Cisco UCS Director APIC Management Guide, Release 5.5

First Published: 2016-06-14

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

CONTENTS

Preface

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

New and Changed Information

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

Table 1: New Features and Changed Behavior in Cisco UCS Director, Release 5.5

Feature	What's New	Where Documented
Shared Layer 3 Outside (L3Out) support	Configure the shared L3Out support.	Configuring Shared Layer 3 Outside, on page 14
AVS VXLAN support	Cisco UCS Director offers AVS support in both VLAN and VXLAN mode.	Environment Variables, on page 17
AVS switch support	Choose DV switch or AV switch as the DV switch environment variable in the virtual network.	Environment Variables, on page 17
Custom environment variable support	Define an environment variable that can be used in the resource group and workflow.	Adding a Custom Environment Variable, on page 27
Resource group support for Hyper-V account	Choose a Hyper-V account and set the environment variable, capabilities, and capacities according to the chosen Hyper-V account.	Adding a Resource Group, on page 28
Support for multiple context Cisco ASA device	Add multiple context Cisco ASA device.	Adding a Resource Group, on page 28

Feature	What's New	Where Documented
Support for tag in data store	Add the data store tags with multiple tag values in the virtual storage service class level.	Adding a Service Offering, on page 41
Update private tenant	Update the vPOD information with multiple data stores and multiple data store clusters for a tenant using the Update Tenant vPOD with Existing Resources workflow.	Onboarding a Cisco UCS Director Tenant, on page 57
Overlapping IP address support	Enable the IP address overlapping for the tiers.	Example: VNX Tenant Onboarding , on page 61 Example: Flexpod ACI – Tenant Infrastructure Configuration, on page 67
Automatic data store selection in tenant onboarding	Choose data stores and data store clusters based on the generic VMware cluster.	Example: Tenant Onboarding with Private Network(s), on page 71

CHAPTER 2

Overview

This chapter contains the following sections:

Cisco UCS Director and Cisco Application Centric Infrastructure

Cisco UCS Director is a unified infrastructure management solution that provides management from a single interface 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 multitenancy, which enables policy-based and shared use of the infrastructure.

Cisco Application Centric Infrastructure (ACI) allows application requirements to define the network. This architecture simplifies, optimizes, and accelerates the entire application deployment cycle.

The combination of Cisco UCS Director and Cisco ACI enables automatic provisioning and delivery of application-centric infrastructure.

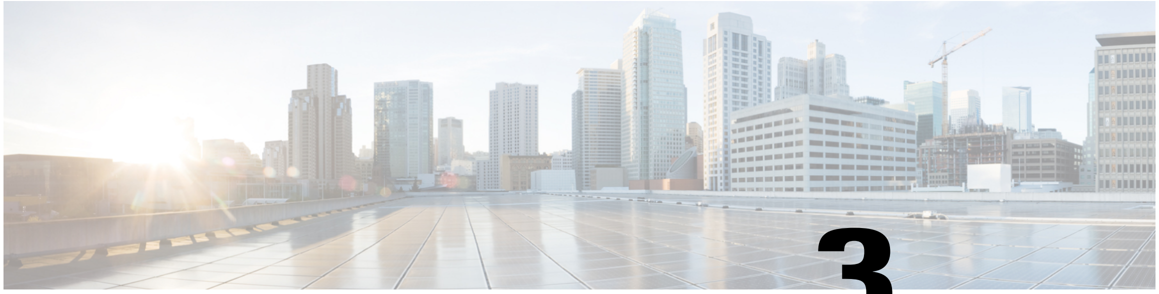
Note To use ACI 1.1(1*), ensure that TLSv1 is enabled in Cisco Application Policy Infrastructure Controller (APIC). In APIC, choose **Fabric > Fabric Resources > Pod Polices > Communication > Default** and enable **TLSv1**.

Cisco Application Policy Infrastructure Controller

The Cisco Application Policy Infrastructure Controller (APIC) is the unified point of automation, management, monitoring, and programmability for the Cisco Application Centric Infrastructure (ACI). The APIC supports the deployment, management, and monitoring of any application anywhere, with a unified operations model for physical and virtual components of the infrastructure. It is the central control engine for the broader cloud network. The APIC programmatically automates network provisioning and control-based on user-defined application requirements and policies.

The Cisco UCS Director orchestration feature allows you to automate APIC configuration and management tasks through operational workflows. A complete list of the APIC orchestration tasks is available in the

Workflow Designer, and in the Task Library. For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.



CHAPTER 3

Configuring APIC Accounts

This chapter contains the following sections:

Adding an APIC Account

Note Cisco APIC accounts are not tied to any specific pod.

Note You cannot edit a pod associated with an account that is part of a resource group. You cannot delete an account that is part of a resource group.

Note When you add an APIC cluster, the controllers in the cluster are automatically discovered. You can view the controller details in the **Summary** tab. To navigate to the **Summary** tab, choose **Physical** > **Network** and choose the APIC account from the **Multi-Domain Managers** list that appears in the left-hand pane.

Note To integrate Cisco UCS Director with ACI fabric, ensure that TLSv1 is enabled on ACI fabric (**Fabric Policies > Pod Policies > Policies - Communication**).

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

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

Step 3 Click **Add**.

Step 4 In the **Add Account** dialog box, choose **APIC** from the **Account Type** drop-down list.

Step 5 Click **Submit**.

Step 6 In the **Add Account** dialog box, complete the following fields:

Name	Description
Account Type field	The account type is displayed.
Account Name field	The multi-domain account name.
Description field	The description of the multi-domain.
Pod field	The list of available pods. Choose a pod to which you want to add the APIC account.
Server IP field	The IP address of one of the APIC controllers in the APIC cluster. **Note** Cisco UCS Director will automatically discover the IP address of other APIC controllers in the APIC cluster.
Use Credential Policy check box	Check this check box to use the policy to assign credentials to the account.
Credential Policy drop-down list	This field appears only when the **Use Credential Policy** check box is checked. Choose the credential policy. **Note** You cannot connect to the device using the SSH or Telnet protocol. If the SSH or Telnet protocol is specified in the selected device credential policy, you will be prompted to check the protocol defined in the credential policy.

Name	Description
Username field	This field appears only when the **Use Credential Policy** check box is unchecked. The name of the user who manages the APIC account. This account uses the username to access the APIC server. This username must be a valid administration account in the APIC server. **Note** For the LDAP credential, the format of the username must be apic:<LDAP Domain Name>\<LDAP User Name>. **Note** The user must have all the required privileges on the APIC server to access the supported features and perform actions such as view and access reports, and execute workflow tasks in Cisco UCS Director.
Password field	This field appears only when the **Use Credential Policy** check box is unchecked. This password is associated with the username.
Protocol drop-down list	This field appears only when the **Use Credential Policy** check box is unchecked. Choose the protocol as **https**.
Port field	This field appears only when the **Use Credential Policy** check box is unchecked. This port is used to access the APIC account.
Contact 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.

Cisco UCS Director tests the connection to the APIC server. If that test is successful, it adds the APIC account and discovers all infrastructure elements in the APIC server. This discovery process and inventory collection takes a few minutes to complete.

Viewing APIC Resources

After creating an APIC account in Cisco UCS Director, you can view related resources of the APIC account.

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

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

Step 3 Expand **APIC Accounts** and click the APIC account.
Cisco UCS Director displays the system overview and controller of the APIC account.

Step 4 Click one of the following tabs to view the details of a specific component in the server:

- **Summary** tab—Displays the system overview and summary of the APIC controller.
- **Fabric Nodes** tab—Displays the list of fabric nodes with their details such as the node name, model, vendor, role, serial, and node ID with the status.

  To view more details about fabric nodes, choose a fabric node and click **View Details**. The following tabs appear:

  - **Fabric Chassis—**Displays the fabric name, ID, model, vendor, serial, revision, and operation status of the fabric chassis.
  - **Fan Slots—**Displays the fabric name, slot ID, type, operation status, and inserted-card details of the fan slots.
  - **Physical Interfaces—**Displays the interface details that include the speed, mode, CFG access VLAN, CFG native VLAN, bundle index, operational duplex mode, operational port state, and reason for the current operation state. The operational state of the port can be one of the following: Unknown, Down, Link-up, and Up.
  - **Fabric Routed Vlan Interfaces—**Displays the status and reason for the current operation status of the fabric-routed VLAN interfaces.
  - **Fabric Encapsulated Routed Interfaces—**Displays a list of the fabric-encapsulated routed interfaces.
  - **Fabric Routed Loopback Interfaces—**Displays a list of the fabric-routed loopback interfaces.
  - **Fabric Management Interfaces—**Displays a list of the fabric management interfaces.
  - **Tunnel Interfaces—**Displays the interface, operation state, reason for the current operation state, tunnel layer, tunnel type, and type of the tunnel interface.

- **System** tab—Displays the system details that include the node name, in-band management IP address, out-of-band management IP address, infrastructure IP address, fabric MAC address, ID, role, and serial number.
- **Fabric Memberships** tab—Displays the fabric membership details that include the node name, serial number, node ID, model, role, IP address, decommissioned status, and supported model.
- **Physical Domains** tab—Displays the physical domains in the APIC server. Click **Add** to add a domain.
- **Tenants Health** tab—Displays the health score of tenants.

  To view more details about a tenant's health, choose a tenant and click **View Details**. The following tabs appear:

  - **EPGs Health—**Displays the health score of endpoint groups (EPGs).
  - **Application Health—**Displays the health score of applications.

- **Nodes Health** tab—Displays the health score of nodes.

  To view more details about the health of the nodes, choose a node and click **View Details**. The following tabs appear:

  - **Access Ports Health—**Displays the health score of access ports.
  - **Fabric Ports Health—**Displays the health score of fabric ports.
  - **Line Cards Health—**Displays the health score of line cards.

- **Access Entity Profile** tab—Displays the names and descriptions of the access entity profiles.

  To view more details about the access entity profile, choose an entity profile and click **View Details**. The following tabs appear:

  - **Policy Groups—**Displays the policy groups of an entity profile.
  - **Domain Associated To Interfaces—**Displays a list of domains that are associated with the interfaces.

- **Link Level Policy** tab—Displays the name, automatic negotiation, speed, link debounce interval, and description of the link level policy.

- **VLAN Pool** tab—Displays the VLAN pools that are added in the APIC server. Click **Add** to add a VLAN pool.

  To view more details about a VLAN pool, choose a VLAN pool and click **View Details**. The following tab appears:

  - **VLAN Pool Range—**Displays the VLAN pool name, mode of allocation, and the pool range. Click **Add** to add a VLAN range to the VLAN pool.

- **CDP Interface Policy** tab—Displays the name and description of the Cisco Discovery Prototol (CDP) interface policy, with the administration status.

- **LLDP Interface Policy** tab—Displays the name and description of the Link Layer Discovery Protocol (LLDP) interface policy, with the receive status and transmit status.

- **Leaf Policy Group** tab—Displays the name and description of the leaf policy group.

- **Tenant(s)** tab—Displays the tenants in the APIC server. Click **Add** to add a tenant.

  To view more details about a tenant, choose a tenant and click **View Details**. The following tabs appear:

  - **Summary—**Displays the overview of the tenant.
  - **Application Profile—**Displays the name, tenant, description, and QoS Class of the tenant application profile. Click **Add** to add a tenant application profile. Choose an application profile and click **View Details** to view the EPGs of the application profile.

    Choose an EPG and click **View Details** to view the provided contracts, consumed contracts, Layer 4 to Layer 7 EPG parameters, consumed contract interface, static node, domain, static path, and subnet of the EPG. In the **Consumed Contract Interface** tab, click **Add** to add a consumed contract interface to EPG.

  - **Deployed Service Graph—**Displays the list of service graphs that are deployed in the tenant. Choose a service graph and click **View Details** to view the Layer 4 to Layer 7 deployed service graph parameters.
  - **Filters—**Displays the tenant, name, and description of the filters. To view the tenant filter rules, choose a filter and click **View Details**.

- **External Bridge Network—**Displays the tenant, name, and description of the external bridge network. Choose a network and click **View Details** to view the following tabs:
    - **External Network—**Choose an external network and click **View Details** to view the provided contracts, and consumed contracts details.
    - **Node Profile—**Choose a node profile and click **View Details** to view the interface profile details.
- **External Routed Networks—**Displays the tenant, name, and description of the external routed network. Choose a network and click **View Details** to view the following tabs:
    - **Route Profile—**Choose a route profile and click **View Details** to view the context details.
    - **Logical Node Profile—**Choose a logical node profile and click **View Details**. The following tabs appear:
        - **Logical Nodes** tab**—**Displays the logical nodes. Click **Add** to add a logical node to the logical node profile of the external routed network. Choose a logical node and click **View Details** to view the static routes to the logical node.
        - **Logical Interface Profile** tab**—**Choose a logical interface profile and click **View Details** to view the logical interface and logical OSPF interface. Click **Add** in the Logical OSPF Interface tab to create an interface profile with the OSPF profile data.
        - **BGP Peer Connectivity** tab**—**Displays the BGP peer connectivity of the logical node profile. Click **Add** to add a peer connection to a node profile.
    - **External Network—**Choose an external network and click **View Details** to view the subnet, provided contracts, and consumed contracts details. You can tag an external network and consumed contract using the **Add Tags** option. The tag is used to identify the network and contract that you want to use in the application container deployment.
- **Bridge Domains—**Displays the tenant, name, description, segment ID, unicast traffic, ARP flooding, multicast IP address, customer MAC address, unicast route, and Layer 2 unknown unicast value.

  To view more details about a bridge domain, choose a bridge domain and click **View Details**. The following tabs appear:
    - **DHCP Relay Label—**Displays the tenant, name, description, and scope of the DHCP relay.
    - **Subnet—**Displays the tenant, bridge domain, description, subnet control, and gateway address of the tenant.
- **Private Networks—**Displays the tenant name, name, description, policy control, and segment of the private networks. Click **Add** to add a private network.
- **BGP Timers—**Displays the tenant, name, graceful restart control, hold interval, keepalive interval, and stale interval of the Border Gateway Protocol (BGP) timer.
- **Contracts—**Displays the tenant, name, description, type, QoS, and scope of the contracts.

  To view more details about a contract, choose a contract and click **View Details**. The following tabs appear:
    - **Contract Subject—**Choose a contract subject and click **View Details** to view the filter chain, filter chain for consumer to provider, filter chain for provider to consumer, provided label, and consumed label. Each tab has the **Add** option to add a filter, in term filter, out term filter, provided label, and consumed label to a contract subject.

- **Exported Tenants—**Displays the contracts of the exported tenants.

