The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.
Preface

This preface contains the following sections:

• Audience, page v
• Conventions, page v
• Related Documentation, page vii
• Documentation Feedback, page vii
• Obtaining Documentation and Submitting a Service Request, page vii

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and/or Cisco UCS Director Express 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

<table>
<thead>
<tr>
<th>Text Type</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI elements</td>
<td>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.</td>
</tr>
<tr>
<td>TUI elements</td>
<td>In a Text-based User Interface, text the system displays appears in this font.</td>
</tr>
<tr>
<td>Text Type</td>
<td>Indication</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System output</td>
<td>Terminal sessions and information that the system displays appear in <em>this font</em>.</td>
</tr>
<tr>
<td>CLI commands</td>
<td>CLI command keywords appear in <em>this font</em>. Variables in a CLI command appear in <em>this font</em>.</td>
</tr>
<tr>
<td>[]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Note**

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

**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.

**Caution**

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

**Timesaver**

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

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, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.
Subscribing to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Overview

This chapter contains the following sections:

- Prerequisites, page 1
- Cisco UCS Director and Cisco Dynamic Fabric Automation, page 1
- Terminology, page 3
- Cisco Dynamic Fabric Automation Overview, page 4
- Mapping Considerations, page 8
- Examining the Orchestration Flow, page 9

Prerequisites

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Director</td>
<td>Release 4.1 (with patches) or later full releases</td>
</tr>
<tr>
<td>Cisco Prime Data Center Network Manager (DCNM)</td>
<td>Release 7.0 or later releases</td>
</tr>
</tbody>
</table>

Cisco UCS Director and Cisco Dynamic 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 Dynamic Fabric Automation (DFA) is a multistage, switching network in which every connected device is reachable through the same number of hops. The Cisco DFA 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). The Cisco DFA 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 DFA 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 DFA organization. A DFA 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 DFA 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 Dynamic Fabric Automation (DFA).

Figure 1: Terms Used in a Cisco DFA 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 (DFA) optimizes data centers through integration. The Cisco DFA 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. This 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/or 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/or multitenancy environments.

Fabric Management

The fabric management network in Cisco Dynamic Fabric Automation (DFA) 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

<table>
<thead>
<tr>
<th>Function</th>
<th>Protocol</th>
</tr>
</thead>
</table>
| Power On Auto provisioning (POAP) for automatically configuring network devices | • Dynamic Host Configuration Protocol (DHCP)  
• Trivial File Transfer Protocol (TFTP)  
• Serial Control Protocol (SCP) |
| Fabric discovery | Simple Network Management Protocol (SNMP) |
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 Dynamic Fabric Automation (DFA). Cisco Prime Data Center Network Manager (DCNM) as an OVA can be deployed on a VMware vSphere infrastructure.

Cisco Prime DCNM provides the following functionality:

- 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.
- 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 DFA 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 Dynamic Fabric Automation (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 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

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

<table>
<thead>
<tr>
<th>Service</th>
<th>Network</th>
<th>Routing</th>
<th>Service Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Firewall</td>
<td>Host Network</td>
<td>N/A</td>
<td>defaultNetworkIpv4EfEdgeServiceProfile</td>
</tr>
<tr>
<td></td>
<td>Static</td>
<td></td>
<td>defaultNetworkIpv4TfEdgeServiceProfile</td>
</tr>
<tr>
<td></td>
<td>Dynamic</td>
<td></td>
<td>serviceNetworkIpv4TfDynamicRoutingProfile</td>
</tr>
<tr>
<td>Tenant External Service Network</td>
<td>Static</td>
<td></td>
<td>defaultExternalNetworkIpv4TfProfile</td>
</tr>
<tr>
<td></td>
<td>Dynamic</td>
<td></td>
<td>externalNetworkIpv4TfDynamicRoutingProfile</td>
</tr>
<tr>
<td>Service Node as Router/Default Gateway</td>
<td>Host Network</td>
<td>N/A</td>
<td>defaultNetworkL2Profile</td>
</tr>
</tbody>
</table>

For NSC Adapter installation information, see the Cisco DCNM 7.0 OVA Installation Guide.

Guidelines and Limitations for Cisco DFA

Cisco Dynamic Fabric Automation (DFA) 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 DFA 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 DFA 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 DFA must come through the Cisco NX-OS device management interface (mgmt0).

- The management port on any Cisco DFA switch must be connected to the same management subnet that includes the Cisco Prime DCNM user interface.

- Every Cisco DFA 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 DFA.

- 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 DFA 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 DFA fabric. So in that sense, we have limited a Cisco UCS Director group to be able to create/map to only one DFA. 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 DFA 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 DFA org/tenant/group selection
2. A DFA 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 DFA fabric (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 DFA fabric, DFA partition, and DFA 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)**

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a DFA, DFA partition, or DFA network.</td>
</tr>
<tr>
<td>2</td>
<td>Cisco UCS Director sends the new organization/partition/network information to the DCNM.</td>
</tr>
<tr>
<td>Process Step</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>3</td>
<td>The new tenant/vrf entry is added to DCNM.</td>
</tr>
<tr>
<td>4</td>
<td>A port group is created on the dvSwitch (however, if you are using a Cisco Nexus 1000V switch download the segment profile).</td>
</tr>
<tr>
<td>5</td>
<td>The port group is made available to the vCenter application.</td>
</tr>
<tr>
<td>6</td>
<td>Cisco UCS Director initiates the VM creation process on vCenter</td>
</tr>
<tr>
<td>7</td>
<td>Cisco UCS Director maps the VM nic to the Cisco DFA network.</td>
</tr>
<tr>
<td>8</td>
<td>The VM is powered on.</td>
</tr>
<tr>
<td>9</td>
<td>The leaf initiates Cisco DFA auto configuration process (based on the VDP or data information).</td>
</tr>
<tr>
<td>10</td>
<td>The Cisco DFA environment is completed (traffic begins to flow if using a dvSwitch).</td>
</tr>
</tbody>
</table>
CHAPTER 2

