Cisco UCS Director Application Container Guide, Release 6.5

First Published: 2017-07-11

Last Modified: 2017-09-27

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.

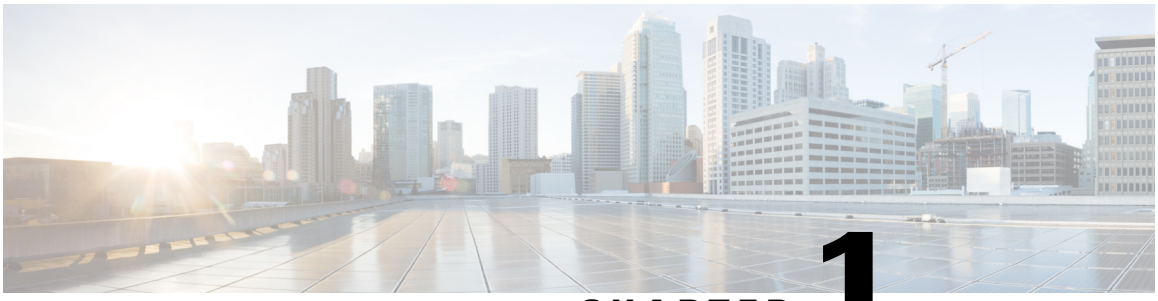
Documentation Feedback

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:

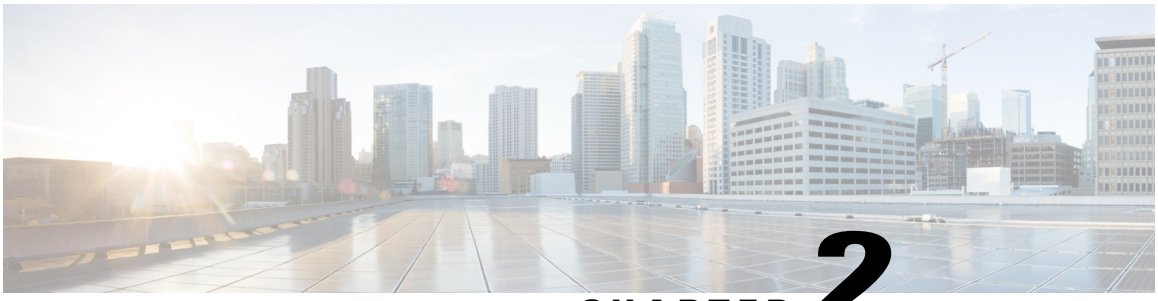
New and Changed Information for this Release

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 and Changed Behavior in Cisco UCS Director, Release 6.5

Feature	Description	Where Documented
Use Linked Clone in VM	Provides support to deploy linked VMs which are two or more related VMs that share virtual disk storage.	Creating an Application Container Template for Fenced Virtual Container, on page 29

Feature	Description	Where Documented
Provision a VM using Content Library Template	Provides support to choose a VM template from the content library VM templates for VM provisioning.	• Creating a Tiered Application Gateway Policy, on page 14 • Creating an Application Container Template, on page 17 • Creating an Application Container Template for Fenced Virtual Container, on page 29 • Creating a Virtual Infrastructure Policy, on page 46 • Creating an Application Template for a VSG, on page 47 • Creating Fabric Application Container Template, on page 56 • Adding an Application Profile, on page 82 • Cloning an Application Profile, on page 93 • Editing an Application Profile, on page 103 • Adding VMs, on page 132



CHAPTER 2

Overview of Application Containers

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 and HyperV virtual machines (VMs) and bare metal 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 Director to 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
- Access Control List (ACL) rules or other L3 services, 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

The application container types that are used in various deployment scenarios, are as follows:

- Fenced Virtual—A fenced virtual container is a collection of VMs with an internal private network that is based on rules specified by the administrator. The fenced container can have one or more VMs that are guarded by a fencing gateway to the public or external cloud. This is the most common type of application container for use with VMs. For more information, see the Setting Up a Fenced Virtual Container chapter in this guide.
- Virtual Secure Gateway (VSG)—A Cisco Virtual Secure Gateway (VSG) container is used to provide enhanced security in virtual environments. 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. For more information, see the Setting Up a Virtual Secure Gateway Application Container chapter in this guide.
- Application Centric Infrastructure Controller (APIC) container—The APIC container is used in the Cisco APIC deployments. 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 a broader cloud network. The APIC programmatically automates network provisioning and control, based on user-defined application requirements and policies. Cisco UCS Director lets you create application containers that support Cisco APIC. For more information about the APIC container, see the Setting Up a Cisco Application Policy Infrastructure Controller Container chapter in this guide, and the Cisco UCS Director APIC Management Guide for this release.
- Fabric—The fabric application container is used in Dynamic Fabric Automation (DFA) network deployments. Cisco Unified Fabric Automation is a multistage, switching network in which every connected device is reachable through the same number of hops. Cisco Unified Fabric Automation Organization fabric enables the use of a scale-out model for optimized growth. For more information on application containers in a DFA network, see the Setting Up a Fabric Container chapter in this guide, and the Cisco UCS Director Unified Fabric Automation Management Guide.

Viewing Application Containers

To view application containers in Cisco UCS Director, choose **Policies** > **Application Containers**.

Choose **Policies** > **Application Containers**.
Application containers use a color scheme to identify the container's status:

- Green—All VMs and bare metal servers (BMs) are powered on, including the gateway (GW) if the container configuration includes a GW.
- Yellow—Any of the requested BMs are still in progress/failed or any of the application VMs are down.
- Blue—Container provisioning is in progress.
- Grey—VMs and BMs are not present in the container.
- Red—All VMs and BMs, including the GW, are powered off.

