Cisco UCS Director Unified Fabric Automation Management Guide, Release 6.5

First Published: 2017-08-23

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

CONTENTS

Preface

Preface vii

Audience vii

Conventions vii

Related Documentation ix

Documentation Feedback ix

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1

New and Changed Information for this Release 1

New and Changed Information for this Release 1

CHAPTER 2

Overview 3

Prerequisites 3

Cisco UCS Director and Cisco Unified Fabric Automation 3

System Flow 4

Terminology 5

Cisco Dynamic Fabric Automation Overview 6

Fabric Management 6

Cisco Prime Data Center Network Manager 7

Cisco Dynamic Fabric Automation Services Support 8

Guidelines and Limitations for Cisco Unified Fabric Automation 9

Mapping Considerations 10

Examining the Orchestration Flow 11

CHAPTER 3

Configuring Cisco Unified Fabric Automation 13

Summary of Steps for Configuring Cisco Unified Fabric Automation 14

Adding a Cloud Account 14

Creating a Cloud 15

Configuring a Cisco Nexus 1000V Switch 16
Adding a Network Element 16
Creating a Cisco Unified Fabric Automation Organization Account 17
Creating a Cisco Unified Fabric Automation Organization 18
Configuring the DFA Orchestrator ID 19
Associating vDCs 19
Creating a Fabric Partition 21
Creating a Cisco Unified Fabric Automation Network 22
Examining the Fabric SegmentID Range 24
Examining a Cisco Unified Fabric Automation Network's Segment Usage 24
Adding a Cisco Unified Fabric Automation Network to a Cisco Unified Fabric Automation Partition 25
Creating a Cisco Unified Fabric Automation Network using vSwitches 27
Creating a Fabric Network using dvSwitches 29
Attaching a Port Group to a VM 30
Adding a Network Policy 31
Choosing a Fabric Port Selector 34
About Multiple Disk VM Provisioning in a Cisco Unified Fabric Automation Network 35
Application Containers in a Cisco Unified Fabric Automation Environment 36
About Application Container Templates 36
Creating Application Container Policies (Cisco Unified Fabric Automation Environment) 36
Creating Application Container Templates (Cisco Unified Fabric Automation Environment) 38
Creating a Custom Workflow for Application Containers 44
Creating an Application Template for a VSG 44
Managing Application Containers 49
Viewing Container Actions 49
Adding VMs 50
Accessing a VM Console 52

CHAPTER 4 **Managing Cisco Unified Fabric Automation Networks 53**
Modifying a Fabric Organization 54
Deleting a Fabric Organization 54
Viewing a Fabric Organization's Details 55

Viewing a Fabric Summary 55
Viewing Fabric General Settings (Fuji 2 Accounts Only) 55
Viewing Fabric Mobility Domains 56
Fabric Domain Switch Mapping 56
Deleting a Fabric Network 57
Modifying a Fabric Network 57
Viewing a Fabric Partition 59
Modifying a Fabric Partition 60
Deleting a Partition 61
Deleting All Partitions 61
Examining the Fabric SegmentID Range 62

Preface

- Audience, page vii
- Conventions, page vii
- Related Documentation, page ix
- Documentation Feedback, page ix
- Obtaining Documentation and Submitting a Service Request, page ix

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.

Text Type	Indication
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

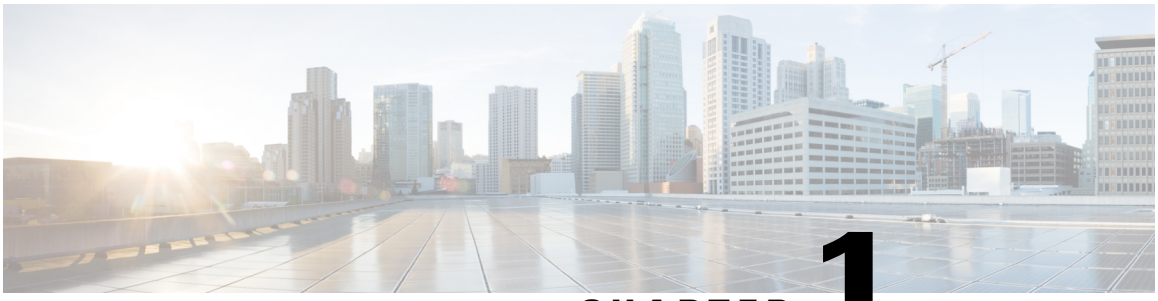
Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

New and Changed Information for this Release

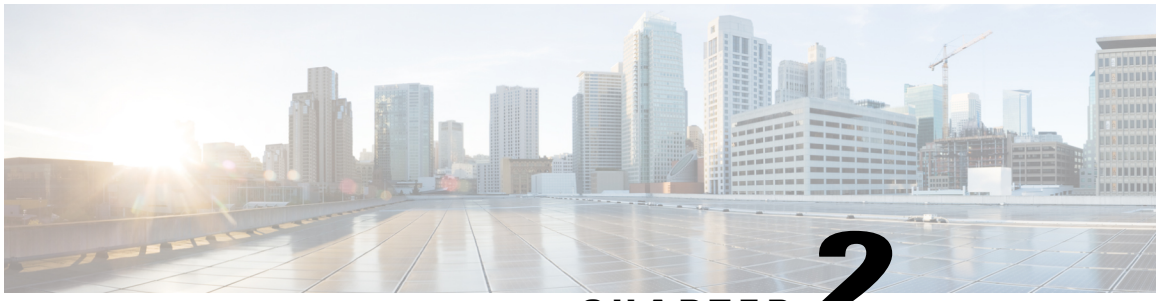
This chapter contains the following sections:

- New and Changed Information for this Release, page 1

New and Changed Information for this Release

No significant changes were made to this guide for the current release.

New and Changed Information for this Release



CHAPTER 2

Overview

This chapter contains the following sections:

- Prerequisites, page 3
- Cisco UCS Director and Cisco Unified Fabric Automation, page 3
- Terminology, page 5
- Cisco Dynamic Fabric Automation Overview, page 6
- Mapping Considerations, page 10
- Examining the Orchestration Flow , page 11

Prerequisites

Prerequisite	Description
Cisco UCS Director	Release 4.1 (with patches) or later full releases
Cisco Prime Data Center Network Manager (DCNM)	Release 7.0 or later releases

Cisco UCS Director and Cisco Unified Fabric Automation

Cisco UCS Director is a unified infrastructure management solution that provides a single pane of management for compute, network, storage, and virtualization layers. Cisco UCS Director uses a workflow orchestration engine with workflow tasks that support the compute, network, storage and virtualization layers. Cisco UCS Director supports multitenency, which enables policy-based and shared utilization of the infrastructure.

Cisco Unified Fabric Automation is a multistage, switching network in which every connected device is reachable through the same number of hops. The Cisco Cisco Unified Fabric Automation Organization fabric enables the use of a scale-out model for optimized growth.

System Flow

Cisco UCS Director acts as an orchestration engine and is responsible for creating tenant (Layer 2 and 3) networks which will eventually be populated with virtual machine (VM) vnics (virtual network interface cards). Cisco Unified Fabric Automation essentially provides the scalable network infrastructure for those newly created networks.

Network parameters, such as the default gateway and subnet masking are communicated to Cisco Prime Data Center Network Management (DCNM) so that its network database for the Cisco Unified Fabric Automation cluster is appropriately populated. When a VM becomes active under a leaf node, the database is queried for the appropriate download and dynamic instantiation of the network configuration.

Cisco UCS Director programs the associated Cisco Nexus 1000V switches or DVSs with a port-group for each network so that the Cisco Nexus 1000V or DVS information is communicated to the virtualization Element Manager (for example, vCenter or SCVMM). When a VM is provisioned, Cisco UCS Director notifies DCNM under which leaf node port (logical) that the VM network traffic is going to arrive on. This step is optional when Virtual Station Interface (VSI) Discovery and Configuration Protocol (VDP) is in use between the host virtual switch and the leaf is in use between the host virtual switch and the leaf. VDP is used during the negotiation phase to collect the new VM (autoconfigured) on the leaf.

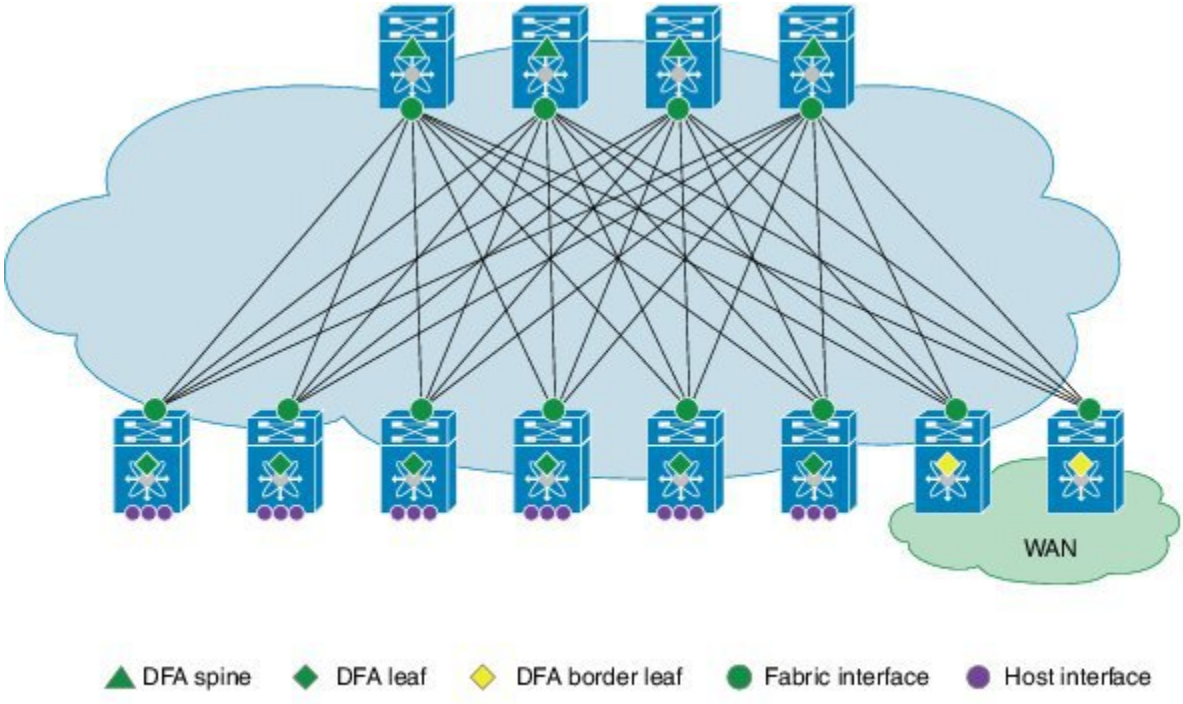
Note Cisco UCS Director uses the Cisco DCNM Representational State Transfer (REST) API to support a Cisco Unified Fabric Automation organization. A Cisco Unified Fabric Automation connection library serves as a backbone of the DCNM REST API connection handler for all DCNM communication needs, which includes inventory, action and workflow orchestration tasks.

Note Some Cisco Unified Fabric Automation features might be supported in future Cisco UCS Director patch releases.

Terminology

The following figure shows the terms that are used for a Cisco Dynamic Fabric Automation (DFA) deployment. You should understand these terms and definitions before you deploy Cisco DFA.

