Cisco UCS Director Application Container 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

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.

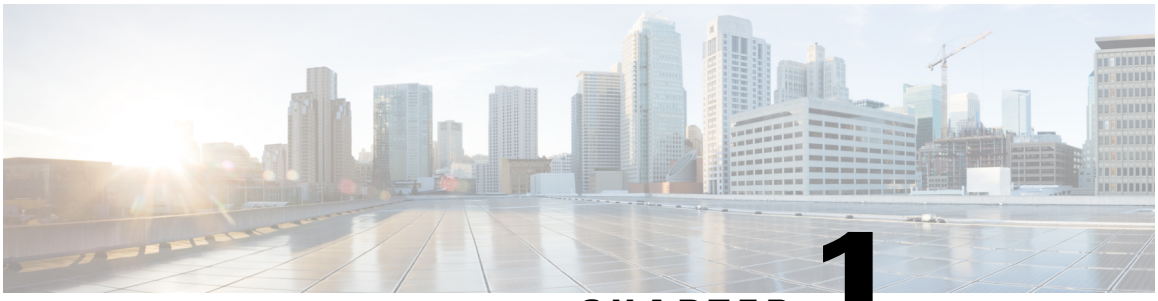
Documentation Feedback

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

This chapter contains the following sections:

New and Changed Information for this Release

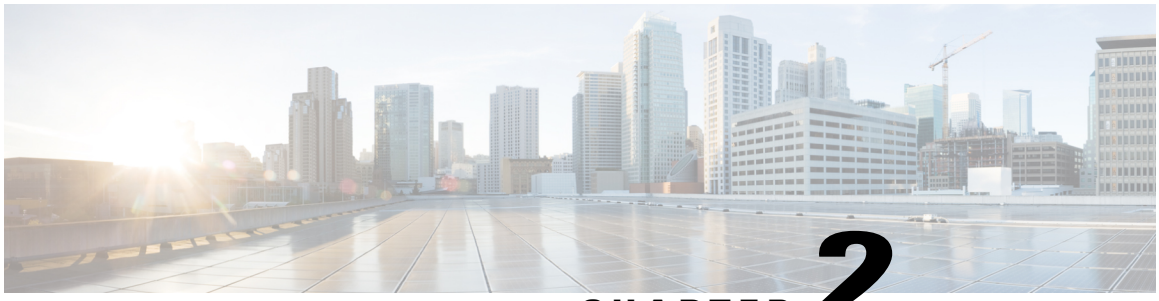
The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

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

Feature	Description	Where Documented
VM Naming Conventions	Specific naming convention is followed for the VM names when application is provisioned for the private network or when adding VMs to an APIC container.	Creating an Application Container Using a Template, on page 63, Adding VMs, on page 26
Support of ASAv9.3.2	You can choose the deployment option using which VM can be deployed. The deployment options are listed based on the OVF for ASAv 9.3.1, ASAv 9.3.2, and later.	Adding an ASAv VM Deployment Policy, on page 71

Feature	Description	Where Documented
Stateful ASA Failover	The configuration of a Cisco ASA firewall in high availability mode now supports stateful failover for the Cisco ASA. Stateful failover ensures that the active unit continually passes per-connection state information to the standby unit. If a failover occurs, this configuration ensures that the same connection information is available at the new active unit.	Adding a Layer 4 to Layer 7 Service Policy, on page 79
Support for Multi-Context Configuration	Layer 4 to Layer 7 policy must accommodate multiple contexts configurations on the ASA devices.	Adding a Layer 4 to Layer 7 Service Policy, on page 79
Support for advanced load balancer parameters	Network device system parameter policy sets the NTP and SNMP parameters that are needed to be configured on a load balancer device.	Adding a Network Device System Parameters Policy, on page 81
SSL Offload Support	The L4-L7 Policy for a load balancer now supports SSL offloading as well as basic load balancing through HTTP. SSL offloading moves the processing of SSL encryption and decryption from the main Web server to a separate device designed for that task. This features increases the performance of the Web server and improves the efficiency of SSL certificate handling. During deployment of an application container, you must provide an SSL certificate for the SSL offloading.	Adding an Application Profile, on page 84
Dynamic Subnet Size per Tier	The maximum number of VM instances per tier allows you to determine the subnet size for each tier.	Adding an Application Profile, on page 84
Support for Tags in Datastore	You can choose the tag values for each tier. During container provisioning, resource is selected based on the tag associated with the tier.	Adding an Application Profile, on page 84

Feature	Description	Where Documented
Application Profile Support for Hyper-V	You can also perform a container provisioning in the Hyper--V environment.	Adding an Application Profile, on page 84
Shared L3Out Feature	To integrate the ACI fabric with shared external Layer 3 network. The network must be tagged and updated on Tenant vPOD in advance and the same tag must be selected for the external network in case of shared L3Out.	Adding an Application Profile, on page 84
Loadbalancer vServer Support	The application container has the ability to view, add, or delete the load balancer L4-L7 services. The newly created VMs are added as real servers to the L4-L7 service .	Configuring L4-L7 Services, on page 111
Contract between Different Containers	You can view and add the contract between tiers of different containers in Cisco UCS Director. You need to drill down each contract to view all the security rules created for each application container in Cisco UCS Director.	Adding Contracts, on page 115
Add vNIC to Container VM	You can add vNIC to the container VM for private network communication between VMs belonging to same network zone.	Adding a Virtual Network Interface Card to a VM, on page 120
Container to show Virtual Routing and Forwarding instance	Added Virtual Routing and Forwarding (VRF) instance in the Tier summary of the Container report.	Viewing Application Container Information, on page 31



CHAPTER 2

Overview

This chapter contains the following sections:

Application Containers

Application containers are a templatized approach to provision the applications for end users. Each application container is a collection of VMware virtual machines (VMs) and baremetal servers (BMs). The application container has an internal private network that is based on rules specified by the administrator. An application container can have one or more VMs and BMs, and can be secured by a fencing gateway (for example, a Virtual Secure Gateway) to the external or public cloud.

Cisco UCS Director supports the application containers and enables you to define container templates with one or more networks and VMs or BMs. When an application container is created from a template, Cisco UCS Director automatically deploys the VMs or BMs and configures the networks and any application services. Cisco UCS Director also automatically configures virtual and physical switches for Layer 2 changes.

When you want to configure Cisco UCS Directorto provision the applications, create one or more application container templates with the appropriate policies, workflows, and templates. The application container template determines how the application is provisioned for the end user. It can define some or all of the following:

- Physical server or virtual machine
- Amount of reserved storage
- Maximum available CPU

- Maximum available memory
- Version of operating system
- Range of VLANs
- Gateway or firewall, if desired
- Load balancer, if desired
- Required approvals, if desired
- Costs associated with the application container, if desired

Cisco UCS Director supports multiple types of application containers. The type of application container that you want to implement depends upon your deployment configuration. The steps required to configure the application container depend upon which type you plan to implement.

Types of Application Containers

There are several application container types for use in various deployment scenarios:

- Fenced Virtual—The most common type of application container for use with VMs.
- Virtual Secure Gateway (VSG)—This container type is used to provide for enhanced security in virtual environments.
- Application Centric Infrastructure Controller (APIC) container—This container type is used in APIC deployments. For more information, see the Cisco UCS Director APIC Management Guide and Implementing Cisco Application Policy Infrastructure Controller Support in this guide.
- Fabric—This container type is used in Dynamic Fabric Automation (DFA) network deployments. For more information on application containers in a DFA network, see the Cisco UCS Director Unified Fabric Automation Guide.
- Virtual Application Container Services (VACS) container—This container type is used in deployments of Cisco Virtual Application Cloud Segmentation Services.

Note This container type is available in Cisco UCS Director only if the VACS modules are installed. For more information, see the Cisco Virtual Application Cloud Segmentation Services Configuration Guide.

Viewing Application Containers

To view application containers in Cisco UCS Director, do the following:

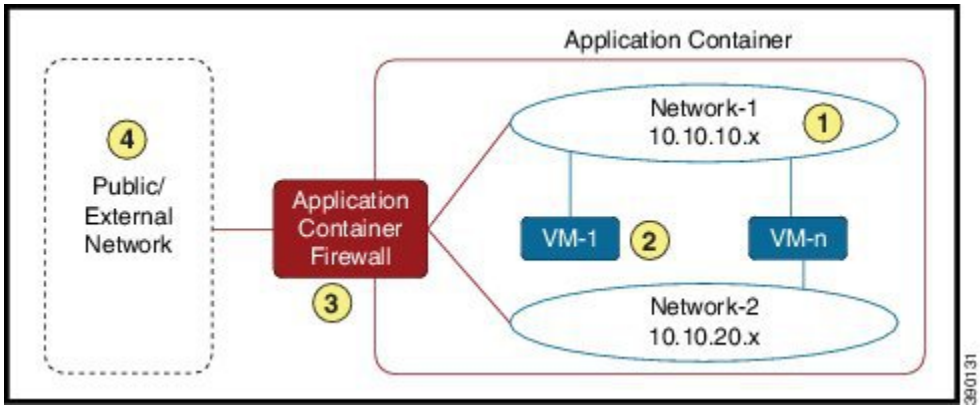
From the menu bar, choose **Policies** > **Application Containers**.
Application containers use a color scheme to identify the container's status:

- Green—All VMs and baremetal servers (BMs) are powered on, including the gateway (GW) if the container configuration includes a GW.
- Yellow—The GW VM is down and one or more of the VMs or BMs are powered on.
- Blue—Container provisioning is in progress, or container provisioning has halted with a failure.
- Gray—Container is empty of VMs and BMs.
- Red—All VMs and BMs, including the GW, are powered off.

Securing a Container Using an ASA Gateway

An example of an application container using an ASA gateway(firewall) is described in the figure and table below.

Figure 1: Example Application Container Secured Using an ASA Gateway (Firewall)



Region	Description
1	One or more internal networks using rules specified by an administrator.
2	One or more VMs attached to one or more networks.
3	A fencing gateway (firewall). In this example an Adaptive Security Appliance (ASA) is used. An ASA allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.
4	Public/external network.

There are several steps required to create and manage an application container using a ASA gateway:

1 **Define gateway policy—**In the gateway policy, you must define the gateway type for the container and on which cloud account (vCenter) the gateway gets deployed.

2 **Define an application container template—**You must define the cloud account on which the container is created, as well as, performing several other tasks:

Note The steps are different for creation of an APIC container. See APIC Application Container Creation Process, on page 70.

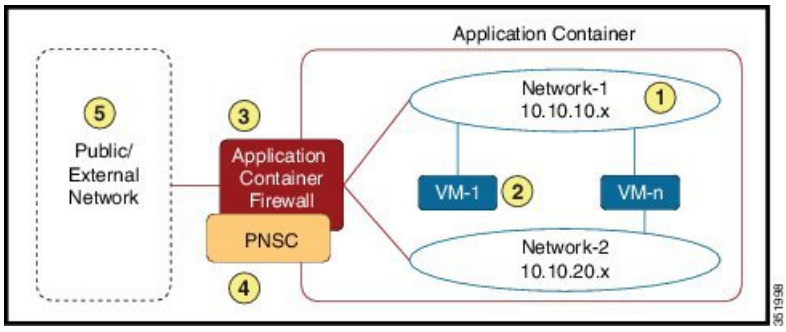
- Configure the network
- Add VMs for the container
- Define port mapping and outbound access control lists (ACLs)
- Choose a gateway policy (created earlier)
- Choose the deployment policies that define VM provisioning
- Choose self-service options for the container
- Choose a workflow (optional)

3 **Create an application container from the defined container template—**An application container is created from the template defined in step 2. You must choose a group for which the container is created.

4 **Application container—**After creating the application container, you can do various management actions, such as power management of the container, adding VMs to a container, cloning or deleting the container, and opening a console for VMs and viewing the reports.

Securing a Container Using a Cisco Virtual Security Gateway

Figure 2: Example Application Container Using a Cisco VSG



Region	Description

1	One or more internal networks using rules specified by an administrator.
2	One or more VMs attached to one or more networks.
3	A fencing gateway (firewall). In this example an Adaptive Security Appliance (ASA) is used. An ASA allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.
4	Cisco Prime Network Security Controller (PNSC) contributes to the deployment of an overlay network, facilitates network services insertion, and enables virtual machine mobility between private and public clouds
5	Public/external network.

Note To create application containers with a Cisco Virtual Security Gateway (VSG) you must meet the following prerequisites:

- Public IP addresses for the Cisco VSG and external gateway must be provided.
- In the Computing Policy all of the hosts need to be associated with a Cisco Nexus 1000 series switch.
- In the Storage Policy you must select the data store associated with the Cisco Nexus 1000 series switch's (associated) host.
- All of the VLAN (IP address) range settings should be pre-configured in the Cisco Nexus 1000 series switch.

There are several steps required to create and manage an application container secured with a Cisco VSG:

1 **Create a PNSC account**

2 **View PNSC reports**

3 **Create a PNSC firewall policy**

4 **Integrate a Cisco VSG into a application container—**This process involves several tasks:

- Upload an OVF file
- Deploy an OVF file
- Create an application container template for a Cisco VSG

Orchestration Tasks for Network Device Management

Cisco UCS Director includes orchestration features that allow you to automate configuration and management of network domain devices in workflows.

A complete list of the network device 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.

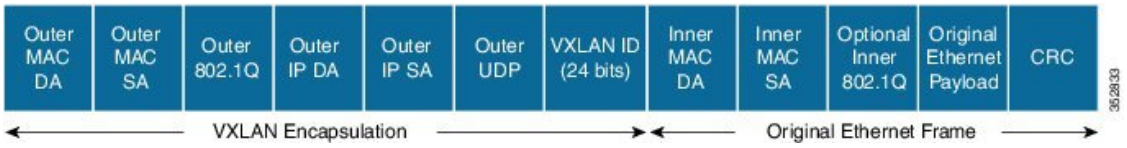
Application Container Support for Cisco VXLANs

Cisco UCS Director supports the use of VXLANs in application containers.

Note APIC containers do not support VXLANs.

Cisco VXLAN is a Layer 2 network isolation technology that is supported by the Cisco Nexus 1000V Series Switch. VXLAN uses a 24-bit segment identifier to scale beyond the 4K limitations of VLANS. VXLAN technology creates LAN segments by using an overlay approach with MAC in IP encapsulation. The Virtual Ethernet Module (VEM) encapsulates the original Layer 2 frame from the virtual machine (VM).

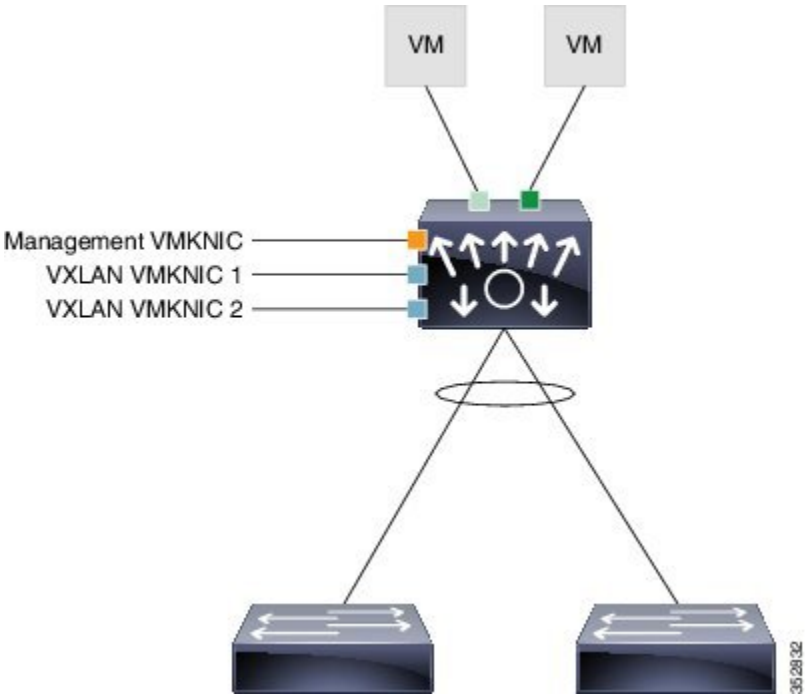
Figure 3: VXLAN encapsulated frame format



Each VEM is assigned an IP address, which is used as the source IP address when encapsulating MAC frames to be sent on the network. This is accomplished by creating virtual network adaptors (VMKNICs) on each

VEM (see figure below). You can have multiple VMKNICs and use them for this encapsulated traffic. The encapsulation carries the VXLAN identifier, which is used to scope the MAC address of the payload frame.

Figure 4: VEM VMKNIC interface with VXLAN Capability



The connected VXLAN is specified within the port profile configuration of the vNIC and is applied when the VM connects. Each VXLAN uses an assigned IP multicast group to carry broadcast traffic within the VXLAN segment. When a VM attaches to a VEM, if it is the first to join the particular VXLAN segment on the VEM, an Internet Group Management Protocol (IGMP) join is issued for the VXLAN's assigned multicast group.

When the VM transmits a packet on the network segment, a lookup is made in the Layer 2 table using the destination MAC of the frame and the VXLAN identifier. If the result is a hit, the Layer 2 table entry will contain the remote IP address to use to encapsulate the frame, and the frame will be transmitted within an IP packet destined for the remote IP address. If the result is a miss (including broadcast/multicast/unknown unicasts), the frame is encapsulated with the destination IP address set to be the VXLAN segment's assigned IP multicast group.

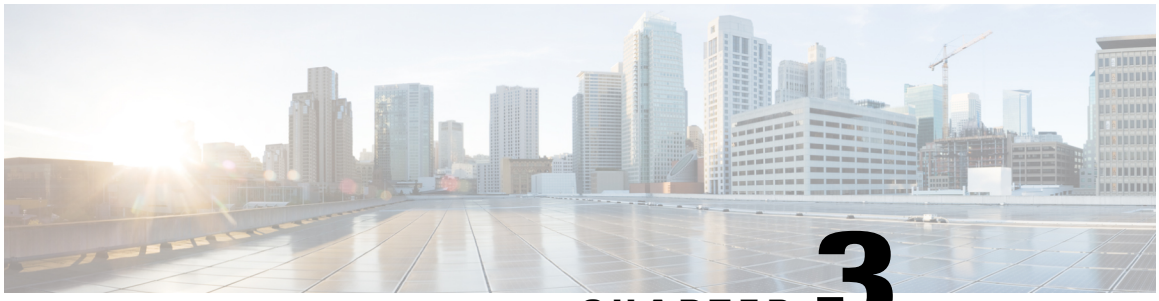
Note The VXLAN format is supported only by the Cisco Nexus 1000V Series Switch.

ASAv Gateway

Cisco UCS Director provides the ability to create an application container that makes use of an Adaptive Security Virtual Appliance (ASAv) gateway. The Cisco ASAv supports both traditional tiered data center deployments and the fabric-based deployments of Cisco Application Centric Infrastructure (ACI) environments. The ASAv provides consistent, transparent security across physical, virtual, application-centric, SDN, and cloud environments.

