		^
			us-west-2 CIDR: 10.220.0.0/16		/ =
			Add Region		
			Leak Routes Target VRF	Routes	
			v10 Internal VRF Route Leaking Schema > Cm-Pm Template > donm-default-tm	10.220.1.0/24 10.220.2.0/24	/ #
			azure10 Internal VRF Route Leaking Schema > Azure Template > doner-default-tri	10.220.1.0/24 10.220.2.0/24	/ =

Step 4 Click the arrow next to the AWS site, and from the drop-down menu, select Template Properties.

Step 5 Click Deploy to sites.

The Deploy to sites window appears, showing where the template will be deployed.

Step 6 Click **Deployment Plan** for additional verification, then click on a site to see the deployment plan for that specific site.

Step 7 Click **Deploy** to have NDO push the configurations to the site specific controllers (NDFC and Cloud Network Controller).

What to do next

Follow the procedures provided in Configure Route Leak from NDFC VRF to AWS VRF, on page 172.

Configure Route Leak from NDFC VRF to AWS VRF

In this section, you will configure the route leak from the NDFC VRF (v10) to the AWS VRF (aws10).

Before you begin

Follow the procedures provided in Configure Route Leak from AWS VRF to Azure VRF, on page 170.

- **Step 1** Click the On-Prem Template that you configured earlier in these procedures and the dcnm-default-tn tenant.
- **Step 2** Click the v10 VRF that you configured earlier in these procedures.
- **Step 3** In the right pane, click **Add Leak Route**.

Figure 207:

≡ ^{el[n]} • Nexus Dashboard A Orchestrator ∨	Feedback
VRF Route Leaking Schema	4/1000 Objects Save Schema の たよ X
View On-Prem Template ~	Add New Template
On Bran Tomplato Internation Associated Sites	Deployed: Jan 24, 2023 06:25 pm VCF Extension DmrRat *
Appendix to sizes Terant: dom-default-in	Deploy to alles Default_VRF_Extension_Universal X V
Template Properties ~	12345 Actions
Filter Merorr - StLECT	FABRIC-RMAP-REDIST-SUBNET Disable RT Auto-Generate
VRFs 🗠	Add VRP
01v	Export O Select
Networks ~	Add Network Import EVIPN () Select
net10 covecad	Export EVPN ©
	Lesk Routes 🔿 Target VRF Routes
	aws10 Internal Vitil Routo Leaking Schema x Jung Translate - Academic - Acade
	azure10 Internal V#P Insure Leaking Schema × Rame Template a dynamic addust in
	Add Leak Route External Prefixes
	· · ·

The Add Leak Routes window appears.

- Step 4 In the Add Leak Routes window, click Select a Target VRF. The Select a Target VRF window appears.
- Step 5 In the Select a Target VRF window, select the AWS cloud site VRF (aws10) that you want to leak routes to, then click Select.

You are returned to the Add Leak Routes window.

- **Step 6** In the Add Leak Routes window, click Add Subnet IP, then add the AWS cloud subnets that you want to propagate to the on-premises site.
 - Note The Add Subnet IP option allows leaking of only selective subnets. Alternatively, you can use the All Subnet IPs option instead in the case where all the prefixes need to be leaked into a destination VRF.

For this use case, you will use the 172.16.10.0/24 subnet.
Figure 208:

≡ cisco Nexus Dashboard Orchestrator ∨ //RF Route Leaking Schema		4 / 1000 Objects
The Hould Leaking Schema		
/iew On-Prem Template ~		NDFC Properties
On-Prem Template Version 1 Applied to 1 alter	Associated State *********************************	
	Add Leak Routes ×	Default_VRF_Universal >
emplate Properties ~	Target VRF	VRF Extension Profile * Default_VRF_Extension_Universal
	aws10 × Routes to Target VRF ①	Loopback Routing Tag 12345
VRFs ~	Type Subnet IP All Subnet IPs	Redistribute Direct Route Map FABRIC-RMAP-REDIST-SUBNET
	IP Address	Disable RT Auto-Generate
Networks v	1/216:00/24 V 0	Select
net10	_	Select
		Import EVPN O Select
		Leak Routes 💭 Target VRF Routes
		Add Leak Route External Prefixes
		Subnet

Step 7 Click Ok.

You are returned to the On-Prem Template page, where you can see the configuration for this route leak from the NDFC VRF to the AWS VRF.

What to do next

Follow the procedures provided in Configure Route Leak from NDFC VRF to Azure VRF, on page 173.

Configure Route Leak from NDFC VRF to Azure VRF

In this section, you will configure the route leak from the NDFC VRF (v10) to the Azure VRF (azure10).