Supported Layer 4 to Layer 7 Services

You can configure an application container to provision either a single tier or a multi-tier application, and you can choose to add application services, such as a load balancer or a firewall, that will be provisioned with the application. Before you create your application container, you need to decide which of these options you want to implement.

Firewall

You can add a firewall as an internal or external gateway to the application. The gateway redirects and creates a tunnel through the firewall to the application. If you use a firewall, the user does not need to know the IP address of any of the application VMs. Instead, the user logs in through the IP address of the gateway and is redirected to the application or database VM. You can also create rules that define the type of traffic that is permitted through the gateway.

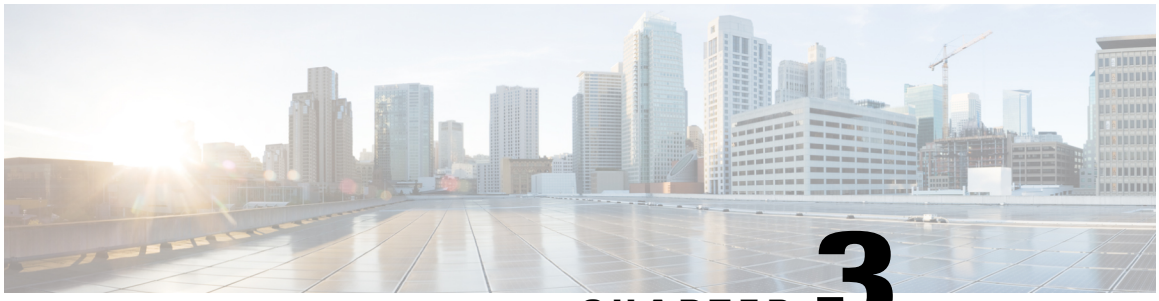
You define the firewall that you want to use in a tiered application gateway policy. This policy is then included in the application container template. You can add one of the following types of firewalls:

- Linux VM—This default option provisions the appropriate firewalls and NAT rules on the VM.
- Cisco ASA—This physical gateway allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.
- Cisco ASAv—This virtual gateway is typically deployed from a VM template, using an ASAv deployment policy, during application provisioning. The ASAv allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.

Load Balancer

You can include a load balancer for a multi-tier application. The load balancer manages communication and workloads between the servers. For example, a load balancer can identify and redirect a user to one of several application servers to ensure that none of the application servers are overloaded.

For information about supported load balancers, see the Cisco UCS Director Compatibility Matrix.



CHAPTER 3

Implementing Gateway

This chapter contains the following sections:

Linux Gateway

This is the default gateway and it provisions the appropriate firewalls and NAT rules on the VM.

Cisco Adaptive Security Appliance Gateway

Cisco UCS Director provides the ability to create an application container that makes use of a physical Adaptive Security Appliance (ASA) gateway.

This physical gateway allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.

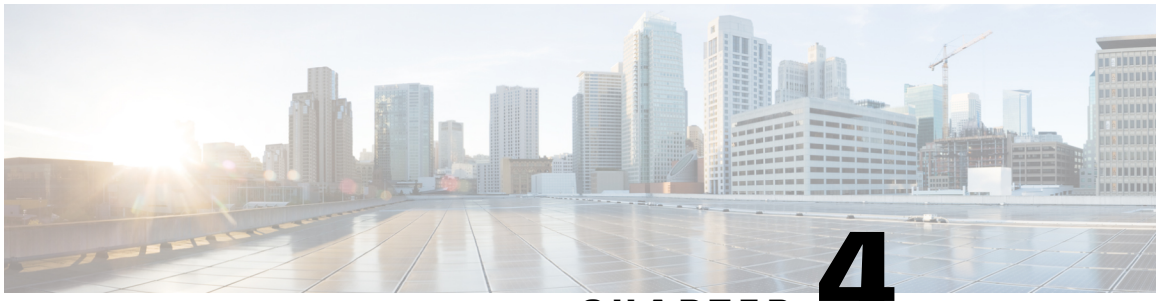
Cisco Adaptive Security Virtual Appliance Gateway

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. As 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 Cisco UCS Director, including creation and deletion of ASAv gateways.



CHAPTER 4

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 address (or port) to correspond to the virtual server IP address 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. To add the F5 load balancer, choose **Administration** > **Physical Accounts**. On the **Physical Accounts** page, click **Managed Network Elements** and then click **Add Network Element**.

2 On adding the F5 load balancer as a managed element, Cisco UCS Director triggers Cisco UCS Director task inventory collection. The polling interval configured on the **System Tasks** specifies the frequency of inventory collection.

3 After the F5 load balancer 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, choose **Physical** > **Network**. On the **Network** page, choose the Pod and click **Managed Network 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

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 (optional)
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 on the **Managed Network Element** screen.

Before You Begin

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

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

Step 2 On the **Physical Accounts** page, click **Managed Network Elements**.

Step 3 Click **Add Network Element**.

Step 4 On the **Add Network Element** screen, 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** screen specifies the frequency of inventory collection.

What to Do Next

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

Adding an F5 Load Balancing Policy

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

Step 2 On the **Application Containers** page, click **F5 Load Balancer Policies**.

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

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

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 field	Expand **Select F5 Account** and choose an **F5 load balancer** account from the available list.