The ASAv brings firewall capabilities to virtualized environments to secure data center traffic within multi-tenant architectures. Because it is optimized for data center environments, the ASAv supports vSwitches. The ASAv can therefore be deployed in Cisco, hybrid, and even non-Cisco data centers, significantly reducing administrative overhead and improving flexibility and operational efficiency.

For ACI deployments, the Cisco Application Policy Infrastructure Controller (APIC) provides a single point of control for both network and security management. APIC can provision ASAv security as a service, manage policy, and monitor the entire environment for a unified view of the entire distributed infrastructure. Many APIC functions can be controlled through UCS Director, including creation and deletion of ASAv gateways.



CHAPTER 3

Creating Application Containers

This chapter contains the following sections:

General Application Container Creation Process

The following process explains the creation of an application container in Cisco UCS Director, such as a fenced virtual application container: The following sections in this chapter provide detailed procedures for completing each step.

Note The process for creating an Application Centric Infrastructure Controller (APIC) managed container is different. For APIC containers, refer to APIC Application Container Creation Process, on page 70.

1. If a gateway is required, create a tiered application gateway policy.
2. If a load balancer is required, create a load balancer policy.
3. Create a virtual infrastructure policy to define the cloud account, the type of container and, if appropriate, the tiered application gateway and load balancer policies.
4. Create an application container template.
   a. Add networks (one network per application tier).
   b. Add virtual machines and baremetal servers.
   c. Add a compute policy, storage policy, network policy, and systems policy. If desired, you can also add a cost model.

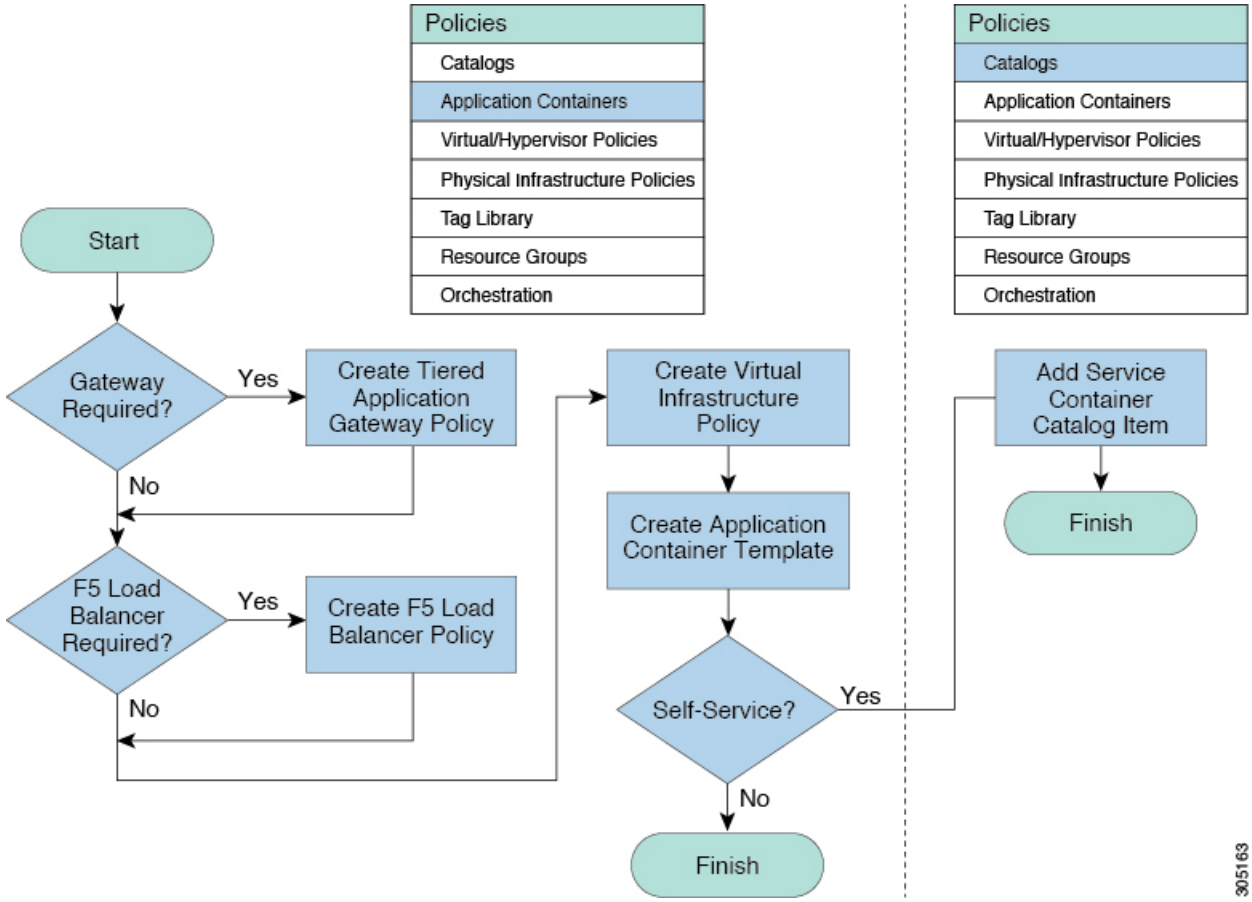
d Add an end user self-service policy and configure the self-service options.

e Add the container setup workflow required to deliver the service offering to the user as part of a service request. The workflow must consider the type of container and the application to be provisioned.

5 Create a container based on the container template.

The figure illustrates the creation of the general application container template within Cisco UCS Director.

Figure 5: Process for Creating a General Application Container Template



Creating Application Container Policies

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

Step 2 Click the **Virtual Infrastructure Policies** tab.

Step 3 Click the **Add Policy** button.

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

Name	Description
Policy Name field	The name of the policy.
Policy Description field	The description of the policy.
Container Type drop-down list	Choose a container type: APIC, Fenced Virtual, VSG, or Fabric.
Select Virtual Account drop-down list	The chosen virtual account (the cloud on which the gateway VM is created).

Step 5 If you chose **Fabric** for your Container type, go to step 6. However, if you chose **Fenced Virtual**, **APIC** or **VSG**, see the following table for what to do next:

Option	Description
Fenced Virtual	Click **Next** and follow the wizard prompts.
APIC	See Creating a Virtual Infrastructure Policy , on page 108
VSG	See Creating a Virtual Infrastructure Policy, on page 43

Step 6 Continue with this step if you chose **Fabric** for your Container type in step 4. In the **Virtual Infrastructure Policy - Fabric Information** dialog box, complete the following fields:

Name	Description
With VSG check box	Check the check box for VSG support. If checked, complete the following: 1 Enter information for the **Service Network Configuration** and **Host Network Configuration**. 2 Go to step 7 to complete the remaining prompts of the wizard. If unchecked, go to step 9.
Fabric account drop-down list	Choose a fabric account.
Switch Type drop-down list	Choose a switch type.
Switch Name drop-down list	Choose the name for the switch.
Alternate Switch Namedrop-down list	Choose an alternate switch name.
Service Network Configuration	
Mobility Domain Id(Service Network + HA) field	If the **AutoSelect Mobility Domain Id** check box is not checked, click **Select** to add the mobility domain id.

Name	Description
Layer 3 check box	Check the check box for Layer 3 support. **Note** You must complete the required predeployment set up for Layer 3 support which includes vpath partition, and service and classifier network setup. This can be completed by creating and executing an orchestration workflow that contains the following tasks from the task library: • Create Fabric Organization (Create vPath Organization) • Create Fabric Partition (Create vPath partition) • Create Fabric Network (Create vPath classifier network) • AddHostVMKernelPortondvSwitch (Add vmknics to N1kv VEM Cluster) • Create Fabric Network (Create vPath Service Network)
Fabric Organization drop-down list	Choose the fabric organization.
Fabric Partition drop-down list	Choose the fabric partition.
Fabric Service Network field	Click **Select** to add the fabric service network.
Host Network Configuration	
Mobility Domain Id(Service Network + HA) field	If the **AutoSelect Mobility Domain Id** check box is not checked, click **Select** to add the mobility domain ID. **Note** If it is Layer 2, the Mobility Domain of the service network and corresponding host network must be the same as the service network, or can be none.
Partition Parameters	
DCI ID field	Enter the DCI ID.
Extend the partition across the fabric check box	Check the check box to enter the partition across the fabric.
Service Node IP Address field	Enter the IP address for the service node.
DNS Server field	Enter the DNS Server.
Secondary DNS Server field	Enter the secondary DNS Server.

Name	Description
Multi Cast Group Address field	Enter the multi-cast group address.
Profile Name field	Click **Select** to add the profile name.

Step 7 Click **Next**.

Step 8 Continue with this step only if you checked the **With VSG** check box in the previous step. In the **Virtual Infrastructure Policy - PNSC Information** complete the following:

Name	Description
PNSC Account drop-down list	Choose a PNSC account.
VSG Template Configuration	
PNSC Firewall Policy	Choose a PNSC Firewall Policy.

Step 9 Click **Next**.

Step 10 In the **F5 Load Balancer Information** dialog box, complete the fields for the F5 Load Balancer.

Step 11 Click **Next**.

Step 12 In the **Virtual Infrastructure Policy - Gateway** dialog box, check the **Gateway required** check box if you want to add a gateway.

Step 13 Click **Next**.

Step 14 In the **Summary** dialog box, click **Submit**.

About Application Container Templates

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

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

Note For more information regarding the container templates and Virtual Secure Gateways (VSGs), see Creating an Application Template for a VSG, on page 45.

Creating Application Container Templates

Before you create an application container, you must create a template.

Note For more information on creating the container templates for use with a VSG, see Creating an Application Template for a VSG, on page 45.

Note With this template, you can create application containers for use in various networks (including DFA Networks). Changes to the template will not affect the existing application containers created with the template. This topic describes the creation of a fenced virtual application container template. The content displayed on your screens may vary slightly depending upon settings in your policy.

Before You Begin

Create a virtual infrastructure policy. See Creating Application Container Policies, on page 14.

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

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

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

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

Step 4 Click **Next**.

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

Name	Description
Select Virtual Infrastructure Policy drop-down list	Choose a policy.

Step 6 Click **Next**.

Step 7 If you chose a fabric-based virtual infrastructure policy in the **Fabric Networks** screen, click the **(+) Add** icon to add a fabric network and complete the following fields; however, if you chose any other virtual infrastructure policy go to step 10.

Name	Description
External Partition check box	Check the check box to enable the host network for the ASA external partition.
Network Name field	A unique name for the network within the container. You can use a maximum of 128 characters,
Network Role	Choose a network role.
Description	The description of the network.
Multicast Group Address	The multicast group address.
Profile Name	Click **Select** to choose a profile.
Gateway IP Address	The IP address of the default gateway for the network.
Network Mask	The network mask (for example, 255.255.255.0).
DHCP Serverv6 Address	The DHCP server address
vrfdhcp field	The VRF DHCP address
mtuvalue field	The maximum transmission unit (MTU) value.
vrfv6dhcp field	The VRF DHCP address.
Gateway IP v6Address	The gateway IPv6 address.
Prefix Length field	The prefix length.
DHCP Scope	
DHCP Enabled check box	Check the check box to enable DHCP.
Service Configuration Parameters	
Start IP field	The start IP address.
End IP field	The end IP address.
Secondary Gateway field	The secondary gateway address.

Step 8 Click **Submit**.

Step 9 Click **Next**.

Step 10 Continue with this step if you did *not* choose Fabric-based virtual infrastructure policy in step 5. Otherwise, go to step 14 to define VMs.
The **Application Container: Template - Internal Networks** screen appears. You can add and configure multiple networks for a container. These networks are applicable to the VM that is provisioned using this template.

Step 11 Click the **(+) Add** icon to add a network. Complete the following fields:

Name	Description
Network Name field	Enter unique network name for the container. You can use a maximum of 128 characters.
Network Type drop-down list	Choose a network type.
Information Source drop-down list	Choose the information source. It can be one of the following: • Inline • Static Pool
VLAN ID Range field	Enter a VLAN ID range.
Network IP Address field	The IP address of the network (for example, 10.10.10.0). A unique subnet is chosen for each internal network.
Network Mask field	The network mask (for example, 255.255.255.0).
Gateway IP Address field field	The IP address of the default gateway for the network. A NIC with this IP is created on the GW VM.

Step 12 Click **Submit**.
Next, you can add and configure the VM that will be provisioned in the application container.

Step 13 Click **OK**.

Step 14 Click the **Add (+)** icon to add a VM. The **Add Entry** screen appears. Complete the following fields:

Name	Description
VM Name field	The VM name.
Description field	The description of the VM.
VM Image drop-down list	Choose the image to be deployed.
Number of Virtual CPUs drop-down list	The number of virtual CPUs to be allocated to the VM.

Name	Description
Memory drop-down list	The memory to be allocated (in MB).
CPU Reservation (MHz) field	The CPU reservation for the VM.
Memory Reservation (MB) field	The memory reservation for the VM.
Disk Size (GB) field	The custom disk size for the VM. To use the template disk size, specify the value of 0. The specified disk size overrides the disk size of the selected image.
VM Password Sharing Option drop-down list	Choose an option for how to share the VM's username and password with the end users. If **Share after password reset** or **Share template credentials** is chosen, the end user needs to specify a username and password for the chosen templates.
Use Network Configuration from Image check box	If checked, use the network configuration from the image and the configuration is applied to the provisioned VM.
VM Network Interface field	Choose the VM network interface information.
Maximum Quality field	The maximum number of instances that can be added in this container after it is created.
Initial Quality field	The number of VM instances to provision when the container is created.

Step 15 Click **Next**.

Step 16 Continue with this step if you did *not* choose Fabric-based virtual infrastructure policy in step 5. Otherwise, go to step 18.

In the **Application Container Template - External Gateway Security Configuration** screen, click the **Port Mappings (+) Add icon** to add port mappings. Complete the following fields:

Name	Description
Protocol drop-down list	Choose a protocol. It can be one of the following: • TCP • UDP
Mapped Port field	Enter the mapped port.
Remote IP Address field	Enter the IP address
Remote Port field	Enter the remote port field.

Step 17 In the **Application Container Template - External Gateway Security Configuration** screen, click the **Outbound ACLs (+) Add icon** to add port mappings. Complete the following fields:

Name	Description
Protocol drop-down list	Choose a protocol. It can be one of the following: • IP • TCP • UDP • ICMP
Select Network drop-down list	Choose a network.
Source address field	Enter a source address.
Destination address field	Enter a destination address.
Action field	Choose an action. It can be one of the following: • Accept • Drop • Reject

Step 18 Click **Next**. The **Application Container: Template - Deployment Policies** screen appears.
You must select the compute, storage, network, system policy, and cost model required for VM provisioning. A policy is a group of rules that determine where and how a new VM is to be provisioned within an application container (based on the availability of system resources).

- The network policy is used only to deploy the outside interface of the virtual firewall (container gateway).

  Note If the gateway type is CISCO ASAv for the container, the network policy must first add the ASAv management interface and then the outside interface in the VM networks, in the same order.

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

Complete the following fields:

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

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

Step 19 Click **Next**. The **Application Container: Template - Options** screen appears.
In this page, you can select options to enable or disable certain privileges for the self-service end user. Complete the following fields:

Name	Description
End User Self-Service Policy drop-down list	Choose a self-service policy for end users.
Enable Self-Service Deletion of Containers check box	Check to allow end users to delete application containers created with this template.

Name	Description
Enable VNC Based Console Access check box	Check to allow virtual network computing (VNC) access to VMs on the container host.
Technical Support Email Address text field	Enter a comma-separated list of email addresses. Automated notifications are sent to these emails.

Step 20 Click **Next**. The **Application Container: Template - Setup Workflows** screen appears. Complete the following field:

Name	Description
Container Setup Workflow drop-down list	Choose a container setup workflow. By default, a workflow is not selected. You can skip this step if the gateway type chosen for this container is **Linux** and the **Virtual Machine Portgroup** is selected in the network policy associated with the container. Choosing a specific workflow is required only if you chose CISCO ASA as the container gateway or **Distributed Virtual Portgroup** as the network policy. For a CISCO ASAv gateway type, choose the **Application Container with ASAv Gateway**. **Note** You must perform some prerequisite steps before you can initiate the task for creating an application container template.

Step 21 Click **Next**. The Application Container Template - Summary screen appears, displaying your current settings.

Step 22 Click **Submit** to complete the creation of the application container template.

What to Do Next

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

Creating a Custom Workflow for Application Containers

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

Note You cannot create an APIC application container by running a workflow directly. For information on creating the APIC application containers, see APIC Application Container Creation Process, on page 70.

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

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

  1 Choose **Virtual Network Type** and enter its name as required in a workflow associated with the container.

  2 Choose a specific workflow. This type of workflow depends on which gateway type was associated with the container. For a Linux gateway, choose **Application Container Setup** workflow. For a CISCO ASA gateway type, choose the **Application Container with ASA Gateway**.

  3 Edit or clone the required workflow by going to the Cisco UCS Director Orchestrator application and editing the workflow on the **Workflow Designer** page.

  4 In the workflow window, double-click the **Allocate Container VM Resources** task.

  5 Choose the required virtual network type (either **Distributed Virtual Portgroup** or **Distributed Virtual Portgroup N1K**).

  6 Specify the primary DVSwitch and alternate DVSwitch names.

  7 Click **Save** to save the workflow.

Managing Application Containers

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

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

Viewing Container Actions

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

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

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

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

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

Note If there are too many action icons to display across the top of the **Application Container** tab, you can display the actions drop-down list by clicking the drop-down icon at the top right corner of the tab.

You can select a container action from the action icons or from the actions drop-down list.

Adding VMs

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

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

Step 2 Click the **Application Containers** tab.

Step 3 Choose a container.

Step 4 Click **Add VMs**.

Step 5 In the **Add VMs** dialog box, click the **Add (+)** icon to add a new VM.

Step 6 From the **Network** drop-down list, choose the network (tier) to which to add the VM.

Step 7 Define the Virtual Machine:

To use a template defined in the application profile, check the **Use Predefined Template** check box.

If instead you want to define the VM using an image and setting the parameters by hand, skip to Step 9.

Step 8 In the Add Entry dialog box, complete the following fields:

Name	Description
Network drop-down list	Select the network (tier) on which to add the VM.
VM Name drop-down list	Enter the name of the VM as defined in the application profile.
Select DRS Rule button	Click the button, then select a distributed resource scheduler (DRS) rule (also called an affinity rule) from the list.
No Of Instances drop-down list	The number of VM instances to create. The drop-down list limits your choices so as not to exceed the maximum number of VMs defined in the application profile.

Skip to Step 10.

Step 9 In the **Add Entry** dialog box, complete the following fields:

Name	Description
Network drop-down list	Select the network (tier) on which to add the VM.