Figure 1: Terms Used in a Cisco Dynamic Fabric Automation Deployment



- Cisco DFA fabric—A multistage, switching network in which every connected device is reachable through the same number of hops. The Cisco DFA fabric enables the use of a scale-out model for optimized growth.
- Cisco DFA switch—A leaf, border leaf, or spine device.
- Leaf—Switches with ports that are connected to ethernet devices, such as servers (host interfaces) and ports (fabric interfaces), that are connected to the Cisco DFA fabric. Leaf switches forward traffic based on the enhanced control plane functionality of Cisco DFA optimized networking, which requires segment ID-based forwarding.
- Border leaf—Switches that connect external network devices or services, such as firewalls and router ports, to a Cisco DFA fabric. Border leaf switches are similar to leaf switches and can perform segment ID-based forwarding.
- Spine—Switches through which all leaf and border leaf switches are connected to each other and to which no end nodes are connected. Spine switches forward traffic based on Cisco DFA optimized networking with enhanced or traditional forwarding.

- Host interface—Leaf to server interfaces that receive traffic for connected VLANs to be extended across the Cisco DFA fabric.
- Fabric interface—Ports through which Cisco DFA switches are connected to one another.

Cisco Dynamic Fabric Automation Overview

Cisco Dynamic Fabric Automation optimizes data centers through integration. This architecture eliminates the need for overlay networks that can hinder traffic visibility and optimization and reduce scalability when physical server and virtual machine environments are integrated. The architecture enables zero-touch provisioning and greater orchestration, while delivering more predictable performance and latency for large cloud networks. The following building blocks are the foundation of Cisco DFA:

- Fabric Management—Simplifies workload visibility, optimizes troubleshooting, and automates fabric component configuration.
- Workload Automation—Integrates with automation and orchestration tools through northbound application programming interfaces (APIs) and also provides control for provisioning fabric components by automatically applying templates that leverage southbound APIs and standard-based protocols. These automation mechanisms are also extensible to network services.
- Optimized Networking—Uses a simple distributed gateway mechanism to support any subnet, anywhere, concurrently. Existing redundancy models are also used to provide N+ redundancy across the entire fabric.
- Virtual Fabrics—Extends the boundaries of segmented environments to different routing and switching instances by using logical fabric isolation and segmentation within the fabric. All of these technologies can be combined to support hosting, cloud, and multi-tenancy environments.
- DCI Automation—Automate the configuration of connecting tenants within the unified fabric to the external world, be it the Internet or other unified fabric networks. These features works in tandem with DCNM (7.1.1 onwards) to enable auto configuration of such requirement.

Note Global VLAN mutually exclude segment ID, (at least for Layer-2 Traffic). A segment ID is a global identifier, there cannot be two global identifier = VLAN + segment ID, you have to decide one or the other. Global VLANs and segment ID can co-exist in the same fabric, if the outer header is not overlapping.

Fabric Management

The fabric management network in Cisco Dynamic Fabric Automation represents a dedicated out-of-band network that is responsible for bootstrapping and managing the individual networking devices, such as spines, leafs, and border leaf switches that are controlled by fabric management. The fabric management network is responsible for transporting the protocols that are required for the different fabric management functions. The following table lists the functions and protocols across the fabric management network.

Table 1: Functions and Protocols Across the Fabric Management Network

Function	Protocol
Power On Auto provisioning (POAP) for automatically configuring network devices	• Dynamic Host Configuration Protocol (DHCP) • Trivial File Transfer Protocol (TFTP) • Secure Copy Protocol (SCP)
Fabric discovery	Simple Network Management Protocol (SNMP)
User-to-machine and machine-to-machine communication	Extensible Messaging and Presence Protocol (XMPP)
Automated network provisioning	Lightweight Directory Access Protocol (LDAP)
DCI Automation	Auto Provisioning of Data Center Interconnect on a border leaf.

The management network, also known as the management access, is the network administrator-facing interface for accessing fabric management. The management network represents the portion of your network from which you, as the network administrator, can connect to an element manager or a network management station (NMS) and to switches and routers.

The Cisco Prime Data Center Network Manager (DCNM) is a turn-key management system for fabric management, visibility, and an extensible set of functions to more efficiently control the data center fabric. Cisco Prime DCNM uses standards-based control protocol components to provide you with an extensive level of customization and integration with an operations support system (OSS) network.

Cisco Prime Data Center Network Manager

An Open Virtual Appliance (OVA) is a prebuilt software solution that comprises one or more virtual machines (VMs) that are packaged, maintained, updated, and managed as a single unit. The Cisco DCNM OVA includes an application functionality that is necessary for Cisco DFA. Cisco Prime DCNM as an OVA can be deployed on a VMware vSphere infrastructure.

Cisco Prime DCNM provides the following functionalities:

- Device auto configuration is the process of bringing up the Cisco DFA fabric by applying preset configuration templates to any device that joins the fabric. Auto configuration installs an image or applies the basic configuration.
- Cable-plan consistency checks the physical connectivity of the fabric against a documented cable-plan for compliance. The lack of compliance prevents specific links from being active and protects the fabric from unwanted errors.
- Common point of fabric access allows you, as a network administrator, to interact with the fabric as a single entity (system) to simplify queries and to eliminate switch by switch troubleshooting efforts.

- Automated network provisioning provides a new layer of automation integration in which the data center fabric-switching infrastructure is automatically provisioned for the physical or virtual workload that is being instantiated.
- Automated profile refresh allows keeping the fabric and the network information in sync in a non-disruptive manner.
- DCI Automation provides a touchless provisioning of datacenter interconnections for the tenants.
- Network, virtual fabric, and host visibility is provided by the management GUI and displays a single set of active network elements that belong to an organization in the fabric.

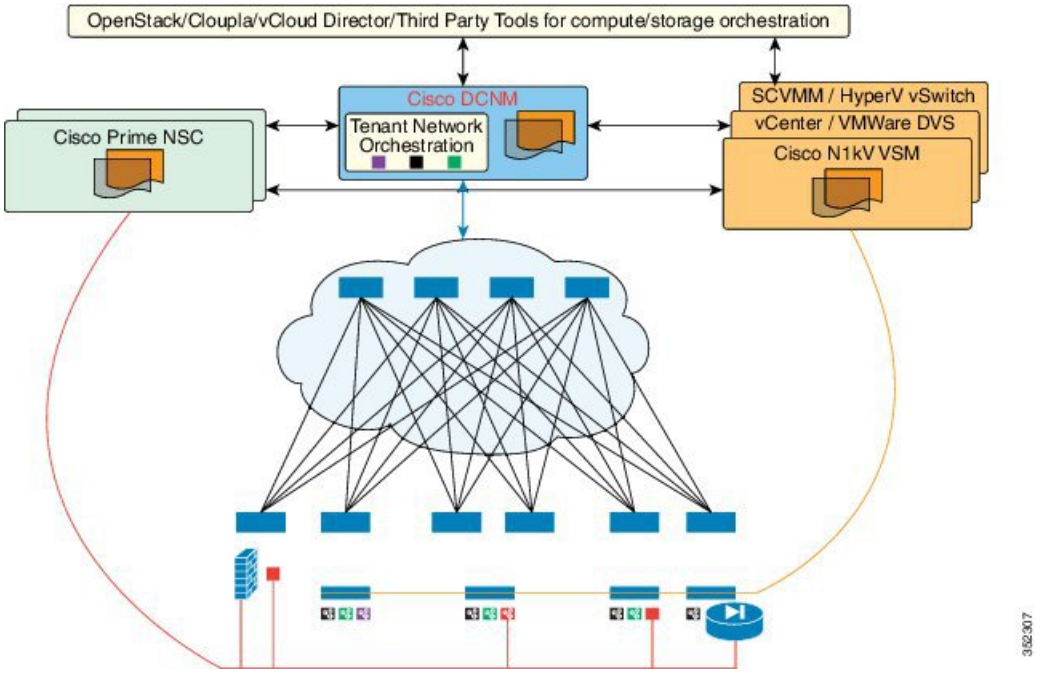
The Cisco DFA DCNM access network is the network administrator facing interface for accessing fabric management and for connecting northbound application program interfaces (APIs) to orchestrators.

Cisco Dynamic Fabric Automation Services Support

Services such as a firewall, load balancer, and virtual private networks (VPNs) are deployed at the aggregation layer in the traditional data center. In a Cisco DFA deployment, services nodes are deployed at regular leaf switches for both east-west and north-south traffic. Services can be physical or virtual services nodes.

The following figure shows the interaction between the Cisco Prime Network Services Controller (NSC) and the Cisco DFA deployment through Cisco Prime Data Center Network Manager (DCNM).

Figure 2: Cisco DFA with Services



The Cisco Prime NSC is the services orchestrator for Cisco DFA. The NSC Adapter in the Cisco Prime DCNM Open Virtual Appliance (OVA) performs the following functions:

- Provides connectivity between Cisco Prime DCNM and the Cisco Prime NSC services orchestrator

- Automatically populates the Cisco Prime NSC with the organizations, partitions, and networks that are created in Cisco Prime DCNM
- Populates Cisco Prime DCNM with the services that are stitched through Cisco Prime NSC
- Allows the use of multiple Cisco Prime NSC instances to match the Cisco Prime DCNM scale

Fabric can be provisioned for services using Cisco UCSD as well without using PNSC for certain scenarios. Containers can be used to orchestrate policies for tenant edge firewall using Physical ASA or ASAv. Containers are integrated with Cisco Prime DCNM to use DFA VLANs to create networks for a firewall's inside and outside interfaces. VSG service networks can also be orchestrated using UCSD; however, in this scenario, PNSC is required for provisioning the VSG. UCSD deploys all the virtual form factor service nodes (ASAv, VSG) using the port groups with DFA VLANs. These networks are also pushed to Cisco Prime DCNM through the Rest APIs. Note that interaction between PNSC and Cisco Prime DCNM is not needed for this approach; UCSD implements this functionality for services.

In Cisco DFA, configuration profile templates and instantiating the profiles on a leaf switch provide network automation. The templates are extended to support services in Cisco DFA. The profile templates are packaged in Cisco Prime DCNM for the services orchestrator. The table below includes a list of profile templates that are available for Cisco DFA services. It is important that you select the correct profile to orchestrate and automate services in the Cisco DFA fabric.

Table 2: Cisco Templates for Services Support

Service	Network	Routing	Service Profile
Edge Firewall	Host Network	N/A	defaultUniversalTfProfile
	Edge Firewall	Static	serviceNetworkUniversalTfStaticRoutingProfile
		Dynamic	serviceNetworkUniversalDynamicRoutingESProfile
	Tenant External Service Network	Static	externalNetworkUniversalTfStaticRoutingESProfile
		Dynamic	externalNetworkUniversalDynamicRoutingESProfile
Service Node as Router/Default Gateway	Host Network	N/A	defaultNetworkL2Profile

For NSC Adapter installation information, see the *Cisco DCNM 7.1 OVA Installation Guide*.

Guidelines and Limitations for Cisco Unified Fabric Automation

Cisco Unified Fabric Automation has the following guidelines and limitations:

- The fabric management network can support only one Dynamic Host Configuration Protocol (DHCP) server. You can use either the DHCP server in Cisco Prime Data Center Network Manager (DCNM) or another designated DHCP server, but not both.

- To ensure that Cisco Unified Fabric Automation device auto configuration does not interfere with other DHCP servers on your network, we recommend that you use a dedicated VLAN and subnet for the fabric management network. Cisco Prime DCNM and the Ethernet out-of-band ports of the Cisco Unified Fabric Automation switches (mgmt0) reside in the fabric management network. You have the option to interconnect the fabric management network with your existing out-of-band management network.
- The management connectivity for Cisco Unified Fabric Automation must come through the Cisco NX-OS device management interface (mgmt0).
- The management port on any Cisco Unified Fabric Automation switch must be connected to the same management subnet that includes the Cisco Prime DCNM user interface.
- Every Cisco Unified Fabric Automation switch to be managed by fabric management must be connected to the fabric management network through the Ethernet out-of-band network.
- A console connection for fabric management is recommended but not required for Cisco Unified Fabric Automation.
- If Cisco Prime DCNM is your repository server, you must upload the Cisco NX-OS kickstart and system images to Cisco Prime DCNM using the Serial Copy Protocol (SCP) or Secure File Transfer Protocol (SFTP).