Step 5 Click **Next**.

Step 6 Click **Submit**.

What to Do Next

Create a virtual infrastructure policy.

Adding an F5 Load Balancing Virtual Infrastructure Policy

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

Step 2 On the **Application Containers** page, click **Virtual Infrastructure Policies**.

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

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

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 **Fenced Virtual** as the container type.

Name	Description
Select Virtual Account drop-down list	Choose a virtual account to which you want to apply the virtual infrastructure policy.

Step 5 Click **Next**.

Step 6 On the **Virtual Infrastructure Policy - Fencing Gateway** screen, complete the following fields:

Name	Description
Gateway Required check box	Check this check box to select a gateway policy, otherwise click **Next**.
Select Gateway Policy drop-down list	If the **Gateway Required** check box is checked, this field allows you to choose a gateway policy for the virtual infrastructure policy.

Step 7 Click **Next**.

Step 8 On the **Virtual Infrastructure Policy - Fencing Load Balancing** screen, complete the following fields:

Name	Description
F5 Load Balancer Required check box	Check this check box to choose an F5 load balancing for the virtual infrastructure policy.
Select F5 Load Balancer Policy drop-down list	If the **F5 Load Balancer Required** check box is checked, this field allows you to choose an F5 load balancing policy.

Step 9 Click **Next** to view the summary of the configuration.

Step 10 Click **Submit**.

What to Do Next

Configure the Tiered Application Gateway Policies.

Creating a Tiered Application Gateway Policy

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

Step 2 On the **Application Containers** page, click **Tiered Application Gateway Policies**.

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

Step 4 On the **Policy Specification** screen, 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 On the **Gateway - Linux** screen, complete the following fields for the Linux gateway type (if applicable):

Name	Description
Provision gateway VM using Content Library template checkbox	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision gateway VM using Content Library template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image for the Gateway drop-down list	This field appears only when the **Provision gateway VM using Content Library template** checkbox is unchecked. 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.
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 On the **Policy Specification** screen, complete the following fields for the Cisco ASA gateway type:

Name	Description
Use Unified Fabric checkbox	Check the box to use unified fabric.
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	This fiels appears only when the **Use Unified Fabric** checkbox is unchecked. The IP address of the outside interface.
Outside Interface VLAN ID field	This fiels appears only when the **Use Unified Fabric** checkbox is unchecked. The VLAN ID associated to the outside interface.
Inside Interfaces field	Choose the inside interfaces from the list.

Step 8 On the **Policy Specification** screen, complete the following fields for the Cisco ASAv gateway type:

Name	Description
Use Unified Fabric checkbox	Check the box to use unified fabric.
ASAv OVF field	Check the checkbox to choose an OVF file for the Cisco ASAv device from the table.
ASAv Policy field	Check the checkbox to 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	Check the checkbox to choose an outside interface from the table.
Inside Interfaces field	Check the checkbox to choose the inside interfaces from the table. If the **Use Unified Fabric** checkbox is checked, you will be able to select an inside interafce from the drop-down list.

Step 9 Click **Next**.

Step 10 Click **Submit** after viewing the summary of the configuration.

Creating an Application Container Template

Note This procedure does not capture the steps to update a 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 a virtual infrastructure policy.

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

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

Step 3 Click **Add Template**. The **Add Application Container Template** 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 Expand **Newtorks** and click **Add (+)** icon to add a network. The **Add Entry to Networks** screen appears. Complete the following fields:

Name	Description
Dynamic Fabric Network check box	If checked, enables the application container for use in Digital Fabric Automation (DFA) 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 address for the container.
Gateway IP Address field	The IP address of the default gateway for the network. A NIC with this IP address is created on the GW VM.

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

Step 9 Click **Next**.

Step 10 Click **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.
Provision VM using Content Library Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image drop-down list	This field appears only when the **Provision VM using Content Library Template** check box is unchecked. Choose the VM image to be deployed.
Number of Virtual CPUs drop-down list	Choose the number of virtual CPUs that can be allowed in the container.
Memory drop-down list	Choose the size of the memory.
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.

Name	Description
VM Network Interfaces field	Expand **VM Network Interfaces**, and click **Add (+)** to add the VM network interface. If you are adding another network interface, click **Add (+)**. To add a new VM network interface, complete the following fields: • **VM Network Interface Name** field—The name of the VM network interface. • **Select the Network** drop-down list—Choose a network. • **Adapter Type** drop-down list —Choose the type of the adapter. • **IP Address** field —The IP address of the network.
Maximum Quantity field	States the maximum number of instances that can be added in this container after it is created.
Initial Quantity field	States the number of VM instances to provision when the container is created.

Step 11 Click **Submit**.

Step 12 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 template.
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 drop-down 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 13 Click **Next**.

Step 14 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 15 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.

Name	Description
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 16 Click **Next**. The **Application Container Template - Setup Workflows** screen appears. Complete the following fields:

Name	Description
Container Setup Workflow drop-down list	Expand **Container Setup Workflow** and check a workflow to establish the application container.

Step 17 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 18 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 47.

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

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

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

Step 3 Choose a template.

Step 4 Click **Create Container**.

Step 5 On the **Create container from template** screen, 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 field	The name of the container. This name must be unique.