Configuration

This chapter contains the following sections:

• Getting Started, page 11
• Adding a Cloud Account, page 12
• Configuring a Cisco Nexus 1000V Switch, page 14
• Creating a New Multi-Domain Manager Account, page 15
• Creating a DFA Organization, page 16
• Associating vDCs, page 17
• Creating a DFA Partition, page 18
• Creating a DFA Network, page 18
• Examining DFA Network Segment Pools, page 20
• Examining A DFA Network's Segment Usage, page 20
• Adding a DFA Network to a DFA Partition, page 21
• Creating a DFA Network using vSwitches, page 23
• Creating a DFA Network using dvSwitches, page 25
• Attaching a Port Group to a VM, page 26
• Adding a Network Policy, page 27
• Choosing a DFA Port Selector, page 29
• About Multiple Disk VM Provisioning in a DFA Network, page 30
• Application Containers in a DFA Environment, page 31

Getting Started

To get started managing a Dynamic Fabric Automation Organization environment from within Cisco UCS Director, perform the following steps.
Before You Begin

**Step 1** Add the Dynamic Fabric Automation Organization account ([Administration > Physical Accounts > Multi-domain Managers > Add](#)).
Make sure you specify a valid range of segments IDs to be used by Cisco UCS Director. If you were to change or modify this information you need to delete the account and add it once again with the correct segment ID range.

**Step 2** Add a vCenter cloud account ([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** On the menu bar, choose [Physical > Network > Multi-domain Managers > DFA Accounts](#) and go to the DFA vDC Switch Association Policy tab. Enable vDC switches for a particular DFA organization account.
With the above steps completed you can now perform the basic administrative DFA 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 DFA organization orchestration tasks ([Physical Network Tasks > Cisco DFA 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** On the menu bar, choose [Administration > Virtual Accounts](#).
Step 2  Choose the Virtual Accounts tab.
Step 3  Click Add (+).
Step 4  From the Cloud Type drop-down list in the Add Cloud dialog box, choose a cloud type.
Step 5  In the Add Cloud dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Type drop-down list</td>
<td>Choose VMware. The following fields are displayed when VMware is chosen. Other cloud types display fields that are specific to that cloud type.</td>
</tr>
<tr>
<td>Cloud Name field</td>
<td>The cloud name. <em>Note</em> 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).</td>
</tr>
<tr>
<td>Server Address field</td>
<td>The vCenter server address.</td>
</tr>
<tr>
<td>Server User ID field</td>
<td>The vCenter server username.</td>
</tr>
<tr>
<td>Server Password field</td>
<td>The vCenter server password.</td>
</tr>
<tr>
<td>Server Access Port field</td>
<td>The server port number.</td>
</tr>
<tr>
<td>VMware Datacenter field</td>
<td>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.</td>
</tr>
<tr>
<td>Server Access URL</td>
<td>The URL for server access.</td>
</tr>
<tr>
<td>Description field</td>
<td>The description of the cloud.</td>
</tr>
<tr>
<td>Contact Email field</td>
<td>The contact email address for the cloud.</td>
</tr>
<tr>
<td>Location field</td>
<td>The location.</td>
</tr>
<tr>
<td>Pod drop-down list</td>
<td>Choose the converged infrastructure pod. By choosing a pod name, the VMware cloud account appears in the converged infrastructure stack.</td>
</tr>
<tr>
<td>Service Provider field</td>
<td>The service provider's name.</td>
</tr>
</tbody>
</table>

Step 6  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 DFA 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
On the menu bar, choose Administration > Physical Accounts.

Step 2
Choose the Managed Network Elements tab.

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

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

Step 4
Click Submit.
Creating a New Multi-Domain Manager Account

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the menu bar, choose Administration &gt; Physical Account.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Multi-Domain Managers tab.</td>
</tr>
<tr>
<td>3</td>
<td>Click (+) Add.</td>
</tr>
<tr>
<td>4</td>
<td>In the Multi-Domain Manager Account dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name field</td>
<td>The multi-domain account name.</td>
</tr>
<tr>
<td>Description field</td>
<td>The description of the multi-domain.</td>
</tr>
<tr>
<td>Account Type field</td>
<td>The account type. Choose DFA to create an account for use in Digital Fabric Automation networks. Choose PNSC to create a Cisco Prime Network Services Controller (PNSC) account.</td>
</tr>
<tr>
<td>Server Address field</td>
<td>The IP address of the DCNM server.</td>
</tr>
<tr>
<td>User ID field</td>
<td>The administrator's user ID.</td>
</tr>
<tr>
<td>Password field</td>
<td>The administrator's user password.</td>
</tr>
</tbody>
</table>
| 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.                                             |
| Port field                  | The port number (based upon the transport type).                                                                                                                                                            |
| 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.                                                                                                                                                      |
| Segment ID Pool field       | The selected segment ID pool.                                                                                                                                                                                |
Creating a DFA Organization

You can also use workflow tasks to create a DFA organization, DFA partition, or DFA network.