Name	Description
VM Name text box	The name you want to assign the VM. During application container deployment, you can update the prefix from what is defined in the application profile.
VM Image drop-down list	The VM image to use. You define these VMs in the vCenter for your cluster.
Number of vCPUs drop-down list	Select the number of virtual CPUs for the VM.
Memory (MB) drop-down list	The size of the VM memory.
Disk Size (GB) text box	The size of the VM disk. If you enter zero, the VM uses the disk size defined in the image.
Select DRS Rule button	Click the button, then select a distributed resource scheduler (DRS) rule (also called an affinity rule) from the list.
Select Storage DRS Rule button (optional)	If you selected a DRS rule using the **Select DRS Rule** button, the **Select Storage DRS Rule** button appears. Click the button, then select a storage DRS rule from the list.
VM Password Sharing Option	The password sharing policy for this VM. Default is to not share the root password.
Network Adapter Type drop-down list	The network adapter for the VM.
Initial Quantity	The number of VMs to create on application startup.

Step 10 Click **Submit**.

Step 11 To create more VMs, repeat the procedure starting with Step 5.

Step 12 When you have defined all the VMs you want, click **Submit** in the **Add VMs** dialog.

Deleting VMs

Before You Begin

- Create and deploy an existing application container with one or more VMs.

- Power off the VMs you want to delete.

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

Step 2 Choose an application container.

Step 3 Click **Decommission Container**.

Step 4 From the list of VMs, select the VM or VMs that you want to delete.

Note The list shows only VMs that are powered off.

Step 5 Click **Submit**.

Step 6 In the confirmation dialog, click **OK**.
The VM is deleted from the selected container.

Accessing a VM Console

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

Before You Begin

Enable access for VMs that you want to access using VNC. See Enabling VNC Console Access, on page 29.

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

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

Step 3 Choose a container.

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

Step 5 From the **Select VM** drop-down list, choose a VM.

Step 6 Click **Submit**. A console of the selected VM opens in a new browser window.

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

Enabling VNC Console Access

To enable console access on an individual VM, follow this procedure:

Step 1 Select **Virtual** > **Compute**.
Step 2 Select the **VM** tab.
Step 3 Select the VM for which to enable console access.
Step 4 Select the **Configure VNC** action.
Step 5 When the **Configure VNC Request** dialog comes up, click **Submit**.

Cloning an Existing Container

As an administrator you can clone an existing container. Cloning transfers all of the settings and configuration data from the VMs that are contained in the original container.

Step 1 On the menu bar, choose **Policies** > **Application Containers**.
Step 2 Click the **Application Containers** tab.
Step 3 Choose a container.
Step 4 Click the **Clone Container** icon. Complete the following fields:

Name	Description
Container Name field	The name of the container.
Container Label field	The container label. This label should be unique.

Step 5 Click **Submit**.

Managing Container Power

Administrators have the ability to disable and enable the power to containers.

Step 1 Choose **Policies** > **Application Containers**.
Step 2 Click the **Application Containers** tab.
Step 3 Choose a container.
Step 4 Click the **Power On Container** icon or **Power Off Container** icon.
Step 5 From the list, select the VMs to power on or off.
Step 6 Click **Submit**.
Step 7 On the confirmation dialog, click **OK**.

Deleting Application Containers

When you delete a container, you also delete the resources that are provisioned for that container. When the **delete container** action is initiated, Cisco UCS Director rolls back the application container setup. A service request is created, reflecting the rollback status.

Step 1 On the menu bar, choose **Policies** > **Application Containers**.
Step 2 Click the **Application Containers** tab.
Step 3 Choose a container.
Step 4 Click the **Delete Container** icon.
Note If you choose to delete an application container with associated L4-L7 services, the L4-L7 services are deleted as well.
If L4-L7 services are associated with the application container, you are prompted to confirm that you want to delete all resources provisioned for the container.
Step 5 If prompted, and if you want to delete the L4-L7 services along with the container, click **Submit**.
Step 6 Click **Submit**. A notice appears confirming that a service request has been generated.
Step 7 Choose **Organization** > **Service Request.**
Step 8 Click the **Service Request** tab.
Step 9 Choose the deletion service request.
Step 10 Click **View Details**.

Viewing Reports

You can generate summary reports, a detailed report with credentials, and a detailed report without credentials for each container.

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

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

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

Step 4 Click **View Reports**.

Step 5 From the **Select Report Type** drop-down list, choose the report you want to view.
Reports "with Credentials" show passwords in plain text. Reports "without Credentials" hide passwords in the report.

Reports for Administrators contain policy information not given in reports for Self-Service Users.

A dialog appears with a report detailing the application container.

Note Any of the reports, in the report header, shows the ID of the Service Request used to create the container.

Viewing Application Container Information

The application container dashboard displays complete information for the APIC application container. There are various tabs you can view for a selected APIC application container.

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

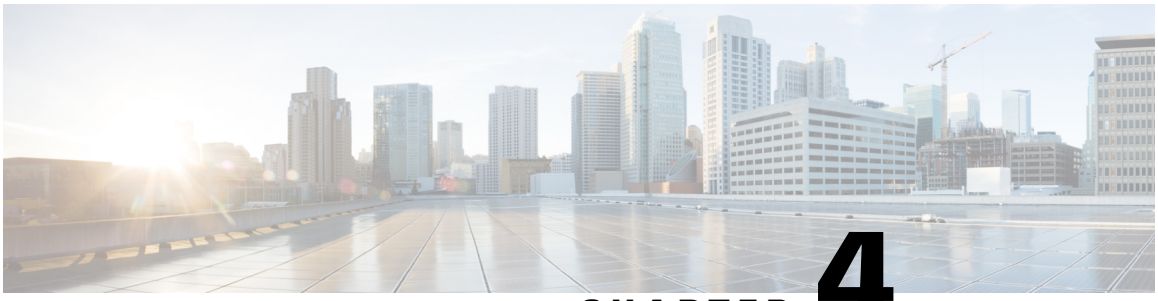
Step 2 Click the **Application Containers** tab, and choose an APIC application container.

Step 3 Click **View Details**.

Step 4 You can view the following information:

Tab	Description
Summary	• **Container—**This pane displays the summary for the application container, such as, name of the container, group, and tenant, number of tiers, number of BMs and VMs per tier, and resource limits for the container. • **Tier—**This pane displays the summary for the tier, such as, number of VMs and BMs, and Virtual Routing and Forwarding (VRF) instance.

Tab	Description
Virtual Machines	Displays the VMs provisioned for the application container. This tab displays the VM name, VM Type, status, IP address, Guest OS, and the time when the VM was provisioned. **Note** Specific naming convention is followed for the VM names for the following actions: • Application provisioning for private network—<VM name specified during container creation time><index of VMs per tier> • Adding VMs to an APIC container—<VM name specified in **Add VM** action><index of VMs per tier>
Bare Metals	Baremetals are physical servers provisioned as part of the application container. This tab displays the baremetal name, OS type, and Service Request ID for each baremetal.
Tier Mapping	Tiers correspond to the networks you defined when you created the application container template. Tiers in a typical application include web, application, and database. The tiers contain VMs and BMs. This tab displays the VMs and BMs contained in each tier, along with its name in an IP address.
L4 L7 Services	Displays the information about L4-L7 services, including service request ID, service name, IP address, service type, device type, and consumer and provider tiers. **Note** If you drill down the service name, you can view the list of real servers.
Contracts	Displays the information about the contracts that define the rule for communication in multi-tier applications. You can drill down each contract to view the security rules.



CHAPTER 4

Self-Service Management Options

This chapter contains the following sections:

Configuring Options on the Self-Service Portal

Management actions can be performed by self-service users only if an administrator enables the options during the application container template creation process. The following list contains the end-user options that can be enabled and disabled (by the administrator) in the application container:

- Access the VM
- Add or delete a vNIC
- Configure lease time
- Create or delete a disk
- Create, delete, or revert a snapshot
- Power the VM on or off
- Reboot, reset, or suspend the VM
- Resize the VM
- Shut down a guest

When you first create an application container, it is associated with a group (customer organization). The users associated with that group can view and perform the enabled management actions on the containers.

Refer to the Cisco UCS Self-Service Portal Guide for this release to obtain information on how to manage application containers using the self-service portal.

Step 1 On the menu bar, choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 Select the **End User Self-Service Policy** tab.

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

Step 4 In the **Add End User Policy** dialog, choose a cloud type from the **Account Type** drop-down list.

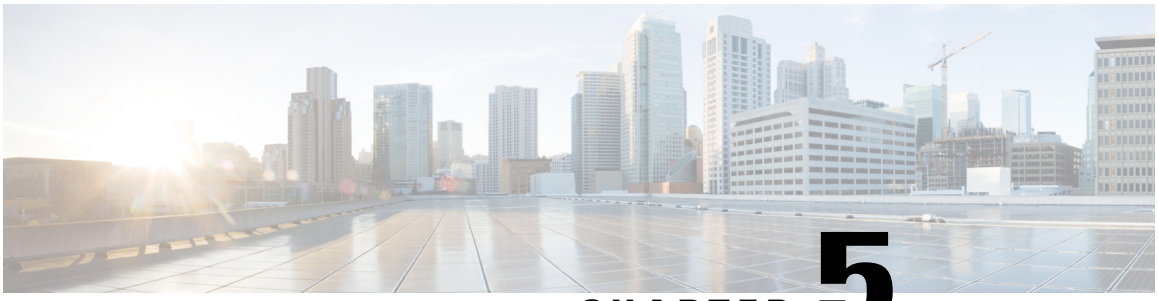
Step 5 In the **End User Policy** dialog, complete the following fields:

Name	Description
Policy Name field	The name of the end user policy.
Policy Description field	A description for the end user policy.
End User Self-Service Options check boxes	Check the actions you want to grant to end users. **Note** Additional options may be available depending on the cloud type you selected.

Step 6 Click **Submit**.

What to Do Next

Select the policy in the **Options** window when you create an application container template.



CHAPTER 5

Securing Containers Using a PNSC and a Cisco VSG

This chapter contains the following sections:

About Prime Network Service Controllers

Prime Network Services Controller (PNSC) is a virtual appliance, based on Red Hat Enterprise Linus (RHEL), that provides centralized device and security policy management of the Cisco Virtual Security (VSG) and Cisco Adaptive Security Appliance 1000V (ASA 1000V) Cloud Firewall.

Note The Cisco Virtual Security Gateway works within the PNSC.

Designed for multi-tenant operation, PNSC provides seamless, scalable, and automation-centric management for virtualized data center and cloud environments. Multi-tenancy refers to the architectural principle that calls for a single instance of the software to run on a Software-as-a-Service (SaaS) server, serving multiple client organizations or tenants. Multi-tenancy is contrasted with a multi-instance architecture, where separate instances are set up for different client organizations. With a multi-tenant architecture, a software application is designed to virtually partition data and configurations, so that each tenant works with a customized virtual application instance.

The components of a PNSC are listed below:

- Creating a Prime Network Service Controller (PNSC) account within Cisco UCS Director.
- Collecting PNSC objects in the inventory.
- Providing PNSC object inventory reports.
- Supporting PNSC object actions.
- Supporting PNSC object workflow tasks.

You can also use Cisco UCS Director to manage your VSGs.

Note In order to see your PNSC configuration, you should download the vCenter extension file from the PNSC and import that into your vSphere client application. After completing that download, execute a PNSC inventory from within Cisco UCS Director. The VM Manager report (under PNSC) will display the corresponding vCenter information.

Adding a PNSC Account

Cisco Prime Network Services Controller (Cisco Prime NSC) is a virtual appliance, based on Red Hat Enterprise Linux, that provides centralized device and security policy management of Cisco virtual services. Designed for multiple-tenant operation, Cisco Prime NSC provides seamless, scalable, and automation-centric management for virtualized data center and cloud environments. The PNSC essentially provides the security component (firewall) to your VSG and application container and separates the VMs from each other. The Cisco Prime Network Services Controller enables the centralized management of Cisco virtual services to be performed by an administrator through Cisco UCS Director .

Note PNSCs are not tied to any specific POD.

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

Step 2 Click the **Multi-Domain Manager Account** tab.

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

Step 4 In the **Multi-Domain Manager Account** dialog box, complete the following fields:

Name	Description
Account Name field	The multi-domain account name.
Description field	Description of the multi-domain.
Account Type field	Description of the account. Choose PNSC.
Server Address field	The IP address of the PNSC server.
User ID field	The administrator's user ID.
Password field	The administrator's user password.
Transport Type drop-down list	Choose a transport type: • HTTP: standard protocol. • HTTPS: standard and secure protocol.
Port field	The port number (based on the transport type).

Name	Description
Description field	A description of the account.
Contact Email field	The email address of the administrator or person responsible for this account.
Location field	The location of the device associated with the account.

Step 5 Click **Submit**.

Viewing PNSC Reports

After creating a PNSC you can view related reports using Cisco UCS Director.

The following reports are available under the **Physical** > **Network** menu.

- Summary
- Tenants
- vDCs
- vApps
- PNSC Firewall Policies
- VM Manager
- Clients
- HA ID Usage Report

Step 1 On the menu bar, choose **Physical > Network** .
The **All Pods** screen appears.

Step 2 In the left-hand pane, click the **Multi-domain Manager**.
The PNSC account entry appears.

Step 3 Click the **Network Accounts** tab.
You can view PNSC accounts that were added under either the Default datacenter or the Multi-domain Manager accounts.

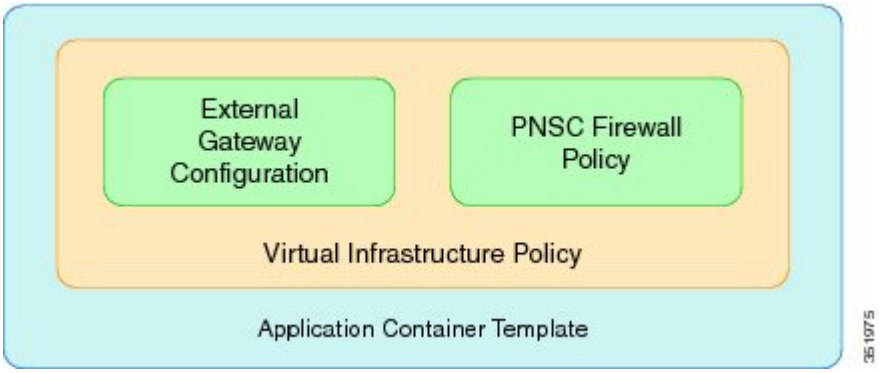
Step 4 Click on a PNSC entry to view the available reports.

Integrating a VSG into an Application Container

You can use Cisco UCS Director to configure a Prime Network Services Controller (PNSC) in addition to its internal firewall (Cisco Virtual Security Gateway), which is then integrated into an application container.

The integration process consists of several stages:

- Upload an OVA file into Cisco UCS Director.
- Create a PNSC firewall policy (used to create a container with a PNSC).
- Create a virtual infrastructure policy. This policy defines which virtual account to use and what type of containers you want to provision.
- Create an application container template. This template uses the virtual infrastructure policy, computing policy, storage policy, and network policy as inputs into the template (as shown below).



The Cisco Virtual Security Gateway (VSG) is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments. The Cisco VSG enables a broad set of multi-tenant workloads that have varied security profiles, so that they can share a common compute infrastructure in a virtual data center private cloud or in a public cloud. By associating one or more virtual machines (VMs) into distinct trust zones, the Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies.

The Cisco VSG provides the following benefits:

- Trusted multi-tenant access—Zone-based control and monitoring with context-aware security policies in a multi-tenant (scale-out) environment to strengthen regulatory compliance and simplify audits. Security policies are organized into security profiles templates to simplify their management and deployment across many Cisco VSGs.
- Dynamic operation—On-demand provisioning of security templates and trust zones during VM instantiation and mobility-transparent enforcement and monitoring as live migration of VMs occur across different physical servers.
- Non-disruptive administration—Administration segregation across security and server teams that provides collaboration, eliminates administrative errors, and simplifies audits.

The Cisco VSG does the following:

- Provides compliance with industry regulations.
- Simplifies audit processes in a virtualized environment.

- Reduces cost by securely deploying virtualized workloads across multiple tenants on a shared compute infrastructure, whether in virtual data centers or private/public cloud computing.

Uploading OVA Files

Cisco UCS Director allows an administrator, group administrator, or end user to upload OVA files to a predefined storage location.

Note Group administrators and end users are the only types with privileges to upload OVA files.

Before You Begin

Ensure that you have the proper access rights.

Step 1 On the menu bar, choose the **Administration** tab.

Step 2 Click the **Upload Files** tab.

Step 3 Click **Upload File**.

Step 4 In the **Upload File** dialog box, complete the following fields:

Name	Description
Folder Type drop-down list	The type of folder containing the OVA file. Choose one of the following: • Public—Choose this role to only reveal public files. • User—Choose this role if you are an end user. End users are not granted extensive privileges. The User role is well suited for first-level support, in which problem identification, remediation, and escalation are the primary goals. • Group—This role can deploy OVA files.
File Name field	The name of the OVA file to upload and display.
Select a file for upload field	Browse to choose the required file. Click **OK** when the **File Upload** confirmation dialog box appears.
File Description field	The description of the file (if required).

Step 5 Click **Submit**.

Step 6 When the **Once Submit Result - Upload Successfully** dialog box appears, click **OK**. Uploaded files are accessible under the **Upload Files** tab.

Creating a PNSC Firewall Policy

You use a firewall policy to enforce network traffic on a Cisco VSG. The Cisco VSG is the internal firewall used as part of PNSC. A key component of the Cisco VSG is the policy engine. The policy engine uses the policy as a configuration that filters the network traffic that is received on the Cisco VSG.

Note The PNSC firewall policy supports both standalone and high availability (HA) modes.

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

Step 2 Click the **Network Accounts** tab.

Step 3 Click on the PNSC account.

Step 4 Click on the **PNSC Firewall Policies** tab.

Step 5 Click **Add**.

Step 6 In the **Create a firewall policy** dialog box, complete the following fields:

Name	Description
Policy Name field	A unique name for the firewall policy.
Policy Description field	A description of the firewall policy.

Step 7 Click **Next**.

Step 8 Click **Add (+)** to create a zone.

Step 9 In the **Add Entry to PNSC Zones** dialog box, complete the following fields:

Name	Description
Zone Name field	A unique name for the zone.
Zone Description field	A description of the zone.
Rules Section	
Attribute Type field	The type of attribute.
Attribute Name field	The name of the attribute.
Operator field	The type of operator.
Attribute Value field	The attribute value.

Step 10 Click **Submit**.

Step 11 Click **OK**.

Step 12 Click **Next**.

Step 13 Click **Add (+)** to create a PNSC ACL rule entry.