Mapping Considerations

In the Cisco UCS Director environment a tenant is represented by a group. A group can have multiple vDCs (Virtual Data Centers). Each vDC is part of one cloud (in VMware terms this is a vCenter). The vDC can have membership to several virtual switches or DVS'. The vSwitches/DVS' can also be part of multiple vDCs. Essentially a vDC is a logical entity associated with a certain set of compute, network, and storage policies. All VMs launched in that particular vDC adhere to those policies.

In the Cisco Unified Fabric Automation environment, there is a three level hierarchy. The hierarchy is composed of organizations (Orgs) which contain one or more partitions (Partitions), which contain one or more networks.

A tenant or group in Cisco UCS Director maps 1:1 with a Cisco Unified Fabric Automation fabric. So in that sense, we have limited a Cisco UCS Director group to be able to create/map to only one Fabric. One or more vDCs are associated with tenants/groups as is the case with Cisco UCS Director today. Multiple partitions can be created under the Fabric from within Cisco UCS Director. There is no binding or direct mapping between a partition and a Cisco UCS Director vDC. However, when a network is created in Cisco UCS Director, a few mandatory inputs are required:

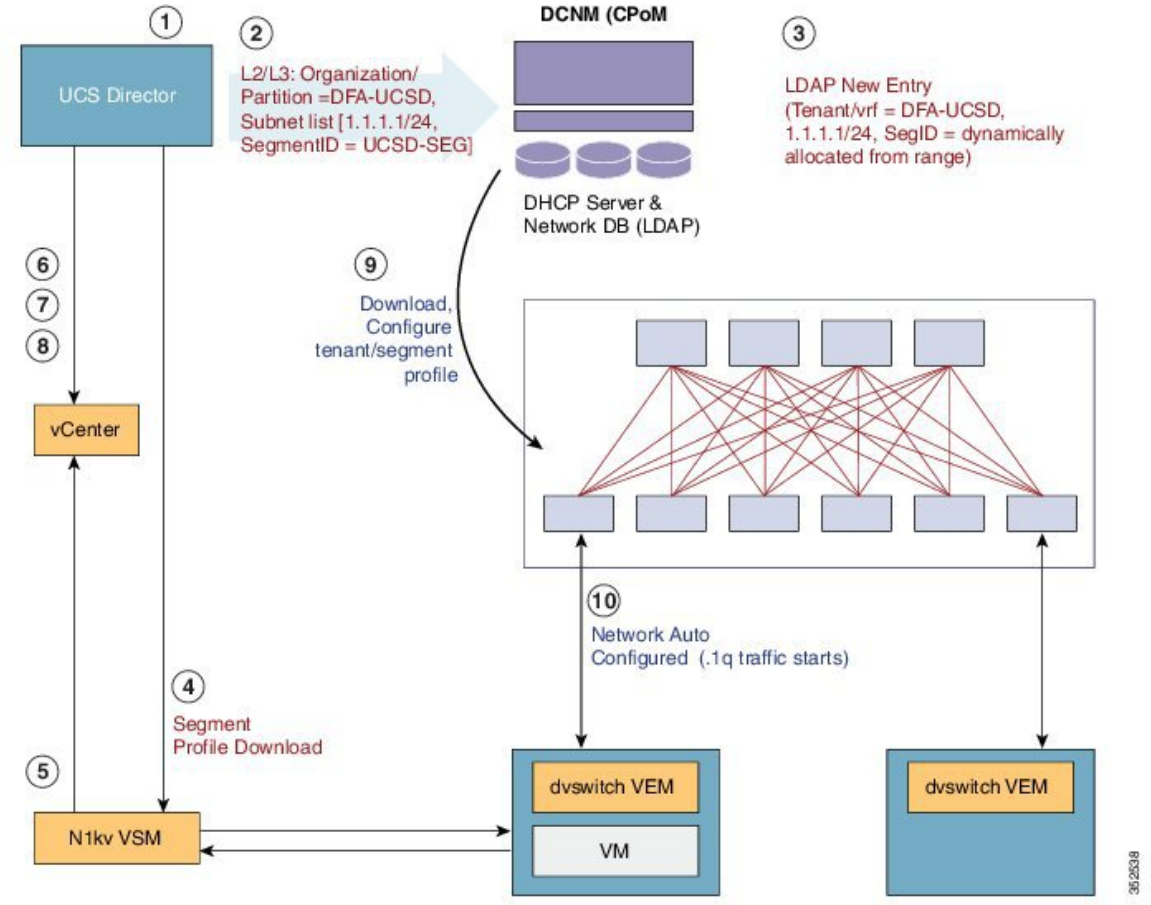
1. A Fabric org/tenant/group selection
2. A Fabric partition selection
3. A Cisco UCS Director vDC selection
4. Layer 3 information associated with the network (for example, namely subnet, default gateway, and subnet mask information)

Moreover, a network creation involves the population of the layer 3 information from Cisco UCS Director to the DCNM via appropriate REST APIs as well creation of an appropriate port-group in a vSwitch or set of vSwitches associated with the selected vDC. The information populated in DCNM is employed for auto-provisioning of resources on the Cisco Unified Fabric Automation (physical network infrastructure), while the existing Cisco UCS Director infrastructure is leveraged to allocate appropriate network resources in the virtual infrastructure.

Examining the Orchestration Flow

The orchestration flow essentially involves two processes: creating a Cisco Unified Fabric Automation fabric, Fabric partition, and Fabric network in the first phase and, in the second phase, deploying the VM. The figure and table below describe the entire orchestration flow between Cisco UCS Director and the DCNM.

Figure 3: Orchestration Workflow (Between Cisco UCS Director and Cisco DCNM)



Process Step	Description
1	Create a Cisco Unified Fabric Automation, Fabric partition, or Fabric network.
2	Cisco UCS Director sends the new organization/partition/network information to the DCNM.
3	The new tenant/vrf entry is added to DCNM.
4	A port group is created on the dvSwitch (however, if you are using a Cisco Nexus 1000V switch download the segment profile).

Process Step	Description
5	The port group is made available to the vCenter application.
6	Cisco UCS Director initiates the VM creation process on vCenter
7	Cisco UCS Director maps the VM nic to the Cisco Cisco Unified Fabric Automation network.
8	The VM is powered on.
9	The leaf initiates Cisco DFA auto configuration process (based on the VDP or data information).
10	The Cisco Cisco Unified Fabric Automation environment is completed (traffic begins to flow if using a dvSwitch).

CHAPTER 3

Configuring Cisco Unified Fabric Automation

This chapter contains the following sections:

- Summary of Steps for Configuring Cisco Unified Fabric Automation, page 14
- Adding a Cloud Account, page 14
- Configuring a Cisco Nexus 1000V Switch, page 16
- Creating a Cisco Unified Fabric Automation Organization Account, page 17
- Creating a Cisco Unified Fabric Automation Organization, page 18
- Associating vDCs, page 19
- Creating a Fabric Partition, page 21
- Creating a Cisco Unified Fabric Automation Network , page 22
- Examining the Fabric SegmentID Range, page 24
- Examining a Cisco Unified Fabric Automation Network's Segment Usage, page 24
- Adding a Cisco Unified Fabric Automation Network to a Cisco Unified Fabric Automation Partition, page 25
- Creating a Cisco Unified Fabric Automation Network using vSwitches, page 27
- Creating a Fabric Network using dvSwitches, page 29
- Attaching a Port Group to a VM, page 30
- Adding a Network Policy, page 31
- Choosing a Fabric Port Selector, page 34
- About Multiple Disk VM Provisioning in a Cisco Unified Fabric Automation Network, page 35
- Application Containers in a Cisco Unified Fabric Automation Environment, page 36

Summary of Steps for Configuring Cisco Unified Fabric Automation

Step 1 Add the Cisco Unified Fabric Automation organization account through **Administration** > **Physical Accounts** > **Multi-Domain Managers**, as shown in Creating a Cisco Unified Fabric Automation Organization Account, on page 17.
Make sure you specify a valid range of segments IDs to be used by Cisco UCS Director. To update the SegmentID Range, choose **DCNM Accounts>Fabric SegmentID Range Management** and highlight the desired DCNM account. The segment id range **Update** button is available when the DCNM account is highlighted.

Step 2 Add a vCenter cloud account through **Administration > Virtual Accounts > Add**).

Step 3 If used, add the Cisco Nexus 1000V account (**Administration >Physical Accounts > Managed Network Elements > Add Network Element**).

Step 4 Check the vCenter cloud inventory under vCenter and verify that you can see the data. It may take a few minutes after the vCenter is added for the inventory to appear.

Step 5 Create several vDCs. You also have to create system, compute, storage, and network policies (refer to the base Cisco UCS Director, Release 4.1 documentation).

Step 6 Choose **Physical > Network**.

Step 7 In the left pane, hoose **Multi-domain Managers > DCNM Accounts** and click **Fabric vDC Switch Association Policy**. Enable vDC switches for a particular Fabric organization account.
With the above steps completed, you can now perform the basic administrative Fabric organization tasks such as:

- Create a group (tenant).
- Create an organization for a group.
- Create a partition within an organization.
- Create a network.
- Create workflows using the Fabric organization orchestration tasks (**Physical Network Tasks > Cisco Tasks** folder). You can also import sample workflows which are included with the Cisco UCS Director Orchestrator.

Adding a Cloud Account

Cisco UCS Director automatically discovers all existing virtual machines (VMs) and images in the newly added cloud account. Typically, the discovery process takes about five minutes. You can add VMware clouds and PowerShell agents.

Creating a Cloud

Step 1 Choose **Administration > Virtual Accounts**.

Step 2 Click **Virtual Accounts**.

Step 3 Click **Add (+)**.

Step 4 On the **Add Cloud** screen, choose a cloud type from the **Cloud Type** drop-down list and complete the following fields:

Name	Description
Cloud Type drop-down list	Choose **VMware**. The following fields are displayed when **VMware** is chosen. Other cloud types display fields that are specific to that cloud type.
Cloud Name field	The cloud name. **Note** Each cloud requires a unique name in Cisco UCS Director. Once a cloud has been added, all reports refer to the cloud using the Cloud Name. Also, single quote characters are not allowed in Cloud Name field (for example, Ven's vCenter).
Server Address field	The vCenter server address.
Server User ID field	The vCenter server username.
Server Password field	The vCenter server password.
Server Access Port field	The server port number.
VMware Datacenter field	The pod name on the vCenter account. This name allows you to discover, monitor and manage the specified pod's resource. Leave the field blank if the entire vCenter account is managed by Cisco UCS Director.
Server Access URL	The URL for server access.
Description field	The description of the cloud.
Contact Email field	The contact email address for the cloud.
Location field	The location.
Pod drop-down list	Choose the converged infrastructure pod. By choosing a pod name, the VMware cloud account appears in the converged infrastructure stack.
Service Provider field	The service provider's name.

Step 5 Click **Add**.

Configuring a Cisco Nexus 1000V Switch

As part of the configuration process you must identify and configure a Cisco Nexus 1000 switch for use within your Cisco Unified Fabric Automation network.

Note This step is optional if you are using a Cisco Nexus 1000V.

Before You Begin

You must have a Cisco DCNM account and a vCenter account. You must have access to a Cisco Nexus 1000V switch.