Name	Description
Container Label field	The label for the container.
Tenant field	Expand **Tenant**, check the tenant that you want to use, and then click **Validate**.
Private Network Name field	This field appears only when the tenant with private network is selected. Click **Select** and choose 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 network.
The following fields appear only when the tenant with private network is selected in the **Tenant** field. 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 field	The maximum number of VM instances in the <*web*> tier.
Maximum Quantity for <APP> tier field	The maximum number of VM instances in the <*application*> tier.
Maximum Quantity for <DB> tier field	The maximum number of VM instances in the <*database*> tier.
Note The internal tier names given in the application profile are dynamically fetched and displayed 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** field.	
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.

Name	Description
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** dialog box.

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 Choose **Organizations** > **Service Requests**.

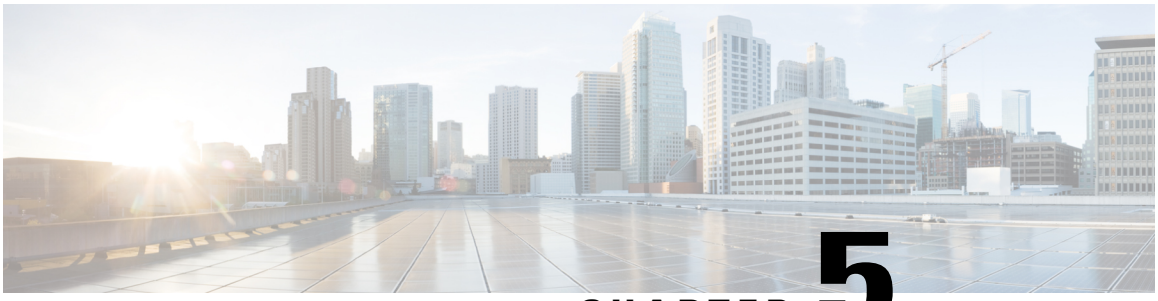
Step 2 Click the **Advanced Filter** button (far right side of interface).

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

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

Step 5 Click **Filter**.

Step 6 Double-click the **Fenced Container Setup** workflow.



CHAPTER 5

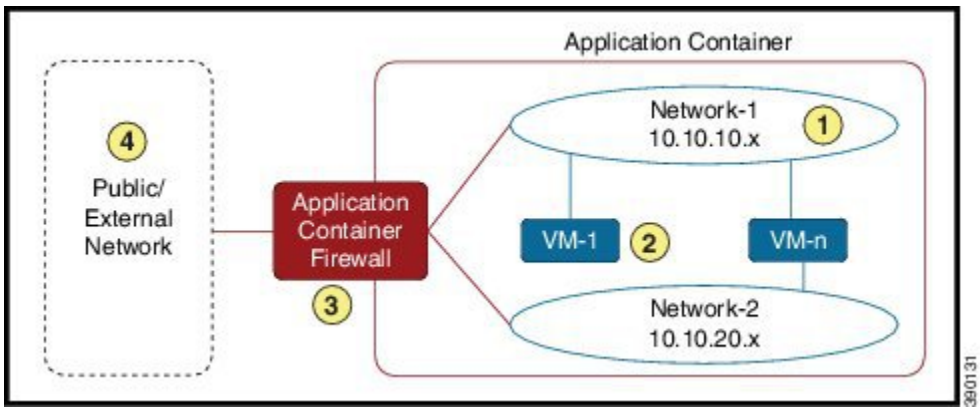
Setting Up a Fenced Virtual Container

This chapter contains the following sections:

Fenced Virtual Container

A fenced virtual container is a collection of virtual machines (VMs) with an internal private network that is created based on rules specified by the administrator. The fenced container can have one or more VMs that are guarded by a fencing gateway to the public or external cloud. Cisco UCS Director provides support for fenced containers and enables you to define container templates with one or more fenced networks and VMs. When a fenced container is created from a template, Cisco UCS Director automatically deploys VMs and configures networks and the firewall. Cisco UCS Director also automatically configures virtual and physical switches for Layer 2 changes.

Figure 1: Fenced Virtual Container - Sample



To create and manage a fenced container, perform the following steps:

1. Define a 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 fenced container template—You must perform the following tasks in the template:
   - Define the cloud account on which the container is created
   - 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 a fenced container from the defined container template—A fenced container is created from the template defined in step 2. You must choose a group for which the container is created.
4. Fenced container—After creating the fenced container, you can do various management actions, such as power management of the container, add VMs to a container, clone or delete the container, and open a console for VMs and view reports.

Fenced Virtual Container Prerequisites

The following is the prerequisite for fenced virtual container configuration:

- If you want to use Distributed Virtual Portgroup or Distributed Virtual Portgroup N1K as the virtual network types in the Allocate Container VM Resources task, ensure that you specify primary DVSwitch and alternate DVSwitch names in the Allocate Container VM Resources task. By default, Virtual Network Portgroup is set as the virtual network type.

Fenced Virtual Container Limitations

The following is the limitation of fenced virtual container:

- F5 Load Balancing is supported on fenced virtual containers.

Fenced Virtual Application Container Creation Process

The following process explains the creation of a fenced virtual application container in Cisco UCS Director:

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.