- **Taboo Contracts—**Displays the tenant, name, description, and scope of the taboo contracts.
- **Relay Policy—**Displays a list of the relay policies.
- **Option Policy—**Displays a list of the option policies.
- **End Point Retention—**Displays the tenant, name, description, hold interval, bounce trigger, bounce entry aging interval, local endpoint aging interval, remote endpoint aging interval, and move frequency of the tenant.
- **OSPF Interface—**Displays the tenant, name, description, network type, priority, cost of interface, interface controls, hello interval, dead interval, retransmit interval, and transmit delay of the Open Shortest Path First (OSPF) interface. Click **Create** to create an OSPF interface policy.
- **OSPF Timers—**Displays the OSPF timer details.
- **IGMP Snoop—**Displays the IGMP snoop details.
- **Custom QOS—**Displays the custom QoS details.
- **Action Rule Profile—**Displays the action rule profiles of the tenant. Click **Create** to create an action rule profile. In the **Create Action Rule Profile** dialog box, enter the name and description of the action rule profile. To set an action rule based on a route tag, check the **Set Rule Based On Route Tag** check box.
- **L4-L7 Service Graph—**Displays the Layer 4 to Layer 7 service graph details. Choose a service graph and click **View Details** to view the following tabs:
    - **Consumer EPG—**Displays the list of EPGs that are labeled as consumer in tenants. When an EPG consumes a contact, the endpoints in the consuming EPG may start communication with any endpoint in an EPG that is providing that contract.
    - **Provider EPG—**Displays the list of EPGs that are labeled as provider in tenants. When an EPG provides a contract, communication with that EPG can be initiated from other EPGs as long as the communication complies with the provided contract.
    - **Nodes—**Displays the list of nodes in the tenant. Choose a node and click **View Details** to view the node functions and connectors of the node. Choose a node function and click **View Details** to view the Layer 4 to Layer 7 function node parameters.
    - **Connections—**Displays the list of connections in the tenant. Choose a connection and click **View Details** to view the connection terminals in the tenant.

- **Function Profile Group——**Displays the function profile groups of tenants. Choose a function profile group and click **View Details** to view the function profiles of the group. Click **Add** to add a function profile. To view more details about a function profile, choose a function profile and click **View Details**. The following tabs appear:
    - **Function Profile Parameter—**Displays the function profile parameters. In the **Function Profile Parameter** tab, you can add an ACL, an interface, and add a bridge group interface to a function profile, and add a network object to a function profile. Choose a function profile parameter and click **View Details** to view the function profile parameter configuration and function profile parameter level-one folder.
    - **L4-L7 Function Profile Parameters—**Displays the list of Layer 4 to Layer 7 function profile parameters.

        - **Function Profile Function Parameter—**Displays the list of function profile function parameters. Click **View Details** to view the function profile function parameter Rel details.

    - **Device Clusters—**Displays the device cluster details. To view more details about a device cluster, choose a device cluster and click **View Details**. The following tabs appear:

        - **Device Cluster State—**Displays the cluster name, device state, and configured status of the device.

        - **Concrete Device—**Displays the list of concrete devices. Choose a concrete device and click **View Details** to view the virtual network interface card (vNIC) to concrete interface and the path to concrete interface.

        - **Logical Interface—**Displays the list of logical interfaces in the device cluster. Choose a logical interface and click **View Details** to view the logical interface details.

    - **Deployed Device Cluster—**Displays the device clusters that are deployed in the tenant.

    - **Logical Device Context—**Displays the logical device context details. Choose the logical device context and click **View Details** to view the logical interface context.

- **L3 Domain** tab—Displays a list of Layer 3 domains in the APIC accounts. To create a Layer 3 domain, click **Create**.

  In the **Create L3 Domain** dialog box, complete the following fields:

    - **L3 Domain** field—Name of the Layer 3 domain.

    - **Associated Attachable Entity Profile** field—Click **Select** and choose an attachable access entry profile that you want to associate with the Layer 3 domain.

    - **VLAN Pool** field—Click **Select** and choose a VLAN pool.

- **L2 Domain** tab—Displays a list of Layer 2 domains in the APIC accounts. To create a Layer 2 domain, click **Create**.

  In the **Create L2 Domain** dialog box, complete the following fields:

    - **L2 Domain** field—Name of the Layer 2 domain.

    - **Associated Attachable Entity Profile** field—Click **Select** and choose an attachable access entry profile that you want to associate with the Layer 2 domain.

    - **VLAN Pool** field—Click **Select** and choose a VLAN pool.

- **VM Networking** tab—Displays the virtual machine (VM) networks with the vendor detail.

  To view more details about a VM network, choose a VM and click **View Details**. The following tab appears:

    - **VMware Domains—**Displays a list of VMware domains with the vendor details. Choose a VMware domain and click **View Details** to view the VMware domain controllers, vCenter credential, and vCenter/vShield. Choose a VMware domain controller and click **View Details** to view the distributed virtual switch (DVS), hypervisors, and virtual machine. Choose a DVS and click **View Details** to view the DVS port groups.

- **L4-L7 Service Device Types** tab—Displays the Layer 4 to Layer 7 service device types with their model, vendor, version, and capabilities.

To view more details about the Layer 4 to Layer 7 service device type, choose a Layer 4 to Layer 7 service device type and click **View Details**. The following tabs appear:

  - **L4-L7 Service Device Properties—**Displays the vendor, package name, package version, and logging level of Layer 4 to Layer 7 service device types.
  - **L4-L7 Service Device Interface Labels—**Displays a list of interface labels.
  - **L4-L7 Service Functions—**Displays a list of service functions. Choose a service function and click **View Details** to view the details of the Layer 4 to Layer 7 service function connectors.

- **Fabric Nodes Topology** tab**—**Displays the topology details of fabric nodes.
- **L2 Neighbors** tab**—**Displays the Layer 2 neighbor details that include the protocol, fabric name, device ID, capability, port ID, local interface, hold time, and platform.
- **Deployed Service Graph** tab**—**Displays the tenant, contract, state, service graph, context name, node function, and description of the APIC account.
- **EPG to Contract Association** tab**—**Displays the details of the contract association with EPGs.
- **Access Port Policy Groups** tab**—**Displays the access port policy group name, link level policy, Cisco Discovery Protocol (CDP) policy, Link Aggregation Control Protocol (LACP) policy, Link Layer Discovery Protocol (LLDP) policy, link aggregation type, and attached entity profile of the accounts in the APIC server.
- **Fabric Interface Profiles** tab**—**Displays the fabric interface profiles of the APIC server.
- **Fabric Configured Switch Interfaces** tab**—**Displays the fabric configured switch interfaces of the APIC server.
- **Fabric Switch Profiles** tab**—**Displays the fabric switch profiles of the APIC server.

Assigning an APIC Account to a Pod

In the **Converged** menu of the user interface (UI), Cisco UCS Director displays the converged stack of devices for a data center. To display the APIC account in the converged UI, assign the APIC account to a pod.

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

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

Step 3 Expand **APIC Accounts** and click the APIC account.
Cisco UCS Director displays the system overview and controller of the APIC account.

Step 4 In the right pane, choose an APIC account that you want to assign to a pod.

Step 5 Click **Assign to Pod**.
The **Assign to Pod** dialog box appears.

Step 6 From the **Select Pod** drop-down list, choose a pod to which you want to assign the APIC account.

Step 7 Click **Submit**.

The APIC account appears in the converged UI.

Handling APIC Failover

APIC controllers are deployed in an APIC cluster. The recommendation is to have a minimum of three APIC controllers per cluster to ensure high availability. When you create an APIC account in Cisco UCS Director, provide the IP address of one of the APIC controllers in the APIC cluster. Cisco UCS Director discovers the other APIC controllers in the APIC cluster and their respective IP addresses.

If the IP address of the controller which was used to manage the APIC device goes down or is not reachable for 45 seconds, Cisco UCS Director tries to use any of the reachable controller IP addresses to interact with the APIC device.

If you have multiple ACI fabrics and each fabric with multiple controllers, one of the controllers of the ACI fabric is used to manage the APIC device. If the controller goes down or is not reachable for 45 seconds, Cisco UCS Director uses the next reachable controller within the ACI fabric.

Configuring Shared Layer 3 Outside

The shared Layer 3 outside (L3Out) feature offers the ability to use one L3Out to provide external network connectivity across numerous tenants.

To use the shared L3Out feature during the application container deployment, ensure that the following prerequisites are met during tenant onboarding and application profile creation.

1. Configure an L3Out in a common tenant. For example, in the tenant named as Common, configure an external network and contract that you want to use for external network connectivity.
2. Tag the external network in the Common tenant with a tag value (example, sample-tag). For more information, see the explanation of the Tenants > External Routed Network > External Network tab in Viewing APIC Resources, on page 8.

Note While tagging the external network, to get the required tag in the **Tag** drop-down list, you must map the APIC External Network as the taggable entity for the tag during the tag creation. To map the taggable entity, check the **Apic External Network** check box under the **Administration** category in the Applicability Rules screen of the **Create Tag** window.

3. Tag the contract in the external network with the same tag value (example, sample-tag) that is used for tagging the external network. For more information, see the explanation of the Tenants > External Routed Network > External Network tab in Viewing APIC Resources, on page 8.

Note While tagging the external network, to get the required tag in the **Tag** drop-down list, you must map the APIC Consumed Contracts to External Networks as the taggable entity for the tag during the tag creation. To map the taggable entity, check the **Apic Consumed Contracts To External Networks** check box under the **Administration** category in the Applicability Rules screen of the **Create Tag** window.

4 After onboarding a tenant, update the tagged external network and contract information in the tenant vPOD of the container using the Tenant Resource Allocation task.

If the IP address overlapping is enabled for the tiers during tenant onboarding, check the **Map to User Input** check box of the **Unique IP Subnet Pool Policy ID** identity in the Tenant Resource Allocation task to set the unique subnet pool. The network tier contacts the shared L3Out using an unique IP address chosen from the unique IP subnet pool. If the IP address overlapping is not enabled during tenant onboarding, the IP subnet pool is used to allocate the IP address to the network tiers.

5 During the application profile creation, choose the same tag for the external network and contract to use the L3Out configuration in the Common tenant. For more information on how to choose the tag for the external network and contract, see the Adding an Application Profile section in the Cisco UCS Director Application Container Guide.

6 Use the application profile in the application container provisioning.

Cisco UCS Director identifies the external network and contract based on the tag and uses those data for external network connectivity of tenants in the container.

CHAPTER 4

Managing Resource Groups

This chapter contains the following sections:

Resource Groups

You can use a resource group to select the appropriate resources for a tenant based on the requirements of an application. Additional concepts, such as a service offering, tenant profile, application profile, and resource group, are all required. Using these resource group concepts, you can onboard tenants and deploy applications based on a dynamic selection of resources. You can share resources in a resource group across tenants or you can dedicate them to a specific tenant.

A resource group is a pool of resources. Each group can contain physical infrastructure resources, virtual infrastructure resources, or a combination of physical and virtual infrastructure resources. Resource groups enable you to onboard tenants into Cisco UCS Director with minimum intervention.

As an infrastructure administrator or system administrator, you can add physical or virtual accounts to a resource group one at a time. Also, you can assign a pod to a resource group where all the accounts in the pod are added to the resource group. For more information about assigning a pod to a resource group, see Adding a Pod to a Resource Group, on page 37.

When an account is added to a resource group, the resource group by default announces all the capabilities and capacities for objects for that account as resource group entity capacities and capabilities. With Cisco UCS Director, you can selectively disable certain capacities or capabilities from the resource group.

Environment Variables

You can configure the environment variable for each resource. These environment variables are used during provisioning of the tenant onboarding and application deployment.

You can set the following default environment variables for both virtual and physical accounts. Also, you can add an environment variable in Cisco UCS Director and use the environment variable in the resource group. For more information on how to add an environment variable, see Adding a Custom Environment Variable, on page 27.

Note The listed environment variables are not required for every workflow. The subset of required environment variables depends on the use case and the specific workflow(s) being executed.

Virtual Compute Environment Variables

Environment Variable	Description	Sample Value
Container Parent Folder	The folder to which you want to add the newly created container.	*APIC*
IP Subnet Pool Policy	The APIC container uses an IP subnet pool policy that is defined in Cisco UCS Director. Each tier inside the container gets a unique subnet address from the IP subnet pool policy. This environment variable is used for container provisioning.	*IP-Pool*

Virtual Storage Environment Variables

No environment variables are required for virtual storage.

Virtual Network Environment Variables

Environment Variable	Description	Sample Value
VMM Domain for VMware	VMware vCenter is configured ACI-vCenter with the Virtual Machine Manager (VMM) domain. When VMware vCenter is associated with Cisco APIC, a distributed virtual switch (DVS) with the same name is created in VMware vCenter. This environment variable is used for tenant onboarding. Choose VMM domain with Cisco AV switch to support AVS in VXLAN mode. Cisco UCS Director offers AVS support in both VLAN and VXLAN mode. The VM gets the VLAN ID or VXLAN ID from the pool assigned to the VMM domain.	*ACI-Bldg4-1-vCenter*

Environment Variable	Description	Sample Value
DV Switch	Choose either DV switch or Cisco AV switch according to the requirement. The DV switch is available on the vCenter account and is used to connect the selected host during onboarding. The Cisco AV switch is used to support AVS in VXLAN mode. This environment variable is used for tenant onboarding.	*virt_switch*

Physical Compute Environment Variables

Environment Variable	Description	Sample Value
Physical Domain for UCS	The physical domain for Cisco UCS. This environment variable is used for baremetal provisioning.	*Phys*
VLAN Pool	The VLAN pool from which you want to assign a VLAN ID for the account.	*ACI3-Eng-VLAN-Pool*
iSCSI PXE Boot Service Profile Template	The template used for creating the host service profile on which you want to provision baremetal. This environment variable is used for baremetal provisioning on a NetApp storage system.	*DR_UCSM;org-root;org-root/ls-ACI-DR-Hosts*
Service Profile Template for Full Width Blade	The service profile template is used to create a service profile. When a service profile is created, the software identifies and selects free servers from the server pool that is associated with the service profile template. This environment variable is used for the VNX tenant onboarding.	*VNX_UCSM;org-root/ls-PSC-FullBlade-Template*

Environment Variable	Description	Sample Value
Service Profile Template for Half Width Blade	The service profile template is used to create a service profile. When a service profile is created, the software identifies and selects free servers from the server pool that is associated with the service profile template. This environment variable is used for the VNX tenant onboarding.	*VNX_UCSM;org-root/ls-PSC-HalfBlade-Template*
IQN Pool	The IQN pool that contains the iSCSI Qualified Names (IQNs) used as initiator identifiers by iSCSI vNICs in a Cisco UCS domain. The IQN pool is used to create a service profile iSCSI boot policy. This environment variable is used for baremetal provisioning on a NetApp storage system.	*IQN_Pool*
Boot Policy	Boot policy for the physical compute account. This environment variable is used for a VNX-type account.	*VNX_UCSM;org-root;org-root//boot-policy-SAN_NEW*
VLAN	VLAN for the physical compute account. This environment variable is used for a VNX-type account.	*VNX_UCSM;fabric/lan/net-MGT-ACI-POOL*

Physical Storage Environment Variables

Environment Variable	Description	Sample Value
Physical Domain for NetApp	The physical domain that is used to connect the NetApp account to the APIC. This environment variable is used for tenant onboarding.	topology/pod-1/paths-201/pathep-[eth1/36] • Pod-1—The pod ID of the APIC account. • Paths-201—The node ID of the leaf to which the NetApp controller is connected. • Pathep-[eth1/36]—The port on which the NetApp controller is connected.