Step 14 In the **Add Entry to PNSC ACL Rules** dialog box, complete the following fields:

Name	Description
Name field	The name of the ACL rule. The name must be unique to the container.
Description field	The description of the ACL rule.
Action drop-down list	The type of action allowed for the rule. Choose one of the following: • **Permit—**Permits use on the matching traffic. • **Drop—**Drops use of the rule on the matching traffic. • **Reset—**Resets the rule on the matching traffic.
Protocol check box	If checked, the rule applies to all protocols. If unchecked, you must specify the operator ('equals', 'notequals') and protocol (for example, IP or EGP).
Source Conditions	
Attribute Type field	The type of attribute.
Attribute Name field	The name of the attribute.
Operator field	The type of operator.
Attribute Value field	The attribute value.
Destination Conditions	
Attribute Type field	The type of attribute.
Attribute Namefield	The name of the attribute.
Operator field	The type of operator.

Step 15 Click **Submit**.

Step 16 Click **Next**.

Step 17 In the **PNSC-VSG Configuration** pane, complete the following fields:

Name	Description
Configuration Section	
VSG OVF URL drop-down list	The URL of the OVF file.
Admin Password for the VSG field	The administrator password for the VSG.
Policy agent shared secret Password field	The policy agent shared password.
Deployment mode drop-down list	The type of deployment. Choose one of the following: • **Standalone—**Standalone mode. • **HA—**High availability mode.
VSG HA Id field	The VSG HA ID. The available range is 1-4095.
VLAN ID Range field	The VLAN ID range (for example, 100-199).
Use same vlan check box	If checked, uses the same VLAN ID for both VSG HA and Data port groups.
Name field	The name of the VSG.
Primary VSG Section (HA mode only)	
Name field	The name of the primary VSG.
Deployment Configuration drop-down list	The deployment configuration. Choose one of the following: • **Deploy Small VSG** • **Deploy Medium VSG** • **Deploy Large VSG**
Disk Format drop-down list	The format to store the virtual disk. Choose one of the following: • Thick Provision Lazy Zeroed • Thick Provision Easy Zeroed • Thin Provision
Secondary VSG (HA mode only)	
Name field	The name of the primary VSG.

Name	Description
Deployment Configuration drop-down list	The deployment configuration. Choose one of the following: • **Deploy Small VSG** • **Deploy Medium VSG** • **Deploy Large VSG**
Disk Format drop-down list	The format to store the virtual disk. Choose one of the following: • **Thick Provision Lazy Zeroed** • **Thick Provision Easy Zeroed** • **Thin Provision**

Step 18 Click **Submit**.

Step 19 Click **OK**.

Creating a Virtual Infrastructure Policy

The virtual infrastructure policy defines which VM to use and what type of container you want to provision. This policy also defines which PNSC account you want to tie to this particular account.

Note Any gateway-related Linux based VM image parameters can be added to this policy.

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

Step 2 Click the **Virtual Infrastructure Policies** tab.

Step 3 click **(+) Add Policy**.

Step 4 In the **Create a virtual infrastructure policy** screen, complete the following fields:

Name	Description
Policy Name field	A unique name for the firewall policy.
Policy Description field	A description of the firewall policy.
Container Type drop-down list	Choose a container type. For virtual infrastructure policies, choose VSG.

Name	Description
Select Virtual Account drop-down list	Choose a virtual account (cloud).

Step 5 Click **Next**.

Step 6 In the **Modify Virtual Infrastructure policy** screen, complete the following fields:

Name	Description
PNSC Account drop-down list	Choose a PNSC account.
VSG Template Configuration section	
PNSC Firewall Policy drop-down list	Choose a policy.

Step 7 Click **Next**.

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

Name	Description
Gateway Type drop-down list	Choose a PNSC account.
VM Image for the Gateway drop-down list	Choose a VM.
Number of Virtual CPUs drop-down list	Choose the number of virtual CPUs.
Memory drop-down list	Choose the amount of memory to allocate to the VM.
CPU Reservation in MHz field	The CPU reservation for the VM.
Memory Reservation in MB field	The memory reservation for the VM.
Root Login for the Template field	The root login for the template.
Root Password for the Template field	The root password for the template.
Gateway Password Sharing Option drop-down list	Choose a sharing option for the gateway.

Step 9 Click **Submit**.

Creating an Application Template for a VSG

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

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

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

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

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

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

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

Note Only one network is allowed per VSG container.

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

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

Step 7 Click **Submit**.

Next, you can add and configure the gateway VM that will be provisioned in the application container.

Step 8 Click **OK**.

Step 9 Click **Next**.
The **VMs** screen appears.

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

Name	Description
VM field	The name of the VM. The full name contains the container name as well as this name.
Description field	The description of the VM.
VM Image drop-down list	Choose an image to be deployed.
Number of Virtual CPUs drop-down list	Choose the number of virtual CPUs to be allocated to the VM.
Memory drop-down list	Choose the amount of memory (in MB) to be allocated to the VM.
CPU Reservation (MHz) field	The CPU reservation for the VM in Mhz.
Memory Reservation (MB) field	The memory reservation for the VM.
Disk Size (GB) field	The custom disk size for the VM. To use the template disk size specify the value of 0. The specified disk size overrides the disk size of the selected image. **Note** If this value is less than template size, this value is ignored.
VM Password Sharing Option drop-down list	Choose an option on how to share the VM's username and password with the end users. If **Share after password reset** or **Share template credentials** is chosen, the end user needs to specify a username and password for the chosen templates.
Use Network Configuration from Image check box	If checked, the network configuration from the image is applied to the provisioned VM.
VM Network Interface field	Choose the VM network interface information. If you are adding another network interface, go to Step 9.
Maximum Quantity field	The maximum number of instances that can be added in this container after it is created.
Initial Quality field	The number of VM instances to provision when the container is created. **Note** Each VM will have a unique name and IP address.

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

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

Step 12 Click **Next**.

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

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

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

Step 15 Click **Submit**.

Step 16 Click **OK**.

Step 17 Click the **Add (+)** icon to add an Outbound ACL. The **Application Container: Template - Security Configuration** dialog box appears. Complete the following fields:

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

Step 18 Click **Submit**.

Step 19 Click **OK**.

Step 20 Click **Next**.

Step 21 In the **Application Container Template - Deployment Policies** page, complete the following fields:

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

Step 22 Click **Next**.

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

Name	Description
Enable Self-Service Power Management of VMs check box	If checked, enables self-service power management of VMs.
Enable Self-Service Power Resizing of VMs check box	If checked, enables self-service resizing of VMs.
Enable Self-Service VM Snapshot Management check box	If checked, enables self-service snapshot management of VMs.
Enable Self-Service Deletion of VMs check box	If checked, enables self-service power deletion of VMs.
Enable Self-Service Deletion of Containers check box	If checked, enables self-service deletion of containers.
Enable VNC Based Console Access check box	If checked, enables VNC-based console access to VM.

Name	Description
Technical Support Email Addresses field	Comma separated list of email addresses of individuals who should receive emails regarding the container provisioning.

Step 24 Click **Next**.

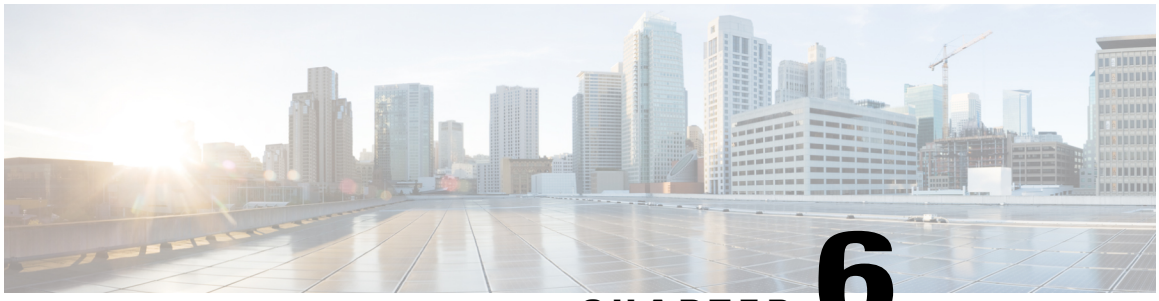
Step 25 Choose a workflow to setup the container.

Step 26 In the **Select** table choose a workflow (for example, Workflow Id 431 Fenced Container Setup - VSG).

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

Step 27 Click **Select**.

Step 28 Click **Submit**.



CHAPTER 6

Implementing Load Balancing

This chapter contains the following sections:

F5 Load Balancing

Cisco UCS Director supports the creation and monitoring of F5 load balancers.

Although load balancing may be prevalent in the routing environment, it is also of growing importance in the virtual networking and VM environment. Server load balancing is a mechanism for distributing traffic across multiple virtual servers, offering high application and server resource utilization.

Server load balancing (SLB) is the process of deciding to which server a load-balancing device should send a client request for service. For example, a client request can consist of an HTTP GET for a web page or an FTP GET to download a file. The job of the load balancer is to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.

Depending on the load-balancing algorithm or predictor that you configure, the F5 BIG-IP performs a series of checks and calculations to determine the server that can best service each client request. F5 BIG-IP bases server selection on several factors, including the server with the fewest connections regarding load, source or destination address, cookies, URLs, or HTTP headers.

A high-level process flow of load balancing is as follows:

1. A client attempts to connect with a service on the load balancer.
2. The load balancer accepts the connection.
3. The load balancer decides which host should receive the connection and changes the destination IP address (or port) in order to match the service of the selected host.
4. The host accepts the load balancer's connection and responds to the original source, to the client (through its default route), and to the load balancer.

5 The load balancer acquires the return packet from the host and changes the source IP (or port) to correspond to the virtual server IP and port, and forwards the packet back to the client.

6 The client receives the return packet, assuming it came from the virtual server, and continues the rest of the process.

Cisco UCS Director enables the management, orchestration, and monitoring of the F5 load balancer. Following is a summary of the crucial processes:

1 Add the F5 load balancer using **Administration** > **Physical Accounts** > **Managed Network Element** > **Add Network Element**.
2 Adding the F5 load balancer is added to Cisco UCS Director as a managed element triggers Cisco UCS Directortask inventory collection. The polling interval configured on the System Tasks tab specifies the frequency of inventory collection.
3 After the F5 is added to the Pod, it is listed with all other components of the pod environment at the account level. To see the F5 component information, navigate to **Physical** > **Network** > **Network Managed Elements**.

There are two ways to implement load balancing on an F5 device using Cisco UCS Director:

1 Use an iApps (BIG-IP) application service.

   iApps application templates let you configure the BIG-IP system for your HTTP applications, by functioning as an interface to consistently deploy, manage, and monitor your servers. You can use default iApps templates or create and customize a template to implement load balancing on the F5 device.

2 Use Cisco UCS Director to:

   - Set up a managed element
   - Create a Pool
   - Add pool members
   - Create a virtual server

About the Workflow Task for F5 Application Container Setup

Cisco UCS Director includes an F5 BIG-IP workflow task to aid in connecting to the Load Balancer using the Workflow Designer. The crucial workflow tasks are:

- Allocate Container VM Resources
- Provision Container - Network
- Provision Container - VM
- Re-Synch Container - VMs
- Setup Container Gateway
- Setup Container F5 Load Balancer
- Send Container Email

Note Only the task titled "Setup Container F5 Load Balancer" is unique in this F5 workflow. This F5 task was recently added to Cisco UCS Director container support. The other tasks previously existed, and are used in other workflows. Two other workflows that aid in the construction of load balancing application containers are *Fenced Container Setup - ASA Gateway* and *Fenced Container Setup*.

F5 Load Balancing Application Container Prerequisites

You must complete the following tasks before you can create and implement an F5 Load Balancing Application Container within Cisco UCS Director.

- Fenced Container Setup
- Fenced Container Setup - ASA Gateway

Tip The Setup Container Load Balancer task is provided for manual creation of the application service. This task is integrated with the Fenced Container Setup-ASA Gateway task to create an F5 load balancing application container.

Requirements for Setup of a F5 Load Balancing Application Container

Cisco UCS Director can create an application container that provides F5 load balancing properties to the contained VMs. The Cisco UCS Director process workflow is summarized below:

1. Create a load balancing policy
2. Add a network element
3. Create a virtual infrastructure policy
4. Create a tiered application gateway policy
5. Create a container template
6. Create a container

F5 Big IP Network Settings Limitations

You must configure the required network settings in the gateway as well as in F5 Big IP device manually.

Note Configuring the VLAN and NAT settings in the gateway, as well as related network settings in the F5 device, cannot be performed using Cisco UCS Director as part of F5 application container support. This particular automation process will be addressed in an upcoming release of Cisco UCS Director.

Adding a Network Element

In order to create a virtual server that supports load balancing, first add a network element in Cisco UCS Director. After a Load Balancer is added as a network element in Cisco UCS Director, it appears under the **Managed Network Element** tab.

Before You Begin

You must be logged in to the appliance to complete this task.

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

Step 2 Choose the **Managed Network Elements** tab.

Step 3 Click **Add Network Element**.

Step 4 In the **Add Network Element** dialog box, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which the network element belongs.
Device Category drop-down list	Choose the device category for this network element. For example: **F5 Load Balancer**.
Device IP field	The IP address for this device.
Protocol drop-down list	Choose the protocol to be used. The list may include the following: • Telnet • SSH • HTTP • HTTPS **Note** When working with an F5 load balancer device, HTTP and HTTPS are the only valid selections.
Port field	The port to use.
Login field	The login name.
Password field	The password associated with the login name.

Step 5 Click **Submit**.

Adding the F5 Load Balancer triggers the system task inventory collection. The polling interval configured on the **System Tasks** tab specifies the frequency of inventory collection.

What to Do Next

To modify or edit a virtual server, choose the server, then click the **Modify** button. To remove a virtual server, choose the server, then click the **Delete** button.

Adding an F5 Load Balancing Policy

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

Step 2 Click the **F5 Load Balancer Policies** tab.

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

Step 4 In the **Add F5 Load Balancer Policy** screen , complete the following fields:

Table 2:

Name	Description
Policy Name field	The name you assign to an F5 load balancer application policy.
Policy Description field	A description of this policy.
Load Balancer Account Type drop-down list	Choose **Physical**.
Select F5 Account drop-down list	Choose an **F5 load balancer** account from the available list.

Step 5 Click **Select**.

Step 6 Click **Next**.

Step 7 Click **Submit**.

What to Do Next

Create a virtual infrastructure policy.

Adding an F5 Load Balancing Virtual Infrastructure Policy

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

Step 2 Click the **Virtual Infrastructure Policies** tab.

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

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

Table 3:

Name	Description
Template Name field	A unique name for the policy.
Template Description field	A description of this policy.
Container Type drop-down list	Choose a container type. Select **Fenced Virtual** for a load balancing application container.
Select Virtual Account drop-down list	Choose a virtual account.

Step 5 Click **Next**.

Step 6 In the **Virtual Infrastructure Policy - Fencing Gateway** pane, complete the following:

Table 4:

Name	Description
Gateway Required check box	If checked, allows you to configure your gateway. Otherwise, click **Next**.
Select Gateway Policy drop-down list	If the **Gateway Required** check box is checked, allows you to assign a gateway policy.

Step 7 Click **Next**.

Step 8 In the **Virtual Infrastructure Policy - Fencing Load Balancing** pane, complete the following:

Table 5:

Name	Description
F5 Load Balancer Required check box	If checked, requires the F5 load balancer to be used for this container.

Name	Description
Select F5 Load Balancer Policy drop-down list	Choose a load balancing policy required for this container.

Step 9 Click **Next**.

Step 10 Click **Submit**.

What to Do Next

Configure the Tiered Application Gateway Policies.

Creating a Tiered Application Gateway Policy

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

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

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

Step 4 In the **Add Gateway Policy** dialog box, complete the following fields:

Name	Description
Policy Name field	The name you assign to an F5 load balancer tiered application gateway policy.
Policy Description field	A description of this policy.
Gateway Type drop-down list	Choose a gateway type.
Select Virtual Account drop-down list	Choose a cloud account to deploy the container.

Step 5 Click **Next**.

Step 6 In the **Add Gateway Policy** dialog box, complete the following fields for the Linux gateway selection (if applicable):

Name	Description
VM Image for the Gateway drop-down list	Choose an VM image for the gateway from the list.
Number of Virtul CPUs field	The number of virtual CPUs allowed as per policy.
Memory drop-down list	Choose the size of the memory.
CPU Reservation in MHz field	The number of CPU reserved as per the policy.

Name	Description
Memory Reservation in MB field	The maximum limit of memory reserved as per the policy in MB.
Root Login for the Template field	The root login name for accessing the template.
Root password for the Template field	The root password for accessing the template.
Gateway Password Sharing Option drop-down list	If and how to share the root password for the gateway VM with end users.

Step 7 In the **Add Gateway Policy** screen , complete the following fields for the Cisco ASA (if applicable) selection:

Name	Description
Select Device drop-down list	Choose a Cisco ASA device.
Outside Interface drop-down list	Choose the outside interface for the Cisco ASA device.
Outside Interface IP Address field	The IP address of the outside interface.
Outside Interface VLAN ID field	The VLAN ID associated to the outside interface.
Inside Interfaces field	Choose **Select** and choose an inside interface.

Step 8 In the **Add Gateway Policy** screen , complete the following fields for the Cisco ASAv (if applicable) selection:

Name	Description
ASAv OVF field	Click **Select** and choose an OVF file for the Cisco ASAv device from the table.
ASAv Policy field	Click **Select** and choose the ASAv deployment policy from the table. This deployment policy is created earlier by choosing **Policies > Virtual / Hypervisor Policies > Service Delivery > ASAv Deployment Policy**.
Outside Interface field	Click **Select** and choose an outside interface from the table.
Inside Interfaces field	Click **Select** and choose an inside interface from the table.

Step 9 Click **Next**.

Step 10 Click **Submit**.

Creating an Application Container Template

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

Before You Begin

Create an application container policy.

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

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

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

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

Step 4 Click **Next**.

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

Name	Description
Select Virtual Infrastructure Policy drop-down list	Choose a policy to deploy the container. **Note** Select a policy that supports load balancing (future wizard screens are then populated with applicable load balancing information).

Step 6 Click **Next**. The **Application Container: Template - Internal Networks** screen appears.
You can add and configure multiple networks for a container. These networks are applicable to the VM that is provisioned using this template.

Step 7 Click the **(+) Add** icon to add a network. The **Add Entry to Networks** dialog box appears. Complete the following fields:

Name	Description
Dynamic Fabric Network check box	If checked, enables the application container for use in Digital Fabric Automation Networks.
Network Name field	The network name. The name should be unique within the container.
Fabric Account drop-down list	Choose a fabric account.

Name	Description
Network IP Address field	The network IP address for the container.
Network Mask field	The network mask.
Gateway IP Address field field	The IP address of the default gateway for the network. A NIC with this IP is created on the GW VM.

Step 8 Click **Submit**.
Next, you can add and configure the VM that will be provisioned in the application container.

Step 9 Click **OK**.

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

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

Step 11 Click Next.