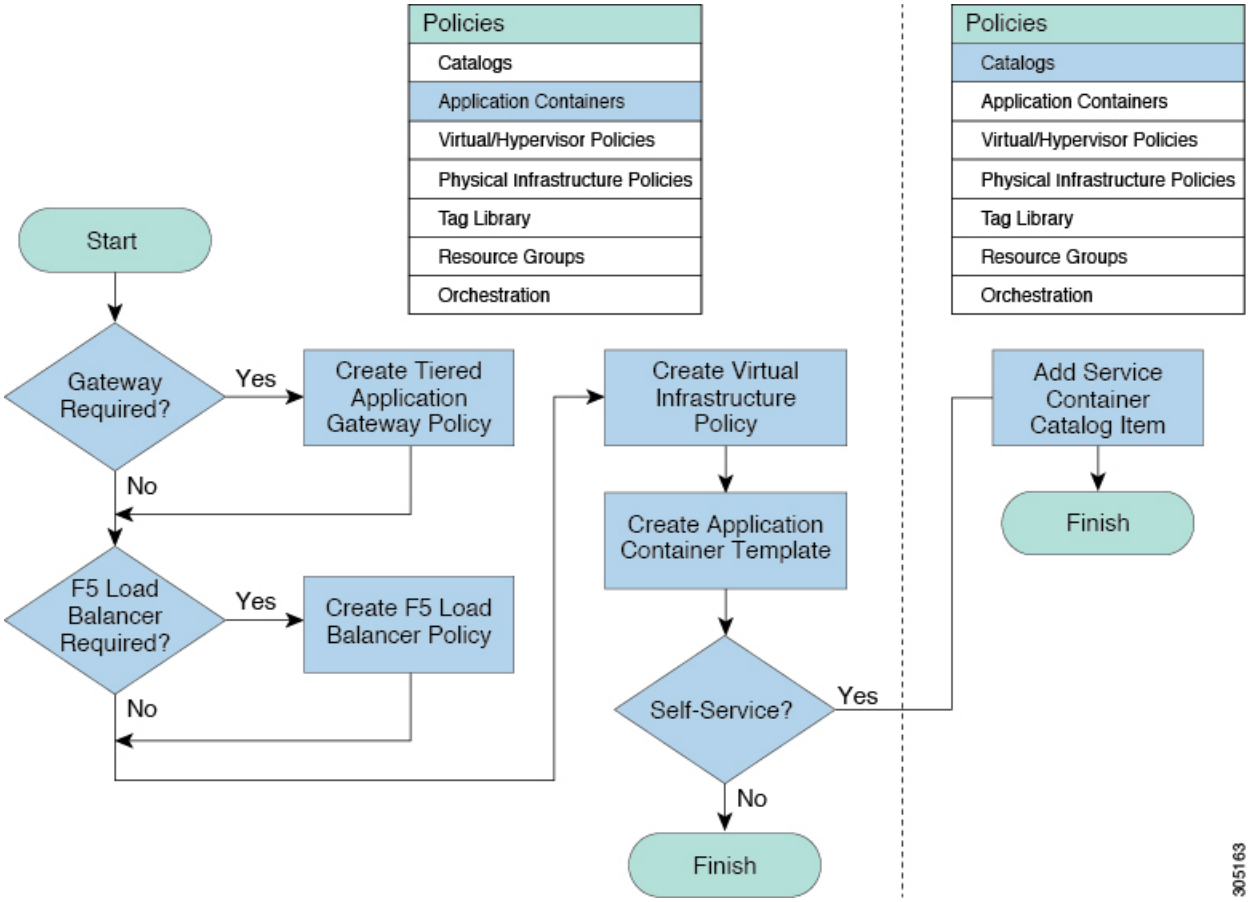
   d Add an end user self-service policy and configure the self-service options.

   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 fenced virtual application container template within Cisco UCS Director.

Figure 2: Process for Creating a Fenced Virtual Application Container Template



Creating a Virtual Infrastructure Policy for a Fenced Virtual Container

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

Step 2 On the **Application Containers** page, click **Virtual Infrastructure Policies**.

Step 3 Click **Add Policy**.

Step 4 In the **Virtual Infrastructure Policy Specification** page, 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 **Fenced Virtual** as the container type.
Select Virtual Account drop-down list	Choose a virtual account to which you want to apply the virtual infrastructure policy.

Step 5 Click **Next** and follow the wizard prompts.

Step 6 On the **Virtual Infrastructure Policy - Fencing Gateway** screen, complete the following fields:

Name	Description
Gateway Required check box	Check this check box to select a gateway policy, otherwise click **Next**.
Select Gateway Policy drop-down list	If the **Gateway Required** check box is checked, this field allows you to choose a gateway policy for the virtual infrastructure policy.

Step 7 Click **Next**.

Step 8 On the **Virtual Infrastructure Policy - Fencing Load Balancing** screen, complete the following fields:

Name	Description
F5 Load Balancer Required check box	Check this check box to choose an F5 load balancing for the virtual infrastructure policy.
Select F5 Load Balancer Policy drop-down list	If the **F5 Load Balancer Required** check box is checked, this field allows you to choose an F5 load balancing policy.

Step 9 Click **Next**.

Step 10 On the **Summary** page, click **Submit**.

What to Do Next

Create an application container template for creating a fenced virtual container.

Creating an Application Container Template for Fenced Virtual Container

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 the **Gateway Required** check box is enabled (optional)
- Options for service end users

Before You Begin

Create a virtual infrastructure policy. See Creating a Virtual Infrastructure Policy for a Fenced Virtual Container, on page 28.

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

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

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

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

Step 4 Click **Next**

Step 5 On the **Application Container Template - Select a Virtual infrastructure policy**screen, from the **Select Virtual Infrastructure Policy** drop-down list, choose a virtual infrastructure policy that is created for the fenced virtual container type.

Step 6 Click **Next**.

Step 7 On the **Application Container Template - Internal Networks** screen, youu can add and configure multiple networks for a container. These networks are applicable to the VM that is provisioned using this template.