Environment Variable	Description	Sample Value
NetApp Static Path	The static path defines the port on the APIC where the NetApp cluster node is connected. This environment variable is used to add the static path to the endpoint group (EPG) during tenant onboarding.	*topology/pod-1/node-302/sys /cdp/inst/if-[eth1/47]adj-1*
Vlan pool	The VLAN pool that is used to create the cluster vServer. This environment variable is used for tenant onboarding.	*Vlan_pool*
SP Port	The storage processor (SP) port for the physical storage account. This environment variable is used for VNX type account.	*VNX-POD;VNX_BLOCK;A-0;50:06:01:60:88:60:1B:6A: 50:06:01:60:08:60:1B:6A ,VNX-POD;VNX_BLOCK;A-1;50:06:01:60:88:60:1B:6A: 50:06:01:61:08:60:1B:6A*
Replication Storage Group	The replication storage group for the physical storage account. This environment variable is used for VNX type account.	
NFS Vlan Pool	This environment variable is used to define a VLAN pool. Individual VLANs are then assigned to a physical storage account dynamically from the pool.	*NetApp-vlan-pool*
SVM mgmt Vlan Pool	The VLAN pool for management of Storage Virtual Machine (SVM).	*NetApp-vlan-pool*
iSCSI_A VLAN Pool	The VLAN pool from which a VLAN is chosen as iSCSI_A VLAN.	*NetApp-vlan-pool*
iSCSI_B VLAN Pool	The VLAN pool from which a VLAN is chosen as iSCSI_B VLAN.	*NetApp-vlan-pool*
APIC vPC Static Path for Node 1	The static path of virtual port channel (vPC) for node 1.	*topology/pod-1/path-101/pathep-[PGr-FAS-A]*
APIC vPC Static Path for Node 2	The static path of virtual port channel (vPC) for node 2.	*topology/pod-1/path-101/pathep-[PGr-FAS-B]*
NFS IP Subnet Pool Policy	The subnet IP pool policy for NFS.	*ip_nfs_subnet_pool*

Environment Variable	Description	Sample Value
iSCSI_A IP Subnet Pool Policy	The IP subnet pool policy to be used for the first iSCSI VLAN.	*NetApp_ISCSI_A_Subnet_pool*
iSCSI_B IP Subnet Pool Policy	The IP subnet pool policy to be used for the second iSCSI VLAN.	*NetApp_ISCSI_B_Subnet_pool*
SVM mgmt IP Subnet Pool Policy	The subnet IP pool policy for SVM management.	*netapp_svm_subnet_pool*
VMNet IP Subnet Pool Policy	The subnet IP pool policy for VM network.	*VMNet_IP_Subnet_pool_policy*
APIC Vlan Pool for Node 1	The APIC VLAN pool from which the VLAN ID needs to be assigned for node 1.	*NetApp-Pool*
APIC Vlan Pool for Node 2	The APIC VLAN pool from which the VLAN ID needs to be assigned for node 2.	*NetApp-Pool*
Cluster Node 1 Identity	The identity of the first Netapp C-mode account node.	*ACI2-CMODE-01*
Cluster Node 2 Identity	The identity of the second Netapp C-mode account node.	*ACI2-CMODE-02*
Default Recovery Point	The recovery point attached to the VNX account.	*RP*
Recovery Point Cluster Identity	The identity of the recovery point attached to the VNX account.	*RP@1649417791*

Physical Network Environment Variables

Environment Variable	Description	Sample Value
IP Pool	The IP pool that is used to assign the IP addresses between the NetApp datastore and host vmkernel. This environment variable is used for tenant onboarding.	*IP_pool*
PXE Server IP Pool	The IP pool of the Preboot eXecution Environment (PXE) server. This environment variable is used for baremetal provisioning.	*pxe_ip_new11*

Environment Variable	Description	Sample Value
BMA EPG Entity	The Cisco UCS Director Baremetal Agent endpoint group (EPG) entity. This environment variable is used for baremetal provisioning.	*VNX_APIC185@common@BMA-AP@PSC_BMA*
Connected to FI A	When configuring the physical setup for FlexPod, VSAN is created for the Fabric Interconnect (FI) A - NXOS switch 1 connection and FI B - NXOS switch 2 connection. In BMA provisioning, zoning is configured for FI A - NXOS controller. Choose this environment variable to specify whether a Cisco Nexus switch is connected to Cisco UCS FI A. This environment variable appears for the MDS switch.	*Yes*
Physical domain for LB	The physical domain that you need to use for the load balancer service.	*Phy_LB_Domain*
Physical LB Path	The physical path of the load balancer service.	*topology/pod-1/node-101/sys/cdp /inst/if-[eth1/12]/adj-1*
DPC Static path 1	The static path of the first Direct Port Channel (DPC).	*topology/pod-1/paths-302/ pathep-[PC_Policy_1Gb]*
DPC Static path 2	The static path of the second DPC.	*topology/pod-1/paths-303/ pathep-[PC_Policy_1Gb]*
Path 1 to L3Out	The first transit path from the ACI leaf to an external router.	*topology/pod-1/protpaths-103-104/pathep-[ifs-n3k-b_PolGrp]*
Path 2 to L3Out	The second transit path from the ACI leaf to an external router.	*topology/pod-1/protpaths-103-104/pathep-[ifs-n3k-a_PolGrp]*
L2 Physical Domain	The physical domain for Layer 2. This environment variable is used for configuring EPG transit.	*L2-2960*
IP Subnet Pool Policy	The pool policy to be used to get the IP addresses for sub-interfaces.	*Ipsubnetpoolpolicy*

Environment Variable	Description	Sample Value
L3 Vlan Pool	The pool to be used to get the VLAN ID that is used to communicate between the external router and ACI fabric. This environment variable is used to configure the external routed network.	*L3out_Pool*
L2 Transit Vlan Pool	The pool to be used to get the VLAN ID for the transit EPG. This environment variable is used for creating a transit EPG.	*L2out_Pool*
Node	The leaf nodes of the APIC account. This environment variable is used for creating a transit EPG.	*topology/pod-1/node-302*
Routed Sub-Interface Path	The sub-interface routed path based on the leaf node selection.	*topology/pod-1/paths-303/pathep-[eth1/47], topology/pod-1/paths-303/pathep-[eth1/48], topology/pod-1/paths-302/pathep-[eth1/47] topology/pod-1/paths-302/pathep-[eth1/48]*
Nexus Switches	The Nexus switches for the APIC account.	*192.0.232.166, 192.0.232.167*
Loop Back IP Subnet Pool Policy	The pool policy to be used to get the IP address for Loop Back.	*loop_back_ip_pool_policy*
L3 Domain	The Layer 3 domain of the APIC account. This environment variable is used to configure the external routed network.	*Phy_L3out_domain*
Router IP Pool	The IP pool to configure router ID for routers on an external Layer 3 network. This environment variable is used to configure the external routed network.	*IP_pool*
LB Cluster IP Pool	The IP pool to provide the cluster management IP address for the load balancer device cluster.	*IP_pool*

Environment Variable	Description	Sample Value
SVI Path	The interface connecting APIC to a router on an external Layer 3 network. This environment variable is used to configure the external routed network.	*topology/pod-1/protpaths-101-102 /pathep-[vpcPG_ec1acifwi001-2_DATA*
SVI IP Pool	The subnet for configuring a switch virtual interface (SVI) on APIC leaves. This environment variable is used to configure the external routed network.	*IP_pool*

Note The following environment variable are not supported in Cisco UCS Director Release 5.4: IP Subnet Pool Policy, iSCSI PXE Boot Service Profile Template, IQN Pool, Replication Storage Group, PXE Server IP Pool, BMA EPG Entity, Physical domain for LB, and Physical LB Path.

The environment variable that need to be defined for VNX tenant onboarding are:

- Physical Compute—Cisco UCS Manager
    - Service Profile Template for Full Width Blade
    - Service Profile Template for Half Width Blade
- EMC VNX Unified
    - SP Port
- VMware Account
    - DV Switch-Virtual Network
    - VMM Domain for VMware-Virtual Network
- APIC (Physical Network)
    - DPC Static Path 1 (for L2 configuration)
    - DPC Static Path 2 (for L2 configuration)
    - L2 Physical Domain (for L2 configuration)
    - IP Subnet Pool Policy (for L3 configuration)
    - L3 VLAN Pool (for L3 configuration)
    - Routed Sub-Interface Path (for L3 configuration)
    - Node (for L3 configuration)
    - Nexus Switches (for L3 configuration)

  - Loop Back IP Subnet Pool Policy (for L3 configuration)

The environment variable that need to be defined for FlexPod tenant onboarding as per the Cisco UCS Director and FlexPod Cisco validated design (CVD) are:

- APIC Account
  - IP Pool
- NetApp
  - Vlan Pool
  - Physical Domain for NetApp
  - NFS Vlan Pool
  - SVM mgmt Vlan Pool
  - APIC vPC Static Path for Node 1
  - APIC vPC Static Path for Node 2
  - NFS IP Subnet Pool Policy
  - SVM mgmt IP Subnet Pool Policy
  - VMNet IP Subnet Pool Policy
  - APIC Vlan Pool for Node 1
  - APIC Vlan Pool for Node 2
  - Cluster Node 1 Identity
  - Cluster Node 2 Identity
  - iSCSI_A VLAN Pool
  - iSCSI_B VLAN Pool
  - iSCSI_A IP Subnet Pool Policy
  - iSCSI_B IP Subnet Pool Policy
- VMware Account
  - DV Switch
  - VMM Domain for VMware-Virtual Network

The environment variable that need to be defined for NetApp tenant onboarding (obsolete) are:

- APIC Account
  - IP Pool
- NetApp
  - Vlan Pool

- NetApp Static Path
- Physical Domain for NetApp

- Virtual Network
    - DV Switch
    - VMM Domain for VMware

Adding a Custom Environment Variable

You can define an environment variable that you want to use in the resource group and workflow. The type of the user-defined environment variable is custom.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Environment Variables** tab.
The environment variables that are available in Cisco UCS Director appear. The type of the preloaded environment variable is default. The type of the user-defined environment variable is custom. Choose anenvironment variable and click **View** to view the name, variable type, and identity type of the environment variable. Click **Delete** to delete the environment variable. You can delete only the user-defined environment variable that is categorized as custom.

Step 3 Click **Add**.

Step 4 In the **Resource Group Environment Variable** dialog box, complete the following fields:

Name	Description
Custom Environment Name field	The name of the environment variable.
Description field	The description of the environment variable.
Resource Type drop-down list	Choose one of the following as the resource type for the environment variable: • VIRTUAL_COMPUTE • VIRTUAL_NETWORK • VIRTUAL_STORAGE • PHYSICAL_COMPUTE • PHYSICAL_STORAGE • PHYSICAL_NETWORK The environment variable is categorized under the chosen resource type.
Input Type drop-down list	Click **Select** and choose the variable type for the environment variable. The variable type can be text, list of variable (LoV), multiple selection, table, and popup table.

Step 5 Click **Submit**.
The added custom environment variable gets listed in the **Environment Variables** tab. You can add this custom environment variable in the Resource Group.

Adding a Resource Group

Before You Begin

Ensure that the IP subnet pool policy and VLAN pool policy are defined to use the policy in the environment. Also, you can add a policy in the **Add Entry to Environment Variables** dialog box when adding a resource group.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Resource Groups** tab.
The resource groups that are available in Cisco UCS Director appear.

- Choose a resource group and click **View** to view the name and description of the resource group.
- View the resources that are associated with a resource group by choosing a resource group and clicking **View Details**. The ID, pod, account name, category, account type, resource type, and resource name of the resources in the resource group are displayed.
- View the capacities and capabilities of a resource by choosing a resource and clicking **View Details**.

Step 3 Click **Add**.

Step 4 In the **Create Resource Group** dialog box, complete the following fields:

Name	Description
Name field	The name of the resource group.
Description field	The description of the resource group.
Enable DR check box	Check this check box to enable the disaster recovery service support for the resource group. **Note** The disaster recovery service support is enabled based on the use case and the workflow being executed.
Accounts Priority drop-down list	This field appears only when the **Enable DR** check box is checked. By default, **Primary** is selected to set the resource group as primary. If you want to set the resource group as secondary, choose **Secondary**.

Name	Description
DRS Resource Group drop-down list	Choose a resource group as a disaster recovery service resource group for handling failover and recovering data during disaster.

Note The primary and secondary resource groups must each have an equal number of accounts in order to support the disaster recovery service.

Step 5 Click **Next**.

Step 6 (Optional) In the **Virtual Compute** screen, choose the virtual compute account and the interested capabilities and capacities:

a) Click the + icon to add a virtual account.

b) In the **Add Entry to Virtual Accounts** dialog box, choose the virtual account.

Note You can choose either a VMware account or a Hyper-V account from the account list. According to the chosen virtual account, you need to choose environment variable, capabilities, and capacities. If the required environment variable is not available in the drop-down list, you can create a new environment variable. For more information on how to create an environment variable, see Adding a Custom Environment Variable, on page 27.

The **Add Entry** dialog box appears.

c) In the **Environment Variables** table, click the + icon.

1. In the **Add Entry to Environment Variables** dialog box, from the **Name** drop-down list, choose an environment variable.
2. In the **Required Value** field, choose the value according to the selected environment variable. When you choose **IP Subnet Pool Policy** from the **Name** drop-down list, click **Select** and choose a policy. You can also add a policy by clicking the + icon.
3. Click **Submit**.

d) In the **Selected Capabilities** table, the capabilities of the chosen virtual account appear by default.
You can opt to disable the capabilities by unchecking the capability in the edit window that appears on clicking the Edit icon. You can remove the capability from the list by clicking the Delete icon.

e) In the **Selected Capacities** table, the capacities of the chosen virtual account appear by default.
You can opt to disable the capacities by unchecking the capacity in the edit window that appears on clicking the Edit icon. You can remove the capacity from the list by clicking the Delete icon.

f) Click **Submit** in the **Add Entry** dialog box.

Note An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 7 Click **Next**.

Step 8 In the **Virtual Storage** screen, choose the virtual compute account and the interested capabilities and capacities.

a) Click the + icon to add a virtual account.

b) In the **Add Entry to Virtual Accounts** dialog box, choose the virtual account.

Note You can choose either a VMware account or a Hyper-V account from the account list. According to the chosen virtual account, you need to choose environment variable, capabilities, and capacities. If the required environment variable is not available in the drop-down list, you can create a new environment variable. For more information on how to create an environment variable, see Adding a Custom Environment Variable, on page 27.

The **Add Entry** dialog box appears.

c) In the **Environment Variables** table, click the + icon.

1. In the **Add Entry to Environment Variables** dialog box, from the **Name** drop-down list, choose an environment variable.
2. In the **Required Value** field, choose the value according to the selected environment variable.
3. Click **Submit**.

d) In the **Selected Capabilities** table, the capabilities of the chosen virtual account appear by default.
You can opt to disable the capabilities by unchecking the capability in the edit window that appears on clicking the Edit icon. You can remove the capability from the list by clicking the Delete icon.

e) In the **Selected Capacities** table, the capacities of the chosen virtual account appear by default.
You can opt to disable the capacities by unchecking the capacity in the edit window that appears on clicking the Edit icon. You can remove the capacity from the list by clicking the Delete icon.

f) Click **Submit** in the **Add Entry** dialog box.

Note An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 9 Click **Next**.

Step 10 In the **Virtual Network** screen, choose the virtual network account and the interested capabilities and capacities:

a) Click the + icon to add a virtual account.

b) In the **Add Entry to Virtual Accounts** dialog box, choose the virtual account.

Note You can choose either a VMware account or a Hyper-V account from the account list. According to the chosen virtual account, you need to choose environment variable, capabilities, and capacities. If the required environment variable is not available in the drop-down list, you can create a new environment variable. For more information on how to create an environment variable, see Adding a Custom Environment Variable, on page 27.

The **Add Entry** dialog box appears.

c) In the **Environment Variables** table, click the + icon.

1. In the **Add Entry to Environment Variables** dialog box, from the **Name** drop-down list, choose an environment variable.
2. In the **Required Value** field, click **Select** and choose a value according to the selected environment variable that you want to use in the environment.
3. Click **Submit**.

d) In the **Selected Capabilities** table, the capabilities of the chosen virtual account appear by default.
You can opt to disable the capabilities by unchecking the capability in the edit window that appears on clicking the Edit icon. You can remove the capability from the list by clicking the Delete icon.

e) In the **Selected Capacities** table, the capacities of the chosen virtual account appear by default.