Step 12 (Optional) Click the **Add (+)** icon to add a new (multiple) VM network interface. Complete the following fields:

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

Step 13 In the **Application Container Template - F5 Application Service** screen, complete the following fields:

Name	Description
Application Service Name field	The name of the application service.
Template field	Choose a network.
IP Address field	The IP address of the network.
Virtual Server IP field	IP address of the virtual server.
Virtual Server Port field	Port used on the virtual server.
FQDN names of Virtual Server field	Name of the FQDN virtual server. **Note** Separate each FQDN name with a comma.
Nodes List	Select a node from the Nodes list and click **Submit**. If the Nodes list fails to present a node that you want to associate with the Virtual Server: • Click**Add (+)** icon to add the nodes. The **Add Entry to Nodes list** dialog box appears. • Provide the Node IP address, the port, and the connection limit; then click **Submit**.

Step 14 Click **Next**.

Step 15 The **Application Container Template - Deployment Policies** screen appears.
You must select the compute, storage, network, system policy, and cost model required for VM provisioning. A policy is a group of rules that determine where and how a new VM is to be provisioned within an application container (based on the availability of system resources).

- The network policy is used only to deploy the outside interface of the virtual firewall (container gateway).
- The selected *Portgroup in Network Policy* should be on the host on which the Gateway VM is provisioned.

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

Complete the following fields:

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

Step 16 Click **Next**. The **Application Container: Template - Options** screen appears.
You can select options to enable or disable certain privileges for the self-service end user.

Complete the following fields:

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

Step 17 Click **Next**. The **Application Container: Template - Setup Workflows** screen appears. Complete the following field:

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

Step 18 Click **Next** to complete the creation of the application container template and review the **Summary** screen.
Note Notice the inclusion of a Load Balancing Criteria Summary entry.

Step 19 Click **Submit**.

Creating an Application Container Using a Template

Once you create a application container template you can use the template administrator to create other application containers. If you want to create a template for use in a VSG environment, see Creating an Application Template for a VSG, on page 45.

Note An application container must use a unique VLAN for its own network. There can be no other port group on (VMware) vCenter using it.

Step 1 Choose **Policies** > **Application Containers**.
Step 2 Click the **Application Container Templates** tab.
Step 3 Choose a template.
Step 4 Click **Create Container**.
Step 5 In the **Create container from template** dialog box, complete the following fields:
Note The combined length of the private network name, service name, and container name must not exceed 32 characters.

Name	Description
Container Name drop-down list	The name of the container. This name must be unique.
Container Label field	The label for the container.
Tenant drop-down list	Choose a tenant.
Private Network Name field	This field appears only in the tenant with private network is selected. The name of a private network associated with the selected tenant.
Network Throughput drop-down list	Choose the throughput of the network. **Note** This field is not supported for a tenant with private networks.

Name	Description
The following fields appear only in the tenant with private network is selected from the **Tenant** drop-down list. That is, these fields appear only for the tenant which has the capability of supporting varied VM instances per internal tier.	
VM Labels Prefix Customization field	The customized prefix name of the VM for each tier. **Note** The prefix name is obtained from the VM label prefix of the application profile where the administrator defines the prefix for each tier. During application container deployment, you can update the prefix from what is defined in the application profile.
The maximum quantity of the internal tiers such as WEB/APP/DB tiers are illustrated only as examples in the following fields. There can be more than three tiers as per the definition in the application profile. The number of fields appear based on the number of internal tiers that are defined as part of the application profile.	
Maximum Quantity for <WEB> tier	The maximum number of VM instances in the <*web*> tier.
Maximum Quantity for <APP> tier	The maximum number of VM instances in the <*application*> tier.
Maximum Quantity for <DB> tier	The maximum number of VM instances in the <*database*> tier.
Note The internal tier names given in the application profile are dynamically fetched and appear in the fields during create container action. if the Maximum Quantity for any internal tier is changed during create container action, this value is considered as maximum number of host size for allocating subnet per tier .	
The following fields will not appear in the tenant with private network is selected in the **Tenant** drop-down list.	
Enable Disaster Recovery check box	Check this check box to enable the disaster recovery service for the container.
Enable Resource Limits check box	Check this check box to specify the number of vCPUs, Memory, Maximum Storage, and maximum number of servers for the container.
Enable Network Management check box	Check this check box to enable the network management service for the container. **Note** This field is applicable only for Layer 4 and Layer 7 devices that are managed by APIC device package.
Tier Label Customization area	This field appears only for APIC containers. The customized name of the tier label.

Step 6 Click **Submit**. The **Submit Result** dialog box appears.
Note Remember to make a note of the service request presented in the **Submit Result** prompt.

Step 7 Click **OK**.
Note You can view the progress of the container's creation by viewing the details of the service request.

Step 8 Click the **Application Containers** tab.
The new container appears in the **Application Containers** pane.

Initiating a Service Request

Note F5 Load Balancing is only supported on Fenced Virtual Containers.

Step 1 On the menu bar, choose **Organization >Service Request**.

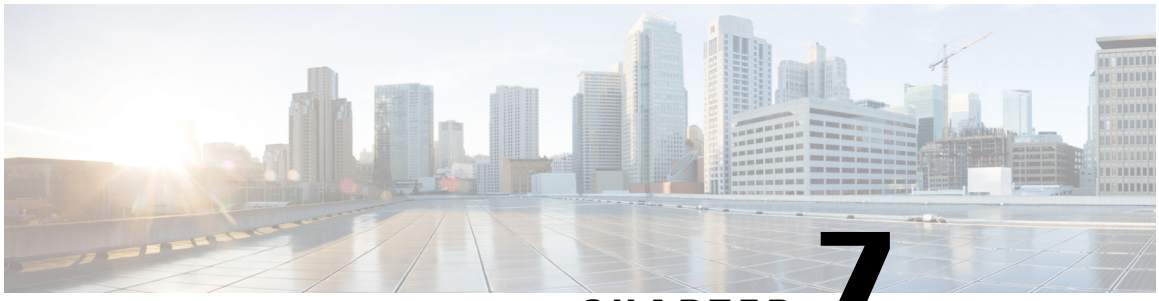
Step 2 Click on the **Advanced Filter** button (far right side of interface).

Step 3 Choose Request Type from the Search drop-down list.

Step 4 Enter Advanced in the **Test** field.

Step 5 Click **Search**.

Step 6 Click the **Fenced Container Setup** workflow.



CHAPTER 7

Implementing Cisco Application Policy Infrastructure Controller Support

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. For more information about the Cisco APIC, see the Cisco UCS Director APIC Management Guide for this release.

The orchestration feature allows you to automate APIC configuration and management tasks in 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 for this release.

APIC Application Containers

Cisco UCS Director lets you create application containers that support Cisco Application Policy Infrastructure Controller (APIC). For additional information see the Cisco UCS Director APIC Management Guide for this release. APIC application containers let you do the following:

- Establish networks in a VMware environment.
- Provision multiple VMs from a network.
- Provide a way to isolate those networks using gateways (for example, Linux, ASAv).
- Allow load balancing the container network using VPX or SDX load balancers.
- Use a Cisco Application Centric Infrastructure Controller (APIC).
- Provision a baremetal server and/or VMs.

APIC Application Container Prerequisites

You must perform the following Cisco UCS Director tasks before you can create an APIC application container. For additional information regarding these tasks refer to the Cisco UCS Director APIC Management Guide for this release.

- Add and configure an APIC account.
- Add a service offering.
- Add a tenant profile.
- Add a tag library. See the Cisco UCS Director Administration Guide for this release for information on creating tags.
- Add a resource group.
- Add a firewall policy (optional).

APIC Application Container Limitations

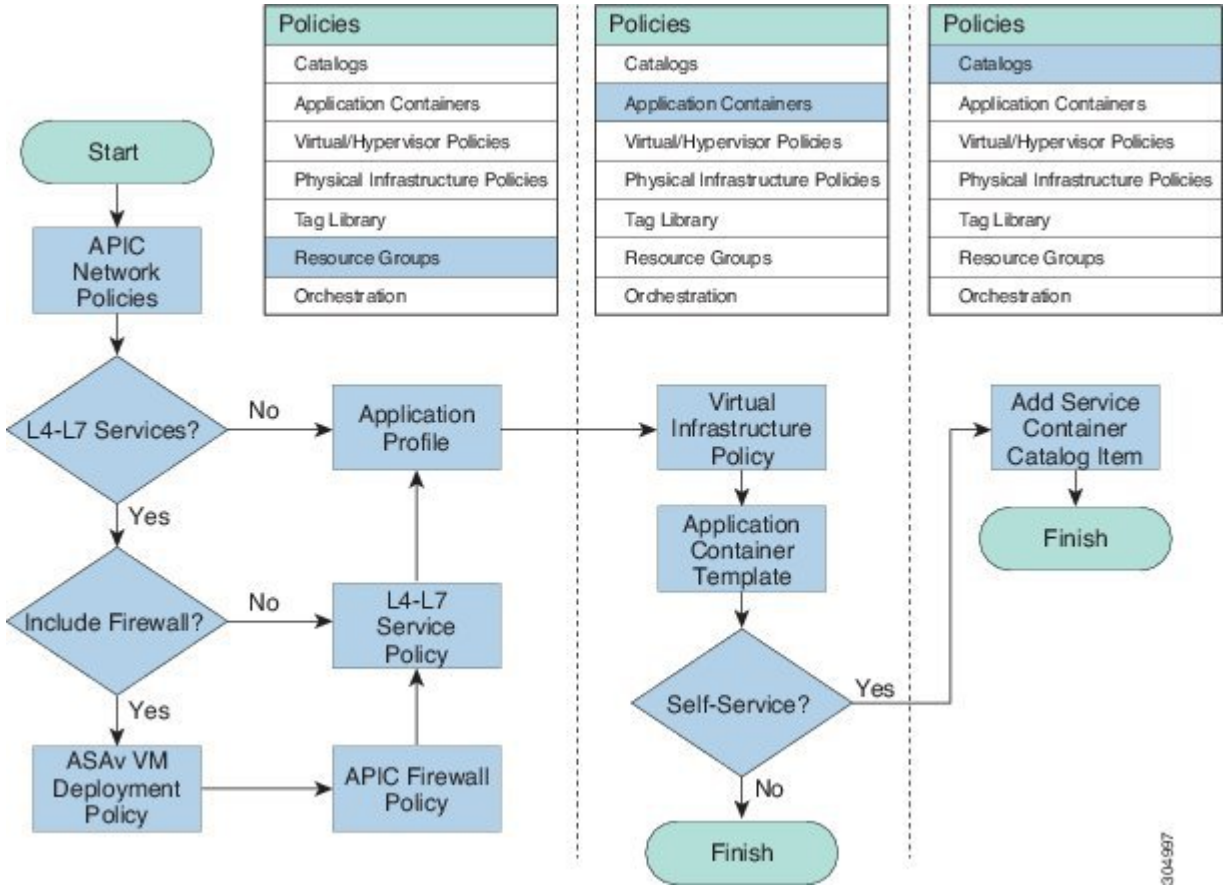
Cisco UCS Director APIC application containers have the following limitations:

- Tenant onboarding must be done before container creation and usage.
- Resource groups must contain the accounts necessary to manage a container's resources. This can be any combination of storage, compute, network, and virtual resources.
- Only VMware hosts deployed on Cisco UCS blade servers can be included in resource groups.

APIC Application Container Creation Process

The figure below illustrates the flow of the APIC Application Container creation process within Cisco UCS Director.

Figure 6: Process for Creating an APIC Application Container



ASAv VM Deployment Policy

The ASAv brings full firewall functionality to virtualized environments in order to secure data center traffic and multi-tenant environments. The ASAv VM deployment policy is used in the **Deploy ASAv VM from OVF** task.

Adding an ASAv VM Deployment Policy

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

Step 2 Click the **ASAv VM Deployment Policy** tab.

Step 3 Click **Add**.

Step 4 In the **ASAv VM Deployment Policy** dialog box, complete the following fields:

Name	Description
Policy Name field	The name of the ASAv VM deployment policy.
ASAv OVF field	Click **Select** and choose a template file in the open virtualization format (OVF).
VM Name field	The name for the ASAv virtual machine (VM) instance. The policy will automatically prefix this VM name with the container name.
Port field	The port number of the firewall appliance.
Username field	The username that is used to access the firewall appliance.
Password field	The password that is used to access the firewall appliance.
Disk Format drop-down list	Choose the virtual disk format. The available formats for provisioning are **Thick Provision Lazy Zeroed**, **Thick Provision Eager Zeroed**, and **Thin Provision**.

Name	Description
Deployment Option drop-down list	Choose the deployment option which is the predefined set of configurations using which VM can be deployed. The deployment options are listed based on the OVF for ASAv 9.3.1, ASAv 9.3.2, and later. The deployment options are listed for ASAv 9.3.1 based on the deploy vCPU count. This count represents the number of vCPUs that the ASAv VM will have when the ASAv VM is deployed. The following deployment options are listed for ASAv 9.3.2 and later: • **ASAv5—**To deploy an ASAv with a maximum throughput of 100 Mbps (uses 1 vCPU and 2 GB of memory). This is the default value. • **ASAv10—**To deploy an ASAv with a maximum throughput of 1 Gbps (uses 1 vCPU and 2 GB of memory). • **ASAv30—**To deploy an ASAv with a maximum throughput of 2 Gbps (uses 4 vCPUs and 8 GB of memory). **Note** Till the release of ASAv 9.5.2 version, the OVA file was provided for ASAv deployment for VMware environment. Starting from ASAv 9.5.2 version, the OVA file is not available on Cisco.com, instead, the zip file is displayed. The zip file contains two OVA files from which you can choose the **asav-vi.ovf** file and not the **asav-esxi.ovf** file.

Step 5 Click **Submit**.

APIC Firewall Policy

You can create a firewall policy rule that permits network traffic over specific ports between endpoints.

When creating an application profile, you can choose to use a firewall or load balancer for each tier in an application profile. When you create an L4-L7 policy, you can choose a firewall policy from one of the firewall policies that you created in Cisco UCS Director.

The firewall policy is used in the following APIC tasks where you have selected firewall as service:

- Create L4-L7 Service Graph

- Add Function Node to L4-L7 Service Graph

Adding an APIC Firewall Policy

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

Step 2 Click the **APIC Firewall Policy** tab.

Step 3 Click **Add**.

Step 4 In the **Create Firewall Policy** dialog box, complete the following fields:

Name	Description
Policy Specification pane	
Name field	The name of the firewall policy.
Description field	The description of the firewall policy.
ACL(s) Specification pane	

Name	Description
ACL(s) field	The access control lists (ACLs) defined for the firewall policy. Click the + icon to define an ACL. In the **Add Entry** dialog box, complete the following fields: • **Existing ACL List Name** drop-down—Choose an ACL name from the list of existing ACLs. • **New ACL list** check box—If you want to create a new ACL, check this check box. • **New ACL List Name** field—This field appears when you check the **New ACL list** check box. The name of the ACL that you want to create. • **ACL Entry Name** field—The ACL entry that defines the rule for firewall policy. • **Protocol** drop-down list—Choose the protocol for communication. • **Source Any** check box—By default, this check box is checked. Allows to permit or deny any source host or network. • **Source Address** field—This field appears when you uncheck the **Source Any** check box. The IP address, IP address range, or IP address with subnet mask to specify either a single host or a range of them as the source address. • **Destination Any** check box—By default, this check box is checked to apply the ACL entry statement on any destination address. • **Destination Address** field—This field appears when you uncheck the **Destination Any** check box. The IP address, IP address range, or IP address with subnet mask to specify either a single host or a range of them as the destination address. • **Action** drop-down list—Choose **Permit** or **Deny** as the action for the ACL entry. • **Order** field—The sequence in which deny statements or permit statements need to be executed.

Name	Description
Bridge Group Interface(s) pane—Bridge Group Interface(s) must be configured if the firewall is operating in the transparent mode. If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can group the interfaces together in a bridge group, and then configure multiple bridge groups, one for each network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the ASA, and traffic must exit the ASA before it is routed by an external router back to another bridge group in the ASA. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration.	
Bridge Group Interface(s) field	The bridge group interfaces defined for the firewall policy. Click the + icon to define a bridge group ID. In the **Add Entry to Bridge Group Interface(s)** dialog box, complete the following fields: • **Bridge Group ID** field—The unique ID of a bridge group. The value of bridge group ID is an integer between 1 and 100. • **IPv4 Address Value** field—The management IP address of the bridge group.
Interface(s) Specification pane	

Name	Description

Interface(s) field	The interfaces defined for the firewall policy.
	Click the + icon to define an interface.
	In the **Add Entry to Interface(s)** dialog box, complete the following fields:
	• **Interface Name** field—The name of the interface that you need to configure.
	• **IP Pool Option for Virtual IP** drop-down list—The IP pool option allocates a virtual IP address from the range of IP addresses to an interface. Choose one of the following options to automatically assign an IP address for the interface:
	  • **Select IP Pool from existing list**
	  • **Provide IP Pool range**
	• **IP Pool** field—The IP pool from which you want to choose the unreserved virtual IP address for the interface.
	• **Security Level** field—The security level of the interface. The value of security level is an integer between 0 and 100.
	• **Bridge Group ID** drop-down list—Choose a bridge group ID to which you need to assign the interface.
	• **Inbound ACL** drop-down list—Choose an ACL as an inbound access list that apply to traffic as it enters an interface.
	• **Outbound ACL** drop-down list—Choose an ACL as an outbound access list that apply to traffic as it exits an interface.

Assign Interface Specification pane	
External Interface drop-down list	Choose an interface as the external interface.
Internal Interface drop-down list	Choose an interface as the internal interface.

Step 5 Click **Submit**.

APIC Network Policy

The APIC network policy is an optional policy used in the network (tier) configuration of the application profile. The APIC network policy overrides the default settings used to provision an APIC application container. You can create a policy to specify tenant or container private networks, create subnetworks, and create end point groups (EPGs).

Adding an APIC Network Policy

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

Step 2 Click the **APIC Network Policy** tab.

Step 3 Click **Add**.

Step 4 In the **Create Network Policy** dialog box, complete the following fields:

Name	Description
Policy Specification pane	
Name field	The name of the APIC network policy.
Description field	The description of the APIC network policy.
Private Network Specification pane	
Private Network drop-down list	Choose one of the following: • **Container—**To choose private network from container workflow. • **Tenant—**To choose private network from tenant.
Subnet Specification pane	
Create Subnet check box	Check this check box to create a subnet. When you check the **Create Subnet** check box, the following additional fields appear: • **Shared Subnet** check box**—**Check this check box to create a private network with a shared subnet. • **Public Subnet** check box**—**Check this check box to create a private network with a public subnet. • **Private Subnet** check box**—**Check this check box to create a private network with a private subnet.