For these procedures, you will be going through the exact same procedures that you performed in Configure Route Leak from NDFC VRF to AWS VRF, on page 172, except in these procedures, you will be selecting a different target VRF (the Azure target VRF in these procedures).

Before you begin

Follow the procedures provided in Configure Route Leak from NDFC VRF to AWS VRF, on page 172.

- Step 1In the Select a Target VRF window, select the Azure VRF (azure10) that you want to leak routes to, then click Select.
You are returned to the Add Leak Routes window.
- **Step 2** In the Add Leak Routes window, add the subnets that you want to propagate to the Azure cloud.

For this use case, you will use the 172.16.10.0/24 subnet. Therefore, you will click the dropdown menu and choose the 172.16.10.0/24 subnet.

Figure 209:

CISCO Nexus Dashboard . Orchestrato		Feedback
VRF Route Leaking Schema		4 / 1000 Objects Save Schema 🕖 🏷 🗙
View On-Prem Template ~	Associated Sites • Associated Sites • + 5 pp 1 total land based and based	NDPC Properties
Tenant: donm-default-to	Add Look Doutes	VRF Profile * Default_VRF_Universal K ~
Template Properties ~		VRF Extension Profile * Default_VRF_Extension_Universal X v
	azure10 × Routes to Tareet VRF ()	Loopback Routing Tag 12345
VRPs ··	Type O	Redistributes Direct Route Map FABRIC-RMAP-REDIST-SUBNET
	PAdress	Disable RT Auto-Generate
Networks ~	172.16.10.0/24 ✓ 🗊 ♦ Add Subnet (P)	Select
net10		Export Q Select
COMPACING .		Select.
		Leak Routes () Target VRF Routes
		Aws10 Internal VM Rose Leading Enternal + Aller VM Rose Leading Enternal + Aller VM Rose Leading Enternal + Aller
		C Add Lesk Roste

Step 3 Click Ok.

You are returned to the On-Prem Template page, where you can see the configuration for this route leak from the NDFC VRF to the AZURE VRF, as well as the route leak from the NDFC VRF to the AWS VRF that you configured in the previous set of steps.

Step 4 Click the arrow next to the on-premises site, and from the drop-down menu, select **Template Properties**.

Step 5 Click Deploy to sites.

Figure 210:

≡ ^{el} leile Nexus Dashboard . Crohestrator ~	Feedback 💄 🕄
VRF Route Leaking Schema	4/1000 Objects Stree Schema 🗿 🤃 🗙
View On-Prem Template ~	Add New Template
Associated Sites	Last Deployed. Jan 24, 2023 08:25 pm
On-Prem Template Version 1 Applied to 1 states Template version 1 Out of Systex 0	VRF Extension Profile * Default_VRF_Extension_Universal X V
Template Properties V	Loopback Routing Tag 12345
Fitter INFORT	SILICT + Create Object FABRIC-RMAP-REDIST-SUBNET
	Disable RT Auto-Generate
vies ~	Select
	Export () Select
Networks V	Add Network Import EVPN () Select
net10 connected	Export EVPN () Select ~
	Leak Routes 〇 Target VRF Routes
	aves10 Internal YB2.16.10.0/24 Temples 4 down down aves10 172.16.10.0/24
	azure10 Internal 172.16.10.0/24 * *
	Add Leak Route External Prefixes

The Deploy to sites window appears, showing where the template will be deployed.

Step 6 Click **Deployment Plan** for additional verification, then click on a site to see the deployment plan for that specific site.

L

Figure 211:

≡ distation Nexus Dashboard . Corchestrator ∨			Fee	daack 上 Θ
VRF Route Leaking Schema			4 / 1000 Objects	⊙ () X
View On-Prem Template ~			Template Ort-Prem Template	
	Associated Sites	Developed Inc. 24, 2022 DE 25 au	Template Settings	~
Deployment Plan				×
General Information © Temptate On-Prem Template	Schema VRF Route Leaking Schema	Tenant dcnm-default-tn		
Plan Sydney			Oreated Obeleted Modified OExisting @Sh	ladow
O down-default-tin O 110 O 1100 O 110 O 1100 O 1100 O 1100 O 1100 O 1100 O 1100 O 1100			(View Pg	yload

Step 7 Click **Deploy** to have NDO push the configurations to the site specific controllers (NDFC and Cloud Network Controller).

What to do next

Verify that the configurations were deployed successfully using the procedures provided in Verify the Configurations, on page 175.