You can opt to disable the capacities by unchecking the capacity in the edit window that appears on clicking the Edit icon. You can remove the capacity from the list by clicking the Delete icon.

f) Click **Submit** in the **Add Entry** dialog box.

Note An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 11 Click **Next**.

Step 12 (Optional) In the **Physical Compute** screen, choose the physical compute account and the interested capabilities and capacities:

a) Click the + icon to add a compute account.

b) In the **Add Entry to Compute Accounts** dialog box, choose the compute account.
The **Add Entry** dialog box appears.

c) In the **Environment Variables** table, click the + icon.

1 In the **Add Entry to Environment Variables** dialog box, from the **Name** drop-down list, choose an environment variable.

2 In the **Required Value** field, click **Select** and choose a value according to the selected environment variable. When you choose **Vlan pool** from the **Name** drop-down list, click **Select** to choose a policy. You can also add a policy by clicking the + icon.

3 Click **Submit**.

d) In the **Selected Capabilities** table, click the + icon to choose a resource and resource capability. Click **Submit**.

e) In the **Selected Capacities** table, click the + icon to choose a resource and resource capacities. Click **Submit**.

f) Click **Submit** in the **Add Entry** dialog box.

Note An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 13 Click **Next**.

Step 14 (Optional) In the **Physical Storage** screen, choose the physical storage account and the interested capabilities and capacities:

a) Click the + icon to add a storage account.

b) In the **Add Entry to Storage Accounts** dialog box, choose the storage account.
The **Add Entry** dialog box appears.

c) In the **Environment Variables** table, click the + icon.

1 In the **Add Entry to Environment Variables** dialog box, from the **Name** drop-down list, choose an environment variable.

2 In the **Required Value** field, click **Select** and choose a value according to the selected environment variable. When you choose **Vlan pool** from the **Name** drop-down list, click **Select** to choose a policy. You can also add a policy by clicking the + icon.

3 Click **Submit**.

The IP address and subnet mask of the storage device must be within the IP address range specified based on the policy.

d) In the **Selected Capabilities** table, click the + icon to choose a resource and resource capability. Click **Submit**.

e) In the **Selected Capacities** table, click the + icon to choose a resource and resource capacities. Click **Submit**.

f) Click **Submit** in the **Add Entry** dialog box.

Note An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 15 Click **Next**.

Step 16 (Optional) In the **Physical Network** screen, choose the physical network account and the interested capabilities and capacities:

a) Click the + icon to add a network account.

b) In the **Add Entry to Network Accounts** dialog box, choose the storage account.
The **Add Entry** dialog box appears.

c) In the **Environment Variables** table, click the + icon.

1 In the **Add Entry to Environment Variables** dialog box, from the **Name** drop-down list, choose an environment variable.

2 In the **Required Value** field, click **Select** and choose a value according to the selected environment variable. When you choose **IP Pool** from the **Name** drop-down list, click **Select** and choose an IP pool policy.

3 Click **Submit**.

d) In the **Selected Capabilities** table, click the + icon.

1 In the **Add Entry to Selected Capabilities** dialog box, from the **Select Resource** drop-down list, choose **FC Capability on MDS** or **Zone Support**.

2 In the **Resource Capability** field, choose a value from the list of values that are displayed according to the selected resource.

3 Click **Submit**.

e) In the **Selected Capacities** table, click the + icon to choose a resource and resource capacities. Click **Submit**.

f) Click **Submit** in the **Add Entry** dialog box.

Note An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 17 Click **Next**.

Step 18 In the **L4L7 Devices** screen, choose the firewall specification and load balancer specification:

a) In the **Firewall Specification** table, click the + icon.
In the **Add Entry** dialog box, complete the following fields:

Name	Description
Firewall Type drop-down list	Choose **VIRTUAL** or **PHYSICAL** as the firewall type.
The following fields appear when you choose **VIRTUAL** as the firewall type:	
Virtual Accounts field	Click **Select** and choose a virtual account.
VM Deployment Policy field	Choose a VM deployment policy. Click the + icon to add a VM deployment policy. For more information about how to add a VM deployment policy, see the Adding an ASAv VM Deployment Policy section in the Cisco UCS Director Application Container Guide.

Name	Description
Firewall Management Port Group field	Click **Select** and choose a port group of vCenter. The management interface will be placed in the chosen port group during ASAv deployment.
Management IP Pool field	Click **Select** and choose an IP pool that you want to use for assigning management IP address.
Regular HA IP Pool field	Click **Select** and choose an IP pool (private IP range) to allocate IP address from the pool. This pool is used as failover link between primary and secondary ASA devices. This pool is used when the firewall HA is enabled in the Layer 4 through Layer 7 service policy.
Stateful HA IP Pool field	Click **Select** and choose an IP pool (private IP range) to allocate IP address from the pool. This pool is used as state link between primary and secondary Cisco ASA devices. This pool is used when the stateful failover is enabled in the Layer 4 through Layer 7 service policy. The stateful HA IP pool and regular HA IP pool must be in different subnets to avoid network IP conflict.
The following fields appear when you choose **PHYSICAL** as the firewall type.	
Apic Accounts field	Click **Select** and choose an APIC account.
Multi Context Enabled check box	Check the **Multi Context Enabled** check box if the multiple context configuration is enabled on the Cisco ASA device.
Firewall Cluster IP field	This field appears only when the **Multi Context Enabled** check box is checked. The IP address of the physical Cisco ASA device. This IP address is configured as the Admin Context IP address.
Cluster Username field	This field appears only when the **Multi Context Enabled** check box is checked. The username of the cluster that is used by APIC to access ASA.
Cluster Password field	This field appears only when the **Multi Context Enabled** check box is checked. The password of the cluster that is used by APIC to access ASA.
Firewall/Context IP field	The IP address that is used to reach the firewall device. If the **Multi Context Enabled** check box is checked, this field collects the User Context IP address of the virtual ASA device that is configured on Day 0.
Port field	The port number of the firewall device.

Name	Description
Username field	The username that is used to access the firewall device. If the **Multi Context Enabled** check box is checked, this field collects the username of the user context.
Password field	The password that is used to access the firewall device. If the **Multi Context Enabled** check box is checked, this field collects the password of the user context.
Physical Domain field	Click **Select** and choose a physical domain from the list. Click the + icon to add a physical domain.
Static Path field	Click **Select** and choose a static path from the table. Cisco UCS Director displays the path types, such as VPC and leaf, in the table.
Port Channel Name field	The port channel interface of the Cisco ASA device which is connected to leaf (for example, Po1, Port-channel1).
Channel Group Id field	This field appears only when the **Multi Context Enabled** check box is unchecked. The unique ID of the channel group.
Port Channel Member Interfaces field	This field appears only when the **Multi Context Enabled** check box is unchecked. The interface name(s) of the port channel member. **Note** Enter the interface name without space. If there are more than one interfaces, enter the interface names separated by comma.

b) Click **Submit**.

Note If the multiple context is enabled on the Cisco ASA device, repeat the Step 18 a to add the details for each context.

c) In the **Load Balancer Specification** table, click the + icon.

In the **Add Entry to Load Balancer Specification** dialog box, complete the following fields:

Name	Description
Load Balancer Type drop-down list	Choose **Virtual** or **Physical** as the load balancer type.
Virtual Accounts field	This field appears when you choose the load balancer type as **Virtual**. Click **Select** and choose a virtual account.
Apic Accounts field	This field appears when you choose the load balancer type as **Physical**. Click **Select** and choose an APIC account.

Name	Description
Load Balancer IP field	The IP address that is used to reach the NetScalar device.
Port field	The port number of the NetScalar device.
Load Balancer Gateway field	The gateway IP address of the NetScalar device.
Username field	The username that is used to access the NetScalar device.
Password field	The password that is used to access the NetScalar device.
Function Profile field	Optional. Click **Select** and choose a function profile from the list.
VMs field	This field appears when you choose the load balancer type as **Virtual**. Click **Select** and choose a VM from the list.
Physical Domain field	This field appears when you choose the load balancer type as **Physical**. Click **Select** and choose a physical domain from the list. Click the + icon to add a physical domain.
Interface field	This field appears when you choose the load balancer type as **Physical**. The interface that is used for the device cluster configuration (for example, LA_1).
Static Path field	This field appears when you choose the load balancer type as **Physical**. Click **Select** and choose a static path.

d) Click **Submit**.

Step 19 Click **Submit**.

Editing a Resource Group

When editing a resource group, you can add accounts to the resource group, edit the accounts that are added to the resource group, and delete accounts from the resource group.

You can delete an account from a resource group only when the account is not associated with other resource group objects, such as a tenant profile.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Resource Groups** tab.

Step 3 Select a resource group from the table.

Step 4 Click **Edit**.

Step 5 In the **Edit Resource Group** dialog box, complete the following fields for the resource group:

Name	Description
Name field	The name of the resource group.
Description field	The description of the resource group.
Enable DR check box	Check this check box to enable the disaster recovery service support for the resource group. **Note** The disaster recovery service support is enabled based on the use case and the workflow being executed.
Accounts Priority drop-down list	This field appears only when the **Enable DR** check box is checked. By default, **Primary** is selected to set the resource group as primary. If you want to set the resource group as secondary, choose **Secondary**.
DRS Resource Group drop-down list	Choose a resource group as a disaster recovery service resource group for handling failover and recovering data during disaster.

Step 6 Click **Next**.

Step 7 (Optional) The **Virtual Compute** screen displays the virtual compute accounts added to the resource group. Choose an account and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 8 Click **Next**.

Step 9 The **Virtual Storage** screen displays the virtual storage accounts added to the resource group. Choose an account and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 10 Click **Next**.

Step 11 The **Virtual Network** screen displays the virtual network accounts added to the resource group. Choose an account and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 12 Click **Next**.

Step 13 The **Physical Compute** screen displays the physical compute accounts added to the resource group. Choose an account and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 14 Click **Next**.

Step 15 The **Physical Storage** screen displays the physical storage accounts added to the resource group. Choose an account and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 16 Click **Next**.

Step 17 The **Physical Network** screen displays the physical network accounts added to the resource group. Choose an account and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 18 Click **Next**.

Step 19 In the **L4L7 Devices** screen, edit the firewall specification and load balancer specification as required.

Step 20 Click **Submit**.

Adding a Pod to a Resource Group

To add all accounts in a pod to a resource group, add the pod itself to the resource group.

Note You can also add a multi-domain manager account to a resource group using the **Add Pod to Resource Group** option, provided that the multi-domain manager account is associated with a pod.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Resource Groups** tab.

Step 3 Click **Add Pod to Resource Group**.

Step 4 In the **Resource Group** dialog box, complete the following fields:

Name	Description
Select drop-down list	Choose one of the following: • **Existing Resource Group—**To add a pod to the existing resource group. ◦ **Name** drop-down list—Choose the resource group. • **Add New Resource Group—**To create a new resource group and add a pod to the newly added resource group. ◦ **Name** field—The name of the resource group. ◦ **Description** field—The description of the resource group.
Pod field	Choose the pod that you want to add to the resource group.

Step 5 Click **Submit**.

Managing Tags of a Resource Group

You can add a tag to a resource group, edit the assigned tag, and delete the tag from the resource group.

Note The Manage Tag dialog box displays tags according to the Taggable Entities that are assigned during creation. For more information on how to create a tag, see the Cisco UCS Director Administration Guide.

The resources need to be grouped based on the resource capabilities. Use a tag to group the resources. You can create the tag library based on the resource type, capacity, quality, and capability of each resource, so as to group the resources in a proper pattern.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Resource Groups** tab.

Step 3 Choose a resource group.

Step 4 Click **Manage Tag**.

Step 5 In the **Manage Tags** dialog box, click the **+** icon to add a tag.
Alternatively, you can click **Add Tags** in the **Resource Groups** tab.

a) In the **Add Entry to Tag** dialog box, complete the following fields:

Name	Description
Tag Name drop-down list	Choose the name of the tag.
Tag Value drop-down list	Choose the value of the tag.

b) Click **Submit**.
c) Click **OK**.

Step 6 In the **Manage Tag** dialog box, choose a tag and click the pencil icon to edit a tag.

a) In the **Edit Tag Entry** dialog box, complete the following fields:

Name	Description
Tag Name drop-down list	Choose the name of the tag.
Tag Value drop-down list	Choose the value of the tag.

b) Click **Submit**.
c) Click **OK**.

Step 7 In the **Manage Tag** dialog box, choose a tag and click the **cross** icon to delete a tag.
Alternatively, you can click **Delete Tags** in the **Resource Groups** tab.

a) In the **Delete Tag Entry** dialog box, choose the tag(s) and click **Submit**.
b) Click **OK**.

Step 8 Click **Submit**.

Step 9 Click **OK**.

Deleting a Resource Group

Note You cannot delete a resource group that is in use.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Resource Groups** tab.

Step 3 Choose the resource group that you want to delete.

Step 4 Click **Delete**.
The **Delete Resource Group** dialog box appears.

Step 5 Click **Submit**.

Tenant

A tenant is a customer who uses resources in Cisco UCS Director to deploy and manage their application.

When a customer wants to deploy an application in Cisco UCS Director, the customer is onboarded as a tenant and the infrastructure is provided to deploy the application, using the APIC use case workflows.

To view the list of tenants that are onboarded in Cisco UCS Director choose **Policies** > **Resource Groups**. Choose a tenant and click **View Details** to view the service offerings of the tenant. Choose a service offering and click **View Details** to view the resource groups of a tenant.

Note If the disaster recovery support is enabled for the tenant, the resource groups of the primary site and the disaster recovery site are displayed.

To view the resource entity, reserved resources, and resources available for use in tenant and container, choose the resource group and click **View Details**. The following tabs appear:

- **Resource Entity—**Displays the details of the entity in the resource group. The details include name, type, component, resource group, tenant resource allocation type, application resource allocation type, container, and state of the resource entity.
- **Tenant Resource Limits—**Displays availability of both virtual and physical resources in a tenant. The resources reserved during tenant onboarding are displayed along with the used and available resource values. The VDCs Limit column specifies the maximum number of containers that are reserved for the tenant. The Available Number of VDCs column represents the number of containers that are available for provisioning. The physical resource limits display the blades that are reserved as part of tenant onboarding, along with the number of blades used for baremetal provisioning.
- **Container Resource Limits—**Displays availability of both virtual and physical resources in a container. The resource limits that are set during container creation are displayed along with the used and available resources.

  Note If a container is created without a resource limit, the value of the virtual resources is displayed as Not Set.

- **Private Network—**Displays the private networks created for the tenant. Choose a private network and click **View Details** to view the supernet and subnet pools of the private network. The **Supernets** tab lists the supernets available for the tiers. The **Subnets** tab displays the sub-network pool that is used for load balancer configuration during the container deployment.

The tenant-specific and container-specific resource limits assist in provisioning VMs and BMs.

Service Offerings

A service offering defines the resources required to provision an application. Each service offering must include one or more service classes that represents the capacity and capability needed for the following resource layers:

- Virtual Compute
- Virtual Storage
- Virtual Network
- Physical Compute
- Physical Storage
- Physical Network
- Layer 4 to Layer 7 Services

When you define a service offering, you can specify the usage of resource groups as one of the following:

- Shared—The resources are shared among the applications or tenants.
- Dedicated —The resources are dedicated to a single application or tenant.