Name	Description
EPG Specification pane	
QOS field	The QOS name that need to be assigned to EPG.
EPG Specification pane	
Deploy Immediacy drop-down list	Choose whether to deploy the domain immediately or on as-needed basis.
Resolution Immediacy drop-down list	Choose how policies are pushed to leaf nodes: • **Immediate** field—All policies, including VLAN bindings, NVGRE bindings, VXLAN bindings, contracts, and filters, are pushed to leaf nodes upon attaching a Hypervisor physical NIC. The Link Layer Discovery Protocol (LLDP) or OpFlex is used to resolve Hypervisor-to-leaf node attachment. • **On Demand** field—Policies are pushed to leaf nodes only upon attaching a physical NIC and associating a virtual NIC with a port group (an EPG).
Forwarding drop-down list	Choose the forwarding method of the bridge domain: **Optimize** or **Custom**.
L2 Unknown Unicast drop-down list	This drop-down list appears when you choose **Custom** in the **Forwarding** drop-down list. Choose the forwarding method for unknown layer destinations.
Unknown Multicast Flooding drop-down list	This drop-down list appears when you choose **Custom** in the **Forwarding** drop-down list. Choose the forwarding method for multicast traffic for unknown layer destinations.
ARP Flooding check box	This check box appears when you choose **Custom** in the **Forwarding** drop-down list. Check this check box to enable ARP flooding. If ARP flooding is disabled, unicast routing is performed on the target IP address.
Unicast Routing check box	This check box appears when you choose **Custom** in the **Forwarding** drop-down list. This check box is checked by default. Check this check box to enable unicast routing. Unicast routing is the forwarding method based on predefined forwarding criteria (IP or MAC address).

Step 5 Click **Submit**.

Layer 4 to Layer 7 Service Policy

The APIC has an open northbound API that allows you to not only provision services in the fabric, but also to provision Layer 4 to Layer 7 services, such as firewall and load balancer, that attach to the fabric.

Adding a Layer 4 to Layer 7 Service Policy

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

Step 2 Click the **L4 - L7 Service Policy** tab.

Step 3 Click **Add**.

Step 4 In the **Add L4-L7 Service Policy** dialog box, complete the following fields:

Name	Description
L4-L7 Service Specification pane	
Name field	The name of the Layer 4 to Layer 7 service policy.
Description field	The description of the Layer 4 to Layer 7 service policy.

Name	Description
Allow Firewall check box	If checked, the firewall service is applicable for the Layer 4 to Layer 7 service policy. When you choose the **Allow Firewall** check box, the following additional fields appear: • **Firewall Type** drop-down list—Choose the firewall type. • **Device Package** field—Click **Select** and choose the correct device package based on the supported APIC version. • **Firewall Policy** field—Click **Select** and choose a firewall policy from the list. Click the + icon to add a firewall policy. For more information about how to add a firewall policy, see Adding an APIC Firewall Policy, on page 73. • **Multi Context Enabled** check box—This check box appears only when **PHYSICAL** firewall type is selected. Check this check box to identify if a multiple security context enabled ASA is used for firewall configuration. If this check box is not checked, you can use the physical ASA appliance. **Note** You can choose to have physical ASA as firewall for containers in Hyper-V environment in addition to the VMware environment. • **Enable Firewall HA** check box—This check box appears only when **VIRTUAL** firewall type is selected. Check this check box to enable high availability for the firewall service. • **Enable Stateful Failover** field—Optional. This field appears if you check the **Enable Firewall HA** check box. You can choose to enable or disable the stateful failover for ASA in high availability mode from the drop-down list. Stateful failover is disabled by default. If failover is configured in ASAv, Gig0/8 is the failover_lan interface and Gig0/7 is the optional failover_link for the stateful failover interface configuration. • **Transparent Mode** check box—Check this check box to run transparent firewall mode. **Note** This feature is supported in VDC with managed network service.

Name	Description
Allow Load Balancer check box	If checked, the load balancer service is applicable for the Layer 4 to Layer 7 service policy. When you choose the **Allow Load Balancer** check box, the following additional fields appear: • **Load Balancer Type** drop-down list—Choose the load balancer type. • **Device Package** field— Click **Select** and choose a device package from the list. • **Enable Load Balancer HA** check box—Check this check box to enable high availability for the load balancer service. **Note** The load balancer service is the only supported service for a tenant with multiple private networks.
Summary pane—The summary of the Layer 4 to Layer 7 service policy is displayed.	

Step 5 Click **Submit**.

Network Device System Parameters Policy

Network device system parameters policy sets the NTP and SNMP parameters that are needed to be configured on a load balancer (LB) device. The network device system parameters policy is optionally selected during creation of a Layer 4 to Layer 7 service policy to define the NTP and SNMP parameters for configuring a LB device.

While provisioning an APIC container, you have to choose the application profile with the created Layer 4 to Layer 7 service policy so that the corresponding NTP and SNMP parameters are set on device clusters in APIC and configured on the LB device.

Adding a Network Device System Parameters Policy

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

Step 2 Click the **Network Device System Parameters Policy** tab.

Step 3 Click **Add**.

Step 4 In the **Add Network Device Policy** dialog box, complete the following fields:

Name	Description
NTP Parameters Pane	
NTP Server field	The IP address or host name of the NTP server.
SNMP Parameters Pane	
Trap Class drop-down list	Choose one of the following as the trap class: • Generic—To implement the pre-defined traps such as cold start, warm start, link down, link up, authentication failure, and EGP neighbour loss. • Specific—To use the device specific trap.
Trap Destination field	The IP address of the system to which the appliance forwards traps received by managed devices.
Community Name field	The global community string associated with SNMP traps. Traps sent from the device will provide this string as a community name. The community name can be in any alphanumeric format. The special characters such as hyphen (-), period (.), pound (#), space (), ampersand (@), equals (=), colon (:), and underscore (_) are allowed.
Permissions drop-down list	Choose one of the following as the permission to communicate information between SNMP manager and agent: • get—To access and retrieve the current value of one or more MIB objects on an SNMP agent. • get_next—To browse the entire tree of MIB objects sequentially. • get_bulk—To retrieve data in units as large as possible within the given constraints on the message size. • set—To update the current value of a MIB object. • all
User Name field	Name of the SNMP user.
Group field	Name of the SNMP group.
Authentication Type drop-down list	Choose MD5 or SHA as the type of authentication protocol to authenticate the messages sent on behalf of the SNMP user.

Name	Description
Authentication Password field	The password to be used for the chosen authentication type.
Privacy Type drop-down list	Choose AES or DES as the privacy type to encrypt the message sent on behalf of the SNMP user.
Privacy Password field	The password to be used for the chosen privacy type.

Step 5 Click **Submit**.

What to Do Next

You choose the network device policy during creation of a Layer 4 to Layer 7 service policy to define the NTP and SNMP parameters for configuring a LB device.

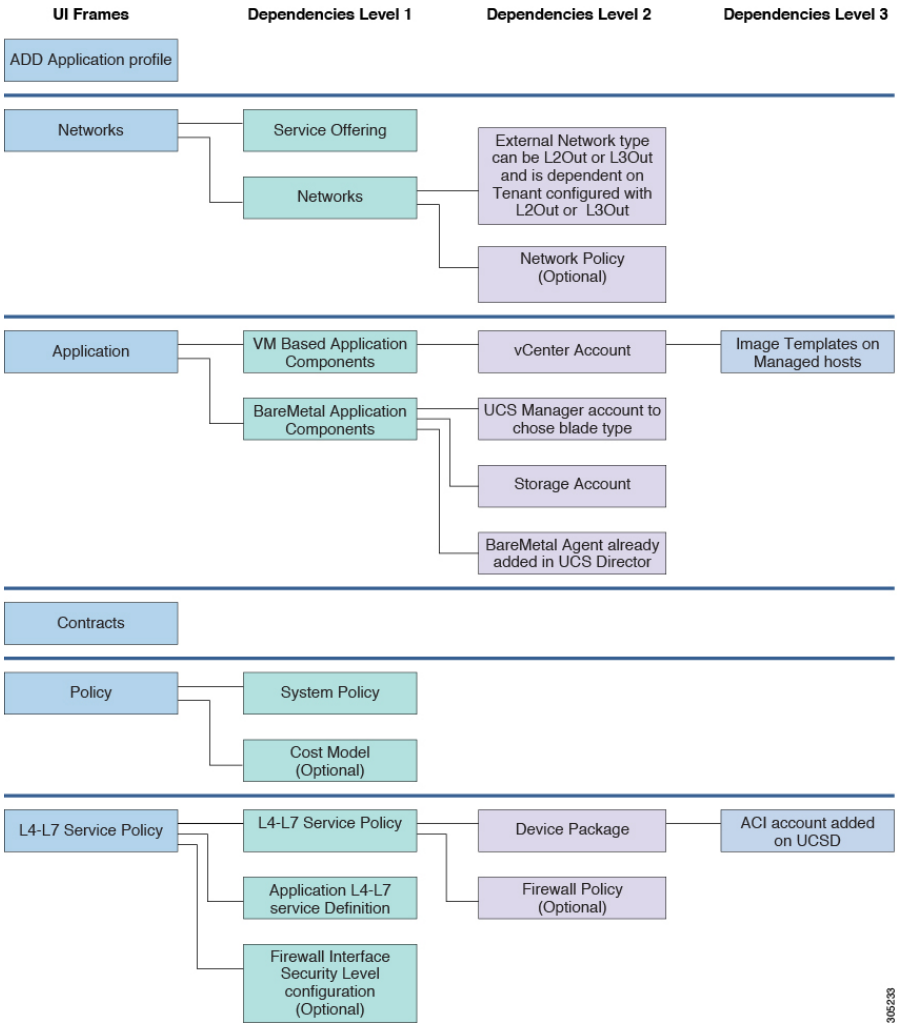
Application Profiles

An application profile is a description of the infrastructure required for the deployment of an application. These infrastructure requirements include baremetal configurations, virtual machines (VMs), L4-L7 policies, and connection policies.

Note You can perform a container provisioning either in the VMware environment or Hyper-V environment.

The following image explains the dependencies of the application profile:

Figure 7: Application Profile – Dependencies



Adding an Application Profile

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

Step 2 Click the **Application Profile** tab.
The application profiles that are available in Cisco UCS Director appear. Choose an application profile and click **View** to view the name, description, and service offering of the application profile.

When you choose an application profile and click **View Details**, the following tabs appear:

Name	Description
Tiers	Displays the tier name, description, physical network service class, and virtual network service class of the application profile.
VMs	Displays the VM name, description, selected network, virtual compute service class, and virtual storage service class of the application profile.
BMs	Displays the VM name, description, selected network, physical compute service class, and physical storage service class of the application profile.

Step 3 Click **Add**.

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

Name	Description
Name field	The name of the application profile. Once added, the name cannot be modified.
Description field	The description of the application profile.

Step 5 Click **Next**.

Step 6 In the **Networks** screen, complete the following fields:

Name	Description
Service Offering drop-down list	Click **Select** and choose a service offering from the list. The service offering must belong to the tenant for which you will create containers with this application profile. Click the + icon to add a service offering. For more information about how to add a service offering, see the Cisco UCS Director APIC Management Guide.
Networks field	Define the network types and the number of networks that are needed in the application. For more information on how to configure a network, see the *next Step*.

Step 7 (Optional). In the Network field of the **Networks** screen, click the + icon to configure the tier for application.
In the **Add Entry to Networks** dialog box, complete the following fields:

Name	Description
Network field	Enter the name of the network.

Name	Description
Description field	Enter the description of the network.
Network Type drop-down list	Choose one of the following as the network type: • **Internal** • **External** • **Infrastructure** • **Failover** **Note** When a tenant needs multiple private networks, you need to define only **Internal** and **External** network types.
Interested Tag Value field	Click **Select** and choose the tag values for each tier. During container provisioning, resource is selected based on the tag associated with the tier. **Note** You can select more than one tag (the tag that is used for VMware cluster or datastore cluster). For example, if you select a datastore tag (ds tag - gold) and a VMware cluster tag (cluster tag - ESXi cluster tag), during the datastore selection, the datastore tagged with the gold value is selected. **Note** To avail shared L3Out support, choose the tag value that is used for tagging the external network and contract of a common tenant.
APIC Network Policy drop-down list	This field appears only when you choose network type as **Internal**. Choose the APIC network policy from the list. Click the + icon to add an APIC network policy. For more information about how to add an APIC network policy, see Adding an APIC Network Policy, on page 77.

Name	Description
L2/L3 Selection drop-down list	This field appears only when you choose network type as **External**. By default, **L2Out** is selected to integrate the ACI fabric with external Layer 2 network. • **L2Out—**To integrate the ACI fabric with external Layer 2 network. • **L3Out—**To integrate the ACI fabric with external Layer 3 network. • **SharedL3Out—**To integrate the ACI fabric with shared external Layer 3 network. The network must be tagged and updated on Tenant vPOD in advance and the same tag must be selected for the external network in case of shared L3Out.
Use Existing L2/L3 Out config available in the tenant check box	This field appears only when you choose network type as **External**. By default, the check box is checked to use the L2/L3 out configuration defined in the tenant while creating a container. **Note** When a container is created based on an application profile, tenants having L2 out or L3 out configuration are displayed according to the L2/L3 selection in the application profile.

Step 8 Click **Next**.

Step 9 In the **Application** screen, do the following:

a) In the **VM Based Application Components** field, click the + icon.

b) In the **Add Entry to VM Based Application Components** dialog box, complete the following fields:

Name	Description
VM Name field	Enter the name of the VM.
Description field	Enter the description of the VM.
Network drop-down list	Choose the network from the list.
Image Selection Type drop-down list	Choose one of the following for the image selection: • **All Images** • **Image Tag based selection—**When you choose the image tag-based selection, the **Tag** field appears. Click the + icon to add a tag.

Name	Description
VM image drop-down list	Choose the VM image from the list of images. The list varies according to the option selected in the **Image Selection Type** drop-down list. **Note** All the VM images are listed from managed cloud irrespective of the cloud type. **Note** The images that satisfy the following conditions are displayed for selection: • The images that have VMware tools installed. • The images that are not assigned to any group.
Virtual Compute Service Class drop-down list	Choose the service class for the virtual compute category.
Virtual Storage Service Class drop-down list	Choose the service class for the virtual storage category.
VM Password Sharing Option drop-down list	Choose how you want to share the root or administrator password for the VM with end users: • **Do not share** • **Share after password reset** • **Share template credentials** Specify the root login ID and root password for the template that appears when you choose **Share after password reset** or **Share template credentials** as the password sharing option.
VM Network Interfaces field	Click the + icon to add a VM network interface.
Maximum Quantity field	The maximum number of VM instances per tier. **Note** This number allows you to determine the subnet size for each tier. This number will be overridden with the value defined during application container deployment. The value is accepted even when the number of resources are less when compared to the maximum quantity in the application profile.
Initial Quantity field	The number of VM instances to be provisioned when the application is created.

c) Click **Submit**.

Step 10 In the **Application** screen, do the following:

a) In the **Bare Metal Application Components** field, click the + icon.

b) In the **Add Entry to Bare Metal Application Components** dialog box, complete the following fields:

Name	Description
Instance Name field	Enter the name of the baremetal instance.
Description field	Enter the description of the baremetal instance.
Network drop-down list	Choose the network.
Target BMA drop-down list	Choose the baremetal agent (BMA) for PXE setup.
Bare Metal image drop-down list	Choose the baremetal image.
Blade Type drop-down list	Choose one of the following as the blade type for the APIC container: • **Half Width** • **Full Width**
Physical Compute Service Class drop-down list	Choose the service class for the physical compute category.
Physical Storage Service Class drop-down list	Choose the service class for the physical storage category.

c) Click **Submit**.

Step 11 Click **Next**.

Step 12 In the **Contracts** screen, you can define the rule for communication in multi-tier applications.
Contracts are policies that enable inter-End Point Group (inter-EPG) communication. These policies are the rules that specify communication between application tiers. If no contract is attached to the EPG, inter-EPG communication is disabled by default. No contract is required for intra-EPG communication because intra-EPG communication is always allowed.

A contract can contain multiple subjects. A subject can be used to realize uni- or bidirectional filters. A unidirectional filter is a filter that is used in one direction, either from consumer-to-provider (IN) or from provider-to-consumer (OUT) filter. A bidirectional filter is the same filter that is used in both directions. It is not reflexive.

A new contract is created for each source-to-destination network pair. For example, if there are multiple rules defined between Web tier as source and application tier as destination network, a single contract will be created on APIC to hold the contract information between Web tier as source and application tier as destination network.

For a contract, a new subject is created if the rule defines unidirectional or bidirectional filter. A subject is reused for multiple rules under same contract depending on whether rule includes unidirectional or bidirectional filter.

A new filter is created for a specific rule. A new filter rule is created for every rule defined between networks.

Click the + icon to add the communication protocol details:

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

Name	Description
Rule Name field	Enter the name of the rule.
Select Source Network drop-down list	Choose the source network to which you want to apply the contract rule. When an external network is chosen as the source network, only the **Rule Name** field, **Select Source Network** drop-down list, and **Select Destination Network** drop-down list are available for configuration. Cisco UCS Director uses the existing contract as tagged and updated in tenant vPOD previous to configuring the application profile based on the tag used in the chosen external network.
Select Destination Network drop-down list	Choose the destination network to which you want to apply the contract rule.
Rule Description field	Enter the description of the rule.
Protocol drop-down list	Choose the protocol for communication.
Apply Both Directions check box	Check the check box to apply the same contract for traffic from source to destination, or from destination to source.
An annotation states that the app/web tier allows the subnet to be created as Shared and Public through the APIC network policy.	
Action drop-down list	Choose the action to be taken for the communication: • **Accept** • **Drop** • **Reject**

b) Click **Submit**.

Step 13 Click **Next**.

Step 14 In the **Policy** screen, do the following:

a) Choose a policy from the **VMware System Policy** drop-down list.
b) Click the + icon to add a new policy to the system policy drop-down list.
c) In the **System Policy Information** dialog box, complete the following fields:

Name	Description
Policy name field	Enter the name of the system policy.

Name	Description
Policy Description field	Enter the description of the system policy.
VM Name Template field	The template to use for the VM name. **Note** If the name template is not specified, the name provided by the end user is used as the VM name.
VM Name Validation Policy drop-down list	Choose the policy for validating the VM name.
End User VM Name or VM Prefix check box	Check the check box to allow the end user to specify the name or prefix for the VM.
Power On after deploy check box	Check the check box to power on the VM after provisioning.
Host Name Template field	Enter the template of the hostname.
Host Name Validation Policy drop-down list	Choose the policy for validating the host name.
Linux Time Zone drop-down list	Choose the time zone for the Linux VM.
Linux VM Max Boot Wait Time drop-down list	Choose the value to specify the maximum length of time that the VM will pause during startup.
DNS Domain field	The name of the DNS domain.
DNS Suffix List field	The list of domain name suffixes that get appended to DNS.
DNS Server List field	The list of DNS servers.
VM Image Type drop-down list	Choose one of the following as the VM image type: • **Windows and Linux** • **Linux Only**
Define VM Annotation check box	Check the check box to define the VM annotation.

d) Click **Close**.
e) Choose a cost model from the **Cost Model** drop-down list to compute the chargeback.
f) Choose the HyperV deployment policy for the HyperV container provision from the **HyperV Deployment Policy** drop-down list.
g) Click **Next**.