Verify the Configurations

In this section, you will verify that the configurations were deployed successfully. Note that for each of these verification steps, the exact command that would be used specifically for the configurations in this use case are shown. Replace the appropriate variables in each command based on your configuration.

Before you begin

Follow the procedures provided in Configure Route Leak from NDFC VRF to Azure VRF, on page 173.

Step 1 Verify the configurations in NDO.

I

≡ disco Nexus Dashboard	d 🙏 Orchestrator 🗸				Feedback 🛓 🧐
Dashboard	Schemas			Tenants	×
Sites	Contennatio			Q. Search	Tenants C
Application Management	Filter by attributes			dcnm-default-tn	General ^
Fabric Management	Name	Templates	Tenants	VRF Route Leaking Schema	Name dcnm-default-tn
Derations	Stretched Schema	2 @2	1		Description
Infrastructure Infrastructure	VRF Route Leaking Schema	3 📀 3	1		Default tenant for NDFC
6/ integration					Associated Sites
					of 4
					Associated Users
					of 1
					Assigned Schemas 5
					of 2
	10 ~ Rows				Topology
					6
					5
					S S several
≡ cisco Nexus Dashboar	d 🔄 🙏 Orchestrator 🗸				Feedback 🛓 💿
e Dathboard	Schemas			Templates	>
Sites	Contennas			Q. Search	Template
Application Management	Filter by attributes			On-Prem Template	General
Fabric Management	Name	Templates	Tenants	VRF Route Leaking Schema	Change Control Status
E Operations	Stretched Schema	2 02	1	- AWS Template VRF Route Leaking Schema	Tenant Name
O Infrastructure	VRF Route Leaking Schema	3 ©3	1	Azure Template VRF Route Leaking Schema	dcnm-default-tn
@ Integration					Sites By Type
					AWS O Azure O
					1 NDFC 0 Total Google Cloud Platform 0
					Application Management
	10 V Rows				ANPS BRIDGE DOMAIN
					0
					CONTRACT EXTERNAL EPO
					PLTER Laout
					1
					I U NETWORKS SERVICE GRAPHS
					I U VRF EPOs

≡ cisco Nexus Dashboard	🔶 Orchestrator 🗸				Feedback 👤 💿
Dathboard	Schemas			Templates	>
Sites	oonomuo			Q Search	Template
Application Management	Filter by attributes			On-Prem Template	General
Fabric Management	Name	Templates	Tenants	VRF Route Leaking Schema	Change Control Status Opployment Successful
Operations	Stretched Schema	2 02	1	VRF Route Leaking Schema	Tenant Name
O Infrastructure	VRF Route Leaking Schema	3 @3	1	Azure Template	dcnm-default-tn
S, undannou	10 v Rows				Sites By Type AMC 0 Ausre 0 0 Active 0 0 Contract Contract 0 Contract Contract Contract O Contre
Cisco Nexus Dashboard Dashboard	s orchestrator ∽ Schemas			Templates	Peedback 1
Sites				Q Search	Azure Template
Application Management	Filter by attributes			On-Prem Template	General
Fabric Management	Name	Templates	Tenants	AWS Template	Change Control Status O Deployment Successful
Operations Infrastructure	Stretched Schema	2 2	1	VRF Route Leaking Schema	
@ Integration	VRF Route Leaking Schema			Anura Tamelata	Tenant Name
		3 ⊘ 3	1	Azure Template VRF Route Leaking Schema	Tenant Name dcnm-default-tn Sites By Type



	ndfc-leaf1 - SecureCRT	-	×
F	lie told View Options Transfer Script Tools Window Help		
-1			
Session Manager Command Manager	A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/gpl-2.1.php and http://www.opensource.org/licenses/old-licenses/library.txt. http://www.opensource.org/licenses/old-licenses/library.txt. ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-leafi# ndfc-		^
	10.220.1.0/24, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 03:01:42, bgp-65084, internal, tag 65091, segid: 153412 tunnelid: 0xa0a0001 encap: VXLAN		
	10.220.2.0/24, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 03:01:42, bgp-65084, internal, tag 65091, segid: 153412 tunnelid: 0xa0a0001 encap: VXLAN 90.1.1.0/24, ubest/mbest: 1/0 *via 10.10.0.1%default, [200/0], 03:06:33, bgp-65084, internal, tag 65092, segid: 153412 tunnelid: 0xa0a0001 encap: VXLAN		
	172.16.10.0/24, ubest/mbest: 1/0, attached *via 172.16.10.1, v1an2310, [0/0], 03:23:02, direct, tag 12345 172.16.10.1/32, ubest/mbest: 1/0, attached *via 172.16.10.1, v1an2310, [0/0], 03:23:02, local, tag 12345 172.16.10.11/32, ubest/mbest: 1/0, attached *via 172.16.10.11, v1an2310, [190/0], 03:20:45, hmm ndfc-leaf1#		~
	Default ~		

The routing table on the on-premises leaf switch shows that the reachable subnets are:

- AWS: 10.220.0.0/16
- Azure: 10.220.0.0/16
- **Step 3** Connect to the Cloud Network Controller deployed on AWS and navigate to **Application Management** > **VRFs**, and verify that you can see the Azure and NDFC VRFs.