Based on the capacity, capability, and resource tags defined in the service offering, the resource groups are filtered and the matching resource groups are selected for further processing in the tenant onboarding and application deployment.

Adding a Service Offering

Before You Begin

If tag-based resource selection is required for any of the resources, ensure that the tags are created in the tag library and are associated with the respective object. So that, the tags are listed when you define resource tag for service class. For more information on how to create a tag, see the Cisco UCS Director Administration Guide.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Service Offering** tab.
The service offerings that are available in Cisco UCS Director appear.

- Choose a service offering and click **View** to view the name, description, and service classes of the service offering.
- View the service classes of the service offering by choosing a service offering and clicking **View Details**.
- View the capabilities, capacity, and resource-group tag of the service class by choosing a service class and clicking **View Details**.

Step 3 Click **Add**.

Step 4 In the **Add Service Offering** dialog box, complete the following fields:

Name	Description
Name field	The name of the service offering.
Description field	The description of the service offering.
Override Mandatory Service Class Requirement check box	If checked, the user can define any number of resource types (minimum of one resource type to maximum of six resource types) for the service class according to the topology. If unchecked, the user has to define all the six resource types (physical compute, physical storage, physical network, virtual compute, virtual storage, and virtual network) for the service class. Even if the user does not define all the virtual and physical infrastructure resource types, Cisco UCS Director looks for resources for the missing resource types along with the defined resource types. **Note** To create a service offering that is used for onboarding a tenant using APIC account and VMware account, check this check box and create a service offering with service class for four resource types (physical network, virtual compute, virtual storage, and virtual network). This service offering needs to be chosen during creation of a tenant profile. The tenant profile will be used for onboarding a tenant using APIC account and VMware account (for example, tenant onboarding with private networks).

Step 5 Click **Next**.

Step 6 In the **Service Class** screen, click the + icon to define the service class that the service offering has to provide.

Step 7 In the **Add Entry to Service Class** dialog box, complete the following fields:

Name	Description
Name field	The name of the service class.
Description field	The description of the service class.
Resource Allocation type for Tenant drop-down list	Choose the type of resource allocation for the tenant. It can be one of the following: • **Dedicated—**To dedicate the resources for a tenant. • **Shared—**To share the resources among the tenants.

Name	Description
Resource Allocation type for Application drop-down list	Choose the type of resource allocation for the application. It can be one of the following: • **Dedicated—**To dedicate the resources for an application. • **Shared—**To share the resources among the applications.
Resource Type drop-down list	Choose the type of resource that you are adding to the service class. It can be one of the following: • **Virtual_Compute** • **Virtual_Storage** • **Virtual_Network** • **Physical_Compute** • **Physical_Storage** • **Physical_Network** The user can define a minimum of two resource types (physical or virtual compute, and physical or virtual network) and a maximum of six resource types (virtual compute, virtual storage, virtual network, physical compute, physical storage, and physical network) during the addition of the service class, only when the **Override Mandatory Service Class Requirement** check box is unchecked.
Resource Tag table	Choose the resource tag from the table that displays resource entity tags. For more information about the tag library, see the Cisco UCS Director Administration Guide. **Note** You can add the data store tags with multiple tag values (for example, gold, silver, bronze) in the virtual storage service class level. **Note** You can add the ESXi cluster tag with multiple tag values in the virtual compute service class level. **Important** You can modify only the required values of the tags defined in this table. You cannot add new tags to this table. For information on how to create a tag, see the Tag Library section in the Cisco UCS Director Administration Guide.

Name	Description
Resource Capability table	By default, the capabilities that are applicable for the VMware and Hyper-V account are displayed according to the chosen resource type. You can edit the value of the resource capability using the Edit icon. You can remove a resource capability from the service offering using the Delete icon. **Important** All the resource capabilities related to the resource type are prepopulated with the default value as **false**. You can modify the capability value.
Resource Capacity table	The available resource capacity for the service offering. To add a resource capacity, click the Add icon and choose the capacity type from the list of capacities that are applicable for the VMware and Hyper-V account. The capacities are displayed based on the chosen resource type. Choose the capacity matching criteria and set the required capacity value. To remove the resource capacity, click the Delete icon. To modify the values of the capacity, click the Edit icon.

Note The tag is used along with resource capability and capacity for filtering the resources in the resource group.

Step 8 Click **Submit**.
The service class information is added to the table. You can define multiple service classes for the service offering.

Step 9 Click **Submit**.

Cloning a Service Offering

Before You Begin

Ensure that the tags are created in the tag library and the tags are associated with the respective object. So that, the tags are listed when you define resource tag for service class. For more information on how to create a tag, see the Cisco UCS Director Administration Guide.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Service Offering** tab.

Step 3 Choose the service offering that you want to clone.

Step 4 Click **Clone Service Offering**.

Step 5 In the **Clone Service Offering** dialog box, complete the following fields:

Name	Description
Name field	The name of the service offering.
Description field	The description of the service offering.
Override Mandatory Service Class Requirement check box	If checked, the user can define any number of resource types (minimum of one resource type to maximum of six resource types) for the service class according to the topology. If unchecked, the user has to define all the six resource types (physical compute, physical storage, physical network, virtual compute, virtual storage, and virtual network) for the service class. Even if the user does not define all the virtual and physical infrastructure resource types, Cisco UCS Director looks for resources for the missing resource types along with the defined resource types. **Note** To create a service offering that is used for onboarding a tenant using APIC account and VMware account, check this check box and create a service offering with service class for four resource types (physical network, virtual compute, virtual storage, and virtual network). This service offering needs to be chosen during creation of a tenant profile. The tenant profile will be used for onboarding a tenant using APIC account and VMware account (for example, tenant onboarding with private networks).

Step 6 Click **Next**.

Step 7 In the **Service Class** screen, click the **+** icon to define the service class that the service offering has to provide.

Step 8 In the **Add Entry to Service Class** dialog box, complete the following fields:

Name	Description
Name field	The name of the service class.
Description field	The description of the service class.
Resource Allocation type for Tenant drop-down list	Choose the type of resource allocation for the tenant. It can be one of the following: • **Dedicated—**To dedicate the resources for a tenant. • **Shared—**To share the resources among the tenants.

Name	Description
Resource Allocation type for Application drop-down list	Choose the type of resource allocation for the application. It can be one of the following: • **Dedicated—**To dedicate the resources for an application. • **Shared—**To share the resources among the applications.
Resource Type drop-down list	Choose the type of resource that you are adding to the service class. It can be one of the following: • **Virtual_Compute** • **Virtual_Storage** • **Virtual_Network** • **Physical_Compute** • **Physical_Storage** • **Physical_Network** The user can define a minimum of two resource types (physical or virtual compute, and physical or virtual network) and a maximum of six resource types (virtual compute, virtual storage, virtual network, physical compute, physical storage, and physical network) during the addition of the service class, only when the **Override Mandatory Service Class Requirement** check box is unchecked.
Resource Tag table	Choose the resource tag from the table that displays resource entity tags. For more information about the tag library, see the Cisco UCS Director Administration Guide. **Note** You can add the data store tags with multiple tag values (for example, gold, silver, bronze) in the virtual storage service class level. **Note** You can add the ESXi cluster tag with multiple tag values in the virtual compute service class level. **Important** You can modify only the required values of the tags defined in this table. You cannot add new tags to this table. For information on how to create a tag, see the Tag Library section in the Cisco UCS Director Administration Guide.

Name	Description
Resource Capability table	By default, the capabilities that are applicable for the VMware and Hyper-V account are displayed according to the chosen resource type. You can edit the value of the resource capability using the Edit icon. You can remove a resource capability from the service offering using the Delete icon. **Important** All the resource capabilities related to the resource type are prepopulated with the default value as **false**. You can modify the capability value.
Resource Capacity table	The available resource capacity for the service offering. To add a resource capacity, click the Add icon and choose the capacity type from the list of capacities that are applicable for the VMware and Hyper-V account. The capacities are displayed based on the chosen resource type. Choose the capacity matching criteria and set the required capacity value. To remove the resource capacity, click the Delete icon. To modify the values of the capacity, click the Edit icon.

Step 9 (Optional) Click the **pencil** icon to edit the values of an already configured service class.

Step 10 (Optional) Click the **cross** icon to delete an already configured service class from the service offering.

Step 11 Click **Submit**.

Editing a Service Offering

Note Do not edit the service offering that is mapped to a resource group and tenant profile. If you edit the service offering that is mapped to a resource group and tenant profile, the tenant that is onboarded using the service offering will be affected.

Before You Begin

Ensure that the tags are created in the tag library and the tags are associated with the respective object. So that, the tags are listed when you define resource tag for service class. For more information on how to create a tag, see the Cisco UCS Director Administration Guide.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Service Offering** tab.

Step 3 Choose the service offering that you want to edit.

Step 4 Click **Edit**.

Step 5 In the **Modify Service Offering** dialog box, complete the following fields:

Name	Description
Name field	The name of the service offering.
Description field	The description of the service offering.
Override Mandatory Service Class Requirement check box	If checked, the user can define any number of resource types (minimum of one resource type to maximum of six resource types) for the service class according to the topology. If unchecked, the user has to define all the six resource types (physical compute, physical storage, physical network, virtual compute, virtual storage, and virtual network) for the service class. Even if the user does not define all the virtual and physical infrastructure resource types, Cisco UCS Director looks for resources for the missing resource types along with the defined resource types. **Note** To create a service offering that is used for onboarding a tenant using APIC account and VMware account, check this check box and create a service offering with service class for four resource types (physical network, virtual compute, virtual storage, and virtual network). This service offering needs to be chosen during creation of a tenant profile. The tenant profile will be used for onboarding a tenant using APIC account and VMware account (for example, tenant onboarding with private networks).

Step 6 Click **Next**.

Step 7 In the **Service Class** screen, click the + icon to define the service class that the service offering has to provide.

Step 8 In the **Add Entry to Service Class** dialog box, complete the following fields:

Name	Description
Name field	The name of the service class.
Description field	The description of the service class.
Resource Allocation type for Tenant drop-down list	Choose the type of resource allocation for the tenant. It can be one of the following: • **Dedicated—**To dedicate the resources for a tenant. • **Shared—**To share the resources among the tenants.
Resource Allocation type for Application drop-down list	Choose the type of resource allocation for the application. It can be one of the following: • **Dedicated—**To dedicate the resources for an application. • **Shared—**To share the resources among the applications.
Resource Type drop-down list	Choose the type of resource that you are adding to the service class. It can be one of the following: • **Virtual_Compute** • **Virtual_Storage** • **Virtual_Network** • **Physical_Compute** • **Physical_Storage** • **Physical_Network** The user can define a minimum of two resource types (physical or virtual compute, and physical or virtual network) and a maximum of six resource types (virtual compute, virtual storage, virtual network, physical compute, physical storage, and physical network) during the addition of the service class, only when the **Override Mandatory Service Class Requirement** check box is unchecked.

Name	Description
Resource Tag table	Choose the resource tag from the table that displays resource entity tags. For more information about the tag library, see the Cisco UCS Director Administration Guide. **Note** You can add the data store tags with multiple tag values (for example, gold, silver, bronze) in the virtual storage service class level. **Note** You can add the ESXi cluster tag with multiple tag values in the virtual compute service class level. **Important** You can modify only the required values of the tags defined in this table. You cannot add new tags to this table. For information on how to create a tag, see the Tag Library section in the Cisco UCS Director Administration Guide.
Resource Capability table	By default, the capabilities that are applicable for the VMware and Hyper-V account are displayed according to the chosen resource type. You can edit the value of the resource capability using the Edit icon. You can remove a resource capability from the service offering using the Delete icon. **Important** All the resource capabilities related to the resource type are prepopulated with the default value as **false**. You can modify the capability value.
Resource Capacity table	The available resource capacity for the service offering. To add a resource capacity, click the Add icon and choose the capacity type from the list of capacities that are applicable for the VMware and Hyper-V account. The capacities are displayed based on the chosen resource type. Choose the capacity matching criteria and set the required capacity value. To remove the resource capacity, click the Delete icon. To modify the values of the capacity, click the Edit icon.

Step 9 Click **Submit**.

Deleting a Service Offering

Note You cannot delete a service offering that is in use.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Service Offering** tab.

Step 3 Choose the service offering that you want to delete.

Step 4 Click **Delete**.

Step 5 In the **Service Offering** dialog box, click **Delete**.

Tenant Profiles

Tenant profiles represent the pairing of one or more service offerings with one or more resource groups. Each tenant profile defines the characteristic of infrastructure requirements and application requirements.

You can create a tenant profile to meet each possible combination of customer and application. You can associate a tenant profile with multiple service offerings and choose a resource group for each service offering. A tenant profile can be shared by more than one tenant.

Adding a Tenant Profile

Before You Begin

If the DR service support is enabled for the tenant profile, the resources that satisfy the following are displayed for choosing a resource group for a specific service offering:

- The DR service is enabled.
- The resource group is configured as primary.
- The primary resource group is mapped with the secondary resource group.
- The primary and secondary resource groups have same number of accounts.
- The resources required for the tenant are available in both the primary and secondary resource groups.

For more information on how to enable DR service and set the resource group as primary or secondary, see Adding a Resource Group, on page 28.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Tenant Profile** tab.

The tenant profiles that are available in Cisco UCS Director appear.

- Choose a tenant profile and click **View** to view the name, description, and service offering of the tenant profile with the resource limit added to the tag.
- View the tenants that are associated with a tenant profile by choosing a tenant profile and clicking **View Details**. The name, resource group, service offering, APIC account, service request ID, and customer assigned for the tenants in the tenant profile are displayed.
- View the service offering of a tenant by choosing a tenant and clicking **View Details**.
- View the resource entity of a tenant by choosing a service offering and clicking **View Details**.

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

Step 4 In the **Add Tenant Profile** dialog box, complete the following fields:

Name	Description
Name field	The name of the tenant profile. Once specified, you cannot edit the name of the profile.
Description field	The description of the tenant profile.
Enable DR check box	Check this check box to enable the disaster recovery service support for the tenant profile. If this check box is checked, the tenant is allocated with resources from both the primary resource group and the secondary resource group.
Service Offering field	The service offerings to be associated with the tenant profile. Click **Select** to view and choose the service offering from the list of service offerings. The service offerings are displayed based on the matching resource group availability. To create a new service offering, click the + icon. For more information about how to create a service offering, see Adding a Service Offering, on page 41. **Note** If you receive an error message instead of the service offerings list, take action according to the error message. For more details, see Troubleshooting a Service Offering List, on page 53.
Resource Group Selection drop-down list	Choose how the resource group selection will be made for the tenant profile: • **Admin Selection—**The resource group is selected by the administrator. • **Resource Group Tag based selection—**The resource group is selected based on the tag.

Step 5 Click **Next**.

Step 6 Click the **Add (+)** icon to choose a resource group for a specific service offering. For each service offering selected for the tenant profile, you can select the resource group.
The resource groups that match the specified requirement of the tenant profile are displayed.

Note If there is no matching resource group for the resource requirements defined in a service offering, Cisco UCS Director will not list any resource group.

Step 7 Click **Submit**.

Troubleshooting a Service Offering List

While creating a tenant profile, you associate a tenant profile with multiple service offerings. The service offerings list is displayed based on the matching resource group availability. If you receive an error message instead of the service offerings list, take action according to the error message.