Step 15 In the **L4-L7 Service Policy** screen, check the **Configure L4-L7 Service** check box to configure the Layer 4 to Layer 7 service in the application profile. If the **Configure L4-L7 Service** check box is checked, the following fields appear:

a) **L4-L7 Service Policy** drop-down list—Choose the Layer 4 to Layer 7 service policy from the list. Click the + icon to add a Layer 4 to Layer 7 service policy. For more information about how to add a Layer 4 to Layer 7 service policy, see Adding a Layer 4 to Layer 7 Service Policy, on page 79.

b) **Application L4-L7 Service Definition** field—Click the + icon. In the **Add Entry to Application L4-L7 Service Definition** dialog box, complete the following fields:

Name	Description
Service Name field	Enter the name of the service.
Consumer drop-down list	Choose the internal tier.
Provider drop-down list	Choose the external tier.
Protocol drop-down list	Choose a protocol. **Note** This field appears only for the load balancer service.
Port drop-down list	The port number of the selected protocol. **Note** This field appears only for the load balancer service.
Services field	Choose the service type by checking one of the following check boxes: • **FIREWALL—**To provide firewall service between consumer and provider. • **LB_SINGLE_ARM—**To configure load balancer service between consumer and provider in the single-arm mode. In the single-arm mode, the load balancer is connected to the network through a single interface. **Note** The single-arm load balancer service is the only supported service type for a tenant with multiple private networks. • **FW_LB_ONE_ARM—**To configure both firewall and single-arm load balancer services between consumer and provider. In the single-arm mode, the load balancer is connected to the network through a single interface. • **FW_LB_SSL_OFFLOAD—**To configure both firewall and load balancer services between consumer and provider along with the SSL offload support.

c) Check the **Customize Firewall Security For Tiers** check box to customize the firewall security for the network tiers in the application profile. The **Firewall Security Levels** field displays the security level configured for the tiers. Choose a tier and click the edit icon to edit the security level.

Step 16 Click **Submit**.

Cloning an Application Profile

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

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

Step 3 Choose an application profile.

Step 4 Click **Clone**.

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

Name	Description
Name field	The name of the application profile. Once added, the name cannot be modified.
Description field	The description of the application profile.

Step 6 Click **Next**.

Step 7 In the **Networks** screen, complete the following fields:

Name	Description
Service Offering drop-down list	Click **Select** and choose a service offering from the list. The service offering must belong to the tenant for which you will create containers with this application profile. Click the + icon to add a service offering. For more information about how to add a service offering, see the Cisco UCS Director APIC Management Guide.
Networks field	Define the network types and the number of networks that are needed in the application. For more information on how to configure a network, see the *next Step*.

Step 8 (Optional). In the Network field of the **Networks** screen, click the + icon to configure the tier for application. In the **Add Entry to Networks** dialog box, complete the following fields:

Name	Description
Network field	Enter the name of the network.
Description field	Enter the description of the network.
Network Type drop-down list	Choose one of the following as the network type: • **Internal** • **External** • **Infrastructure** • **Failover** **Note** When a tenant needs multiple private networks, you need to define only **Internal** and **External** network types.
Interested Tag Value field	Click **Select** and choose the tag values for each tier. During container provisioning, resource is selected based on the tag associated with the tier. **Note** You can select more than one tag (the tag that is used for VMware cluster or datastore cluster). For example, if you select a datastore tag (ds tag - gold) and a VMware cluster tag (cluster tag - ESXi cluster tag), during the datastore selection, the datastore tagged with the gold value is selected. **Note** To avail shared L3Out support, choose the tag value that is used for tagging the external network and contract of a common tenant.
APIC Network Policy drop-down list	This field appears only when you choose network type as **Internal**. Choose the APIC network policy from the list. Click the + icon to add an APIC network policy. For more information about how to add an APIC network policy, see Adding an APIC Network Policy, on page 77.

Name	Description
L2/L3 Selection drop-down list	This field appears only when you choose network type as **External**. By default, **L2Out** is selected to integrate the ACI fabric with external Layer 2 network. • **L2Out—**To integrate the ACI fabric with external Layer 2 network. • **L3Out—**To integrate the ACI fabric with external Layer 3 network. • **SharedL3Out—**To integrate the ACI fabric with shared external Layer 3 network. The network must be tagged and updated on Tenant vPOD in advance and the same tag must be selected for the external network in case of shared L3Out.
Use Existing L2/L3 Out config available in the tenant check box	This field appears only when you choose network type as **External**. By default, the check box is checked to use the L2/L3 out configuration defined in the tenant while creating a container. **Note** When a container is created based on an application profile, tenants having L2 out or L3 out configuration are displayed according to the L2/L3 selection in the application profile.

Step 9 Click **Next**.

Step 10 In the **Application** screen, add VM-based application components:

a) Click the + icon.

b) In the **Add Entry to VM Application Components** dialog box, complete the following fields:

Name	Description
VM Name field	Enter the name of the VM.
Description field	Enter the description of the VM.
Network drop-down list	Choose the network from the list.
Image Selection Type drop-down list	Choose one of the following for the image selection: • **All Images** • **Image Tag based selection—**When you choose the image tag-based selection, the **Tag** field appears. Click the + icon to add a tag.

Name	Description
VM image drop-down list	Choose the VM image from the list of images. The list varies according to the option selected in the **Image Selection Type** drop-down list. **Note** All the VM images are listed from managed cloud irrespective of the cloud type. **Note** The images that satisfy the following conditions are displayed for selection: • The images that have VMware tools installed. • The images that are not assigned to any group.
Virtual Compute Service Class drop-down list	Choose the service class for the virtual compute category.
Virtual Storage Service Class drop-down list	Choose the service class for the virtual storage category.
VM Password Sharing Option drop-down list	Choose how you want to share the root or administrator password for the VM with end users: • **Do not share** • **Share after password reset** • **Share template credentials** Specify the root login ID and root password for the template that appears when you choose **Share after password reset** or **Share template credentials** as the password sharing option.
VM Network Interfaces field	Click the + icon to add a VM network interface.
Maximum Quantity field	The maximum number of VM instances per tier. **Note** This number allows you to determine the subnet size for each tier. This number will be overridden with the value defined during application container deployment. The value is accepted even when the number of resources are less when compared to the maximum quantity in the application profile.
Initial Quantity field	The number of VM instances to be provisioned when the application is created.

c) Click **Submit**.

Step 11 In the **Application** screen, add baremetal application components:

a) Click the + icon.

b) In the **Add Entry to Bare Metal Application Components** dialog box, complete the following fields:

Name	Description
Instance Name field	Enter the name of the baremetal instance.
Description field	Enter the description of the baremetal instance.
Network drop-down list	Choose the network.
Target BMA drop-down list	Choose the baremetal agent (BMA) for PXE setup.
Bare Metal image drop-down list	Choose the baremetal image.
Blade Type drop-down list	Choose one of the following as the blade type for the APIC container: • **Half Width** • **Full Width**
Physical Compute Service Class drop-down list	Choose the service class for the physical compute category.
Physical Storage Service Class drop-down list	Choose the service class for the physical storage category.

c) Click **Submit**.

Step 12 Click **Next**.

Step 13 Click the + icon to add the communication protocol details.

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

Name	Description
Rule Name field	Enter the name of the rule.
Select Source Network drop-down list	Choose the source network to which you want to apply the contract rule. When an external network is chosen as the source network, only the **Rule Name** field, **Select Source Network** drop-down list, and **Select Destination Network** drop-down list are available for configuration. Cisco UCS Director uses the existing contract as tagged and updated in tenant vPOD previous to configuring the application profile based on the tag used in the chosen external network.

Name	Description
Select Destination Network drop-down list	Choose the destination network to which you want to apply the contract rule.
Rule Description field	Enter the description of the rule.
Protocol drop-down list	Choose the protocol for communication.
Apply Both Directions check box	Check the check box to apply the same contract for traffic from source to destination, or from destination to source.
An annotation states that the app/web tier allows the subnet to be created as Shared and Public through the APIC network policy.	
Action drop-down list	Choose the action to be taken for the communication: • **Accept** • **Drop** • **Reject**

b) Click **Submit**.

Step 14 Click **Next**.

Step 15 In the **Policy** screen, do the following:

a) Choose a policy from the **VMware System Policy** drop-down list.

b) Click the + icon to add a new policy to the system policy drop-down list.

c) In the **System Policy Information** dialog box, complete the following fields:

Name	Description
Policy name field	Enter the name of the system policy.
Policy Description field	Enter the description of the system policy.
VM Name Template field	The template to use for the VM name. **Note** If the name template is not specified, the name provided by the end user is used as the VM name.
VM Name Validation Policy drop-down list	Choose the policy for validating the VM name.
End User VM Name or VM Prefix check box	Check the check box to allow the end user to specify the name or prefix for the VM.
Power On after deploy check box	Check the check box to power on the VM after provisioning.

Name	Description
Host Name Template field	Enter the template of the hostname.
Host Name Validation Policy drop-down list	Choose the policy for validating the host name.
Linux Time Zone drop-down list	Choose the time zone for the Linux VM.
Linux VM Max Boot Wait Time drop-down list	Choose the value to specify the maximum length of time that the VM will pause during startup.
DNS Domain field	The name of the DNS domain.
DNS Suffix List field	The list of domain name suffixes that get appended to DNS.
DNS Server List field	The list of DNS servers.
VM Image Type drop-down list	Choose one of the following as the VM image type: • **Windows and Linux** • **Linux Only**
Define VM Annotation check box	Check the check box to define the VM annotation.

d) Click **Close**.
e) Choose a cost model from the **Cost Model** drop-down list to compute the chargeback.
f) Choose the HyperV deployment policy for the HyperV container provision from the **HyperV Deployment Policy** drop-down list.
g) Click **Next**.

Step 16 In the **L4-L7 Service Policy** screen, check the **Configure L4-L7 Service** check box to configure the Layer 4 to Layer 7 service in the application profile. If the **Configure L4-L7 Service** check box is checked, the following fields appear:

a) **L4-L7 Service Policy** drop-down list—Choose the Layer 4 to Layer 7 service policy from the list. Click the + icon to add a Layer 4 to Layer 7 service policy. For more information about how to add a Layer 4 to Layer 7 service policy, see Adding a Layer 4 to Layer 7 Service Policy, on page 79.
b) **Application L4-L7 Service Definition** field—Click the + icon. In the **Add Entry to Application L4-L7 Service Definition** dialog box, complete the following fields:

Name	Description
Service Name field	Enter the name of the service.
Consumer drop-down list	Choose the internal tier.
Provider drop-down list	Choose the external tier.

Name	Description
Protocol drop-down list	Choose a protocol. **Note** This field appears only for the load balancer service.
Port drop-down list	The port number of the selected protocol. **Note** This field appears only for the load balancer service.
Services field	Choose the service type by checking one of the following check boxes: • **FIREWALL—**To provide firewall service between consumer and provider. • **LB_SINGLE_ARM—**To configure load balancer service between consumer and provider in the single-arm mode. In the single-arm mode, the load balancer is connected to the network through a single interface. **Note** The single-arm load balancer service is the only supported service type for a tenant with multiple private networks. • **FW_LB_ONE_ARM—**To configure both firewall and single-arm load balancer services between consumer and provider. In the single-arm mode, the load balancer is connected to the network through a single interface. • **FW_LB_SSL_OFFLOAD—**To configure both firewall and load balancer services between consumer and provider along with the SSL offload support.

c) Check the **Customize Firewall Security For Tiers** check box to customize the firewall security for the network tiers in the application profile. The **Firewall Security Levels** field displays the security level configured for the tiers. Choose a tier and click the edit icon to edit the security level.

Step 17 Click **Submit**.

Editing an Application Profile

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

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

Step 3 Choose an application profile.

Step 4 Click **Edit**.

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

Name	Description
Name field	The name of the application profile. Once added, the name cannot be modified.
Description field	The description of the application profile.

Step 6 Click **Next**.

Step 7 In the **Networks** screen, complete the following fields:

Name	Description
Service Offering field	This field shows the service offering chosen when the application profile was created. It cannot be changed.
Networks field	Define the network types and number of networks that are needed in the application. For more information on how to configure a network, see the *next Step*.

Step 8 (Optional). In the Network field of the **Networks** screen, click the + icon to configure the tier for application.
In the **Add Entry to Networks** dialog box, complete the following fields:

Name	Description
Network field	Enter the name of the network.
Description field	Enter the description of the network.

Name	Description
Network Type drop-down list	Choose one of the following as the network type: • **Internal** • **External** • **Infrastructure** • **Failover** **Note** When a tenant needs multiple private networks, you need to define only **Internal** and **External** network types.
Interested Tag Value field	Click **Select** and choose the tag values for each tier. During container provisioning, resource is selected based on the tag associated with the tier. **Note** You can select more than one tag (the tag that is used for VMware cluster or datastore cluster). For example, if you select a datastore tag (ds tag - gold) and a VMware cluster tag (cluster tag - ESXi cluster tag), during the datastore selection, the datastore tagged with the gold value is selected. **Note** To avail shared L3Out support, choose the tag value that is used for tagging the external network and contract of a common tenant.
APIC Network Policy drop-down list	This field appears only when you choose network type as **Internal**. Choose the APIC network policy from the list. Click the + icon to add an APIC network policy. For more information about how to add an APIC network policy, see Adding an APIC Network Policy, on page 77.
L2/L3 Selection drop-down list	This field appears only when you choose network type as **External**. By default, **L2Out** is selected to integrate the ACI fabric with external Layer 2 network. • **L2Out—**To integrate the ACI fabric with external Layer 2 network. • **L3Out—**To integrate the ACI fabric with external Layer 3 network. • **SharedL3Out—**To integrate the ACI fabric with shared external Layer 3 network. The network must be tagged and updated on Tenant vPOD in advance and the same tag must be selected for the external network in case of shared L3Out.

Name	Description
Use Existing L2/L3 Out config available in the tenant check box	This field appears only when you choose network type as **External**. By default, the check box is checked to use the L2/L3 out configuration defined in the tenant while creating a container. **Note** When a container is created based on an application profile, tenants having L2 out or L3 out configuration are displayed according to the L2/L3 selection in the application profile.

Step 9 Click **Next**.

Step 10 In the **Application** screen, add VM-based application components:

a) Click the + icon.

b) In the **Add Entry to VM Application Components** dialog box, complete the following fields:

Name	Description
VM Name field	Enter the name of the VM.
Description field	Enter the description of the VM.
Network drop-down list	Choose the network from the list.
Image Selection Type drop-down list	Choose one of the following for the image selection: • **All Images** • **Image Tag based selection—**When you choose the image tag-based selection, the **Tag** field appears. Click the + icon to add a tag.
VM image drop-down list	Choose the VM image from the list of images. The list varies according to the option selected in the **Image Selection Type** drop-down list. **Note** All the VM images are listed from managed cloud irrespective of the cloud type. **Note** The images that satisfy the following conditions are displayed for selection: • The images that have VMware tools installed. • The images that are not assigned to any group.
Virtual Compute Service Class drop-down list	Choose the service class for the virtual compute category.
Virtual Storage Service Class drop-down list	Choose the service class for the virtual storage category.

Name	Description
VM Password Sharing Option drop-down list	Choose how you want to share the root or administrator password for the VM with end users: • **Do not share** • **Share after password reset** • **Share template credentials** Specify the root login ID and root password for the template that appears when you choose **Share after password reset** or **Share template credentials** as the password sharing option.
VM Network Interfaces field	Click the + icon to add a VM network interface.
Maximum Quantity field	The maximum number of VM instances per tier. **Note** This number allows you to determine the subnet size for each tier. This number will be overridden with the value defined during application container deployment. The value is accepted even when the number of resources are less when compared to the maximum quantity in the application profile.
Initial Quantity field	The number of VM instances to be provisioned when the application is created.

c) Click **Submit**.

Step 11 In the **Application** screen, add baremetal-based application components:

a) Click the + icon.

b) In the **Add Entry to Bare Metal Application Components** dialog box, complete the following fields:

Name	Description
Instance Name field	Enter the name of the baremetal instance.
Description field	Enter the description of the baremetal instance.
Network drop-down list	Choose the network.
Target BMA drop-down list	Choose the baremetal agent (BMA) for PXE setup.
Bare Metal image drop-down list	Choose the baremetal image.

Name	Description
Blade Type drop-down list	Choose one of the following as the blade type for the APIC container: • **Half Width** • **Full Width**
Physical Compute Service Class drop-down list	Choose the service class for the physical compute category.
Physical Storage Service Class drop-down list	Choose the service class for the physical storage category.

c) Click **Submit**.

Step 12 Click **Next**.

Step 13 Click the + icon to add the communication protocol details.

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

Name	Description
Rule Name field	Enter the name of the rule.
Select Source Network drop-down list	Choose the source network to which you want to apply the contract rule. When an external network is chosen as the source network, only the **Rule Name** field, **Select Source Network** drop-down list, and **Select Destination Network** drop-down list are available for configuration. Cisco UCS Director uses the existing contract as tagged and updated in tenant vPOD previous to configuring the application profile based on the tag used in the chosen external network.
Select Destination Network drop-down list	Choose the destination network to which you want to apply the contract rule.
Rule Description field	Enter the description of the rule.
Protocol drop-down list	Choose the protocol for communication.
Apply Both Directions check box	Check the check box to apply the same contract for traffic from source to destination, or from destination to source.
An annotation states that the app/web tier allows the subnet to be created as Shared and Public through the APIC network policy.	

Name	Description
Action drop-down list	Choose the action to be taken for the communication: • **Accept** • **Drop** • **Reject**

b) Click **Submit**.

Step 14 Click **Next**.

Step 15 In the **Policy** screen, do the following:

a) Choose a policy from the **VMware System Policy** drop-down list.

b) Click the + icon to add a new policy to the system policy drop-down list.

c) In the **System Policy Information** dialog box, complete the following fields:

Name	Description
Policy name field	Enter the name of the system policy.
Policy Description field	Enter the description of the system policy.
VM Name Template field	The template to use for the VM name. **Note** If the name template is not specified, the name provided by the end user is used as the VM name.
VM Name Validation Policy drop-down list	Choose the policy for validating the VM name.
End User VM Name or VM Prefix check box	Check the check box to allow the end user to specify the name or prefix for the VM.
Power On after deploy check box	Check the check box to power on the VM after provisioning.
Host Name Template field	Enter the template of the hostname.
Host Name Validation Policy drop-down list	Choose the policy for validating the host name.
Linux Time Zone drop-down list	Choose the time zone for the Linux VM.
Linux VM Max Boot Wait Time drop-down list	Choose the value to specify the maximum length of time that the VM will pause during startup.
DNS Domain field	The name of the DNS domain.