₹	cisco Cloud Network	Controller (AWS)						Q 0	0000 💶
Dashboard Transform	VRFs								Ø
Cloud Resources	VRFs Leak Routes								
Application Management	Filter by attributes								Actions ~
Tenants				Application	Management		Clou	d Resources	
EPGs	Health	Name		EPGs	Cloud Context Profiles	Regions	VPCs	Routers	Endpoints
Contracts	Healthy	ave-ctrl infra		0	0	0	0	0	0
Filters	Healthy	aws10 Internal		0	1	1	1	1	2
VRFs Services	Healthy	azure10 Internal		0	1	1	1	1	0
Cloud Context Profiles	Healthy	copy		0	0	0	0	0	0
Operations	Healthy	default		0	0	0	0	0	0
Infrastructure v	Healthy	inb		0	0	0	0	0	0
	C Healthy	oob mgmt		0	0	0	0	0	0
	Healthy	overlay-1 internal infra		15	1	1	1	3	12
	C thealthy	stretched-vrf internal		0	1	1	1	1	2
	Healthy	v10 Internal MSC-SAMDOW dcnm-default-tn		0	1	1	1	1	0
	15 🗸 Rows							Page 1 \sim of 1	< < 1-10 of 10
E	-lule Cloud Network	Controller (AWS)						00	0000 0
E Dashboard	Cloud Network	Controller (AWS)	aws10 : 1	VPCs				@ @	0000 💶 ×
Dashboard Topology	VRFs	: Controller (AWS) 🥶	aws10 : \	VPCs			VPC	® ø	••••••
Deshboard Topology Cloud Resources	VRFs Leak Routes	Controller (AWS) 🚥	aws10 : 1	VPCs			e VPC aws10	00	♥ ♥ ♥ ♥ ♥ × ~~ □
	VRFs Leak Routes	: Controller (AWS) 🥶	aws10 : 1 Q Second aws10 10.22 dcnm-default	VPCs 0.0.0/16 t-th > us-west-2			e vec aws10	Q ⊘ ♥ Healthy	×
Destboard Topology Capadogy Capadogy Application Management Agelication Profiles	VRFs Leak Routes	Controller (AWS) 🧰	aws10 : 1 Q Second aws10 10.22 dcnm-default	VPCs 0.0.0/16 1-tn > us-west-2			e vec aws10	Healthy	×
E Dashboard Topology C Topology C Application Anagement Application Profiles EPGs	Cloud Network Cloud Network VRFs Leak Routes Pres to endede Health Health	Controller (AWS) 2005	aws10 : 1 Q Second aws10 10.22 dcnm-default	0.0.0/16 I-tn > us-west-2			contents and the second	Image: Second state Image: Secon	×
E Dashboard Topology Controls Fronts FOS Controls Fronts	Cloud Network Cloud Network VRFs Leak Routes Prev to an open Deater to an open	Controller (AWS) 2005	aws10 : 1 Q Second dom-default	VPCs 0.0.0/16 -th > us-west-2			Ceneral Account dener-default-ten Region us-west-2		× *** C
E Dashboard Topology Conditions Proteins F2Gs Contracts F2Gs Vers Vers	Cloud Network Cloud Network VRFs Leak Routes VRFs Leak Routes Ore to unitate O Healthy O Healthy O Healthy	E Controller (AWS)	aws10 : 1 Q. Second aws10 10.22 dcnm-default	VPCs 0.0.0/16 1-th > us-west-2			vrc aws10		× *** C
E Contractor Profes Contractor Profes Contractor Profes Contractor Verifs Services	CISCO Cloud Network VRFs Leak Routes VRFs Leak Routes Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute Prov ty statute	Rame ave-ctri unta ave-ctri unta dom-default-sn avered birtemati avered birtemati	aws10 : 1 Q see	0.0.0/16 -tm > us-west-2			vrc ews10	C Healthy	× ************************************
E Context Profiles	Cloud Network Cloud Network VRFs Leak Routes Provide setting	E Controller (AWS)	aws10 : Q Section aws10 10.22 dccm-default	VPCs 0.0.0/16 1-th > Us-west-2			vrc wrs10	Healthy	× ************************************