For example, on receiving the error message: *Host is not mounted on UCS servers*, check for the following:

1. Verify that Cisco UCS server is managed by Cisco UCS Director. To check the status of Cisco UCS servers, choose **Physical** > **Compute**, choose the Cisco UCS Manager account, and click the **UCS Discovered Servers** tab.
2. Verify that the vCenter account and Cisco UCS Manager account are in the same resource group, and host in the vCenter account is mounted on the Cisco UCS Manager account.
3. Verify that the Cisco UCS Manager accounts that are available in Cisco UCS Director each have a unique IP address. If more than one account exists with the same IP address, remove one of the accounts that is not part of the resource group.

Cloning a Tenant Profile

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Tenant Profile** tab.

Step 3 Choose the tenant profile that you want to clone.

Step 4 Click **Clone**.

Step 5 In the **Clone Tenant Profile** dialog box, complete the following fields:

Name	Description
Name field	The name of the tenant profile.
Description field	The description of the tenant profile.

Name	Description
Service Offering field	The service offerings to be associated with the tenant profile. Click **Select** to view and choose the service offering from the list of service offerings. The service offerings are displayed based on the matching resource group availability. To create a new service offering, click the + icon. For more information about how to create a service offering, see Adding a Service Offering, on page 41. **Note** If you receive an error message instead of the service offerings list, take action according to the error message. For more details, see Troubleshooting a Service Offering List, on page 53.
Resource Group Selection drop-down list	Choose how the resource group selection will be made for the tenant profile: • **Admin Selection—**The resource group is selected by the administrator. • **Resource Group Tag based selection—**The resource group is selected based on the tag.

Step 6 Click **Next**.

Step 7 Click the + icon to choose a resource group for a specific service offering. For each service offering selected for the tenant profile, you can select the resource group.
The resource groups that match the specified requirement of the tenant profile are displayed.

Note If there is no matching resource group for the resource requirements defined in the service offering, Cisco UCS Director will not list any resource group.

Step 8 Click **Submit**.

Editing a Tenant Profile

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Tenant Profile** tab.

Step 3 Choose the tenant profile that you want to edit.

Step 4 Click **Edit**.

Step 5 In the **Edit Tenant Profile** dialog box, complete the following fields:

Name	Description
Name field	The name of the tenant profile. Once specified, you cannot edit the name of the profile.
Description field	The description of the tenant profile.
Service Offering field	The service offerings to be associated with the tenant profile. Click **Select** to view and choose the service offering from the list of service offerings. The service offerings are displayed based on the matching resource group availability. To create a new service offering, click the + icon. For more information about how to create a service offering, see Adding a Service Offering, on page 41. **Note** If you receive an error message instead of the service offerings list, take action according to the error message. For more details, see Troubleshooting a Service Offering List, on page 53.
Resource Group Selection drop-down list	Choose how the resource group selection will be made for the tenant profile: • **Admin Selection—**The resource group is selected by the administrator. • **Resource Group Tag based selection—**The resource group is selected based on the tag.

Step 6 Click **Next**.

Step 7 Click the + icon to choose a resource group for a specific service offering. For each service offering selected for the tenant profile, you can select the resource group.
The resource groups that match the specified requirement of the tenant profile are displayed.

Note If there is no matching resource group for the resource requirements defined in the service offering, Cisco UCS Director will not list any resource group.

Step 8 Click **Submit**.

Deleting a Tenant Profile

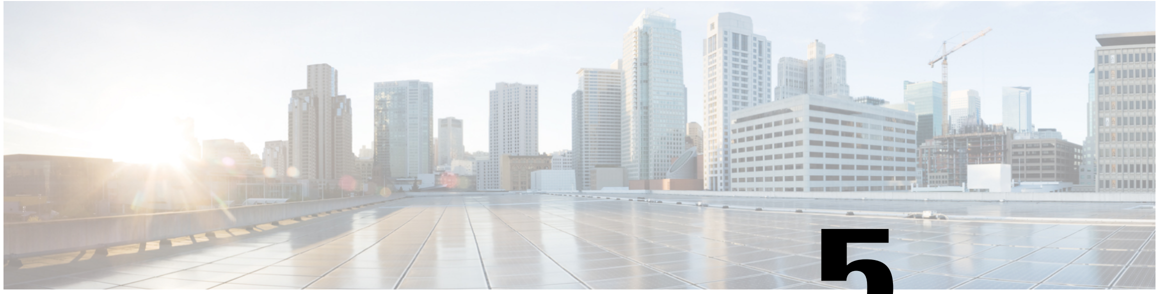
Note You cannot delete a tenant profile that is in use.

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Tenant Profile** tab.

Step 3 Choose a tenant profile from the table.

Step 4 Click **Delete**.
The tenant profile is deleted after confirmation.



CHAPTER 5

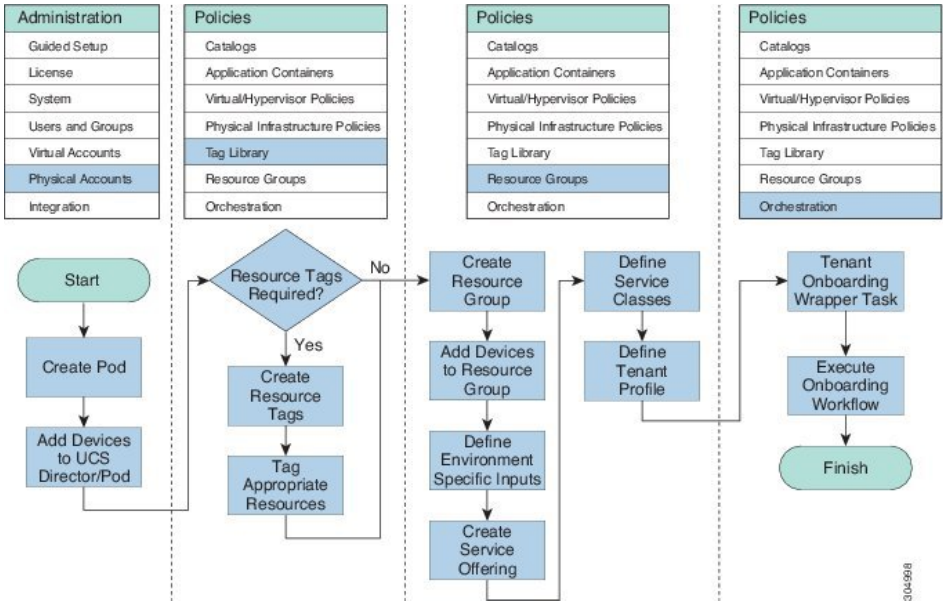
Managing Tenants

This chapter contains the following sections:

Onboarding a Cisco UCS Director Tenant

Cisco UCS Director tenants are essentially customers who share the compute, network, and storage resources that are configured for ACI in Cisco UCS Director. The following image explains the end-to-end process flow of the Cisco UCS Director tenant onboarding process.

Figure 1: APIC Tenant Onboarding Process Flow



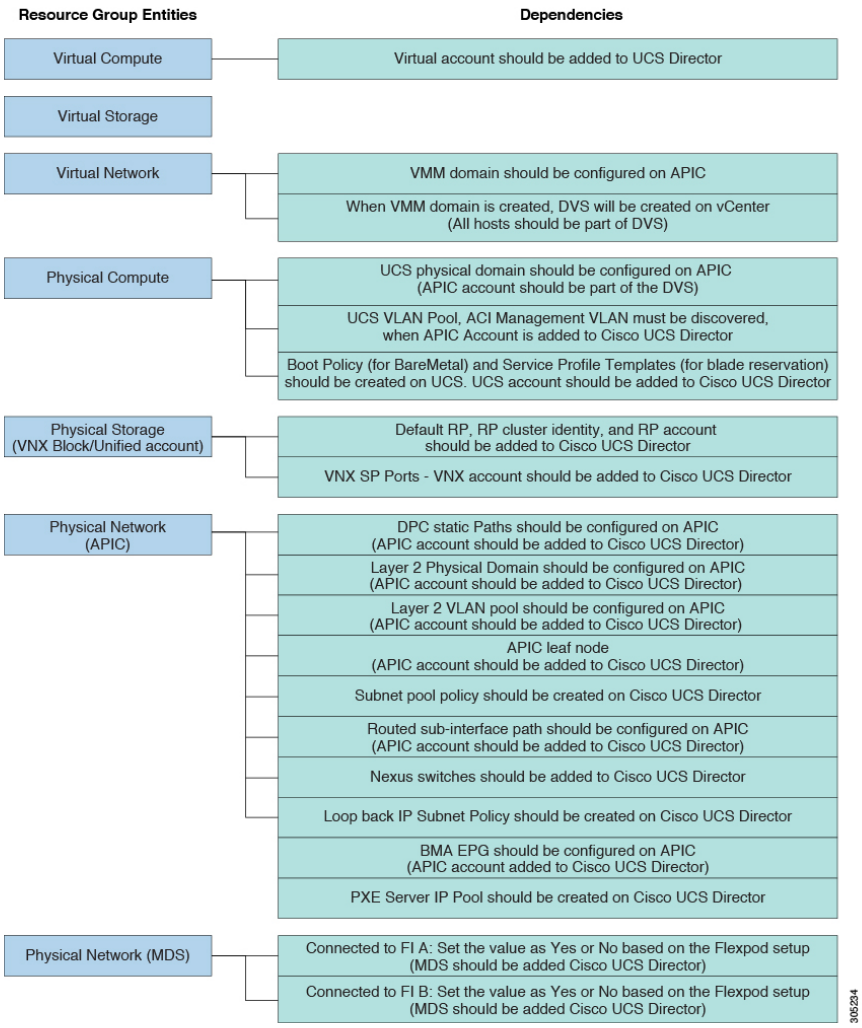
You can also execute the preconfigured tenant onboarding workflow to onboard a tenant. To view the tenant onboarding workflows, choose **Policies** > **Orchestration** and click the **Workflows** tab. In the **Workflows** tab, choose one of the following paths:

- **APIC Usecases** > **Tenant Usecases** > **VNX Storage Tenant Usecases**
- **APIC Usecases** > **Tenant Usecases** > **NetApp Storage Tenant Usecases**

For more information on how to execute a workflow, see the Cisco UCS Director Orchestration Guide.

Ensure that the environment variables are defined for the physical and virtual infrastructure resources in a resource group that is used for onboarding a tenant. The following image explains the dependencies of the physical and virtual infrastructure resources.

Figure 2: Resource Group Entities - Dependency



Resource Group Entities

Dependencies

Virtual Compute
- Virtual account should be added to UCS Director

Virtual Storage

Virtual Network
- VMM domain should be configured on APIC
- When VMM domain is created, DVS will be created on vCenter (All hosts should be part of DVS)

Physical Compute
- UCS physical domain should be configured on APIC (APIC account should be part of the DVS)
- UCS VLAN Pool, ACI Management VLAN must be discovered, when APIC Account is added to Cisco UCS Director
- Boot Policy (for BareMetal) and Service Profile Templates (for blade reservation) should be created on UCS. UCS account should be added to Cisco UCS Director

Physical Storage (VNX Block/Unified account)
- Default RP, RP cluster identity, and RP account should be added to Cisco UCS Director
- VNX SP Ports - VNX account should be added to Cisco UCS Director

Physical Network (APIC)
- DPC static Paths should be configured on APIC (APIC account should be added to Cisco UCS Director)
- Layer 2 Physical Domain should be configured on APIC (APIC account should be added to Cisco UCS Director)
- Layer 2 VLAN pool should be configured on APIC (APIC account should be added to Cisco UCS Director)
- APIC leaf node (APIC account should be added to Cisco UCS Director)
- Subnet pool policy should be created on Cisco UCS Director
- Routed sub-interface path should be configured on APIC (APIC account should be added to Cisco UCS Director)
- Nexus switches should be added to Cisco UCS Director
- Loop back IP Subnet Policy should be created on Cisco UCS Director
- BMA EPG should be configured on APIC (APIC account added to Cisco UCS Director)
- PXE Server IP Pool should be created on Cisco UCS Director

Physical Network (MDS)
- Connected to FI A: Set the value as Yes or No based on the Flexpod setup (MDS should be added Cisco UCS Director)
- Connected to FI B: Set the value as Yes or No based on the Flexpod setup (MDS should be added Cisco UCS Director)

Workflows for Onboarding a Tenant

Cisco UCS Director provides the following preconfigured orchestration workflows for secure tenant onboarding:

- NetApp workflows:
    - ◦ FlexPod ACI - Tenant Infrastructure Configuration—Use this workflow to create an APIC tenant, configure the tenant-dedicated NetApp storage, configure the ACI fabric for NFS data store connectivity, and provide a tenant-dedicated NFS data store to an ESXi cluster. For more information on how to deploy Cisco UCS Director on FlexPod with Cisco Application Centric Infrastructure using the FlexPod ACI - Tenant Infrastructure Configuration workflow, see the Deployment Guide for FlexPod with VMware vSphere 5.5 Update 1, Cisco UCS Director and Cisco Nexus 9000 Cisco Application Centric Infrastructure (ACI).

      Note If the NetApp device uses ONTAP 8.3 operating system, ensure that the following tasks are added before the Create Failover Group tasks:

        - custom BroadcastDomain_CLI
        - SSH command

      This workflow includes the following child workflows:

        - ◦ Tenant Onboarding - L2 Out—Use this workflow to configure the Layer 2 out configuration for the APIC tenant.
        - ◦ Tenant Onboarding - L3 Out—Use this workflow to configure the Layer 3 out configuration for the APIC tenant. When executing this workflow, set the Ethernet interfaces, BGP ID, and subnet IP addresses. In the **Workflow Designer** dialog box, double-click the **SSH Command** task and navigate to **Task Inputs** screen by clicking **Next**. The administrator has to define the sub interface for the configuration by editing the values of the following task inputs:
            - interface ethernet *1/49*.${GenerateVLANfrompool_820.OUTPUT_VLAN_ID}
            - interface ethernet *1/50*.${GenerateVLANfrompool_820.OUTPUT_VLAN_ID}
            - router bgp *10*
            - neighbor ${GetIPAddressFromIPSubnet_7135.IPAddress} remote-as *100*
            - neighbor ${GetIPAddressFromIPSubnet_7136.IPAddress} remote-as *100*

    - ◦ FlexPod ACI - Enable Tenant Infrastructure Support For Guest Attached ISCSI—Use this workflow to configure iSCSI support on the NetApp storage, and configure iSCSI-A and iSCSI-B paths from the storage virtual machine to the ESXi cluster through the ACI fabric.

      Note If the NetApp device uses ONTAP 8.3 operating system, ensure that the following tasks are added before the Create Failover Group tasks:

        - custom BroadcastDomain_CLI
        - SSH command

    - ◦ FlexPod ACI - Enable Connectivity for VM Application Consistent Snapshots—Use this workflow to configure an ACI contract between the tenant-dedicated VMNET EPG and the tenant storage virtual machine management EPG to meet the connectivity requirements defined by the NetApp SnapDrive software.

- VNX Workflows:
    - Tenant Onboarding with MSP - VNX—Use this workflow to onboard a tenant for Managed Service Provider (MSP) organization on the VNX storage device.

      Note If you have not enabled the service provider feature in Cisco UCS Director, the Tenant Onboarding with MSP - VNX workflow will be in the validation failed state. To enable a service provider, choose **Administration > System > Service Provider Feature**, and check the **Enable Service Provider Feature (Requires System Restart)** check box. Restart the service and validate the Tenant Onboarding with MSP workflow.