Name	Description
DNS Suffix List field	The list of domain name suffixes that get appended to DNS.
DNS Server List field	The list of DNS servers.
VM Image Type drop-down list	Choose one of the following as the VM image type: • **Windows and Linux** • **Linux Only**
Define VM Annotation check box	Check the check box to define the VM annotation.

d) Click **Close**.
e) Choose a cost model from the **Cost Model** drop-down list to compute the chargeback.
f) Choose the HyperV deployment policy for the HyperV container provision from the **HyperV Deployment Policy** drop-down list.
g) Click **Next**.

Step 16 In the **L4-L7 Service Policy** screen, edit the Layer 4 to Layer 7 service configuration.

Step 17 Click **Submit**.

Deleting an Application Profile

Note You cannot delete an application profile that is in use.

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

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

Step 3 Choose an application profile from the table.

Step 4 Click **Delete**.

Step 5 In the **Application Profile** confirmation dialog box, click **Delete**.

Creating a Virtual Infrastructure Policy

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

Step 2 Click the **Virtual Infrastructure Policies** tab.

Step 3 Click **Add Policy**.

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

Name	Description
Policy Name field	Enter a unique name for the policy.
Policy Description field	Enter a description of the virtual infrastructure policy.
Container Type drop-down list	Choose a container type. Choose **APIC** to create a Virtual Infrastructure Policy for APIC container. **Note** If an application container policy is created using the **No Gateway** option, a gateway VM is not provisioned (irrespective of the container type).

Step 5 Click **Next**.

Step 6 In the **Virtual Infrastructure Policy - APIC Information** screen, complete the following fields.

Note If an application container policy is created using the **No Gateway** option, a gateway VM is not provisioned.

Name	Description
Application Profile drop-down list	Choose an application profile.
+ icon	Click this icon to create a new application profile. You will be prompted to create a new application profile as described in the Cisco UCS Director APIC Management Guide.

Step 7 Click **Next**.

Step 8 The **Virtual Infrastructure Policy - Summary** screen displays the current configuration.

Step 9 Click **Submit**.

Creating an Application Container Template

Before you can create an APIC application container you must create a template.

Before You Begin

Create a virtual infrastructure policy.

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

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

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

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

Step 4 Click **Next**.

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

Name	Description
Select Virtual Infrastructure Policy drop-down list	Choose an APIC policy.
+	Click the + icon to create a new infrastructure policy. See Creating a Virtual Infrastructure Policy , on page 108.

Step 6 Click **Next**. The **Application Container - Options** screen appears. Complete the following selections:

Name	Description
End User Self-Service Policy dropdown	Select an end-user policy. See Configuring Options on the Self-Service Portal, on page 33
Enable Self-Service Deletion of Containers check box	If checked, allows the end user to delete the application container.
Enable VNC Based Console Access check box	If checked, allows the end user to open VNC consoles to VMs in the browser.
Technical Support Email Addresses field	Enter a comma-separated list of email addresses for the technical support contact person(s).

Step 7 Click **Next** to view the **Summary** screen.

Step 8 Click **Submit** to complete the creation of the application container template.

Creating an APIC Application Container

Once you create an application container template you can use the template administrator to initiate a service request that will create an application container.

Before You Begin

Create an application container template.

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

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

Step 3 Choose an **APIC** template.

Step 4 Click **Create Container**.

Step 5 In the **Create container from template** dialog box, complete the following fields:

Name	Description
Container Name drop-down list	Enter the name of the container. This name must be unique.
Container Label field	Enter the label for the container.
Tenant list	Choose a tenant. **Note** If your application template has Layer 2 or Layer 3 tier requirement, the list shows only tenants for which Layer 2 or Layer 3 is configured.
Customer Organizations drop-down list	Choose an organization within the tenant (optional).
Enable Resource Limits check box	Check this check box to specify the number of vCPUs, Memory, Maximum Storage, and maximum number of servers for the container
Enable Network Management check box	Check this check box to put the container under APIC management.
Tier Label Customization area	This area does not appear for a tenant with multiple private networks. The customized name of the tier label.

Step 6 Click **Submit**. The **Submit Result** dialog box appears.
Note Make a note of the service request ID presented in the **Submit Result** prompt.

Step 7 Click **OK**.
Note You can view the progress of the created container by viewing the details of the service request.

Step 8 Click the **Application Containers** tab.
The new container appears in the **Application Containers** pane.

Note The service request may require some time to run. Check the service request progress to determine if the entire workflow has run successfully before trying to use the container.

Configuring L4-L7 Services

APIC application containers support L4-L7 services. This procedure describes how to configure L4-L7 services for an existing container. You can add loadbalancer service using **userAPIAddLBService** API.

Before You Begin

Create an APIC application container.

Note This section describes how to add an L4-L7 service to an existing application container. You can instead configure L4-L7 services in an APIC application profile, where they will be deployed with every application container using that profile. For more information on configuring L4-L7 services in an application profile, see Layer 4 to Layer 7 Service Policy, on page 79 .

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

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

Step 3 Click on an existing application container.

Step 4 Click the **Configure L4-L7 Services** icon.

Step 5 In the **L4-L7 Configuration** dialog box, complete the following fields:

Name	Description
Service Type drop-down list	Choose any one of the following service types: • **Firewall** (default value) • **Load Balancer (One Arm)** • **Load Balancer (One Arm, SSL Offload)** **Note** This service type appears only if the container is already configured with **Firewall and Load Balancer (One Arm, with SSL Offload)** chain. • **Firewall and Single Arm Load Balancer** • **Firewall and Load Balancer (One Arm, with SSL Offload)** **Note** If the chosen container does not support L4-L7 services, the service types are not listed in the **Service Type** drop-down list.
Service Name field	Enter a unique name for the service.

Name	Description
Consumer drop-down list	Select a network (tier) as the service consumer.
Provider drop-down list	Select a network (tier) as the service provider.
The following fields appear only if the Load Balancer service type is chosen from the **Service Type** drop-down list.	
LB Servers	This field does not appear if the container for a tenant with multiple private networks is selected. Enter each IP address of the load balancer server with a comma.
Protocol drop-down list	Choose a protocol.
Port field	This field does not appear if the container for a tenant with multiple private networks is selected. The port number of the selected protocol.
The following fields appear only if the **Load Balancer (One Arm, SSL Offload)** is chosen from the **Service Type** drop-down list.	
SSL Port field	The port number of the SSL enabled vServer.
Certificate field	A valid SSL certificate.
Key field	Unique key for the SSL certificate.
The following fields appear only if the container for the tenant with multiple private networks is selected.	
Front End Port	The front end port number.
Back End Port	The back end port number.
CookieName	Enter the name of the cookie.
LB Method	Choose the load balancer method.
PersistenceType	Choose the persistence type.

Step 6 Click **Submit**.

Adding Firewall Rules

Before You Begin

Cisco UCS Director allows an administrator or end user to create an APIC application container with L4-L7 services.

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

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

Step 3 Click an existing application container.

Step 4 Choose any L4-L7 service with Firewall service type.
The **Firewall Rules** screen appears.

Step 5 Click the **Add Rule (+)** icon to add a new firewall rule.

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

Name	Description
Interface Name drop-down list	Choose the name of the interface.
ACL Direction drop-down list	Choose **Inbound** or **Outbound** as the ACL direction.
ACE Name field	Enter the ACE name that defines the firewall rule.
Protocol drop-down list	Choose the protocol for communication.
Source Port Range field	This field appears only if TCP or UDP protocol is selected. Enter the source port range.
Destination Port Range field	This field appears only if TCP or UDP protocol is selected. Enter the destination port range.
Source Any check box	This check box is checked to permit any source host or network.
Source Address field	This field appears when you uncheck the **Source Any** check box. The IP address, IP address range, or IP address with subnet mask to specify either a single host or a range of them as the source address.
Destination Any check box	This check box is checked to apply the ACE entry statement on any destination address.
Destination Address field	This field appears when you uncheck the **Destination Any** check box. The IP address, IP address range, or IP address with subnet mask to specify either a single host or a range of them as the destination address.

Name	Description
Action drop-down list	Choose **Permit** or **Deny** as the action for the ACE entry.
Order field	The sequence in which deny statements or permit statements need to be executed.

Step 7 Click **Submit**.

To make changes to a firewall rule, choose the firewall rule and click **Modify Rule**. To remove a firewall rule, choose the firewall rule and click **Delete Rule**.

Adding Real Servers to Load Balancer Service

Before You Begin

Cisco UCS Director allows an administrator or end user to create an APIC application container with L4-L7 services.

Step 1 On the menu bar, choose **Policies** > **Application Containers**.
Step 2 Click the **Application Container** tab.
Step 3 Click an existing application container.
Step 4 Choose any L4-L7 service with Load Balancer service type.
The **LB Servers** screen appears.
Step 5 In the **Add Servers** dialog box, choose any VM(s) from the table.
Step 6 In the **Port** field , enter the port number.
The selected VMs are configured with this port number.
Step 7 Click **Submit**.

To remove the load balancer server, click **Remove Servers**.

Deleting L4-L7 Services

Before You Begin

Create and deploy an existing application container with one or more L4-L7 services.

Step 1 On the menu bar, choose **Policies** > **Application Containers**.
Step 2 Choose an application container.
Step 3 Click **L4 L7 Services**.
Step 4 From the list of L4-L7 services, choose the service that you want to delete.
Step 5 Click **Delete**.
Step 6 In the confirmation dialog, click **Delete**.

Adding Contracts

You can view the contract or security rules created for each application container in Cisco UCS Director. You can add the security rules between the tiers of a same container or different containers within that tenant.

Before You Begin

Create an APIC application container.

Step 1 On the menu bar, choose **Policies** > **Application Containers**.
Step 2 Click the **Application Container** tab.
Step 3 Click an existing application container.
Step 4 Click the **Contracts** tab.
Step 5 Click the **Add Contract** (+) icon to add a new contract.
Step 6 In the **Add Entry to Contracts** dialog box, complete the following fields:

Name	Description
Select Source Network drop-down list	Click **Select** and choose the source network in the source/destination container to which you want to apply the contract.
Select Destination Network drop-down list	Click **Select** and choose the destination network in the source/destination container to which you want to apply the contract.
Note If the contract is between the tiers of the same container, you can choose the tiers that belong to the same container, otherwise, you can choose the tiers from different containers.	

Name	Description
Create Rule check box	Check the check box to create a rule. If the check box is checked, a contract and a filter rule is created. If the check box is not checked, only an empty contract is created.
The following fields appear when the **Create Rule** check box is checked:	
Rule Name field	The name of the rule.
Rule Description field	The description of the rule.
Protocol drop-down list	Choose the protocol for communication.
Apply Both Directions check box	Check the check box to apply the same contract for traffic from source to destination, and or from destination to source.
The following fields appear only if TCP or UDP protocol is selected:	
Source Port Start	Enter the starting range of the source port number.
Source Port End	Enter the ending range of the source port number.
Destination Port Start	Enter the starting range of the destination port number.
Destination Port End	Enter the ending range of the destination port number.
Action drop-down list	Choose the action to be taken for the communication: • **Accept** • **Drop** • **Reject**

Step 7 Click **Submit**.
You can drill down each contract to view the following reports:

- Security Rules—List all the rules between the tiers of different containers.
- Contract Details—Display contract name, subject, filter, and rules for that contract.

Note When you delete the last rule for a contract, respective contract gets deleted.

Adding Security Rules

You need to drill down each contract to view all the security rules created for each application container in Cisco UCS Director.

Before You Begin

Cisco UCS Director allows an administrator and end user to create an APIC application container to add the security rules created for each application container.

Step 1 Click **Add** to add a new security rule.

Step 2 In the **Add Entry to Contracts** dialog box, complete the following fields:

Name	Description
Select Source Network drop-down list	Click **Select** and choose the source network to which you want to apply the security rule.
Select Destination Network drop-down list	Click **Select** and choose the destination network to which you want to apply the security rule.
Rule Name field	The name of the rule.
Rule Description field	The description of the rule.
Protocol drop-down list	Choose the protocol for communication.
Apply Both Directions check box	Check the check box to apply the same contract for traffic from source to destination, and or from destination to source.
The following fields appear only if TCP or UDP protocol is selected:	
Source Port Start	Enter the starting range of the source port number.
Source Port End	Enter the ending range of the source port number.
Destination Port Start	Enter the starting range of the destination port number.
Destination Port End	Enter the ending range of the destination port number.
Action drop-down list	Choose the action to be taken for the communication: • **Accept** • **Drop** • **Reject**

Step 3 Click **Submit**.
The security rule is created for the application container.

Deleting Security Rules

You need to drill down each contract to view all the security rules created for each application container inCisco UCS Director.

Before You Begin

Create an APIC application container.

Step 1 Choose any existing security rule that you want to delete.
Step 2 Click **Delete** to delete the selected security rule.
A confirmation dialog box appears.
Step 3 Click **Delete**.
The security rule is deleted.

Service Chaining

In an APIC container, you can create both a firewall and a load balancer in series between two networks. This process is called L4-L7 service chaining, or just service chaining, and the resulting firewall - load balancer series is called a service chain.

There are two ways to create a service chain in an APIC container:

- Create the service chain in an existing container. See Configuring L4-L7 Services, on page 111.
- Create both the firewall and the load balancer as part of a container's Application Profile. In this case, both services are provisioned when the container is created. See Adding an Application Profile, on page 84 and Adding a Layer 4 to Layer 7 Service Policy, on page 79.

If the VDC shows **Enable Network Management** as disabled, the following configurations are performed by default:

- The load balancer is linked to Firewall using the infrastructure network.
- A SNIP is created by default on the load balancer using one of the free IP address of the infrastructure network.
- A default route is added to the load balancer which points to the Firewall.

Adding VMs to an Existing Container

You can add VMs to an existing APIC container in the same way you add VMs to other types of containers. See Adding VMs, on page 26.

Note You can add only one network adapter when adding a VM to an existing container using an image. You can use a predefined template with multiple adapters if you created such a template in your application profile.

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

Before You Begin

Create an APIC application container.

Adding Tier/Network

Before You Begin

Create an APIC application container.

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

Step 2 Choose an existing application container.

Step 3 Click **Add Tier/Network** .

Step 4 In the **Add Tier/Network** dialog box, complete the following fields:

Name	Description
Tier/Network Name field	The name of the tier or network.
Tier Label field	The label for the tier.
Isolate Network check box	If this check box is checked, a new tier is created and associated with the selected tier. **Note** For isolated tier, subnet is taken from private IP subnet policy which is provided during tenant creation, in addition to public subnet pool policy. If this check box is not checked, only a new tier is created. **Note** For non-isolated tier, subnet is taken from the tenant assigned subnet. The non-isolated tier creation is not allowed, if the selected container has reached maximum number of allowed tiers.

Name	Description
Parent Tier drop-down list	This field appears only when the **Isolate Network** check box is checked. Choose the parent tier.

Step 5 Click **Submit**.
The new tier or network is created. You can select a virtual machine and add vNIC to the container network.

Adding a Virtual Network Interface Card to a VM

Before You Begin

Create and deploy an existing application container with one or more VMs. Before adding the virtual network interface card (vNIC) to the VM, the VM provisioned in the container must run the VMware tools and the ethernet interfaces must be up.

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

Step 2 Click the **Application Container** tab.
Click an existing application container.

Step 3 Click the **Virtual Machines** tab.
From the list of VMs, select a VM.

Step 4 Click **Add vNICs**.

Step 5 In the **Add vNICs to Container Network** dialog box, complete the following fields:

Name	Description
Network drop-down list	Choose the tier/network within the same application container that the VM resides in. **Note** The non-isolated tier/network to which the VM is already connected is filtered out from the list. **Note** The isolated tier/network to which the selected VM is part of the tier/network is also filtered out from the list.
VM Credentials	
Username	Enter the username of the VM.
Password	Enter the password of the VM.

Step 6 Click **Submit**.
The VM is powered OFF to add vNIC to the container VM. The VM is powered ON once the vNIC is added to the container network.

Deleting a Virtual Network Interface Card

Before You Begin

Create and deploy an existing application container with one or more VMs.

Step 1 On the menu bar, choose **Policies** > **Application Containers**.
Step 2 Click the **Application Container** tab.
Click an existing application container.
Step 3 Click the **Virtual Machines** tab.
From the list of VMs, select a VM of the vNIC that you want to delete.
Step 4 Click **Delete vNICs**.
Step 5 In the **Delete VM vNICs** dialog box, choose the vNIC that you want to delete.
Step 6 Click **Submit**.
The VM vNIC is deleted.

Adding Baremetal Servers to an Existing Container

Note Baremetal servers are supported only in APIC containers.

Before You Begin

Before adding baremetal servers to a container, you must add Baremetal Agent to Cisco UCS Director. See the Cisco UCS Director Baremetal Agent Installation and Configuration Guide for this release.

Step 1 Choose **Policies** > **Application Containers**.
Step 2 Click the **Application Containers** tab.
Step 3 Choose a container.
Step 4 Click **Add BMs**.
Step 5 In the **Add BMs** dialog box, click the **Add (+)** icon to add a new BM.
Step 6 In the **Add Entry** dialog box, complete the following fields:

Name	Description
Instance Name field	Enter the name you want to assign to the BM instance.
Description field	(Optional) Type a description.
Network dropdown	Choose the network (tier) to which to add the BM component.
Bare Metal Image	The BM image to use. This list is retrieved from the Baremetal Agent.
Blade Type dropdown	Choose one of the following as the blade type for the container: • Half Width • Full Width

Step 7 Click **Submit**.

Step 8 To add more BMs, repeat the procedure starting with Step 5.

Step 9 When you have defined all the required BMs, click **Submit** in the **Add BMs** dialog.

Adding a Disk

Before You Begin

Create and deploy an existing application container with one or more baremetal servers.

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

Step 2 Choose an application container.

Step 3 Click **Bare Metals**.

Step 4 Choose any baremetal server to which the disk is to be added.

Step 5 Click **Add Disk**.

Step 6 In the **Add Disk to BM** dialog box, enter the disk size in GB.

Step 7 Click **Submit**.

Deleting a Disk

Before You Begin

Create and deploy an existing application container with one or more disks associated with a bare metal server.

Step 1 On the menu bar, choose **Policies** > **Application Containers** .
Step 2 Choose an application container.
Step 3 Click **Bare Metals**.
Step 4 Choose the baremetal server from which the disk is to be deleted .
Step 5 Click **Delete Disk**.
Step 6 Choose the BM LUNs identity number that you want to delete from the table.
Step 7 Click **Submit**.
Step 8 In the confirmation dialog box, click **OK**.

Deleting Baremetal Servers

Before You Begin

Create and deploy an existing application container with one or more baremetal servers.

Step 1 On the menu bar, choose **Policies** > **Application Containers**.
Step 2 Choose an application container.
Step 3 Click **Bare Metals**.
Step 4 From the list of the baremetal servers, choose the baremetal server that you want to delete.
Step 5 Click **Delete BM**.
The baremetal server and the associated disks are deleted.