E Dentioner Context Portes Application Management Application Profiles EPOn Contexts Filters Vitr's Services Codo Context Porties External Networks Codo Context Porties External Networks	Cloud Network VRFs VRFs Leak Routes Provide and a set of the set o	E Controller (AWS)	aws10 : 1 Q Seen aws10 10.22 dccm-defaul	VPCs 0.0.0/16 -tm > us-west-2			vrc wrs10 Ceneral Account Region us-vest-2 Cloud Resources	Healthy Healthy Generating Jones	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Dashboard Image: Dashboard Tookoy Image: Dashboard	cisco c	Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Contr	aws10 : 1 Q See aws10 10.22 occm-default	0.0.0/16 -tm > US-west-2			ve to veto	Constraints	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
Image: second	Cloud Network VRFs Leak Routes VRFs Leak Routes Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Note Prov ty an Not	Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Contr	aws10 : 1 Q Seed avento 10.22 doom-default	0.0.0/16 to > us-west-2			vrc wrc wrs10 Ceneral Account dcom-default-in Ragion uz-west-2 Cloud Resources 1 Baytes 1 Servery Deep. Acplication Management		0 0 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
E Candination Profiles Parking Control Profiles Franzis Application Anargement A Application Profiles F2Gs Contracts F2Gs Contracts F3Gr Services Cloud Context Profiles External Networks Context Profiles External Networks Context Profiles Context P	Cloud Network VRFs Leak Routes VRFs Leak Routes Prov ty an bats Prov	Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Controller (AWS) Contr	aws10 : 1 Q See dcm-default	0.00/16 1: th > us-west-2			Vic and a set of the set of	Contractions of the end of the en	O O Com Com
Image: second	Cloud Network VRFs Leak Routes Prev ty streactes Prev ty streactes	Controller (AWS) Rame Rame Rame Rame Rame Rame Controller Rame Rame Rame	aws10:1	0.0.0/16 t-th> US-VEST-2			vrc ws10	Chealthy Healthy Healthy Learna Chealthy Jone O Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D Decense D D Decense D D D D D D D D D D D D D	© © © © © × ··· □ · · · · · · · · ·
Dashboard Tookky Tookky Oud Resources V Application Management Application Profiles EPGoat Contracts Filters Vitr's Senkices Countext Profiles External Networks Vitr's Bonkices Countext Profiles Countext Profiles Vitr's Denkices Vitr's Countext Profiles Vitr's <th></th> <th>Controller (AWS) Name Name Name Name Name Controller Name Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controler Controle</th> <th>aws10 : 1 Q. exem-default</th> <th>VPCs 0.0.0/16 t-tm > Us-west-2</th> <th></th> <th></th> <th>vro vro v</th> <th>Contenting Terms</th> <th>C C C C C C C C C C C C C C C C C C C</th>		Controller (AWS) Name Name Name Name Name Controller Name Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controller Controler Controle	aws10 : 1 Q. exem-default	VPCs 0.0.0/16 t-tm > Us-west-2			vro v	Contenting Terms	C C C C C C C C C C C C C C C C C C C
Image: Second	Cloud Network VRFs Leak Routes VRFs Leak Routes Provide antity	Controller (AWS) Controller (A	aws10:1	0.0.0/16 t-tin > us-west-2			vrc wrc wr	C Pealthy Healthy Healthy Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Meanses Mean	© © © © © × ··· C ·· C ·· C ·· C ·· C ·· C ·· C