### Configuration

#### Step 1
On the menu bar, choose Physical > Network.

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

#### Step 3
Double-click the Dynamic Fabric Account entry.

#### Step 4
Click the Dynamic Fabric Organization tab.

#### Step 5
Click Create Organization.

#### Step 6
In the Add Dynamic Fabric Organization dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Account drop-down list</td>
<td>Choose a Cisco Prime Data Center Network Manager (DCNM) account.</td>
</tr>
<tr>
<td>Organization Name field</td>
<td>The name of the organization.</td>
</tr>
<tr>
<td>Description field</td>
<td>The description of the organization.</td>
</tr>
<tr>
<td>Orchestration Source field</td>
<td>The name of the Cisco UCS Director server (used to input the source field in DCNM when an organization is created).</td>
</tr>
<tr>
<td>Select Group drop-down list</td>
<td>Choose a user group.</td>
</tr>
</tbody>
</table>

  **Note**  A user group can have only one DFA organization.

#### Step 7
Click Add.
Associating vDCs

Before You Begin
Create a vDC, DFA account and a DFA switch.

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

Step 1
On the menu bar, choose Policies > Orchestration.

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

Step 3
On the left pane of the Workflows tab, choose the workflow folder and click the arrow next to the folder to show the workflows.

Step 4
Double-click the Create VDC DFA 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:

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

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

Step 8
Click Submit.

Step 9
Click the Execute Now button.

Step 10
Examine the Submit Workflow dialog box to confirm the proper inputs were selected.

Step 11
Click Submit.
Creating a DFA Partition

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

**Step 1**
On the menu bar, choose **Physical > Network**.

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

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

**Step 4**
Click the **DFA Partition** tab.

**Step 5**
Click **Create Partition**.

**Step 6**
In the **Create DFA Partition** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Partition Name</strong> field</td>
<td>The name of the partition.</td>
</tr>
<tr>
<td><strong>Description</strong> field</td>
<td>The description of the partition.</td>
</tr>
<tr>
<td><strong>Fabric Account</strong> field</td>
<td>Fabric account name.</td>
</tr>
<tr>
<td><strong>Service Node IP Address</strong> field</td>
<td>IP address of service node.</td>
</tr>
<tr>
<td><strong>DNS Server</strong> field</td>
<td>IP address of DNS server.</td>
</tr>
<tr>
<td><strong>Secondary DNS Server</strong> field</td>
<td>IP address of the secondary DNS server.</td>
</tr>
<tr>
<td><strong>Organization Name</strong> drop-down list</td>
<td>Choose an organization.</td>
</tr>
</tbody>
</table>

**Step 7**
Click **Add**.

Creating a DFA Network

Each DFA network can have associated network pools.

**Step 1**
On the menu bar, choose **Physical > Network**.

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

**Step 3**
Double-click the **Dynamic Fabric Account** entry.

**Step 4**
Click the **DFA Network** tab.

**Step 5**
Click **Create Network**.

**Step 6**
In the **Create DFA Network** dialog box, complete the following fields:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fabric Account</strong></td>
<td>The name of the partition.</td>
</tr>
<tr>
<td><strong>Organization Name</strong></td>
<td>The description of the partition.</td>
</tr>
<tr>
<td><strong>Partition Name</strong></td>
<td>Choose a partition from the drop-down list.</td>
</tr>
<tr>
<td><strong>Network Name</strong></td>
<td>Name of the new network.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Description of the network.</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td>Network gateway address.</td>
</tr>
<tr>
<td><strong>Subnet mask</strong></td>
<td>Network subnet address.</td>
</tr>
<tr>
<td><strong>Switch Type</strong></td>
<td>Choose the switch type.</td>
</tr>
<tr>
<td><strong>Select Switches</strong></td>
<td>Choose a switch to enable association.</td>
</tr>
<tr>
<td><strong>Profile Name</strong></td>
<td>Choose a profile name.</td>
</tr>
<tr>
<td><strong>Profile Parameters section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>DHCP Server Address</strong></td>
<td>IP address of the DHCP server.</td>
</tr>
<tr>
<td><strong>Enable IPv6</strong></td>
<td>If checked, enables the use of IPv6 addresses.</td>
</tr>
<tr>
<td><strong>Network ID section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Segment Id</strong></td>
<td>Segment Id of network. Not visible if the <strong>AutoSelect</strong> check box is selected.</td>
</tr>
<tr>
<td><strong>AutoSelect (20000-30000)</strong></td>
<td>If checked, allows for segment to be dynamically selected</td>
</tr>
<tr>
<td></td>
<td>(from within a 20000 - 30000 range). This value is the value chosen when the administrator added the DFA account to Cisco UCS Director</td>
</tr>
<tr>
<td><strong>DHCP Scope section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Enable DHCP</strong></td>
<td>If checked, enables the use of a DHCP server.</td>
</tr>
<tr>
<td><strong>IP Range</strong></td>
<td>Range of IP addresses for this network that the assigned DHCP server can lease.</td>
</tr>
<tr>
<td><strong>Service Configuration Parameters</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Start IP</strong></td>
<td>Starting IP address of service.</td>
</tr>
</tbody>
</table>
Examining DFA Network Segment Pools

Each network can have an associated network pool. Each network has an account ID. The Cisco DFA assigns a segment pool 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 pools.