Adding a Network Element

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 Click **Managed Network Elements**.

Step 3 Click **Add Network Element** and complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which the network belongs.
Device Category drop-down list	Choose the device category for this network element.
Device IP field	The IP address of this device.
Protocol drop-down list	Choose the protocol to be used. This can be either **telnet** or **ssh**.
Port field	The port to use.
Login field	The login name.
Password field	The password associated with the login name.
Enable Password field	The enable password for this network element.

Step 4 Click **Submit**.

Creating a Cisco Unified Fabric Automation Organization Account

Make sure you specify a valid range of segments IDs to be used by Cisco UCS Director. To update the SegmentID Range, choose **DCNM Accounts>Fabric SegmentID Range Management** and highlight the desired DCNM account. The segment id range **Update** button is available when the DCNM account is highlighted.

The Segment ID Range Specified in the creation of the DCNM Account should be different from the ranges present in the L2 Segment ID Range for DCNM Version 7.1(x). Earlier DCNM versions can be given any valid range.

Note Cisco Fabric Organization networks are not tied to any specific pod.

Step 1 Choose **Administration** > **Physical Account**.

Step 2 Click **Multi-Domain Managers**.

Step 3 Click **(+) Add**.

Step 4 On the **Add Account** screen, choose **DCNM** from the drop-down list to create an account for use in Digital Fabric Automation networks.
PNSC is not used in UCSD unless required for specific items, such as VSG deployment.

Step 5 Click **Submit**

Step 6 On the **Multi-Domain Manager Account** screen, complete the following fields. All other field are information only.

Name	Description
Account Name field	The multi-domain account name.
Description field	The description of the multi-domain.
Server Address field	The IP address of the DCNM server.
User ID field	The administrator's or root user's user ID.
Password field	The administrator's user password.
Transport Type drop-down list	Choose a transport type: • HTTP — Standard protocol. • HTTPS — Standard and secure protocol. This is the default selection for DFA Organization networks.

Name	Description
Port field	The port number (based upon the transport type).
SegmentID Pool field	The selected segment ID pool. The selected range should not be used by any other Orchestrator.
VlanID Pool field	The selected Vlan ID pool. The range for Fabric Network Creation is 2 - 4093.
Contact Email field	The email address of the administrator or person responsible for this account.
Location field	The location of the device associated with the account.

Step 7 Click **Submit**.

Step 8 Choose the newly created account.

Step 9 Click **Test Connection** to verify that the account is operational.

Creating a Cisco Unified Fabric Automation Organization

Note You can also use workflow tasks to create a Cisco Unified Fabric Automation organization, partition, or network.

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Manager** entry.

Step 3 Double-click the **DCNM Accounts** entry.
Along with the double-click, you can select the arrow button, double-click on the DCNM Account created, and see the Fabric Organization screen.

Step 4 Click **Fabric Organization**.

Step 5 Click **Create Organization**.

Step 6 On the **Create Fabric Organization** screen, complete the following fields:

Name	Description
Organization Name field	The name of the organization.
Description field	The description of the organization.

Name	Description
Orchestration Source field	The name of the Cisco UCS Director server (used to input the source field in DCNM when an organization is created).
Select Group drop-down list	Choose a user group. **Note** A user group can have only one Fabric organization.

Step 7 Click **Add**.

Configuring the DFA Orchestrator ID

The DFA Orchestrator ID is one of the parameters that is used in the creation of a DFA organization by Cisco UCS Director. By default, this field holds the following value:

UCSD -<UCSD IP Address>

To change the DFA Orchestrator value, enter a new IP address.

Step 1 Choose **Administration > System**.
Step 2 Click **DFA Orchestrator ID**.
Step 3 Enter the **DFA Orchestration Source Name** value.
Step 4 Click **Save**.

Associating vDCs

Before You Begin

Create a Fabric vDC, Fabric account and a Fabric switch.

Note You can also associate Fabric vDC switch association through an action task (**Physical > Network > DCNM Accounts > Fabric VDC Switch Association Policy > Add**).

Step 1 Choose **Policies > Orchestration**.

Step 2 In the **Orchestration** pane, click **Workflows**.

Step 3 On the left pane of the **WorkFlows** screen, choose the workflow folder and click the arrow next to the folder to show the workflows.

Step 4 Double-click the **Create VDC Fabric Switch Association** workflow. Workflow Designer appears.

Step 5 Click the **Edit Workflow Properties** button.

Step 6 In the **Edit Workflow Details** pane, complete the following fields:

Name	Description
Workflow Name field	The name of the workflow.
Description field	The description of the workflow.
Workflow Context drop-down list	Choose a workflow context.
Save as Compound Task check box	If checked, saves workflow as a compound task.
Place in New Folder check box	If checked, place workflow in new folder.
Select Folder drop-down list	Choose a folder to store the workflow.

Step 7 In the **Modify User Inputs** pane, click on the **(+) Add** button to locate and add a Fabric Account, Fabric Switch, and a Fabric vDC.

Step 8 Click **Submit**.

Step 9 Click the **Execute Now** button.

Step 10 Examine the **Submit Workflow** screen to confirm the proper inputs were selected.

Step 11 Click **Submit**.

Creating a Fabric Partition

You can create multiple (Level 2 network) fabric partitions. Each network can have associated network pools.

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Manager** entry.

Step 3 Double-click the **DCNM Accounts** entry.
Along with the double-click, you can select the arrow button, double-click on the DCNM Account created, and see the Fabric Partition screen.

Step 4 Click **Fabric Partition**.

Step 5 Click **Create Partition**.

Step 6 On the **Create Partition** screen, complete the following fields:

Name	Description
Organization Name drop-down list	Choose an organization.
Partition Name field	The name of the partition.
Description field	The description of the partition.
Fabric Account field	Fabric account name.
DCI ID	
Extend the Partition across the Fabric check box	Placing a check mark in this box will extend the partition across the fabric
Service Node IP Address field	IP address of service node.
DNS Server field	IP address of DNS server.
Secondary DNS Server field	IP address of the secondary DNS server.
Multicast Group Address field	
Profile Name drop-down list	Select the Profile Name from the drop-down list
Profile Parameters section	
Border LeafRt field	Only visible if there is a Profile Name selected

Step 7 Click **Add**.

Creating a Cisco Unified Fabric Automation Network

Each fabric network can have associated network pools.

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Manager** entry.

Step 3 Double-click the **DCNM Accounts** entry.
Along with the double-click, you can select the arrow button, double-click on the DCNM Account created, and see the Fabric Network screen.

Step 4 Click **Fabric Network**.

Step 5 Click **Create Network**.

Step 6 On the **Create Fabric Network** screen, complete the following fields:

Name	Description
Fabric Account drop-down list	Choose a Fabric Account from the drop-down list.
Organization Name drop-down list	Choose an organization from the drop-down list
Partition Name drop-down list	Choose a partition from the drop-down list.
Network Name field	Name of the new network.
Multicast Group Address field	
Network Role drop-down list	Choose a network role from the drop-down list.
Description field	Description of the network.
Gateway field	Network gateway address.
Subnet Mask field	Network subnet address.
Switch Type drop-down list	Choose the switch type.
Select Switches drop-down list	Choose a switch to enable association.
Profile Name drop-down list	Choose a profile name.
Profile Parameters section	
DHCP Server Address field	IP address of the DHCP server.
vrfDhcp field	
mtuValue field	

Name	Description
dhcpServerv6Address field	
vrfv6Dhcp field	
Enable IPv6 check box	If checked, enables the use of IPv6 addresses.
Gateway IPv6 Address field	Visible if Enable IPv6 box is checked.
Prefix Length field	Visible if Enable IPv6 box is checked.
Network ID section	
Segment Id field	Segment Id of network. Not visible if the **AutoSelect** check box is selected.
AutoSelect (72000-78000) check box	If checked, allows for segment to be dynamically selected (from within a 72000 - 78000 range). This value is the value chosen when the administrator added the Fabric account to Cisco UCS Director.
Mobility Domain ID select button	Click the select button to choose the Mobility Domain ID. If the DCNM Version is 7.0(2), then a text box will be selected.
AutoSelect Mobility Domain ID check box	If checked, allows the Mobility Domain ID to be autoselected.
VLAN ID field	Enter a Vlan ID.
DHCP Scope section	
Enable DHCP check box	If checked, enables the use of a DHCP server.
IP Range field	Range of IP addresses for this network that the assigned DHCP server can lease.
Service Configuration Parameters	
Start IP field	Starting IP address of service.
End IP field	The range of static IP addresses that can be assigned to specific important service devices.
Secondary Gateway IP Address field	IP address of secondary gateway server (Cisco DCNM).

Step 7 Click **Add**.

Examining the Fabric SegmentID Range

Each network can have an associated segment ID range. Each network has an account ID. Cisco Unified Fabric Automation assigns a segment ID range to one Orchestrator. OpenStack can also talk to Cisco Data Center Network Manager (DCNM). When Cisco UCS Director Orchestrator creates a network, it uses the segments listed in these segment ID ranges.

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Manager** entry.

Step 3 Double-click the **DCNM Accounts** entry.
Along with the double-click, you can select the arrow button, double-click on the DCNM Account created, and see the **Fabric SegmentID Range Management** screen.

Step 4 Click **Fabric SegmentID Range Management**. The Account Name, Orchestrator Name, and SegmentID Range are displayed.

Examining a Cisco Unified Fabric Automation Network's Segment Usage

This view allows you to see who is using which network ID, segment pool, segment ID, and so on.

Step 1 Choose **Physical** > **Network**.

Step 2 Click the **Multi-domain Manager** entry in the left-hand column.

Step 3 Double-click the **DCNM Accounts** entry.
Along with the double-click, you can select the arrow button, double-click on the DCNM Account created, and see the Fabric Network Segment Usage screen.

Step 4 Click **Fabric Network Segment Usage**. The details of segment usage are displayed.

Adding a Cisco Unified Fabric Automation Network to a Cisco Unified Fabric Automation Partition

Note Do not make the network available to all vCenters. You must enable the Cisco Cisco Unified Fabric Automation on a particular switch.

Before You Begin

Create a partition and ensure that you can access Cisco Prime DCNM and a vCenter account. You also need information about the Cisco Nexus 1000V switch to be used with this network. Whenever you create a network, you can create multiple profiles. See the **Profile Name** drop-down list to choose a profile and how it will be used (for example, the **defaultNetworkIpv4EfProfile** selection). The available profiles are available through Cisco DCNM.

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Manager** entry.

Step 3 Double-click the **DCNM Accounts** entry.

Step 4 Click **Fabric Partition**.

Step 5 Double-click on a partition. The **Fabric Network** screen appears.

Step 6 Click **Create Network**.

Step 7 On the **Create Fabric Network** screen, complete the following fields:

Name	Description
Network Name field	The network name.
Multicast Group Address field	Multicast group address value.
Network Role drop-down list	Choose a Host Network from the drop-down list.
Description field	The description of the network.
Gateway field	The name of the gateway server.
Subnet Mask field	The network's subnet mask.
Switch Type drop-down list	Choose a switch type (**dvSwitch** or **vSwitch**). Anyone accessing this switch has access to the Cisco DFA.
Profile Name drop-down list	Choose a profile from the drop-down list.
Profile Parameters section	
DHCP Server Address field	IP address of the DHCP server.