Step 8 Click **Add (+)** to add a network. On the **Add Entry to Networks** screen, 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 address (for example, 255.255.255.0).
Gateway IP Address field	The IP address of the default gateway for the network. A NIC with this IP address is created on the GW VM.

Step 9 Click **Submit**.
Next, you can add and configure the VM that will be provisioned in the application container.

Step 10 Click **Next**.

Step 11 On the **Application Container Template - VMs**, click **Add (+)** 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.
Provision VM using Content Library Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image drop-down list	This field appears only when the **Provision VM using Content Library Template** check box is unchecked. Choose the image to be deployed.

Name	Description
Use Linked Clone check box	This check box is enabled only when you choose a VM template with a snapshot. Check this box to deploy new VMs using linked clone feature which enables them to be provisioned faster and storage efficient.
Snapshot field	This field appears only when the **Use Linked Clone** check box is checked. Click **Select** to choose a snapshot that need to be used to provision a new VM using linked clone feature.
Number of Virtual CPUs drop-down list	The number of virtual CPUs to be allocated to the VM.
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, the network configuration from the image is applied to the provisioned VM.
VM Network Interface field	Enter the VM network interface information.
Maximum Quantity field	The maximum number of instances that can be added in this container after it is created.
Initial Quantity field	The number of VM instances to provision when the container is created.

Step 12 Click **Submit**.

Step 13 Click **Next**.

Step 14 On the **Application Container Template - External Gateway Security Configuration** screen, click **Add (+)** to add port mappings. On the **Add Entry to Port Mappings** screen, 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 15 On the **Application Container Template - External Gateway Security Configuration** screen, click the **Add (+)** to add outbound ACL. On the **Add Entry to Outbound ACLs** screen, 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 16 Click **Submit**.

Step 17 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
Compute Policy drop-down list	Choose a compute 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 18 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
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.
Enable VNC Based Console Access check box	Check to allow VNC access to VMs on the container host.
Technical Support Email Address field	Enter a comma-separated list of email addresses. Automated notifications are sent to these emails.

Step 19 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 20 Click **Next**. The **Application Container Template - Summary** screen appears, displaying your current settings.

Step 21 Click **Submit** to complete the creation of the application container template.

What to Do Next

You can customize certain aspects of template using the custom workflow task. See Creating a Custom Workflow for Fenced Virtual Containers, on page 34.

Creating a Custom Workflow for Fenced Virtual Containers

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

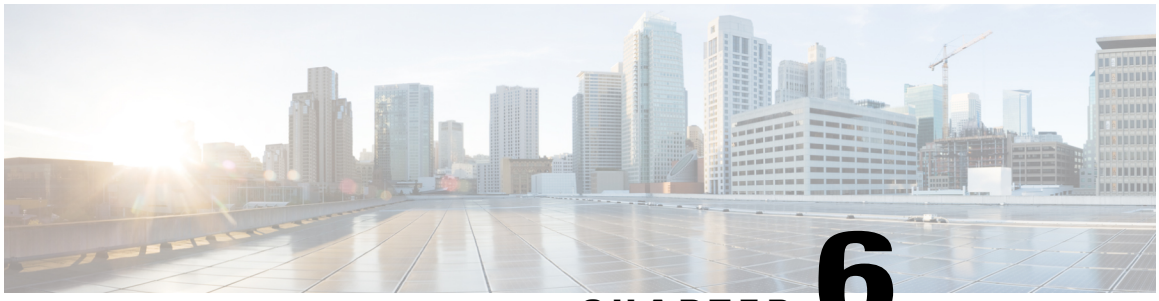
- **Gateway Type: CISCO ASA—**If the gateway type is CISCO ASA for the container, you must specifically choose **Application Container with ASA Gateway** from the list of available workflows. You can search for the workflow and check its check box in order to select it.
- **Distributed Virtual Portgroups—**If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



CHAPTER 6

Setting Up a Virtual Secure Gateway Application Container

This chapter contains the following sections:

Virtual Secure Gateway Application Containers

Cisco Virtual Secure Gateway (VSG) container type is used to provide enhanced security in virtual environments. 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.

Cisco VSG is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments. Cisco VSG enables a broad set of multi-tenant workloads that have varied security profiles to 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, Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies.

Cisco VSG provides the following benefits:

- Trusted Multi-tenant Access—Granular, zone-based control and monitoring with context-aware security policies applied in a multi-tenant (scale-out) environment to strengthen regulatory compliance and simplify audits. Security policies are organized into security profile 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—Administrative segregation across security and server teams while enhancing collaboration, eliminating administrative errors, and simplifying audits.

Cisco VSG does the following:

- Enhances compliance with industry regulations.
- Simplifies audit processes in virtualized environments.
- Reduces cost by securely deploying a broad set of virtualized workloads across multiple tenants on a shared compute infrastructure, whether in virtual data centers or private/public cloud computing environments.

Virtual Security Gateway Application Container Prerequisites

The following is the prerequisite for the VSG Container configuration:

- When executing the Allocate Container VM Resources task, the default virtual network type is Distributed Virtual Portgroup N1K for VSG container. Ensure that you modify the primary DVSwitch name for VSG container.

Virtual Security Gateway Application Container Limitations

VSG Application Container Creation Process

Adding a PNSC Account

PNSC 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, the PNSC 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 PNSC 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 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

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

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Account Type field	Choose PNSC as the account type and click **Submit**.
Account Name field	The multi-domain account name.