Step 4 Remaining in the Cloud Network Controller deployed on AWS, perform a verification on the route table view.

💿 VPC aws10			Actions 🗸 🗖 🖬 🔿 -	
Overview Topology Cloud Resources Application Mana	igement Event Analytics	Subnets for CIDR Block 10.220.0.0/16		×
General Account dcm-odfault-in Region us-west-2	Settings Cloud Access Phylioge Inherited (Routing Only) Cloud Provider ID	10.220.2.0/24	setter 10 220 2.0/24 Settings Cloud Access Privilege Inherited (Routing Only) Cloud OIDP's Submet. 10 220 2.0/24	
Cloud Resources 1 4 0 Bugers Court Analatity Zones Decrement 1 0 2 Security Dangs Instrument Endperture 0 0 1	CLDRS CLDR Block Range 10.220.0.0/16	р Х	Name - Route Table Settings Name ans10-egress Oper State configured Cloud Provider ID mi-08c-112-4e/560077cf Direction	~
Applicants Portilas 1 VEPS Desire Counts Leaves Counts Desire			egress Entries Destination Address * Next Hop 172.16.10.0/24 tgw- Hub Network 90.1.1.0/24 tgw- Hub Network 10.220.0.0/16 [Deems] local	
				30.5
OVERVIEW TOPOLOgy Cloud Descurses Application House	nement Event Analytics	Subnets for CIDR Block 10.220.0.0/16	Actions 🗸 📕 🛤 🔿 –	- × ×
VPC aws10 Overview Topology Cloud Resources Application Mana General Account dram-default-in Region us-west-2	germent Event Analytics Settings Cloud Access Phylioge Inherited (Boulder ID Cloud Provider ID CIDRs	Subnets for CIDR Block 10.220.0.0/16 10.220.2.0/24 10.220.1.0/24	Actions V 📕 => 🔿 –	× ×
VPC aws10 Overview Topology Cloud Resources Application Manz General Account domn-default in Region Region Region Region Cloud Resources I 4 0 Region Cloud Resources I 0 2 Dedams D	gement Event Analytics Settings Cloud Access Phillege Interired (Routing Only) Cloud Provider ID CDRs CIDR Block Range 10.220.0.0/18	Subnets for CIDR Block 10.220.0.0/16 10.220.2.0/24 10.220.1.0/24	Action V R D C C	× × ×
Overview Topology Cloud Resources Application Mana General Account Account Account Account Region Brance Brance Image Ourst Analytics Brance Brance Image Ourst Analytics Brance Brance Image Ourst Analytics Brance Brance Image Discources Brance Brance	germent Event Analytics Settings Cloud Access Phillings Interfed Routing Orb) Cloud Provider ID CIDRs CLOR Block Range 10.220.0.0/16	Subnets for CIDR Block 10.220.0.0/16	Actors V R = 0 0 -	× × ×

Step 5 In the AWS console, perform a verification on the route table view.

WS III Services Q Search		[Alt+S]		>	⑦ Oregon ▼ der	mo @ 1173-
VPC dashboard X EC2 Global View 🖄 New	VPC > Route tables > rtb-(utotable [aux10.com	roccl			
Filter by VPC:	rtb- / rc	butetable-laws lo:eg	ressj		A	ctions V
Select a VPC		delana de la				
Virtual private cloud	You can now check network connectivity with Re	achability Analyzer		R	un Reachability Analyze	r X
Your VPCs						
Subnets	Details Info					
Route tables						
nternet gateways	Route table ID	Main Main	Explicit subnet accession	Edos accariatio		
gress-only internet			subnet-	/ subnet-[10.220.1.0/24]		
ateways	VPC vpc-lcontext-faws101-addr-	Owner ID				
arrier gateways	[10.220.0.0/16]					
HCP option sets						
lastic IPs						
lanaged prefix lists	Routes Subnet associations Edge associ	iations Route propagation T	ags			
ndpoints						
ndpoint services	Routes (3)				Edit	routes
AT gateways	(o)				Luit I	outes
ering connections	Q. Filter routes		Both 🔻		< 1	> ©
ecurity						
etwork ACLs	Destination V	Target			ed	V
curity groups	10.220.0.0/16	local	⊘ Active	No		
etwork Analysis	90.1.1.0/24	tgw-i	⊘ Active	No		
eachability Analyzer	172.16.10.0/24	tgw-i	⊘ Active	No		
Intundi Assess Anthone						

Step 6 Connect to the Cloud Network Controller deployed on Azure and navigate to **Application Management** > **VRFs**, and confirm that you can see the AWS and NDFC VRFs:

I

Ŧ	cisco	Cloud Network C	Controller (Azure) 🔥	zure					Q 0	0000 💶
Dashboard Topology A Cloud Resources	VRFs l	S Leak Routes								٥
Application Management										Actions ~
Tenants					Application	Management		Cloud	d Resources	
Application Profiles		Health	Name		EPGs	Cloud Context Profiles	Regions	Virtual Networks	Routers	Endpoints
Contracts		Healthy	ave-ctrl		0	0	0	0	0	0
Filters		-	aws10 Internal		0	1	1	1	0	0
VRFs		♦ Healthy	MSC-SHADOW dcnm-default-tn							
Services Cloud Context Profiles		• Healthy	azure10 Internal Moo dcnm-default-tn		0	1	1	1	0	0
External Networks		Thealthy	copy		0	0	0	0	0	0
Operations		Healthy	default common		0	0	0	0	0	0
1º Administrative V		Healthy	inb mgmt		0	0	0	0	0	0
		♥ Healthy	oob mgmt		0	0	0	0	0	0
		Healthy	overlay-1 Internal		12	1	1	1	2	10
		♥ Healthy	stretched-vrf internal koo dcnm-default-tn		0	1	1	1	0	0
		• Healthy	v10 Internal MSC-SHADOW dcnm-default-tn		0	1	1	4	0	0
	15	∼ Rows							Page 1 v of 1	≪ ≪ 1-10 of 10
Ŧ	-iji-ij cisco	Cloud Network	Controller (Azure) 🔥	Azure					Q 2	0000 🗉
Cashboard		Cloud Network	Controller (Azure) 🔥	azure	: Virtual Networl	ĸs			0	0000
Dashboard Topology	VRF	Cloud Network (Controller (Azure) 🔥	azure10	: Virtual Networl	ks		- Virtual Network	00	×
Dashboard Topology Cloud Resources	VRFs	Cloud Network (S Leek Routes	Controller (Azure) 🔥	azure10	: Virtual Networl	ks		Wrbal Network azure10	00	×
Dashboard Topology Cloud Resources Application Management	VRFs	Cloud Network (S Leak Routes	Controller (Azure) 🔥	azure azure10	: Virtual Networl	ks		Virbail Network azure10	Q € Healthy	× C
Dashboard Topology Cloud Resources Cloud Resources Clinat Resources	VRFs	Cloud Network C S Leak Routes	Controller (Azure) 🔥	azure10	: Virtual Network	ks		Virtual Network azure 10 General	Q Ø ♥ Healthy	× C
Dashboard Topology Cloud Resources Cloud Resources Cloud Resources Application Management Application Profiles EPGe	VRFs	Cloud Network (S Leak Routes	Controller (Azure)	Azure azure10 Q Second azure10 90.1 dcnm-defaul	: Virtual Network	ks		Virtual Network azure 10 General Account dcom-defuilt-tn	Q Image: Second seco	× 2 0 0 0 0 2 2 2
Dashboard Topology Cloud Resources Cloud Resources Cloud Resources Application Management Application Profiles FPGs Contracts	VRFs 1	Cloud Network (Cloud Network (Cloud Network (Network	Controller (Azure)	azure 10 Q Second azure 10 90.1 dcnm-defaul	: Virtual Network	ks		Vitual Network azure10 General Account dcnm-default-tn Region	Image: Second secon	× × ~
Dashboard Topology Cloud Resources Cloud Resources Cloud Resources Application Management Application Profiles EPGa Constructs FRers	VRFs	Cloud Network (Leak Routes	Controller (Azure)	azure10	. Virtual Networl	KS		What Network azure 10 General Account docm-default-th Region eastus	♥ ♥ Healthy	× × ~
Dashboard Topology Topology Cloud Resources C	VRF:	Cloud Network (CS Leak Routes Health Health Healthy Healthy	Controller (Azure)	azure10 Q parate azure10 90.1 dcren-defaul	.0.0/16	KS		Vitual Network: azure 10 General Account doom-default-in Region eastus Class Baseserese	♥ ♥ Healthy	× × •••• 2
		Cloud Network (Leak Routes	Controller (Azure)	azure10 Q becc azure10 00.1 azure10 00.1	. Virtual Networl	KS		Vitual Network: azure 10 General Account doom-default-in Region eastus Cloud Resources	♥ ♥ Healthy	× ••• 0 ••• 0
		Cloud Network (S Leak Routes	Controller (Azure)	azure10 Q azure10 00.1 dcnm-defaul	: Virtual Networl	KS		Vitual Network azure 10 General Account down-detault-in Region eastus Cloud Resources 1 I	Healthy	
		Cloud Network (Leak Routes	Controller (Azure)	azure10 Q Beec azure10 00.1 dcnm-defaul	: Virtual Networl	KS		Vitual Network azure 10 General Account down-detault-in Region eastus Cloud Resources	Healthy	×
	VRFs	Cloud Network (S Leak Routes	Controller (Azure)	azure10 Q Beec azure10 00.1 dcnm-defaul	: Virtual Networl	KS		What Network azure 10 General Account Account Goundeduit-in Region eastus Cloud Resources I gugen I J J Lindente from from	Healthy 0 numero 0 numero 0 numero	× · · · C
		Cloud Network (C S Leak Routes	Controller (Azure)	azure10 Q beneficial azure10 00.1 doren-defaul	: Virtual Networl	KS		What Network azure 10 General Account Account Account Cloud Resources I I I Account Acco	C Healthy 0 Normal 0 Verset Hockner	
	VRF: VRF:	Cloud Network (S Leak Routes Leak Routes Healthy	Controller (Azure)	azure10 Q and azure10 00.1 d crm-defaul	. Virtual Networl	KS		Virtual Version's acture 1 0 Version Version's Constant Version's Count desault-In Region Count Response Count Response Count Response I I Region I Application Management	Healthy Healthy Number of the second seco	× · · · C
		Cloud Network (CS Leak Routes Health Heal	Controller (Azure)	azure10 Q mene azure10 90.1 dcm-defaul	.00/16 	KS		Studi Network azure 10 Seneral Account doom-default-in Region eastus Cloud Resources I unyues I Application Management O Application Management	C C C C C C C C C C C C C C C C C C C	× * * * * * * * * * * * * * * * * * * *
		Cloud Network (S Leak Routes Leak Routes Healthy	Controller (Azure)	azure10 Q	. Virtual Networl	KS		Virtual Vertainerk actual 10 Vertainerk Account Account Account Account Count Account Account A	C Healthy	
Denhbard Topokoy Topokoy Topokoy Topokoy Constructs Constructs Contructs Cont		Cloud Network (S Leak Routes Reath Health	Controller (Azure)	azure10 Q mene azure10 90.1 dcm-defaul	.00/16 	KS		Statistication Section	C C C C C C C C C C C C C C C C C C C	