Examining A DFA Network's Segment Usage

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End IP field</td>
<td>The range of static IP addresses that can be assigned to specific important service devices.</td>
</tr>
<tr>
<td>Network Role field</td>
<td>Currently selected role for Cisco DCNM.</td>
</tr>
<tr>
<td>Secondary Gateway IP Address field</td>
<td>IP address of secondary gateway server (Cisco DCNM).</td>
</tr>
</tbody>
</table>

Step 7  
Click Add.

Step 1  
On the menu bar, choose Physical > Network.

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

Step 3  
Double-click the Dynamic Fabric Account entry.

Step 4  
Click the Dynamic Fabric Segment Pool tab. The details of the segment pool are displayed.

Step 1  
On the menu bar, choose Physical > Network.

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

Step 3  
Double-click the Dynamic Fabric Account entry.

Step 4  
Click the Dynamic Fabric Network Segment Usage tab. The details of segment usage are displayed.
Adding a DFA Network to a DFA Partition

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.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the menu bar, choose Physical &gt; Network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the left pane, click the Multi-domain Manager entry.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Double-click the Dynamic Fabric Account entry.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the Dynamic Fabric Partition tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Double-click on a partition. The Dynamic Fabric Network tab appears.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Create Network.</td>
</tr>
<tr>
<td>Step 7</td>
<td>In the Create DFA Network dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name field</td>
<td>The network name.</td>
</tr>
<tr>
<td>Description field</td>
<td>The description of the network.</td>
</tr>
<tr>
<td>Gateway field</td>
<td>The name of the gateway server.</td>
</tr>
<tr>
<td>Subnet Mask field</td>
<td>The network's subnet mask.</td>
</tr>
<tr>
<td>Switch Type drop-down list</td>
<td>Choose a switch type (dvSwitch or vSwitch). Anyone accessing this switch has access to the Cisco DFA.</td>
</tr>
<tr>
<td>Select Switches button</td>
<td>Choose a switch. You can choose a vCenter at this stage. The inventory is automatically collected from the vCenter (as well as their related switches).</td>
</tr>
<tr>
<td>Profile Name drop-down list</td>
<td>Choose a profile.</td>
</tr>
</tbody>
</table>

Profile Parameters section

<table>
<thead>
<tr>
<th>DHCP Server Address field</th>
<th>IP address of the DHCP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IPv6 check box</td>
<td>If checked, enables the use of IPv6 addresses.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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. |
| Segment Id field            | Segment Id in use by server. This must be a unique value for each network. |
| AutoSelect (20000-30000) check box | If checked, allows for segment to be dynamically selected (from within a 20000 - 30000 range). |

**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). |

**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 DFA network allows you to create network segments dynamically, which makes them visible to the dvSwitches and Cisco Nexus 1000V switches.
Creating a DFA Network using vSwitches

Each DFA network can have associated network pools. Creating a DFA 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: On the menu bar, choose Physical > Network.
Step 2: In the left pane, click the Multi-domain Manager entry.
Step 3: Click the Dynamic Fabric Account entry.
Step 4: Choose the DCNM entry.
Step 5: Choose the DFA Network tab.
Step 6: Click Create Network.
Step 7: In the Create DFA Network dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition Name field</td>
<td>Choose a partition from the drop-down list.</td>
</tr>
<tr>
<td>Network Name field</td>
<td>Name of the new network.</td>
</tr>
<tr>
<td>Description field</td>
<td>Description of the network.</td>
</tr>
<tr>
<td>Gateway field</td>
<td>Network gateway address.</td>
</tr>
<tr>
<td>Subnet mask field</td>
<td>Network subnet address.</td>
</tr>
<tr>
<td>Switch Type drop-down list</td>
<td>Choose the vSwitches option from the drop-down list. When prompted, check the check box of a corresponding switch.</td>
</tr>
<tr>
<td>Select Switches drop-down list</td>
<td>Choose a switch.</td>
</tr>
<tr>
<td>Profile Name drop-down list</td>
<td>Choose a profile name.</td>
</tr>
<tr>
<td>Profile Parameters section</td>
<td></td>
</tr>
<tr>
<td>DHCP Server Address field</td>
<td>IP address of the DHCP server.</td>
</tr>
<tr>
<td>Enable IPv6 check box</td>
<td>If checked, enables the use of IPv6 addresses.</td>
</tr>
<tr>
<td>Gateway IPv6 Address field</td>
<td>Gateway IPv6 address for DHCP server. Only visible when the Enable IPv6 check box is checked.</td>
</tr>
<tr>
<td>Prefix Length field</td>
<td>Prefix used for IPv6 addresses. Only visible when the Enable IPv6 check box is checked.</td>
</tr>
<tr>
<td>Network ID section</td>
<td></td>
</tr>
</tbody>
</table>
### 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 a Vlan and mobility ID is required.

**Mobility Domain Id** check box | Visible only when configuring vSwitches. If checked, allows for segment to be dynamically selected (from within a 20000 - 30000 range).

**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 8** Click **Add**.
Creating a DFA Network using dvSwitches

Each DFA network can have associated network pools. Creating a DFA 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
On the menu bar, choose Physical > Network.

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

Step 3
Click the Dynamic Fabric Account entry.

Step 4
Choose the DCNM entry.

Step 5
Choose the DFA Network tab.

Step 6
Click Create Network.