Name	Description
Description field	The description of the multi-domain account.
Server Management drop-down list	From the drop-down list, choose **All Servers** or **Selected Servers** to manage servers accordingly.
Server Address field	The IP address of the PNSC server.
Use Credential Policy check box	Check this check box if you want to use a credential policy for this account rather than enter the information manually.
Credential Policy drop-down list	If you checked the **Use Credential Policy** check box, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
User ID field	This field appears only when the **Use Credential Policy** check box is unchecked. The user ID to access the account.
Password field	This field appears only when the **Use Credential Policy** check box is unchecked. The password associated with the username.
Shared Secret Password field	This field appears only when the **Use Credential Policy** check box is unchecked. The pre-shared secret key of the account.
Transport Type drop-down list	This field appears only when the **Use Credential Policy** check box is unchecked.Choose a transport type: • HTTP—A standard protocol. • HTTPS—A standard and secure protocol.
Port field	This field appears only when the **Use Credential Policy** check box is unchecked. The port number (based on the transport type).
Contact Email field	The email address of the administrator or person responsible for this account.
Location field	The location of the device associated with the account.

Step 5 Click **Submit**.

Viewing PNSC Reports

After creating a PNSC account, 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 Choose **Physical** > **Network**.

Step 2 Expand **Multi-domain Manager**.
You can view PNSC accounts that were added under the Multi-domain Manager accounts.

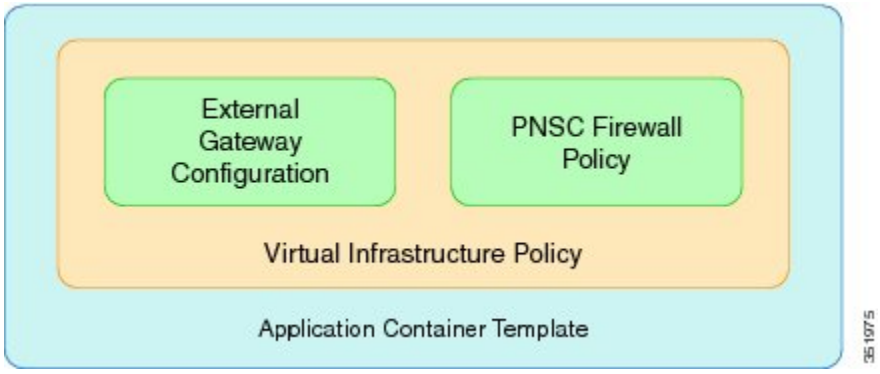
Step 3 Click a PNSC entry to view the available reports.

Integrating a VSG into an Application Container

You can use Cisco UCS Director to configure a 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.



Uploading OVA Files

Cisco UCS Director allows an administrator, a group administrator, or an 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 Choose **Administration** > **Integration**.

Step 2 On the **Integration** page, click **User OVF Management**.

Step 3 Click **Upload File**.

Step 4 On the **Upload File** screen, 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.
File field	Drop the OVA file or click **Select a File** to browse and choose the required file.
File Description field	The description of the file (if required).

Step 5 Click **Submit**.

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 Choose **Physical** > **Network**.

Step 2 Expand **PNSC accounts** listed under **Multi-Domain Managers**.

Step 3 Click PNSC account for which you want to create a firewall policy.

Step 4 Click **PNSC Firewall Policies**.

Step 5 Click **Add**.

Step 6 On the **Create Firewall 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.

Step 7 Click **Next**.

Step 8 Expand PNSC Zones and click **Add (+)** to create a zone.

Step 9 On the **Add Entry to PNSC Zones** screen, complete the following fields:

Name	Description
Zone Name field	A unique name for the zone.
Zone Description field	A description of the zone.
Zone Conditions	Expand **Zone Conditions** and click **Add** to add the zone condition.
Attribute Type drop-down list	Choose Network or VM as the type of attribute.
Attribute Name drop-down list	Choose the attribute from the list which varies according to the attribute type.
Operator drop-down list	Choose a type of operator.

Name	Description
Attribute Value field	Enter the attribute value based on the chosen attribute type.

Step 10 Click **Submit**.

Step 11 Click **Next**.

Step 12 Expand **PNSC ACL Rules** and click **Add (+)** to create a PNSC ACL rule entry.

Step 13 On the **Add Entry to PNSC ACL Rules** screen, 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.
Condition Match Criteria drop-down list	Choose a condition that need to be met.
Protocol/Service drop-down list	Choose protocol or service from the list.
Any 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 drop-down list	Choose the type of attribute.
Attribute Name drop-down list	Choose the name of the attribute from the drop-down list that vaies as per the attribute type.
Operator drop-down list	Choose the type of operator.
Attribute Value field	The attribute value.
Destination Conditions	
Attribute Type drop-down list	Choose the type of attribute.

Name	Description
Attribute Name drop-down list	Choose the name of the attribute from the drop-down list that vaies as per the attribute type.
Operator drop-down list	Choose the type of operator.
Attribute Value field	The attribute value.

Step 14 Click **Submit**.

Step 15 Click **Next**.

Step 16 On the **PNSC-VSG Configuration** screen, complete the following fields:

Name	Description
Use Unified Fabric check box	Check the check box to use unified fabric.
VSG OVF URL drop-down list	Choose an OVA file from the list of OVA files that are uploaded to Cisco UCS Director.
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.
Network Type drop-down list	Choose the network type from the list.
VLAN ID Range field	The VLAN ID range (for example, 100-199).
Use same vlan/vxlan check box	If checked, uses the same VLAN ID or VXLAN 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.