Step 7 Remaining in the Cloud Network Controller deployed on Azure, navigate to **Cloud Resources** > **Virtual Networks**, then click the azure10 VNet and use the information in the Overview page for additional verifications.

Dverview Topology Cloud Resources Application Management Event Analytics		Subnets for CIDR Block 90.1.0.0/16				
				L.	S subnet	
General Account dorm-default-tn Region eastus Cloud Resources	0 Boses 0	1 Steeds Servity Draw	Settings Cloud Access Phyllege Intertted (Routing & Security) Cloud Context Profile azure10-eastus CIDR CIDR Block Range 90.1.0.0/16 Cloud Provider ID	90.1.1.0/24	Cloud Access Phyliogs Cloud Access Phyliogs Cloud Access Phyliogs Cloud Access Phyliogs Cloud CIDP's Subset 90.11.0/24 Name - Route Table Settings Name aure O sepres	~
Application Security Groups	Virtual Machines	Endpoints			Oper State configured Cloud Provider ID	
Application Manager	ent					
0 Application Profiles	O EPGe	1 Cloud Context Profiles			Direction	
1 vers	O Service Graphs				Entries Destination Address * Next Hop	
					172.16.10.0/24 10.90.1.36 Hub Network	

Step 8 In the Azure console, perform additional verifications.

	∠ Search resources, services, and docs (G+/)		E & @ @ R	ambsingh@cisco.com cisco-iнseu-мкт
Home >				
Virtual networks ∞ … Cisco-INSBU-MKT				×
🕂 Create 🔘 Manage view 🗸 🖒 Refresh 🛓 Export to	CSV 😵 Open query 🛛 🖉 Assign tags			
Filter for any field Subscription equals all Re	esource group equals all $ imes$ Location equals all $ imes$ $^{ ext{th}}_{ ext{P}}$ Add filter			
			No grouping V	$\ensuremath{\exists} \ensuremath{List} \ensuremath{view} \ensuremath{\checkmark} \ensuremath{\checkmark}$
Name 🕆	Resource group 14	Location †	Subscription \uparrow_{\downarrow}	
azure10	CAPIC_dcnm-default-tn_azure10_eastus	East US	huyeduon-Demo05	
🗌 🖘 overlay-1	azurendfc	East US	huyeduon-Demo05	
Stretched-vrf	CAPIC_dcnm-default-tn_stretched-vrf_eastus	East US	huyeduon-Demo05	

Microsoft Azure	P Search resources, services, and docs (G+/) ■						ę 🖉 🛛 🔿	R ambsingh@ci	SCO.COM
Home > Virtual networks > azure10 Virtual networks « Cisco-INSBU-MKT + Create (@ Manage view < ····	Azure10 Subnets Virtual network P Search «	☆ … + Subnet + Gate	way subnet 💍 Refre	sh 우, Manage users	Delete				×
Filter for any field Name 1:	Overview Activity log Access control (IAM)	P Search subnets	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group 👈	Route table ↑↓	
acureto verlay-1 e> stretched-wrf	 Tags Diagnose and solve problems 	subnet-90.1.1.0_24	90.1.1.0/24	÷	251	2	subnet-90.1.1.0_24	rt-azure 10_egress	
	Settings								

I