Name	Description
vrfDhcp field	
mtuValue field	specify an mtu value between 1500 and 9216.
dhcpServerv6Address field	
vrfv6Dhcp field	
Enable IPv6 check box	If checked, enables the use of IPv6 addresses.
Gateway IPv6 Address field	IPv6 address field used by the gateway. **Note** This field is visible only if the Enable IPv6 check box is selected.
Prefix Length field	Prefix length used by the IPv6 address. **Note** This field is visible only if the Enable IPv6 check box is selected.
Network Id section	
Segment ID field	Segment Id in use by server. This must be a unique value for each network.
AutoSelect (50000-70000) check box	If checked, allows for segment to be dynamically selected (from within a 50000 - 70000 range).
Mobility Domain ID field	
AutoSelect Mobility Domain ID check box	If checked, automatically chooses the Mobility Domain ID.
DHCP Scope section	
Enable DHCP check box	If checked, enables DHCP for the network.
IP Range field	The IP range of the DHCP server.
Service Configuration Parameters section	
Start IP field	The starting IP address value (static range only).
End IP field	The ending IP address value (static range only).
Secondary Gateway field	

Step 8 Click **Add**. Cisco UCS Director creates a port group on the vSwitch. Once the port group is available, you can create a VM. Any VM can use this port group. The Cisco Cisco Unified Fabric Automation network allows you to create network segments dynamically, which makes them visible to the dvSwitches and Cisco Nexus 1000V switches.

Creating a Cisco Unified Fabric Automation Network using vSwitches

Each Cisco Unified Fabric Automation network can have associated network pools. Creating a Cisco Unified Fabric Automation network using vSwitches and dvSwitches are very similar. However, vSwitches can be mapped to one network adapter or to multiple network adapters. vSwitches that have no associated network adapters can also be implemented as well.

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Managers** entry.

Step 3 Click the **DCNM Accounts** entry.

Step 4 Click **Fabric Network**.

Step 5 Click **Create Network**.

Step 6 On the **Create Fabric Network** screen, complete the following fields:

Name	Description
Partition Name field	Choose a partition from the drop-down list.
Network Name field	Name of the new network.
Description field	Description of the network.
Gateway field	Network gateway address.
Subnet mask field	Network subnet address.
Switch Type drop-down list	Choose the **vSwitches** option from the drop-down list.When prompted, check the check box of a corresponding switch.
Select Switches drop-down list	Choose a switch.
Profile Name drop-down list	Choose a profile name.
Profile Parameters section	
DHCP Server Address field	IP address of the DHCP server.
Enable IPv6 check box	If checked, enables the use of IPv6 addresses.

Name	Description
Gateway IPv6 Address field	Gateway IPv6 address for DHCP server. Only visible when the Enable IPv6 check box is checked.
Prefix Length field	Prefix used for IPv6 addresses. Only visible when the Enable IPv6 check box is checked.
Network ID section	
Segment ID field	Segment ID of network. Not visible if the **AutoSelect** check box is selected. **Note** This field is not required when creating a network on a vSwitch or (VMWare) dvSwitch. The VDP protocol is not used and only a Vlan and mobility ID is required.
Mobility Domain ID select button	Click to choose a Mobility Domain ID from a list.
Mobility Domain ID check box	If checked, allows for the Mobility domain ID to be dynamically selected.
DHCP Scope section	
Enable DHCP check box	If checked, enables the use of a DHCP server.
IP Range field	IP range in use for the DHCP server.
Service Configuration Parameters	
Start IP field	Starting IP address of service.
End IP field	The range of static IP addresses that can be assigned to specific important service devices.
Secondary Gateway field	Secondary network gateway address.

Step 7 Click **Add**.

Creating a Fabric Network using dvSwitches

Each Fabric network can have associated network pools. Creating a Fabric network using vSwitches and dvSwitches are very similar. A dvSwitch acts like a global switch, enabling administrators to associate a single switch with all ESX or ESXi hosts in a datacenter, rather than configure a vSwitch for each individual host.

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Managers** entry.

Step 3 Click the **DCNM Accounts** entry.

Step 4 Click **Fabric Network**.

Step 5 Click **Create Network**.

Step 6 On the **Create Fabric Network** screen, complete the following fields:

Name	Description
Partition Name field	Choose a partition from the drop-down list.
Network Name field	Name of the new network.
Description field	Description of the network.
Gateway field	Network gateway address.
Subnet mask field	Network subnet address.
Switch Type drop-down list	Choose the **dvSwitches** option from the drop-down list. When prompted, check the check box of a corresponding switch.
Select Switches drop-down list	Choose a switch.
Profile Name drop-down list	Choose a profile name.
Profile Parameters section	
DHCP Server Address field	IP address of the DHCP server.
Enable IPv6 check box	If checked, enables the use of IPv6 addresses.
Gateway IPv6 Address field	Gateway IPv6 address for DHCP server. Only visible when the Enable IPv6 check box is checked.
Prefix Length field	Prefix used for IPv6 addresses. Only visible when the Enable IPv6 check box is checked.
Network ID section	

Name	Description
Segment ID field	Segment ID of network. Not visible if the **AutoSelect** check box is selected. **Note** This field is not required when creating a network on a vSwitch or (VMWare) dvSwitch. The VDP protocol is not used and only Vlan and Mobility Domain ID are required.
Mobility Domain ID select button	Click to choose a Mobility Domain ID from a list.
AutoSelect Mobility Domain ID check box	If checked, allows for the Mobility domain ID to be dynamically selected.
DHCP Scope section	
Enable DHCP check box	If checked, enables the use of a DHCP server.
IP Range field	IP range in use for the DHCP server.
Service Configuration Parameters	
Start IP field	Starting IP address of service.
End IP field	The range of static IP addresses that can be assigned to specific important service devices.
Secondary Gateway field	Secondary network gateway address.

Step 7 Click **Add**.

Attaching a Port Group to a VM

A Cisco DFA is in a network level infrastructure. It lets you create network segments dynamically and then you make the network visible to the vSwitch, dvSwitch and Cisco Nexus 1000 switches once the port group is available. Any VM that uses this port group becomes connected to the Cisco Cisco Unified Fabric Automation network. Attaching a port group to a VM is the last step in the configuration process.

Before You Begin

Create a VM.

Step 1 Choose **Virtual** > **Network**.

Step 2 In the left-hand pane, choose a vCenter.

Step 3 Click **Port Groups**.

Step 4 Choose a port group.

Step 5 Click **Assign Group**.

Step 6 On the **Select Group** screen, complete the following fields:

Name	Description
Group Name drop-down list	Choose a group.
Label field	The label associated to the group.

Step 7 Click **Submit**.

Adding a Network Policy

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **VMware Network Policy**.

Step 3 Click **Add**.

Step 4 On the **Network Policy Information** screen, complete the following fields:

Name	Description
Policy Name field	The name of the network policy.
Policy Description field	The description of the network policy.
Cloud Name drop-down list	Choose the cloud account to which the policy applies.
Allow end user to select optional NICs check box	Check if you want to provide vNICs selection during the creation of a service request-deployment configuration.
VM Networks field	Expand the **VM Networks** table to add a new entry to the VM network.

Step 5 Click **Add** in the VM Networks section to add and configure multiple vNICs. These vNICs are applicable to the VM that is provisioned using this policy.

Note To add or replace vNICs for provisioned or discovered VMs using VM actions, you must configure the vNICs.

Step 6 On the **Add Entry to VM Networks** screen, complete the following fields:

Name	Description
NIC Alias field	The name for the new NIC
Mandatory check box	If **Allow end user to select optional NICs** is checked on the **Network Policy Information** screen, this box is pre-selected. If the **Allow end user to select optional NICs** box was not checked, and this check box is not selected, then the **NIC Alias** field is optional. **Note** At least one of the NICs should have the **Mandatory** option selected. The NICs that have the **Mandatory** option selected are used in VM provisioning and there will be no option for the user during VM service request creation.
Allow end user to choose portgroups check box	Check to allow the end user to choose port groups during provisioning.
Show policy level portgroups check box	Checking this check box along with the **Allow end user to choose portgroups** check box lists all the selected portgroups of NICs in the policy.
Copy Adapter from Template check box	Check if you do not need custom settings. Clear this check box for custom settings. The **Adapter Type** drop-down list is not visible when you check this check box.
Allow the end user to override IP Address check box	Check to allow users to override the IP address.
Adapter Type drop-down list	Choose the adapter type. Select this option if the user wants to have the same Adapter Type that is available in the template. **Note** This option is not visible if the **Copy Adapter from Template** option is chosen.

Step 7 Click **Add (+)** in the **Port Groups** section. The **Add Entry to Port Groups** screen appears.

Step 8 Click **Select** to choose the port group name.

Step 9 From the **Select IP Address Type** drop-down field, choose **DHCP** (default) or **Static**.

a) If you choose **Static**, you must choose **IP Pool Policy** (default) or **Inline IP Pool**.
If you choose **IP Pool Policy**, click **Select to choose a static IP pool**. On the **Select** screen, choose from the list of preconfigured static IP pool(s). If no preconfigured static IP pools exist, see Adding a Static IP Policy for more information.

b) If you choose **Inline IP Pool**, complete the following fields:

Name	Description
Static IP Pool field	The static IP pool. For example: 10.5.0.1 - 10.5.0.50, 10.5.0.100, 10.5.1.20-10.5.1.70
Subnet Mask field	The subnetwork mask for the pool. For example: 255.255.255.0
Gateway IP Address field	The IP address of the default gateway for this network.
Allow IP Overlap drop-down list	Indicate whether IP overlap is allowed or not. By default, overlapping IP is not enabled. Enabling overlapping of IP implies the following: • You can create an IP pool and have IP addresses overlap within that pool. • You can create two static IP pools and have the IP addresses overlap between the pools
Scope drop-down list	The scope of the IP pool overlap. The options are: • MSP Organization This option is visible only if you have enabled MSP. • Group/Customer Organization • Container **Note** This option is visible only if you select Yes in the **Allow IP Overlap** drop-down list.
User Group ID field	Choose **Select** to check the user group. All the user groups created in the system are displayed.
Container ID field	Choose **Select** to check the container.

Step 10 Check **IPv6** to configure IPv6.
You must configure the identical fields that you specified for IPv4 configuration.

Step 11 Click **Submit**.

Step 12 Click **Submit** on the **Add Entry to VM Networks** screen.

Step 13 Click **Submit** on the **Network Policy Information** screen.

Choosing a Fabric Port Selector

Before You Begin

Create a vDC, Fabric account and a Fabric switch.

Step 1 Choose **Policies** > **Orchestration**.

Step 2 In the **Orchestration** pane, click **Workflows**.

Step 3 On the left pane of the **WorkFlows** section, choose the workflow folder and click the arrow next to the folder to show the workflows.

Step 4 Double-click the **FabricPortGroupSelector** task.

Note This task will take Fabric Port Group or any port group as input and provide the output as well.

Step 5 On the **Edit Task (FabricPortGroupSelector)** screen, complete the following fields:

Name	Description
Task Name field	The name of the task.
Task Category drop-down list	The **Cisco Fabric Tasks** category is chosen.
Task Type drop-down list	The **FabricPortGroupSelector** type is chosen.
Comment field	Comments that pertain to this task.
Retry Execution check box	If checked, retries the workflow execution.

Step 6 Click **Next**.

Step 7 On the **User Input Mapping** screen, complete the following fields:

Name	Description
Manage Workflow User Inputs field	The name of the task.
Port Group section	
Map to User Input check box	If checked, maps port group to user input.
User Input drop-down list	The **Port Group** user input type is chosen.
Fabric Port Group section	
Map to User Input check box	If checked, maps port group to user input.

Step 8 Click **Next**.

Step 9 On the **Task Inputs** screen, complete the following fields.

Name	Description
Revalidate button	Binds all the necessary parameters identified in this task to the environment.
Fabric Port Group button	Click the **Select...** button to choose a DFA port group.

Step 10 Click **Submit**.