Step 7
In the Create DFA Network dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition Name field</td>
<td>Choose a partition from the drop-down list.</td>
</tr>
<tr>
<td>Network Name field</td>
<td>Name of the new network.</td>
</tr>
<tr>
<td>Description field</td>
<td>Description of the network.</td>
</tr>
<tr>
<td>Gateway field</td>
<td>Network gateway address.</td>
</tr>
<tr>
<td>Subnet mask field</td>
<td>Network subnet address.</td>
</tr>
<tr>
<td>Switch Type drop-down list</td>
<td>Choose the dvSwitches option from the drop-down list. When prompted, check the check box of a corresponding switch.</td>
</tr>
<tr>
<td>Select Switches drop-down list</td>
<td>Choose a switch.</td>
</tr>
<tr>
<td>Profile Name drop-down list</td>
<td>Choose a profile name.</td>
</tr>
<tr>
<td>Profile Parameters section</td>
<td></td>
</tr>
<tr>
<td>DHCP Server Address field</td>
<td>IP address of the DHCP server.</td>
</tr>
<tr>
<td>Enable IPv6 check box</td>
<td>If checked, enables the use of IPv6 addresses.</td>
</tr>
<tr>
<td>Gateway IPv6 Address field</td>
<td>Gateway IPv6 address for DHCP server. Only visible when the Enable IPv6 check box is checked.</td>
</tr>
<tr>
<td>Prefix Length field</td>
<td>Prefix used for IPv6 addresses. Only visible when the Enable IPv6 check box is checked.</td>
</tr>
<tr>
<td>Network ID section</td>
<td></td>
</tr>
</tbody>
</table>
### 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 DFA network. Attaching a port group to a VM is the last step in the configuration process.

### Step 8

Click Add.

### Table: Configuration Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Segment Id field</strong></td>
<td>Segment Id of network. Not visible if the AutoSelect check box is selected. If checked, allows for segment to be dynamically selected (from within a 20000 - 30000 range).</td>
</tr>
<tr>
<td><strong>Mobility Domain Id check box</strong></td>
<td>If checked, selects the vCenter IP address. It can be either entered manually or Cisco UCS Director can enter a value (if auto select was also checked).</td>
</tr>
<tr>
<td><strong>DHCP Scope section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Enable DHCP check box</strong></td>
<td>If checked, enables the use of a DHCP server.</td>
</tr>
<tr>
<td><strong>IP Range field</strong></td>
<td>IP range in use for the DHCP server. Only available if the Enable DHCP check box is checked.</td>
</tr>
<tr>
<td><strong>Start IP field</strong></td>
<td>Starting IP address of service.</td>
</tr>
<tr>
<td><strong>End IP field</strong></td>
<td>The range of static IP addresses that can be assigned to specific important service devices.</td>
</tr>
<tr>
<td><strong>Secondary Gateway field</strong></td>
<td>Secondary network gateway address.</td>
</tr>
</tbody>
</table>
Before You Begin
Create a VM.

Step 1  On the menu bar, choose Virtual > Network.
Step 2  In the left-hand pane, choose a vCenter.
Step 3  Click the Port Groups tab.
Step 4  Choose a port group.
Step 5  Click Assign Group.
Step 6  In the Select Group dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name drop-down list</td>
<td>Choose a group.</td>
</tr>
<tr>
<td>Label field</td>
<td>The label associated to the group.</td>
</tr>
</tbody>
</table>

Step 7  Click Submit.

Adding a Network Policy

Step 1  On the menu bar, choose Policies > Virtual/Hypervisor Policies > Network.
Step 2  Choose the VMWare Network Policy tab.
Step 3  Click Add (+).
Step 4  In the Network Policy Information dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name field</td>
<td>The name of the network policy.</td>
</tr>
<tr>
<td>Policy Description field</td>
<td>The description of the network policy.</td>
</tr>
<tr>
<td>Cloud Name drop-down list</td>
<td>Choose the cloud account to which the policy applies.</td>
</tr>
<tr>
<td>Allow end user to select optional NICs check box</td>
<td>Check this check box if you want to provide vNICs selection during the creation of a service request-deployment configuration.</td>
</tr>
</tbody>
</table>

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

**Step 6**

In the **Add Entry to VM Networks** dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC Alias field</td>
<td>The name for the new NIC</td>
</tr>
<tr>
<td>Mandatory check box</td>
<td>If the Allow end user to select optional NICs check box in the Network Policy dialog box was selected, this check box is pre-selected. If the Network Policy dialog box was not selected, 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 field selected are used in VM provisioning and there will be no option of the user during VM service request creation.</td>
</tr>
<tr>
<td>Allow end user to choose portgroups check box</td>
<td>Check the check box to allow the end user to choose port groups during provisioning.</td>
</tr>
<tr>
<td>Copy Adapter from Template check box</td>
<td>Check the check box if you do not need custom settings. Uncheck for custom settings.</td>
</tr>
<tr>
<td>Adapter Type drop-down list</td>
<td>Choose the adapter type. Check 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.</td>
</tr>
</tbody>
</table>

**Step 7**

Click **Add (+)** in the **Port Groups** section. The **Add Entry to Port Groups** dialog box displays.