      This workflow includes the following child workflows:

        - Tenant Onboarding - L2 Out—Use this workflow to configure the Layer 2 out configuration for the APIC tenant.
        - Tenant Onboarding - L3 Out—Use this workflow to configure the Layer 3 out configuration for the APIC tenant.
        - DR Cluster with RP support—Use this workflow to create replica of data cluster with the RP support in a tenant. Provide the following RP-related information in addition to the cluster information: RP account identity, RP cluster identity, and tenant CG identity.

          When updating a tenant, provide the primary and secondary CG copy identities. To handle a failover scenario for a tenant with the disaster recovery (DR) support, same LUN ID and host LUN (HLU) ID are needed in the primary and secondary sites. During tenant onboarding, the same LUN ID and HLU ID are reserved on the primary and secondary sites, based on the availability of the selected VNX account and VMware host.
        - DR Tenant Onboarding with MSP - VNX—Use this workflow to onboard a tenant with the DR support for MSP organization on the VNX storage device.
        - Tenant Onboarding - Datastore Cluster Creation - VNX—Use this workflow to create data store cluster for a tenant.
        - Reserve Blade on UCSM—Use this workflow to reserve half- or full-width blades on Cisco UCS Manager for the tenant.

    - Tenant Onboarding - VNX—Use this workflow to onboard a tenant for a user group on the VNX storage device.

      This workflow includes the following child workflows:

        - Tenant Onboarding - L2 Out—Use this workflow to configure the Layer 2 out configuration for the APIC tenant.
        - Tenant Onboarding - L3 Out—Use this workflow to configure the Layer 3 out configuration for the APIC tenant.
        - DR Cluster with RP support—Use this workflow to create a replica of a data cluster with RP support in a tenant.

    Provide the following RP-related information in addition to the cluster information: RP account identity, RP cluster identity, and tenant CG identity. When updating a tenant, provide the primary and secondary consistency group (CG) copy identities.

    To handle a failover scenario for a tenant with the disaster recovery (DR) support, the same LUN ID and host LUN (HLU) ID are needed in the primary and secondary sites. During tenant onboarding, the same LUN ID and HLU ID are reserved on the primary and secondary sites, based on the availability of the selected VNX account and VMware host.

  - DR Tenant Onboarding with MSP - VNX—Use this workflow to onboard a tenant with the DR support for MSP organization on the VNX storage device.
  - Reserve Blade on UCSM—Use this workflow to reserve half- or full-width blades on Cisco UCS Manager for the tenant.

- Update Tenant:
  - Update Tenant - Datastore Cluster Creation - VNX—Use this workflow to add VNX data store to the tenant data store cluster.
  - Update Tenant - VNX—Use this workflow to update the physical and virtual resources of the tenant, such as memory, number of CPUs, number of VDCs, and number of full-width and half-width blades.
  - DR Update Tenant - VNX—Use this workflow to update the physical and virtual resources of the tenant, such as memory, number of CPUs, number of VDCs, number of full-width and half-width blades, and reserved space of the physical server.
- Tenant Onboarding with Private Network(s)—Use this workflow to onboard a tenant with one or more private networks.
- Update Tenant vPOD with Existing Resources—Use this workflow to update the vPOD information with multiple data stores and multiple data store clusters, for a tenant. Choose the tenant that you want to update, and the service offering with which the tenant is onboarded. The data stores and data store clusters must be part of VMware generic cluster that has been selected during tenant onboarding.

Example: VNX Tenant Onboarding

This section describes the step-by-step process involved in onboarding a tenant on the VNX storage device for Managed Service Provider (MSP) organization through the user interface.

Step 1 Add a pod. For more information, see the Cisco UCS Director Administration Guide.

Step 2 Add the following types of accounts to the pod:

- Physical Compute—Cisco UCS Manager
- Physical Storage—EMC VNX Unified
- Physical Network—APIC account. For more information, see Adding an APIC Account, on page 5.
- Virtual Account—VMware

For more information on how to create physical and virtual accounts, see the Cisco UCS Director Administration Guide.

Step 3 Add the pod to a resource group using the **Add Pod to Resource Group** option, to associate the accounts in the pod to the resource group. For more information, see Adding a Pod to a Resource Group, on page 37.

Step 4 Choose the resource group and click **Edit** to define the environment variable for each account. For more information, see Editing a Resource Group, on page 35.
The environment variables that you want to define for the VNX tenant onboarding are:

- Virtual Compute
  - Container Parent Folder—The folder to which you want to add the newly created container.
- Virtual Storage—None.
- Virtual Network
  - VMM domain for VMware—This environment variable is used for onboarding a tenant. vCenter is configured with the Virtual Machine Manager (VMM) domain. When vCenter is associated with the APIC, the distributed virtual switch (DVS) with the same name is created in vCenter.

    Cisco UCS Director offers AVS support in both VLAN and VXLAN mode. The VM gets the VLAN ID or VXLAN ID from the pool assigned to the VMM domain. Choose a VMM domain with the Cisco AV switch to support AVS in the VXLAN mode.
  - DV Switch—This environment variable is used for onboarding a tenat. The DV Switch is used to connect the selected host during tenant onboarding.
- Physical Compute
  - Service Profile Template for Full Width blade—This environment variable is used for the VNX tenant onboarding. The service profile template is used to create a service profile. When a service profile is created, the service profile chooses the free servers from the server pool that is associated with the service profile template.
  - Service Profile Template for Half Width blade—This environment variable is used for the VNX tenant onboarding. The service profile template is used to create a service profile. When a service profile is created, the service profile chooses the free servers from the server pool that is associated with the service profile template.
- Physical Storage
  - SP Port—The storage processor (SP) port for the physical storage account.

  If the disaster recovery support is enabled for the onboarding a tenant, define the following environment variables for the physical storage:

  - Default Recovery Point—The recovery point attached to the VNX account.
  - Recovery Point Cluster Identity—The identity of the recovery point attached to the VNX account.
- Physical Network
  - DPC Static path 1—The static path of the first Direct Port Channel (DPC).
  - DPC Static path 2—The static path of the second DPC.

- L2 Physical Domain—The physical domain of layer 2.

Note To onboard a tenant with Layer 2 configuration, set the value for the DPC Static Paths and L2 Physical Domain.

Step 5 Add a service offering and define the service class for each resource type (physical compute, physical storage, physical network, virtual compute, virtual storage, and virtual network). The service offering defines the resource requirements of the tenant. For more information on how to add a service offering, see Adding a Service Offering, on page 41.

Step 6 Add a tenant profile. In the **Add Tenant Profile** dialog box, choose the service offering that you added in Step 5 and add the resource group to the service offering. For more information on how to add a tenant profile, see Adding a Tenant Profile, on page 51.

Step 7 Enable the service provider feature in Cisco UCS Director as follows:

a) On the menu bar, choose **Administration > System > Service Provider Feature**.
b) Check the **Enable Service Provider Feature (Requires System Restart)** check box. The first level and second-level organization names appear.
c) Click **Submit**.

Step 8 Restart the service to enable the service provider.

Step 9 Validate the Tenant Onboarding with MSP workflow to move the workflow from the validation failed state to valid state.

Step 10 Edit the VNX Tenant Onboarding workflow to enter the mandatory input values as follows:

a) Choose **Policies** > **Orchestration** and click the **Workflow** tab.
b) Choose **APIC Usecases > Tenant Usecases > VNX Storage Tenant Usecases**.
c) Choose the Tenant Onboarding with MSP - VNX workflow and click **Edit Workflow**.
d) In the **Edit Workflow Details** screen, do the necessary changes.
e) Click **Next**.
f) In the **Edit User Inputs** screen, do the following:

  - Set the values for data store size limit, VM over subscription, CPU reservation, maximum number of subnets, and maximum number of tiers per VDC. For instance, you can set the values as:
    - Datastore Size Limit (GB)—75 GB
    - VM Over Subscription—5
    - CPU Reservation (MHz)—2000
    - Maximum number of Subnets—32
    - Maximum number of Tiers per VDC—8

g) Click **Next**.
h) Click **Submit**.

Step 11 Choose the VNX Tenant Onboarding workflow and click **Validate Workflow** to validate the workflow.

Step 12 Double-click the VNX Tenant Onboarding workflow.

Step 13 In the **Workflow Designer** dialog box, click **Edit Workflow Properties** to view the tasks and to edit user inputs that are used for task input mapping for this workflow, if necessary.

Step 14 (Optional) Add an advanced type catalog for onboarding a tenant and publish the catalog as follows:

a) On the menu bar, choose **Policies** > **Catalogs**.

b) Click **Add**.
c) From the **Catalog Type** drop-down list, choose **Advanced**.
d) In the **Add Catalog** dialog box, enter the basic information for the catalog.
e) Click **Next**.
f) In the **vApp Workflow** screen, click **Select** and choose the VNX Tenant Onboarding workflow.
g) Click **Submit**.

Step 15 Onboard a tenant in one of the following ways:

- Executing the Tenant Onboarding with MSP - VNX workflow.

1 Choose **Policies** > **Orchestration** and click the **Workflow** tab.

2 Choose **APIC Usecases > Tenant Usecases**.

3 Choose the Tenant Onboarding with MSP - VNX workflow and click **Execute Now**.

4 In the **Executing Workflow: Tenant Onboarding with MSP - VNX** screen, complete the following fields:

Field	Description
Tenant Profile field	Click **Select** and choose a tenant profile that was added in Step 6.
Service Offering field	Click **Select** and choose a service offering that was added in Step 5.
Tenant Name field	The name of the tenant.
Tenant Description field	The description of the tenant.
MSP Admin Username field	The username of the MSP who can access the tenant.
MSP Admin Password field	The password to access the tenant.
MSP Admin Email field	The email address of the MSP who can access the tenant.
Datastore Size (GB) field	The datastore size of the tenant in GB.
Memory Reservation (MB) field	The maximum limit of memory reserved for the tenant in MB.
No of CPU field	The number of CPUs needed for the tenant.
No of VDCs field	The number of virtual data centers (VDCs) needed for the tenant. **Note** The number of VDCs determine the subnet size for the supernets provided (while tenant onboarding) for each tier of the application container.
No of Half Width Blades field	The number of half width blades needed for the tenant.

Field	Description
No of Full Width Blades field	The number of full width blades needed for the tenant.
Replication Required drop-down list	By default, **No** is displayed. If you choose **Yes**, the DR Tenant Onboarding with MSP - VNX workflow is invoked. A tenant with the DR support is onboarded for MSP organization on the VNX storage device.
L2 Or L3 External Network Configuration drop-down list	Choose one of the following to perform Layer 2 out or Layer 3 out configuration during tenant onboarding: • **None—**To use only the normal network configuration for the tenant. • **L2 out—**To configure the Layer 2 out configuration for the tenant. • **L3 out—**To configure the Layer 3out configuration for the tenant.
L2 VLAN ID field	The VLAN ID to be assigned for the layer 2 port.
L2 IP Subnet (x.x.x.x/n) field	The IP subnet pool from which the IP address need to be assigned to layer 2 ports.
Tenant IP Subnet (x.x.x.x/n) field	The IP subnet pool from which the IP address need to be assigned to tenant.
Create Shared IP Subnet Pool check box	Check the check box to share the IP address among tiers in the tenant.
Private IP Subnet Pool Policy field	Click **Select** and choose a subnet pool policy from which the private IP address is assigned to tenants
Resource Selection For Network Device (ND) drop-down list	Choose one of the following: • **Use Tenant Resources—**To use the resources allocated for the tenant. • **Use Existing Resources—**To use the common resources available in the vCenter. • **Provision New Resources—**To define new resources by providing input in the **Datastore Size (GB) (For ND)**, **No of CPU (For ND)**, and **Memory Reservation (MB) (For ND)** fields.
Provide input in the following fields only when **Provision New Resources** is chosen from the **Resource Selection For Network Device (ND)** drop-down list.	

Field	Description
Datastore Size (GB) (For ND) field	The maximum size of the data store in GB that can be allotted for the network devices.
No of CPU (For ND) field	The maximum number of CPU allotted for the network devices.
Memory Reservation (MB) (For ND) field	The maximum memory reservation for the network devices in MB.

Note During provisioning of container VM, Cisco UCS Director uses the tenant resource pool and data store. During provisioning of network related VM, Cisco UCS Director uses the network device resource pool and data store.

5 Click **Submit**.

- Creating a service request.

1 On the menu bar, choose **Organizations** > **Service Requests**.

2 Click the **Service Requests** tab.

3 Click **Create Request**.

4 In the **Create Service Request** dialog box, choose the **Group**, **Catalog Type** (Advanced), and the **Catalog** (which is created in Step 14).

5 Click **Next**.

6 In the **Custom Workflow** screen, provide the custom workflow input values.

  - From the **Replication Required** drop-down list, choose **Yes** to invoke the **DR Tenant Onboarding with MSP - VNX** workflow is invoked. A tenant with the DR support is onboarded for MSP organization on the VNX storage device.
  - Provide the IP range for the IP subnet pool. Each container gets a unique subnet address from the IP subnet pool. By default, the overlapping of the IP addresses is not allowed. If you want to enable the IP address overlapping for the tiers, check the **Create Shared IP Subnet Pool** check box.

7 Review the summary for the service request.

8 Click **Submit**.

- Using the userAPISubmitVAppServiceRequest REST API.

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

2 Click the **REST API Browser** tab.

3 Enter **userAPISubmitVAppServiceRequest** in the **Search** field at the top right corner of the **Rest API Browser** tab.

4 Double-click **userAPISubmitVAppServiceRequest**. The REST API browser displays the following tabs: API Examples, Details, and Summary.

5 In the **API Examples** tab, click **Generate URL**.

6 In the param0 variable, pass the catalog name.

7 In the param1 variable, pass such tenant details as tenant name, tenant description, MSP admin details, data store size, memory reservation, number of CPUs, number of VDCs, number of half-width blades, number of full-width blades, L2 or L3 external network configuration, L2 VLAN ID, L2 IP subnet, and replication required.

Note For onboarding a tenant without Layer 2 configuration, pass **none** as the value for the following variables: L2 or L3 external network configuration, L2 VLAN ID, and L2 IP subnet.

8 Click **Execute REST API**. The REST API browser displays the service request ID in the **Response** field.

9 Choose **Organizations** > **Service Requests**. In the **Service Request** tab, choose the service request and click **View Details** to view the workflow status and log details of the service request.

Example: Flexpod ACI – Tenant Infrastructure Configuration

This section describes the step-by-step process involved in onboarding a tenant on the NetApp storage device using the Flexpod ACI – Tenant Infrastructure Configuration workflow.

Step 1 Add a pod. For more information, see the Cisco UCS Director Administration Guide.

Step 2 Add the following types of accounts to the pod:

- Physical Compute—Cisco UCS Manager
- Physical Storage—NetApp Cluster-Mode
- Physical Network—APIC account. For more information, see Adding an APIC Account, on page 5.
- Virtual Account—VMware

For more information on how to create physical and virtual accounts, see the Cisco UCS Director Administration Guide.

Step 3 Add the pod to a resource group using the **Add Pod to Resource Group** option, to associate the accounts in the pod with the resource group. For more information, see Adding a Pod to a Resource Group, on page 37.

Step 4 Choose the resource group and click **Edit** to define the environment variable for each account. For more information, see Editing a Resource Group, on page 35.
The environment variables that you want to define for the NetApp tenant onboarding are:

- Virtual Compute
  - Container Parent Folder—The folder to which you want to add the newly created container.
- Virtual Storage—None.

- Virtual Network
    - VMM domain for VMware—This environment variable is used for onboarding a tenant. vCenter is configured with the Virtual Machine Manager (VMM) domain. When vCenter is associated with the APIC, the distributed virtual switch (DVS) with the same name is created in vCenter.