Step 11 Click **Execute Now**.

Step 12 Examine the **Submit Workflow** screen to confirm the proper inputs were selected.

Step 13 Click **Submit**.

About Multiple Disk VM Provisioning in a Cisco Unified Fabric Automation Network

Cisco UCS Director supports virtual machine (VM) provisioning of multiple disks from a template. You can configure VM disk provisioning on a preferred single datastore or multiple datastores in a Cisco Cisco Unified Fabric Automation network. You can also configure individual disk policies for each additional disk in a template.

Cisco UCS Director classifies the disks into the following categories:

- System
- Data
- Database
- Swap
- Log

Note The disk categories that are defined by Cisco UCS Director are for disk labeling only. For specific information on VM provisioning refer to the UCS Director Administration Guide.

Application Containers in a Cisco Unified Fabric Automation Environment

An application container is a collection of virtual machines (VMs) with an internal private network that is based on rules specified by an administrator. The application container can have one or more VMs that are (optionally) guarded by a fencing gateway (for example, a Cisco Virtual Secure Gateway) to the external/public cloud. In order to create an application container you must create a system, network, and computing policies. For complete information on creating application containers see the Cisco UCS Director Application Containers Guide.

About Application Container Templates

To create an application container template, you must provide information regarding the following elements. This information is used to create your containers:

- Virtual account (cloud)
- Network configuration
- VM configuration
- Container security
- Select Network, Storage, Compute, and Cost Model policies
- Select the gateway policy, if **Gateway Required** check box is enabled (optional)
- Options for service end users

Note For more information regarding the container templates and Virtual Secure Gateways (VSGs), see Creating an Application Template for a VSG, on page 44.

Creating Application Container Policies (Cisco Unified Fabric Automation Environment)

Step 1 Choose **Policies** > **Application Containers**.

Step 2 Click **Virtual Infrastructure Policies**.

Step 3 Click **Add Policy**.

Step 4 In the **Virtual Infrastructure Policy Specification** pane, complete the following fields:

Name	Description
Policy Name field	The name of the policy.

Name	Description
Policy Description field	The description of the policy.
Container Type drop-down list	Choose **Fabric** and click**Next** to confirm your selection and follow the wizard prompts. **Note** For Cisco Dynamic Fabric Automation environment, the creation of a gateway is optional.
Select Virtual Account drop-down list	The chosen virtual account (the cloud on which the gateway VM is created).

Step 5 Click **Next**.

Step 6 In the **Virtual Infrastructure Policy - Fabric Information** pane, complete the following fields:

Name	Description
With VSG check box	Check this box for VSG support.
Fabric Name field	Choose a fabric account.
Switch Type drop-down list	Choose a switch type.
Switch Name drop-down list	Choose a switch name.
Alternate Switch Name drop-down list	Choose an alternate switch.
Mobility Domain ID field	Choose from drop-down list if AutoSelect Mobility Domain ID is not checked.
AutoSelect Mobility Domain ID check box	Check to AutoSelect Mobility Domain ID.
Partition Parameters section	
DCI ID field	
Extend the Partition across the Fabric check box	
Service Node IP Address field	Not applicable for ASA gateway.
DNS Server field	
Secondary DNS Server field	
Multi Cast Group Address field	
Profile Name drop-down	Choose a Profile Name from the drop-down.

Name	Description
Profile Parameters section	
Border LeafRT field	Visible if a Profile Name is chosen.

Step 7 Click **Next**.

Step 8 In the **Virtual Infrastructure Policy - Fencing Gateway Information** pane, complete the following fields:

Name	Description
Gateway Type field	Choose a fabric account.
Select Device drop-down list	Choose a switch type.
Outside Interface drop-down list	Choose a switch name.
Outside Interface IP Address field	The outside IP address.
Outside Interface VLAN ID field	The outside VLAN ID.
Inside Interfaces drop-down list	Choose an inside interface to apply to the context.

Step 9 Click **Submit**.

Creating Application Container Templates (Cisco Unified Fabric Automation Environment)

Note For information on creating container templates for use with a VSG, see Creating an Application Template for a VSG, on page 44.

Note This procedure does not create an updating template. If you change templates, it is applied only to the newly created containers from that template. With this template you can create application containers for use in a variety of networks (including Fabric Networks).

Before You Begin

Creating an application container policy.

Step 1 Choose **Policies** > **Application Containers**.

Step 2 Click **Application Container Templates**.

Step 3 Click **Add Template**. The **Application Container Template** screen appears. Complete the following fields:

Name	Description
Template Name field	The name of the new template.
Template Description field	The description of the template.

Step 4 Click **Next**.

Step 5 The Application Container Template - Select a Virtual infrastructure policy screen appears. Complete the following selection:

Name	Description
Select Virtual Infrastructure Policy drop-down list	Choose a policy (the policy created for use with your Fabric environment).

Step 6 Click **Next**.

Step 7 Click **(+)** to add a new **Fabric Network** entry.

Step 8 In the **Add Entry to Fabric Networks** screen, complete the following fields:

Note If an application container policy is created using the **No Gateway** option, a gateway VM is not provisioned (irrespective of the container type)

Name	Description
Network Name field	Name of the new network.
Network Role drop-down list	Choose a network role.
Description field	Description of the network.
Profile Name drop-down list	Choose a profile name.
Gateway IP address field	IP address of the gateway server.
Network Mask check box	The network mask.
DHCP Server Address field	IP address of the DHCP server.
Gateway IPv6 Address check box	IPv6 address field used by the gateway.
Prefix Length field	Prefix length used by the IPv6 address.

Name	Description
Start IP field	Starting IP address of service.
End IP field	The range of static IP addresses that can be assigned to specific important service devices.
Secondary Gateway field	IP address of secondary gateway server (Cisco DCNM).

Step 9 Click **Next**. The **Application Container: Template - Internal Networks** screen appears.
You can add and configure multiple networks for a container. These networks are applicable to the VM that is provisioned using this template.

Step 10 Click the **(+) Add** icon to add a network. The **Add Entry to Networks** screen appears. Complete the following fields:

Name	Description
DCNM Networks check box	If checked, enables the application container for use in Digital Fabric Automation Networks.
Network Name field	The network name. The name should be unique within the container.
Fabric Account drop-down list	Choose a fabric account.
Network IP Address field	The network IP address for the container.
Network Mask field	The network mask.
Gateway IP Address field field	The IP address of the default gateway for the network. A NIC with this IP is created on the GW VM.

Step 11 Click **Submit**.
Next, you can add and configure the VM that will be provisioned in the application container.

Step 12 Click **OK**.

Step 13 Click the **Add (+)** icon to add a VM. The **Add Entry to Virtual Machines** screen appears. Complete the following fields:

Name	Description
VM field	The VM name.
Description field	The description of the VM.
VM Image drop-down list	Choose the image to be deployed.

Name	Description
Number of Virtual CPUs drop-down list	Choose the network mask.
Memory drop-down list	Choose the IP address of the default gateway for the network.
CPU Reservation (MHz) field	The CPU reservation for the VM.
Memory Reservation (MB) field	The memory reservation for the VM.
Disk Size (GB) field	The custom disk size for the VM. To use the template disk size specify the value of 0. The specified disk size overrides the disk size of the selected image.
VM Password Sharing Option drop-down list	Choose an option on how to share the VM's username and password with the end users. If **Share after password reset** or **Share template credentials** is chosen, the end user needs to specify a username and password for the chosen templates.
VM Network Interface field	Choose the VM network interface information. If you are adding another network interface, go to Step 9.
Maximum Quality field	States the maximum number of instances that can be added in this container after it is created.
Initial Quality field	States the number of VM instances to provision when the container is created.

Step 14 (Optional) Click the **Add (+)** icon to add a new (multiple) VM network interface. Complete the following fields:

Name	Description
VM Network Interface Name field	The name of the VM network interface.
Select the Network drop-down list	Choose a network.
IP Address field	The IP address of the network.

Step 15 Click **Next**. The **Application Container: Template - External Gateway Security Configuration** screen appears. You can specify the security configuration components such as port mapping and outbound access control lists (ACLs).

Step 16 Click the **Add (+)** icon to add a port mapping. Complete the following fields:

Name	Description
Protocoldrop-down list	Choose a protocol.
Mapped Port drop-down list	Choose the mapped port for the selected protocol.
Remote IP Address field	The IP address of the internal system.

Name	Description
Remote Port field	The remote machine's port number.

Step 17 Click **Submit**. The **Add Entry to Outbound ACLs** screen appears. Complete the following fields:

Name	Description
Protocol drop-down list	Choose a protocol.
Select Network drop-down list	The network to which the rules need to apply.
Source Address field	The source classless inter domain routing (CIDR) IP address.
Destination Address field	The destination CIDR IP address.
Action field	The action that is applied on the network traffic.

Step 18 Click **Next**.

Step 19 Click **Next**. The **Application Container Template - Deployment Policies** screen appears.
You must select the compute, storage, network, system policy, and cost model required for VM provisioning. A policy is a group of rules that determine where and how a new VM is to be provisioned within an application container (based on the availability of system resources).

- The network policy is used only to deploy the outside interface of the virtual firewall (container gateway).
- The selected *Portgroup in Network Policy* should be on the host on which the Gateway VM is provisioned.
- The network policy can use either a *Static IP Pool or DHCP*. However, for container type VSG the network policy should use a Static IP Pool only. The VSG VM requires IP addresses as input. There is no current provision to specify DHCP for deploying a VSG VM.
- The network adapter settings for a provisioned VM (container gateway) should be similar to the settings in the template. You may or may not have to check the *Copy Adapter from Template* check box in the network policy used for this application container.

Complete the following fields:

Name	Description
Compute Policy drop-down list	Choose a computer policy.
Storage Policy drop-down list	Choose a storage policy.
Network Policy drop-down list	Choose a network policy.
Systems Policy drop-down list	Choose a systems policy.
Cost Model drop-down list	Choose a cost model.

Step 20 Click **Next**. The **Application Container: Template - Options** screen appears.
In this page, you can select options to enable or disable certain privileges to the self-service end user.

Complete the following fields:

Name	Description
Enable Self-Service Power Management of VMs checkbox	If checked, enables self-service power management of VMs.
Enable Self-Service Resizing of VMs checkbox	If checked, enables self-service resizing of VMs.
Enable Self-Service VM Snapshot Management checkbox	If checked, enables self-service VM snapshot management.
Enable VNC Based Console Access checkbox	If checked, enables self-service VNC based console access.
Enable Self-Service Deletion of Containers checkbox	If checked, enables self-deletion of containers.
Technical Support Email Addresses field	The technical support email address. A detailed technical email is sent to one or more email addresses entered into this field after a container is deployed.

Step 21 Click **Next**. The **Application Container: Template - Setup Workflows** screen appears. Complete the following field:

Name	Description
Container Setup Workflow drop-down list	Choose a workflow to establish the application container.

Step 22 Click **Next** to complete the creation of the application container template and review the Summary pane.

Step 23 Click **Submit**.

What to Do Next

See the *Custom Workflow for Application Containers* information on customizing certain aspects of a template.

Creating a Custom Workflow for Application Containers

Note For more information about using the orchestration to run workflows, see the Cisco UCS Director Orchestration Guide for this release.

Note You cannot create an APIC application container by running a workflow directly. For information on creating the APIC application containers, see APIC Application Container Creation Process.