**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**, the **Add Entry** dialog box appears. Choose **IP Pool Policy** (default) or **Inline IP Pool**. If you choose IP Pool Policy, click **Select to choose a static IP pool**. In the **Select** dialog box, 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static IP Pool field</td>
<td>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</td>
</tr>
<tr>
<td>Subnet Mask field</td>
<td>The subnetwork mask for the pool. For example: 255.255.255.0</td>
</tr>
<tr>
<td>Gateway IP Address field</td>
<td>The IP address of the default gateway for this network.</td>
</tr>
</tbody>
</table>
Choosing a DFA Port Selector

Before You Begin

Create a vDC, DFA account and a DFA switch.

| Step 1 | On the menu bar, choose Policies > Orchestration. |
| Step 2 | In the Orchestration pane, click the Workflows tab. |
| Step 3 | On the left pane of the Workflows tab, choose the workflow folder and click the arrow next to the folder to show the workflows. |
| Step 4 | Double-click the DFA Port Group Selector task. |
| Note | This task will take DFA Port Group or any port group as input and provide the output as well. |
| Step 5 | In the Edit Task (DFA Port Group Selector) pane, complete the following fields: |

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name field</td>
<td>The name of the task.</td>
</tr>
<tr>
<td>Task Category drop-down list</td>
<td>The Cisco DFA Tasks category is chosen.</td>
</tr>
<tr>
<td>Task Type drop-down list</td>
<td>The DFA Port Group Selector type is chosen.</td>
</tr>
<tr>
<td>Comment field</td>
<td>Comments that pertain to this task.</td>
</tr>
<tr>
<td>Retry Execution check box</td>
<td>If checked, retries the workflow execution.</td>
</tr>
</tbody>
</table>

| Step 6 | Click Next. |
| Step 7 | In the User Input Mapping pane, complete the following fields: |

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Workflow User Inputs</td>
<td>The name of the task.</td>
</tr>
<tr>
<td>Port Group section</td>
<td></td>
</tr>
<tr>
<td>Map to User Input check box</td>
<td>If checked, maps port group to user input.</td>
</tr>
</tbody>
</table>
### About Multiple Disk VM Provisioning in a DFA 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 DFA 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 DFA 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 gateway policy (optional)
- Options for service end users

Note

For information regarding container templates and Virtual Secure Gateways (VSGs) see Creating an Application Template for a VSG.

Creating Application Container Policies (DFA environment)

Step 1
Choose Policies > Application Containers.

Step 2
Click the Virtual Infrastructure Policies tab.

Step 3
Click the Add Policy button.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name field</td>
<td>The name of the policy.</td>
</tr>
<tr>
<td>Policy Description</td>
<td>The description of the policy.</td>
</tr>
<tr>
<td>Container Type drop-down list</td>
<td>Choose DFA and click Next to confirm your selection and follow the wizard prompts.</td>
</tr>
</tbody>
</table>

Note
For Cisco Dynamic Fabric Automation environment, the creation of a gateway is optional.
Creating Application Container Policies (DFA environment)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Virtual Account drop-down list</td>
<td>The chosen virtual account (the cloud on which the gateway VM is created).</td>
</tr>
</tbody>
</table>

**Step 5**
Click Next.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Name field</td>
<td>Choose a fabric account.</td>
</tr>
<tr>
<td>Switch Type drop-down list</td>
<td>Choose a switch type.</td>
</tr>
<tr>
<td>Switch Name drop-down list</td>
<td>Choose a switch name.</td>
</tr>
<tr>
<td>Alternate Switch Name drop-down list</td>
<td>Choose an alternate switch.</td>
</tr>
</tbody>
</table>

**Step 7**
Click Next.

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

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

**Step 9**
Click Submit.
Creating Application Container Templates (DFA Environment)

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

**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 DFA Networks).

**Before You Begin**
Creating an application container policy.

---

**Step 1**
On the menu bar, choose **Policies > Application Containers**.

**Step 2**
Click the **Application Container Templates** tab.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>The name of the new template.</td>
</tr>
<tr>
<td>Template Description</td>
<td>The description of the template.</td>
</tr>
</tbody>
</table>

**Step 4**
Click **Next**.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Virtual Infrastructure Policy</td>
<td>Choose a policy (the policy created for use with your DFA environment).</td>
</tr>
</tbody>
</table>

**Step 6**
Click **Next**.

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name</td>
<td>Name of the new network.</td>
</tr>
</tbody>
</table>

---

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 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.
**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 dialog box appears. Complete the following fields:

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

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VM Network Interface Name</strong> field</td>
<td>The name of the VM network interface.</td>
</tr>
<tr>
<td><strong>Select the Network</strong> drop-down list</td>
<td>Choose a network.</td>
</tr>
<tr>
<td><strong>IP Address</strong> field</td>
<td>The IP address of the network.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol drop-down list</td>
<td>Choose a protocol.</td>
</tr>
<tr>
<td>Mapped Port drop-down list</td>
<td>Choose the mapped port for the selected protocol.</td>
</tr>
<tr>
<td>Remote IP Address field</td>
<td>The IP address of the internal system.</td>
</tr>
<tr>
<td>Remote Port field</td>
<td>The remote machine's port number.</td>
</tr>
</tbody>
</table>

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

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

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:
Choose a computer policy.

Choose a storage policy.

Choose a network policy.

Choose a systems policy.