      Cisco UCS Director offers AVS support in both VLAN and VXLAN mode. The VM gets the VLAN ID or VXLAN ID from the pool assigned to the VMM domain. Choose VMM domain with Cisco AV switch to support AVS in VXLAN mode.
    - DV Switch—This environment variable is used for onboarding a tenant. The DV Switch is used to connect the selected host during tenant onboarding.
- Physical Compute
    - Physical Domain for UCS—This environment variable is used for baremetal provisioning. The physical domain for Cisco UCS.
    - Vlan Pool—The VLAN pool from which you want to assign a VLAN ID for the account.
- Physical Storage
    - Physical Domain for NetApp—The physical domain that is used to connect the NetApp account to the APIC.
    - Vlan pool—The VLAN pool that is used to create the cluster vServer.
    - SP Port—This environment variable is used for VNX-type accounts. The storage processor (SP) port for the physical storage account.
    - NFS Vlan Pool—This environment variable is used to define a VLAN pool. Individual VLANs are then assigned to physical storage account dynamically from the pool.
    - SVM mgmt Vlan Pool—The VLAN pool for management of a Storage Virtual Machine (SVM).
    - iSCSI_A VLAN Pool—The VLAN pool from which a VLAN is chosen as iSCSI_A VLAN.
    - iSCSI_B VLAN Pool—The VLAN pool from which a VLAN is chosen as iSCSI_B VLAN.
    - APIC vPC Static Path for Node 1—The static path of virtual port channel (vPC) for node 1.
    - APIC vPC Static Path for Node 2—The static path of virtual port channel (vPC) for node 2.
    - NFS IP Subnet Pool Policy—The subnet IP pool policy for NFS.
    - iSCSI_A IP Subnet Pool Policy—The IP subnet pool policy to be used for the first iSCSI VLAN.
    - iSCSI_B IP Subnet Pool Policy—The IP subnet pool policy to be used for the second iSCSI VLAN.
    - SVM mgmt IP Subnet Pool Policy—The subnet IP pool policy for SVM management.
    - VMNet IP Subnet Pool Policy—The subnet IP pool policy for VM network.
    - APIC Vlan Pool for Node 1—The APIC VLAN pool from which the VLAN ID must be assigned for node 1.
    - APIC Vlan Pool for Node 2—The APIC VLAN pool from which the VLAN ID must be assigned for node 2.
    - Cluster Node 1 Identity—The identity of the first Netapp C-mode account node.

    - Cluster Node 2 Identity—The identity of the second Netapp C-mode account node.

- Physical Network
    - IP Pool—The IP pool that is used to assign the IP addresses between the NetApp data store and host vmkernel.
    - DPC Static path 2—The static path of the second DPC.
    - L2 Physical Domain—The physical domain of Layer 2.

Note To onboard a tenant with Layer 2 configuration, set the value for the DPC Static Paths and L2 Physical Domain.

Step 5 Add a service offering and define the service class for each resource type (physical compute, physical storage, physical network, virtual compute, virtual storage, and virtual network). The service offering defines the resource requirements of tenant. For more information on how to add a service offering, see Adding a Service Offering, on page 41.

Step 6 Add a tenant profile. In the **Add Tenant Profile** dialog box, choose the service offering that you have added in Step 5 and add the resource group to the service offering. For more information on how to add a tenant profile, see Adding a Tenant Profile, on page 51.

Step 7 Edit the Flexpod ACI – Tenant Infrastructure Configuration workflow to enter the mandatory input values as follows:

a) Choose **Policies** > **Orchestration** and click the **Workflow** tab.
b) Choose **APIC Usecases > Tenant Usecases > NetApp Storage Tenant Usecases**.
c) Choose the Flexpod ACI – Tenant Infrastructure Configuration and click **Edit Workflow**.
d) In the **Edit Workflow Details** screen, do the necessary changes.
e) Click **Next**.
f) In the **Edit User Inputs** screen, set the values for mandatory parameters.

- Set the values for VM over subscription, CPU reservation, maximum number of subnets, and maximum number of tiers per VDC. For instance, you can set the values as:
    - Maximum number of Subnets—32
    - Maximum number of Tiers per VDC—8
    - VM Over Subscription—5
    - CPU Reservation (MHz)—2000

g) Click **Next**.
h) Click **Submit**.

Step 8 Choose the Flexpod ACI – Tenant Infrastructure Configuration workflow and click **Validate Workflow** to validate the workflow.

Step 9 Double-click the Flexpod ACI – Tenant Infrastructure Configuration workflow.

Step 10 In the **Workflow Designer** dialog box, click **Edit Workflow Properties** to view the tasks and edit user inputs that are used for task-input mapping for this workflow, if necessary.

Step 11 Add an advanced type catalog for onboarding a tenant and publish the catalog as follows:

a) On the menu bar, choose **Policies** > **Catalogs**.
b) Click **Add**.
c) From the **Catalog Type** drop-down list, choose **Advanced**. Click **Submit**.

d) In the **Add Catalog** dialog box, enter the basic information for the catalog.

e) Click **Next**.

f) In the **vApp Workflow** screen, click **Select** and choose the Flexpod ACI – Tenant Infrastructure Configuration workflow.

g) Click **Submit**.

Step 12 After publishing a catalog, you can onboard a tenant in one of the following ways:

- Creating a service request.

  1 On the menu bar, choose **Organizations** > **Service Requests**.

  2 Click the **Service Requests** tab.

  3 Click **Create Request**.

  4 In the **Create Service Request** dialog box, choose the **Group**, **Catalog Type** (Advanced), and the **Catalog** (that is created in Step Step 11).

  5 Click **Next**.

  6 In the **Custom Workflow** screen, provide the custom workflow input values. You have to provide the IP range for the IP subnet pool. Each container gets a unique subnet address from the IP subnet pool. By default, the overlapping of the IP addresses is not allowed. If you want to enable the IP address overlapping for the tiers, check the **Create Shared IP Subnet Pool** check box.

  7 Review the summary for the service request.

  8 Click **Submit**.

- Using the userAPISubmitVAppServiceRequest REST API.

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

  2 Click the **REST API Browser** tab.

  3 Enter **userAPISubmitVAppServiceRequest** in the **Search** field at the top right corner of the **Rest API Browser** tab.

  4 Double-click **userAPISubmitVAppServiceRequest**. The REST API browser displays the following tabs: API Examples, Details, and Summary.

  5 In the **API Examples** tab, click **Generate URL**.

  6 In the param0 variable, pass the catalog name.

  7 In the param1 variable, pass such tenant details as tenant name, tenant description, tenant profile, tenant service offering, tenant contact email address, tenant SVM admin password, data store capacity, data store capacity unit, data store storage snapshot policy, SVM root volume load sharing (LS) snapmirror schedule, memory reservation in MB, number of CPUs, number of VDCs, L2 or L3 external network configuration, L2 VLAN ID, and L2 IP Subnet address.

  8 Click **Execute REST API**. The REST API browser displays the service request ID in the **Response** field.

  9 Choose **Organizations** > **Service Requests**. In the **Service Request** tab, choose the service request and click **View Details** to view the workflow status and log details of the service request.

Example: Tenant Onboarding with Private Network(s)

This workflow is used to onboard a tenant using only the APIC account and VMware account. This section describes the step-by-step process involved in onboarding a tenant with multiple private networks, using the APIC account and VMware account.

Note This example is validated using SDX with VPX instances in one-arm mode.

Before You Begin

- Ensure that appropriate tags are created for VMware cluster, data store cluster, and data stores. Also ensure that these tags are used to tag the VMware cluster, data stores cluster, and data stores in virtual compute and virtual storage, manually.
- Ensure that the ESXi clusters and hosts are defined.
- Ensure that the data store and data store clusters are defined.

Step 1 Add a pod. For more information, see the Cisco UCS Director Administration Guide.

Step 2 Add the following types of accounts to the pod:

- Physical Network—APIC account. For more information, see Adding an APIC Account, on page 5.
- Virtual Account—VMware

For more information on how to create physical and virtual accounts, see the Cisco UCS Director Administration Guide.

Step 3 Add the pod to a resource group using the **Add Pod to Resource Group** option, to associate the accounts in the pod with the resource group. For more information, see Adding a Pod to a Resource Group, on page 37.

Step 4 Choose the resource group and click **Edit** to define the environment variable for each account. For more information, see Editing a Resource Group, on page 35.
The environment variables that you need to define for the tenant onboarding are:

- Virtual Compute
  - ◦ Container Parent Folder—The folder to which you want to add the newly created container.
  - ◦ IP Subnet Pool Policy—This environment variable is used for provisioning a container. The APIC container uses the IP subnet pool policy that is defined in Cisco UCS Director. Each tier inside the container gets a unique subnet address from the IP subnet pool policy.
- Virtual Storage—None.
- Virtual Network

  - VMM domain for VMware—This environment variable is used for onboarding a tenant. vCenter is configured with the Virtual Machine Manager (VMM) domain. When vCenter is associated with the APIC, the distributed virtual switch (DVS) with the same name is created in vCenter.

    Cisco UCS Director offers AVS support in both VLAN and VXLAN mode. The VM gets the VLAN ID or VXLAN ID from the pool assigned to the VMM domain. Choose a VMM domain with the Cisco AV switch to support AVS in the VXLAN mode.

  - DV Switch—This environment variable is used for onboarding a tenant. The DV Switch is used to connect the selected host during tenant onboarding.

- Physical Network
  - L3 Domain—This environment variable is used to configure the external routed network. The Layer 3 domain of the APIC account.
  - Path 1 to L3Out—The first transit path from the ACI Leaf to external router.
  - Path 2 to L3Out—The second transit path from the ACI Leaf to external router.
  - L3 Vlan Pool—This environment variable is used to configure the external routed network. The pool to be used to get the VLAN ID that is used to communicate between the router and Nexus.
  - Router IP Pool—This environment variable is used to configure the external routed network. The IP pool to configure a router ID for any routers on an external Layer 3 network.
  - SVI IP Pool—This environment variable is used to configure the external routed network. The subnet for configuring a switch virtual interface (SVI) on APIC leaves.
  - Node—This environment variable is used for creating transit EPG. The leaf nodes of the APIC account.
  - SVI Path—This environment variable is used to configure the external routed network. The interface connecting APIC to a router on an external Layer 3 network.
  - L2 Physical Domain—This environment variable is used for configuring transit EPG. The physical domain for Layer 2.
  - L2 Transit Vlan Pool—This environment variable is used for creating transit EPG. The pool to be used to get the VLAN ID for the transit EPG.
  - LB Cluster IP Pool—The IP pool to provide the cluster management IP address for the load balancer device cluster.

Step 5 Add a service offering. During addition of the service offering, ensure that you check the **Override Mandatory Service Class Requirement** check box and define the service class for each resource type (physical network, virtual compute, virtual storage, and virtual network). The service offering defines the resource requirements for the tenant. For more information on how to add a service offering, see Adding a Service Offering, on page 41.

Step 6 Add a tenant profile. In the **Add Tenant Profile** dialog box, choose the service offering that you added in Step 5 and add the resource group to the service offering. For more information on how to add a tenant profile, see Adding a Tenant Profile, on page 51.

Step 7 To onboard a tenant with multiple private networks, execute the tenant onboarding workflow as follows:

a) Choose **Policies** > **Orchestration** and click the **Workflow** tab.
b) Choose **APIC Usecases > Tenant Usecases**.
c) Choose the Tenant Onboarding with Private Network(s) workflow and click **Execute Now**.

d) In the **Executing Workflow: Tenant Onboarding with Private Network(s)** screen, complete the following fields:

Field	Description
Tenant Profile field	Click **Select** and choose a tenant profile that was added in Step 6.
Service Offering field	Click **Select** and choose a service offering that was added in Step 5.
Tenant Name field	The name of the tenant.
Tenant Description field	The description of the tenant.
Group Admin Username field	The username of the group administrator who can access the tenant.
Group Admin Password field	The password to access the tenant.
Group Admin Email field	The email address of the group administrator who can access the tenant.
No of VDCs field	Number of virtual data centers (VDCs) that are needed for the tenant. **Note** The number of VDCs determines the subnet size for the supernets provided (while tenant onboarding) for each tier of the application container.
Automatic Datastore Selection check box	Check this check box to choose data stores and data store clusters based on the selected generic VMware cluster.
VMWare ESXi Cluster field	Click **Select** and choose a VMware ESXi cluster based on the VMware account available in the resource group.
VMWare Datastore Clusters field	This field is optional if the **Automatic Datastore Selection** check box is checked. Click **Select** and choose one or more VMware data store clusters which have the matching data stores, from the selected VMware ESXi cluster. The selected data store clusters are added to the vPOD.
VMWare Datastores field	This field is optional if the **Automatic Datastore Selection** check box is checked. Click **Select** and choose one or more VMware data stores from the selected VMware ESXi cluster based on the application tier tag value mapping and the data store size requirement during the onboarding. The selected data stores are added to the vPOD.

Field	Description
Area ID field	The identification (ID) of an area that is a logical collection of networks, routers, and links which have the same area identification.
Private Network Profile field	Click the add icon to add a private network to the tenant. In the **Add Entry to** dialog box, complete the following fields: • Private Network—The name of the private network. • Subnets—The subnetwork pool that is used for load-balancer configuration during the container deployment. At least two subnetworks must be defined for the load-balancer configuration. For example, subnetwork for load balancer 1 is 10.1.1.0/24 and subnetwork for load balancer 2 is 10.1.2.0/24. • Supernets—The supernetwork for the tiers. Add supernetwork for tier 1, tier 2, and tier 3. For example, supernetwork for tier 1 is 10.1.3.0/24, supernetwork for tier 2 is 10.1.4.0/24, and supernetwork for tier 3 is 10.1.5.0/24. • Click **Submit**.

e) Click **Submit**.

Note If the resources are not available in accordance with the container-tier tag mapping, the container provisioning fails.

Offboarding a Cisco UCS Director Tenant

Step 1 On the menu bar, choose **Policies** > **Resource Groups**.

Step 2 Click the **Tenant Profile** tab.

Step 3 Choose a tenant profile and click **View Details**.
The tenants that are onboarded using the tenant profile appear.

Step 4 Choose the tenant that you want to offboard and click **Delete**.

Step 5 In the **Tenant** dialog box, click **Delete** to confirm deletion of the tenant.
The service request that was created related to the tenant is rolled back.

Note Alternately, you can delete a tenant from the **Tenant** tab (**Policies** > **Resource Groups**). In the **Tenant** tab, choose the tenant and click **Delete**.

If the tenant is associated with a container, an error message is displayed. Roll back the service request to completely clean up the resources and container associated with the tenant. You can roll back the service request by using the **Archive** action (**Organizations** > **Service Requests**) or by using the userAPIRollbackWorkflow API.

CHAPTER 6

Deploying Multi-Tier Applications

This chapter contains the following sections:

About Multi-Tier APIC Application Deployment

To deploy a multi-tier Application Policy Infrastructure Controller (APIC) application in Cisco UCS Director, you must create or use an existing application profile. An application profile defines the following:

- The Application Centric Infrastructure (ACI) network tiers for delivering application resources for the associated tenant profile.
- The suitable resource group that in turn defines the capacity and quality of the Cisco UCS physical, virtual, compute, and storage resources for each application component.
- The ACI network services that are required to deliver the appropriate service quality and security for the application.

For more information about how to create an application profile and deploy a multi-tier APIC application using the APIC container, see the Cisco UCS Director Application Container Guide.