If you use a workflow to create an application container template, you must perform some manual steps. There are two scenarios that you do encounter:

- **Gateway Type: CISCO ASA—**If the gateway type is CISCO ASA for the container, you must specifically choose **Application Container with ASA Gateway** from the list of available workflows. You can search for the workflow and check its check box in order to select it.
- **Distributed Virtual Portgroups—**If you choose the **Distributed Virtual Portgroup** in the network policy that is associated with the container, then you must perform the following steps manually:

  1. Choose **Virtual Network Type** and enter its name as required in a workflow associated with the container.
  2. Choose a specific workflow. This type of workflow depends on which gateway type was associated with the container. For a Linux gateway, choose **Application Container Setup** workflow. For a CISCO ASA gateway type, choose the **Application Container with ASA Gateway**.
  3. Edit or clone the required workflow by going to the Cisco UCS Director Orchestrator application and editing the workflow on the **Workflow Designer** page.
  4. In the workflow window, double-click the **Allocate Container VM Resources** task.
  5. Choose the required virtual network type (either **Distributed Virtual Portgroup** or **Distributed Virtual Portgroup N1K**).
  6. Specify the primary DVSwitch and alternate DVSwitch names.
  7. Click **Save** to save the workflow.

Creating an Application Template for a VSG

Step 1 Choose **Policies** > **Application Containers**.

Step 2 On the **Application Containers** page, click **Application Container Templates**.

Step 3 Click **Add Template**. The **Add Application Container Template** page appears. Complete the following fields:

Name	Description
Template Name field	The name of the new template.

Name	Description
Template Description field	The description of the template.

Step 4 Click **Next**. The **Application Container Template - Select a Virtual Infrastructure policy** screen appears. In this screen, you choose the cloud on which the application container is deployed. Complete the following field:

Name	Description
Select Virtual Infrastructure Policy drop-down list	Choose a virtual infrastructure policy to deploy to the container.

Step 5 Click **Next**. The **Application Container: Template - Internal Networks** screen appears.

Note Only one network is allowed per VSG container.

Step 6 Click **Add (+)** icon to add a network. The **Add Entry to Networks** screen appears. Complete the following fields:

Name	Description
Network Name field	The network name. The name should be unique within the container. You can use a maximum of 128 characters.
Network Type drop-down list	Choose the network type.
Information Source drop-down list	Choose the information source from the list.
VLAN ID Range field	The VLAN ID range. This value controls the number of containers that can be cloned or created.
Network IP Address field	The network IP address for the container.
Network Mask field	The network mask.
Gateway IP Address field	The IP address of the default gateway for the network. A NIC with this IP address is created on the GW VM. **Note** The IP address is configured on the inside interface of the gateway.

Step 7 Click **Submit**.
Next, you can add and configure the gateway VM that will be provisioned in the application container.

Step 8 Click **OK**.

Step 9 Click **Next**.
The **Application Conatiner Template - VMs** screen appears.

Step 10 Click **Add (+)** to add a VM. Complete the following fields:

Name	Description
VM field	The name of the VM. The full name contains the container name as well as this name.
Description field	The description of the VM.
Provision VM using Content Library Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image drop-down list	This field appears only when the **Provision VM using Content Library Template** check box is unchecked. Choose an image to be deployed.
Number of Virtual CPUs drop-down list	Choose the number of virtual CPUs to be allocated to the VM.
Memory drop-down list	Choose the amount of memory (in MB) to be allocated to the VM.
CPU Reservation (MHz) field	The CPU reservation for the VM in Mhz.
Memory Reservation (MB) field	The memory reservation for the VM.
Disk Size (GB) field	The custom disk size for the VM. To use the template disk size specify the value of zero. The specified disk size overrides the disk size of the selected image. **Note** If this value is less than template size, this value is ignored.
VM Password Sharing Option drop-down list	Choose an option on how to share the VM's username and password with the end users. If **Share after password reset** or **Share template credentials** is chosen, the end user needs to specify a username and password for the chosen templates.
Use Network Configuration from Image check box	If checked, the network configuration from the image is applied to the provisioned VM.
VM Network Interfaces field	Expand VM Network Interafces and choose the VM network interface information. If you are adding another network interface, go to Step 11.
Maximum Quantity field	The maximum number of instances that can be added in this container after it is created.
Initial Quantity field	The number of VM instances to provision when the container is created. **Note** Each VM will have a unique name and IP address.

Step 11 (Optional) Click **Add (+)** to add a new (multiple) VM network interface. Complete the following fields:

Name	Description
VM Network Interface Name field	The name of the VM network interface.
Select the Network drop-down list	Choose a network.
IP Address field	The IP address of the network.

Step 12 Click **Next**.

Step 13 Click **Ok**.
The **Application Container Template - External Gateway Security Configuration** screen appears. You can specify the security configuration components, such as port mapping and outbound access control lists (ACLs).

Step 14 Click **Add (+)** to add a port mapping. Complete the following fields:

Name	Description
Protocol drop-down list	Choose a protocol for the port mapping.
Mapped Port drop-down list	Choose the mapped port for the selected protocol.
Remote IP Address field	The IP address of the remote machine.
Remote Port field	The remote machine port number.

Step 15 Click **Submit**.

Step 16 Click **OK**.

Step 17 Click **Add (+)** icon to add an Outbound ACL, in the **Application Container Template - External Gateway Security Configuration** screen. Complete the following fields:

Name	Description
Protocol drop-down list	Choose a protocol.
Select Network drop-down list	The network to which the rules need to apply.
Source Address field	The source classless inter domain routing (CIDR) IP address.
Destination Address field	The destination CIDR IP address.
Action field	The action that is applied on the matching network traffic.

Step 18 Click **Submit**.

Step 19 Click **OK**.

Step 20 Click **Next**.

Step 21 On the **Application Container Template - Deployment Policies** screen, complete the following fields:

Name	Description
Compute Policy drop-down list	Choose a policy to deploy all of the compute components of the virtual container.
Storage Policy drop-down list	Choose a policy to deploy all of the storage components of the virtual container.
Network Policy field	Choose a policy to deploy to the container gateway. Hosts considered to be part of the computing policy should be associated with the Cisco Nexus 1000 (used to deploy Cisco VSG). **Note** This field is only used for the outside interface of the container gateway. Also, resource allocation should be associated with a Cisco Nexus 1000 Series switch.
Systems Policy field	The value used for DNS and other OS license configurations.
Cost Model field	Choose a cost model.
Use common network policy check box	Check the check box to use the common network policy defined above for the VSG management network.
Management Network Policy drop-down list	If the **Use common network policy** is unchecked, choose a network policy for the VSG management network.

Step 22 Click **Next**.

Step 23 On the **Application Container Template - Options** screen, complete the following fields:

Name	Description
End User Self-Service Policy drop-down list	Choose an end user self-service policy applicable for the application container template.
Enable Self-Service Deletion of Containers check box	If checked, enables self-service deletion of containers.
Enable VNC Based Console Access check box	If checked, enables VNC-based console access to VM.
Technical Support Email Addresses field	Enter the comma-separated list of email addresses of individuals who should receive emails regarding the container provisioning.

Step 24 Click **Next**.

Step 25 Choose a workflow to setup the container.

Step 26 Expand the workflow list and select a workflow (for example, Workflow Id 431 Fenced Container Setup - VSG).

Note A workflow should contain allocated resources. For example, if it is a VSG workflow it should contain a Cisco Nexus 1000 Series resource.

Step 27 Click **Select**.

Step 28 Click **Submit**.

Managing Application Containers

As an administrator, you can perform the following management actions on application containers:

- Add VMs
- Open Console
- Clone Template
- Manage Container Power
- Delete Containers
- View Reports

Viewing Container Actions

Actions available to apply to a container are context-sensitive. You can use the action icons at the top of the **Application Containers** page or the **More Actions** drop-down list to perform these actions.

Step 1 Choose **Policies** > **Application Containers**.

Step 2 On the **Application Containers** page, click **Application Containers**.

Step 3 Choose a container to display all of the available actions.

Note To enable a self-service user to perform actions on a container, give self-service users permission by checking **Enable Self-Service** when creating the container template.

Adding VMs

Note You cannot add VMs to the container through the **Add VMs to Container** workflow. You can add VMs only by clicking **Add VMs** or by using the API.

Step 1 Choose **Policies** > **Application Containers**.

Step 2 On the **Application Containers** page, click **Application Containers**.

Step 3 Choose an application container.

Step 4 From the **More Actions** drop-down list, choose **Add VMs**.

Step 5 On the **Add VMs** screen, expand the virtual machines list and click **Add**.
Define the virtual machine in one of the following ways:

- Use a VM image and manually set the parameters. See Step 6.
- Use a template defined in the application profile. See Step 7.

Step 6 On the **Add Entry to Virtual Machines** screen, leave the **Use Predefined Template** check box unchecked and complete the following fields:

Name	Description
Network drop-down list	Choose the network (tier) on which you want to add the VM.
VM Name field	Enter the name you want to assign to the VM. During application container deployment, you can update the prefix from what is defined in the application profile.
Provision new VM using Content Library VM Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision new VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image list	This field appears only when the **Provision new VM using Content Library VM Template** check box is unchecked. Expand the list and select a VM image to use. You define these VMs in the vCenter for your cluster.
Use Linked Clone check box	This check box is enabled only when you choose a VM template with a snapshot. Check this box to deploy new VMs using linked clone feature which enables them to be provisioned faster and storage efficient.

Name	Description
Snapshot field	This field appears only when the **Use Linked Clone** check box is checked. Click **Select** to choose a snapshot that need to be used to provision a new VM using linked clone feature.
Number of vCPUs drop-down list	Choose the number of virtual CPUs for the VM.
Memory (MB) drop-down list	Choose the size of the VM memory.
Disk Size (GB) field	Enter the size of the VM disk. If you enter zero, the VM uses the disk size defined in the image.
Select DRS Rule list	Expand the list and select a distributed resource scheduler (DRS) rule (also called an affinity rule).
Select Storage DRS Rule list	Expand the list to choose a storage distributed resource scheduler (DRS) rule. **Note** This field appears only if you chose a DRS rule from **Select DRS Rule**.
VM Password Sharing Option drop-down list	Choose the password sharing policy for this VM. Default is to not share the root password.
Network Adapter Type drop-down list	Choose the network adapter for the VM.
Initial Quantity drop-down list	Choose the number of VMs to create on application startup.

Skip to Step 8.

Step 7 On the **Add Entry to Virtual Machines** screen, check the **Use Predefined Template** check box and complete the following fields:

Name	Description
Network drop-down list	Choose the network (tier) on which you want to add the VM.
VM Name drop-down list	Choose the name of the VM as defined in the application profile.
Select DRS Rule list	Expand the list and select a DRS rule (also called an affinity rule).
No Of Instances drop-down list	Choose the number of VM instances to provision. The drop-down list limits your choices so as not to exceed the maximum number of VMs defined in the application profile.

Step 8 Click **Submit**.

Step 9 To add more VMs, repeat this procedure starting with Step 5.

Step 10 After you finish adding VMs, on the **Add VMs** screen, click **Submit**.

Accessing a VM Console

Before You Begin

You must enable proper console access rights on individual VMs that you want to access using VNC. See Enabling VNC Console Access.

Step 1 Choose **Policies** > **Application Containers**.

Step 2 On the **Application Containers** page, click **Application Containers**.

Step 3 Choose an application container.