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Self-Service Power Management of VMs</strong> checkbox</td>
<td>If checked, enables self-service power management of VMs.</td>
</tr>
<tr>
<td><strong>Enable Self-Service Resizing of VMs</strong> checkbox</td>
<td>If checked, enables self-service resizing of VMs.</td>
</tr>
<tr>
<td><strong>Enable Self-Service VM Snapshot Management</strong> checkbox</td>
<td>If checked, enables self-service VM snapshot management.</td>
</tr>
<tr>
<td><strong>Enable VNC Based Console Access</strong> checkbox</td>
<td>If checked, enables self-service VNC based console access.</td>
</tr>
<tr>
<td><strong>Enable Self-Service Deletion of Containers</strong> checkbox</td>
<td>If checked, enables self-deletion of containers.</td>
</tr>
<tr>
<td><strong>Technical Support Email Addresses</strong> field</td>
<td>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.</td>
</tr>
</tbody>
</table>

Step 21

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Container Setup Workflow</strong> drop-down list</td>
<td>Choose a workflow to establish the application container.</td>
</tr>
</tbody>
</table>

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

During the creation of an application container template, you must perform some manual steps. There are two scenarios that you might 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 checkbox 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 is required in a workflow associated to the container.
  2. Choose a specific workflow. This type of workflow depends on the gateway type, Linux or CISCO ASA, was associated with the container. For the Linux gateway, choose Application Container Setup workflow. For the 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 in the Workflow Designer page.
  4. In the workflow window, double click on 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.

Managing Application Containers

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

• Add VMs
• Open Console
• Clone Template
• Container Power Management
• Delete Containers
• View Reports
**Viewing the Management Action**

You can export reports of service requests for all groups or any particular group into a tabular format.

---

**Step 1**
On the menu bar, choose **Policies > Application Containers**.

**Step 2**
Click the **Tiered Applications** tab.

**Step 3**
Choose a container or right-click on the container to bring up all of the actions.

*Note*  
To view the container actions for a self-service user, you must give permission by enabling the **Enable Self-Service** checkbox (when creating the container template).

---

**Adding VMs**

---

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

**Step 2**
Click the **Tiered Applications** tab.

**Step 3**
Choose a container.

**Step 4**
Click **Add VMs**.

**Step 5**
In the **Manage VMs** dialog box, choose a VM.

**Step 6**
(Optional) Click **Submit**. The workflow is executed but the VM is not provisioned.

**Step 7**
Click the **Edit** icon. The **Edit Virtual Machines Entry** dialog box appears.

**Step 8**
Enter the number of VMs to create.

**Step 9**
Click **Submit**. The maximum quantity allowed is verified.

**Step 10**
Click **Submit** once again to finalize the process.

*Note*  
You can only add additional VMs to an existing application container. This condition is dependent upon the quantity specified in the **Maximum Quantity** field in the **Add Entry to Virtual Machines** field (when you created the application container template).
Accessing an Open Console

You can view the console on your VMs if you have the proper access rights.

Step 1
On the menu bar, choose Policies > Application Containers.

Step 2
Click the Tiered Applications tab.

Step 3
Choose a container.

Step 4
Click Open Console. The Access Console dialog box appears.

Step 5
Choose a VM.

Step 6
Click Submit. A page appears in your browser that provides you with access to the console of the selected VM.

Note
For automatic configuration of a VNC console on a container, you must provide permission by checking the Enable VNC Based Console Access checkbox while you created the application container template.
Managing DFA Networks

This chapter contains the following sections:

- Modifying a DFA Organization, page 41
- Deleting a DFA Organization, page 42
- Viewing a DFA Organization's Details, page 42
- Enabling a DFA Network, page 43
- Deleting a DFA Network, page 43
- Modifying a DFA Network, page 44
- Viewing a DFA Partition, page 45
- Modifying a DFA Partition, page 46
- Deleting a DFA Partition, page 47
- Examining DFA Network Segment Pools, page 47

Modifying a DFA Organization

Step 1
On the menu bar, choose Physical > Network.

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

Step 3
Double-click the Dynamic Fabric Account entry.

Step 4
Click the Dynamic Fabric Organization tab.

Step 5
Choose a DFA.

Step 6
Click Create Modify Organization.

Step 7
In the Modify Dynamic Fabric Organization dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Name field</td>
<td>The name of the organization.</td>
</tr>
</tbody>
</table>
Deleting a DFA Organization

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong> field</td>
<td>The description of the organization.</td>
</tr>
<tr>
<td><strong>Orchestration Source</strong> field</td>
<td>Source server for the orchestration engine. This field is not available for modification.</td>
</tr>
<tr>
<td><strong>Group Name</strong> field</td>
<td>The group name. Once created, this field is not available for modification.</td>
</tr>
</tbody>
</table>

**Step 8**  Click Save.

Viewing a DFA Organization's Details

**Step 1**  On the menu bar, choose Physical > Network.
**Step 2**  Click the Multi-domain Manager entry in the left-hand column.
**Step 3**  Double-click the Dynamic Fabric Account entry.
**Step 4**  Click the Dynamic Fabric Organization tab.
**Step 5**  Choose a DFA.
**Step 6**  Click View Details to view the DFA's details.
Enabling a DFA Network

Each DFA network can have associated network pools.

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the left pane, click the Multi-domain Manager entry.
Step 3 Click the Dynamic Fabric Account entry.
Step 4 Click the DFA Network tab.
Step 5 Click a DFA network entry.
Step 6 Click Enable Network.
Step 7 In the Enable Network Switch Association dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Type drop-down list</td>
<td>Choose the switch type.</td>
</tr>
<tr>
<td>Select Switches drop-down list</td>
<td>Choose a switch.</td>
</tr>
</tbody>
</table>

Step 8 Click Add.

Deleting a DFA Network

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the left pane, click the Multi-domain Manager entry.
Step 3 Click the Dynamic Fabric Account entry.
Step 4 Click the DFA Network tab.
Step 5 Click a DFA network entry.
Step 6 Click Delete Network.
Step 7 Click Delete.
Modifying a DFA Network

Each DFA network can have associated network pools.

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the left pane, click the Multi-domain Manager entry.
Step 3  Click the Dynamic Fabric Account entry.
Step 4  Click the DFA Network tab.
Step 5  Click a DFA network entry.
Step 6  Click Modify Network.
Step 7  In the Modify DFA Network dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name field</td>
<td>Name of the new network.</td>
</tr>
<tr>
<td>Network Role field</td>
<td>Currently selected role for Cisco DCNM.</td>
</tr>
<tr>
<td>Description field</td>
<td>Description of the network.</td>
</tr>
<tr>
<td>Gateway field</td>
<td>Network gateway address.</td>
</tr>
<tr>
<td>Subnet mask field</td>
<td>Network subnet address.</td>
</tr>
<tr>
<td>Switch Type drop-down list</td>
<td>Choose the switch type.</td>
</tr>
<tr>
<td>Profile Name drop-down list</td>
<td>Choose a profile name.</td>
</tr>
<tr>
<td>Profile Parameters section</td>
<td></td>
</tr>
<tr>
<td>DHCP Server Address field</td>
<td>IP address of the DHCP server.</td>
</tr>
<tr>
<td>Enable IPv6 check box</td>
<td>If checked, enables the use of IPv6 addresses.</td>
</tr>
<tr>
<td>Gateway IPv6 Address field</td>
<td>IPv6 address field used by the gateway.</td>
</tr>
<tr>
<td>Note</td>
<td>This field is visible only if the Enable IPv6 check box is selected.</td>
</tr>
<tr>
<td>Prefix Length field</td>
<td>The length used by the IPv6 address.</td>
</tr>
<tr>
<td>Note</td>
<td>This field is visible only if the Enable IPv6 check box is selected.</td>
</tr>
</tbody>
</table>

Network ID section

<p>| Segment Id field            | Segment Id of network. Not visible if the AutoSelect check box is selected. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Domain Id text field</td>
<td>Visible only when configuring vSwitches. If checked, allows for segment to be dynamically selected (from within a 20000 - 30000 range).</td>
</tr>
<tr>
<td>DHCP Scope section</td>
<td></td>
</tr>
<tr>
<td>Enable DHCP check box</td>
<td>If checked, enables the use of a DHCP server.</td>
</tr>
<tr>
<td>IP Range field</td>
<td>Range of IP addresses for this network that the assigned DHCP server can lease.</td>
</tr>
<tr>
<td>Service Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td>Start IP field</td>
<td>Starting IP address of service.</td>
</tr>
<tr>
<td>End IP field</td>
<td>The range of static IP addresses that can be assigned to specific important service devices.</td>
</tr>
<tr>
<td>Network Role field</td>
<td>Currently selected role for Cisco DCNM.</td>
</tr>
<tr>
<td>Secondary Gateway IP Address field</td>
<td>IP address of secondary gateway server (Cisco DCNM).</td>
</tr>
</tbody>
</table>

**Step 8**  
Click Save.

**Viewing a DFA Partition**

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

- Account Name
- Network Name
- Network Description
- Profile Name
- Mobility Domain
- Segment ID
- VLAN
- Segment ID
Modifying a DFA Partition

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the menu bar, choose <strong>Physical &gt; Network</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>In the left pane, click the <strong>Multi-domain Manager</strong> entry.</td>
</tr>
<tr>
<td>3</td>
<td>Double-click the <strong>DFA Accounts</strong> entry.</td>
</tr>
<tr>
<td>4</td>
<td>Click the <strong>DFA Partition</strong> tab.</td>
</tr>
<tr>
<td>5</td>
<td>Choose a DFA account to modify.</td>
</tr>
<tr>
<td>6</td>
<td>Click <strong>Modify Partition</strong>.</td>
</tr>
<tr>
<td>7</td>
<td>In the <strong>Modify DFA Partition</strong> dialog box, complete the following fields:</td>
</tr>
<tr>
<td></td>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Partition Name</strong> field</td>
<td>The name of the partition.</td>
</tr>
<tr>
<td><strong>Description</strong> field</td>
<td>The description of the partition.</td>
</tr>
<tr>
<td><strong>Fabric Account</strong> field</td>
<td>Fabric account name.</td>
</tr>
<tr>
<td><strong>Service Node IP Address</strong> field</td>
<td>IP address of service node.</td>
</tr>
<tr>
<td><strong>DNS Server</strong> field</td>
<td>IP address of DNS server.</td>
</tr>
<tr>
<td><strong>Secondary DNS Server</strong> field</td>
<td>IP address of the secondary DNS server.</td>
</tr>
<tr>
<td>8</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
Deleting a DFA Partition

Step 1  On the menu bar, choose Physical > Network.
Step 2  In the left pane, click the Multi-domain Manager entry.
Step 3  Double-click the Dynamic Fabric Account entry.
Step 4  Click the Dynamic Fabric Partition tab.
Step 5  Click Delete Partition.
Step 6  Click Delete.

Examining DFA Network Segment Pools

Each network can have an associated network pool. Each network has an account ID. The Cisco DFA assigns a segment pool 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 pools.

Step 1 On the menu bar, choose Physical > Network.
Step 2 In the left pane, click the Multi-domain Manager entry.
Step 3 Double-click the Dynamic Fabric Account entry.
Step 4 Click the Dynamic Fabric Segment Pool tab. The details of the segment pool are displayed.