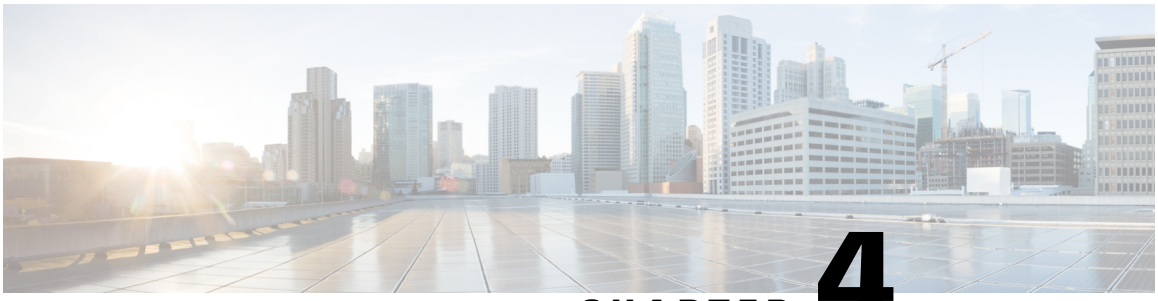
Step 4 From the **More Actions** drop-down list, choose **Open Console**.

Step 5 On the **Access VM Console** screen, from the **Select VM** drop-down list, choose a VM.

Step 6 Click **Submit**.

A console of the selected VM opens in a new browser window.

Note For automatic configuration of a VNC console on a container, you must provide permission by checking the **Enable VNC Based Console Access** check box when you create the application container template.



CHAPTER 4

Managing Cisco Unified Fabric Automation Networks

This chapter contains the following sections:

- Modifying a Fabric Organization, page 54
- Deleting a Fabric Organization, page 54
- Viewing a Fabric Organization's Details, page 55
- Viewing a Fabric Summary, page 55
- Viewing Fabric General Settings (Fuji 2 Accounts Only), page 55
- Viewing Fabric Mobility Domains, page 56
- Fabric Domain Switch Mapping, page 56
- Deleting a Fabric Network, page 57
- Modifying a Fabric Network, page 57
- Viewing a Fabric Partition, page 59
- Modifying a Fabric Partition, page 60
- Deleting a Partition, page 61
- Deleting All Partitions, page 61
- Examining the Fabric SegmentID Range, page 62

Modifying a Fabric Organization

Step 1 Choose **Physical** > **Network**.
Step 2 In the left pane, click the **Multi-domain Manager** entry.
Step 3 Double-click the **DCNM Accounts** entry.
Step 4 Click **Fabric Organization**.
Step 5 Choose a Fabric.
Step 6 Click **Modify Organization**.
Step 7 On the **Modify Fabric Organization** screen, complete the following fields:

Name	Description
Organization Name field	The name of the organization.
Description field	The description of the organization.
Orchestration Source field	Source server for the orchestration engine. This field is not available for modification.
Group Name field	The group name. Once created, this field is not available for modification.

Step 8 Click **Save**.

Deleting a Fabric Organization

Step 1 Choose **Physical** > **Network**.
Step 2 In the left pane, click the **Multi-domain Manager** entry.
Step 3 Double-click the **DCMN Accounts** entry.
Step 4 Click **Fabric Organization**.
Step 5 Choose a Fabric.
Step 6 Click **Delete Organization**.
Step 7 Click **Delete** when prompted.

Viewing a Fabric Organization's Details

Step 1 Choose **Physical** > **Network**.
Step 2 In the left pane, click the **Multi-domain Manager** entry.
Step 3 Double-click the **DCNM Accounts** entry.
Step 4 Click **Fabric Organization**.
Step 5 Choose a Fabric.
Step 6 Click **View Details** to view the Fabric's details.

Viewing a Fabric Summary

SUMMARY STEPS

1. Choose **Physical** > **Network**.
2. In the left pane, click the **Multi-domain Manager** entry.
3. Double-click the **DCNM Accounts** entry to view the account details.

DETAILED STEPS

Step 1 Choose **Physical** > **Network**.
Step 2 In the left pane, click the **Multi-domain Manager** entry.
Step 3 Double-click the **DCNM Accounts** entry to view the account details.
By default, the **Summary** screen is selected and a summary of the selected DCNM account is displayed in the right pane.

Viewing Fabric General Settings (Fuji 2 Accounts Only)

SUMMARY STEPS

1. Choose **Physical** > **Network**.
2. In the left pane, click the **Multi-domain Manager** entry.
3. Double-click the **DCNM Accounts** entry to view the account details.
4. Click **Fabric General Setting** to view the general setting information for the fabric.

DETAILED STEPS

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Manager** entry.

Step 3 Double-click the **DCNM Accounts** entry to view the account details.
By default, the **Summary** screen is selected and a summary of the selected DCNM account is displayed in the right-hand pane.

Step 4 Click **Fabric General Setting** to view the general setting information for the fabric.

Viewing Fabric Mobility Domains

SUMMARY STEPS

1. Choose **Physical** > **Network**.
2. In the left pane, click the **Multi-domain Manager** entry.
3. Double-click the **DCNM Accounts** entry to view the account details.
4. Click **Fabric Mobility Domains** to view the fabric mobility domain information.

DETAILED STEPS

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Manager** entry.

Step 3 Double-click the **DCNM Accounts** entry to view the account details.
By default, the **Summary** screen is selected and a summary of the selected DCNM account is displayed in the right-hand pane.

Step 4 Click **Fabric Mobility Domains** to view the fabric mobility domain information.

Fabric Domain Switch Mapping

The first time a network is created with any mobility domain, the reference is kept, so that subsequently selecting the same switch with a different mobility domain is not allowed.

For example, the user has a default Mobility Domain as md0 and has created several networks. In UCSD, the rule is that one switch can be mapped with one mobility domain. So, if the N1K switch was selected while creating the network, then it is mapped with the md0 Mobility Domain.

If the user logs in to DCNM and updates the Default Mobility Domain to a different domain name, for example, Cluster_10, and then does an Inventory Collection, the UCSD is updated and the default Mobility Domain will show as Cluster_10 in the General Settings screen.

However, the original Mobility Domain and the associated Switch Mapping will not be updated since there are networks in UCSD. Attempting to associate the same switch with another mobility domain in UCSD is not allowed until the mapping between md0 and the initial N1K association is removed. if there are networks already created in UCSD, the association will not be removed.

The following are suggested workarounds:

- Remove the DCNM account and re-add it into UCSD. This will not remove any networks from DCNM
- Delete the network already created with md0 so UCSD will remove the association
- Delete the network in DCNM that has the older Mobility association and do Inventory Collection in UCSD

Deleting a Fabric Network

Step 1 Choose **Physical** > **Network**.
Step 2 In the left pane, click the **Multi-domain Manager** entry.
Step 3 Click the **DCNM Accounts** entry.
Step 4 Click **Fabric Network**.
Step 5 Choose a Fabric network entry.
Step 6 Click **Delete Network**.
Step 7 Click **Delete**.

Modifying a Fabric Network

Each Fabric network can have associated network pools.

Step 1 Choose **Physical** > **Network**.
Step 2 In the left pane, click the **Multi-domain Manager** entry.
Step 3 Click the **DCNM Accounts** entry.
Step 4 Click **Fabric Network**.
Step 5 Click a Fabric network entry.
Step 6 Click **Modify Network**.
Step 7 On the **Modify Fabric Network** screen, complete the following fields:

Name	Description
Network Name field	Name of the network.
Multicast Group Address field	

Name	Description
Network Role drop-down list	Currently selected role for Cisco DCNM.
Description field	Description of the network.
Gateway field	Network gateway address.
Subnet mask field	Network subnet address.
Profile Name drop-down list	Choose a profile name.
Profile Parameters section	
DHCP Server Address field	IP address of the DHCP server.
vrfDHCP field	
mtuValue field	Enter a value between 1500 and 9216.
dhcpServerv6Address field	
vrfv6Dhcp field	
Enable IPv6 check box	If checked, enables the use of IPv6 addresses.
Gateway IPv6 Address field	IPv6 address field used by the gateway. **Note** This field is visible only if the **Enable IPv6** check box is selected.
Prefix Length field	The length used by the IPv6 address. **Note** This field is visible only if the **Enable IPv6** check box is selected.
Network ID section	
Segment ID field	Displays Segment ID of network.
Mobility Domain ID field	Displays Mobility domain ID.
VLAN ID field	Displays Vlan ID number.
DHCP Scope section	
Enable DHCP check box	If checked, enables the use of a DHCP server.
IP Range field	Range of IP addresses for this network that the assigned DHCP server can lease.
Service Configuration Parameters	

Name	Description
Start IP field	Starting IP address of service.
End IP field	The range of static IP addresses that can be assigned to specific important service devices.
Secondary Gateway field	IP address of secondary gateway server (Cisco DCNM).

Step 8 Click **Save**.

Viewing a Fabric Partition

Viewing the details of a Fabric partition provide insight into the following partition elements:

- Account Name
- Network Name
- Network Description
- Profile Name
- Mobility Domain
- Segment ID
- VLAN
- Segment ID
- DVS IdD

Step 1 Choose **Physical** > **Network**.
Step 2 In the left pane, click the **Multi-domain Manager** entry.
Step 3 Double-click the **DCNM Accounts** entry.
Step 4 Click **Fabric Partition**.
Step 5 Choose a Fabric account to view.
Step 6 Click **View Details**.

Modifying a Fabric Partition

You can create multiple (Level 2 network) Cisco Unified Fabric Automation partitions. Each network can have associated network pools.

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Manager** entry.

Step 3 Double-click the **DCNM Accounts** entry.

Step 4 Click **Fabric Partition**.

Step 5 Choose a DCNM account to modify.

Step 6 Click **Modify Partition**.

Step 7 On the **Modify Fabric Partition** screen, complete the following fields:

Name	Description
Partition Name field	The name of the partition.
Description field	The description of the partition.
DCI ID field	
Extend the Partition across the Fabric check box	
Service Node IP Address field	IP address of service node.
DNS Server field	IP address of DNS server.
Secondary DNS Server field	IP address of the secondary DNS server.
Multicast Group Address field	
ProfileName Select button	Select a profile name from a pop-up list.
Profile Parameters	
Border LeafRt field	

Step 8 Click **Save**.

Deleting a Partition

To delete a SELECTED partition or partitions:

Step 1 Choose **Physical** > **Network**.
Step 2 In the left pane, click the **Multi-domain Manager** entry.
Step 3 Double-click the **DCNM Accounts** entry.
Step 4 Click **Fabric Partition**.
Step 5 Click the partition to be deleted. Use the <ctrl> click to select multiple partitions.
Step 6 Click **Delete Partition**.
Step 7 Click **Delete**.

Deleting All Partitions

To delete ALL partitions:

SUMMARY STEPS

1. Choose **Physical** > **Network**.
2. In the left pane, click the **Multi-domain Manager** entry.
3. Double-click the **DCNM Accounts** entry.
4. Click **Fabric Partition**.
5. Click **Delete All Partitions**.
6. Click **Delete**.

DETAILED STEPS

Step 1 Choose **Physical** > **Network**.
Step 2 In the left pane, click the **Multi-domain Manager** entry.
Step 3 Double-click the **DCNM Accounts** entry.
Step 4 Click **Fabric Partition**.
Step 5 Click **Delete All Partitions**.
Step 6 Click **Delete**.

Examining the Fabric SegmentID Range

Each network can have an associated segment ID range. Each network has an account ID. Cisco Unified Fabric Automation assigns a segment ID range to one Orchestrator. OpenStack can also talk to Cisco Data Center Network Manager (DCNM). When Cisco UCS Director Orchestrator creates a network, it uses the segments listed in these segment ID ranges.

Step 1 Choose **Physical** > **Network**.

Step 2 In the left pane, click the **Multi-domain Manager** entry.

Step 3 Double-click the **DCNM Accounts** entry.
Along with the double-click, you can select the arrow button, double-click on the DCNM Account created, and see the **Fabric SegmentID Range Management** screen.

Step 4 Click **Fabric SegmentID Range Management**. The Account Name, Orchestrator Name, and SegmentID Range are displayed.