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**
Secondary VSG (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**

Step 17 Click **Submit**.

Step 18 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 Choose **Policies** > **Application Containers**.

Step 2 On the **Application Containers** page, click **Virtual Infrastructure Policies**.

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

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

Name	Description
Policy Name field	The unique name for the virtual infrastructure policy.
Policy Description field	The description of the virtual infrastructure policy.
Container Type drop-down list	Choose the VSG container type.
Select Virtual Account drop-down list	Choose a virtual account (cloud).

Step 5 Click **Next**.

Step 6 On the **Virtual Infrastructure Policy - PNSC Information** screen, complete the following fields:

Name	Description
PNSC Account field	Expand the PNSC accounts and choose a PNSC account.
VSG Template Configuration section	
PNSC Firewall Policy drop-down list	Choose a firewall policy.

Step 7 Click **Next**.

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

Name	Description
Gateway Required check box	Check this box if gateway is required.
Select Gateway Policy drop-down list	This field appears only when the **Gateway Required** check box is chosen. Choose a gateway policy.
Gateway Summary	Displays a summary of the gateway set for the virtual infrastructure policy.

Step 9 Click **Next**. The **Virtual Infrastructure Policy - Summary** screen appears, displaying your current settings.

Step 10 Click **Submit**.

Creating an Application Template for a VSG

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

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

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

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

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

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

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

Note Only one network is allowed per VSG container.

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

Name	Description
Network Name field	The network name. The name should be unique within the container. You can use a maximum of 128 characters.
Network Type drop-down list	Choose the network type.
Information Source drop-down list	Choose the information source from the list.
VLAN ID Range field	The VLAN ID range. This value controls the number of containers that can be cloned or created.
Network IP Address field	The network IP address for the container.

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

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

Step 8 Click **OK**.

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

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

Name	Description
VM field	The name of the VM. The full name contains the container name as well as this name.
Description field	The description of the VM.
Provision VM using Content Library Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image drop-down list	This field appears only when the **Provision VM using Content Library Template** check box is unchecked. Choose an image to be deployed.
Number of Virtual CPUs drop-down list	Choose the number of virtual CPUs to be allocated to the VM.
Memory drop-down list	Choose the amount of memory (in MB) to be allocated to the VM.
CPU Reservation (MHz) field	The CPU reservation for the VM in Mhz.
Memory Reservation (MB) field	The memory reservation for the VM.
Disk Size (GB) field	The custom disk size for the VM. To use the template disk size specify the value of zero. The specified disk size overrides the disk size of the selected image. **Note** If this value is less than template size, this value is ignored.

Name	Description
VM Password Sharing Option drop-down list	Choose an option on how to share the VM's username and password with the end users. If **Share after password reset** or **Share template credentials** is chosen, the end user needs to specify a username and password for the chosen templates.
Use Network Configuration from Image check box	If checked, the network configuration from the image is applied to the provisioned VM.
VM Network Interfaces field	Expand VM Network Interafces and choose the VM network interface information. If you are adding another network interface, go to Step 11.
Maximum Quantity field	The maximum number of instances that can be added in this container after it is created.
Initial Quantity field	The number of VM instances to provision when the container is created. **Note** Each VM will have a unique name and IP address.

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

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

Step 12 Click **Next**.

Step 13 Click **Ok**.

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

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

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

Step 15 Click **Submit**.

Step 16 Click **OK**.

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

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

Step 18 Click **Submit**.

Step 19 Click **OK**.

Step 20 Click **Next**.

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

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

Step 22 Click **Next**.

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

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

Step 24 Click **Next**.

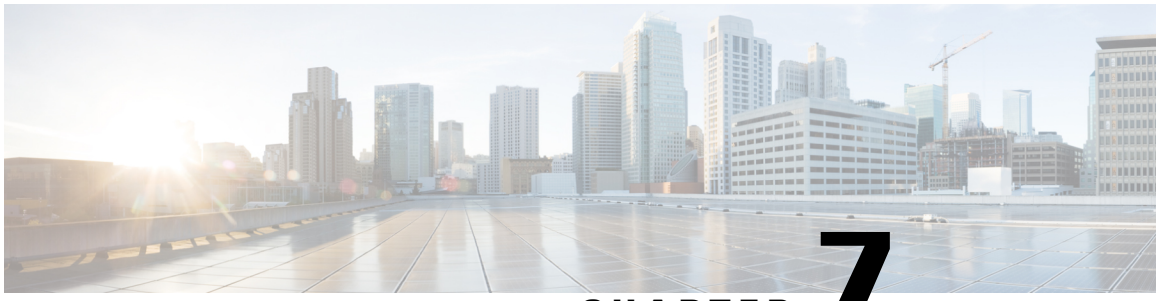
Step 25 Choose a workflow to setup the container.

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

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

Step 27 Click **Select**.

Step 28 Click **Submit**.



CHAPTER 7

Setting Up a Fabric Container

This chapter contains the following sections:

Fabric Application Container

The fabric application container type is used in Dynamic Fabric Automation (DFA) network deployments. Cisco Unified Fabric Automation is a multistage, switching network in which every connected device is reachable through the same number of hops. Cisco Unified Fabric Automation Organization fabric enables the use of a scale-out model for optimized growth.

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

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

Note For more information on application containers in a DFA network, see the Cisco UCS Director Unified Fabric Automation Management Guide.

Fabric Application Container Limitations

The following is the limitation of Fabric Container:

- F5 Load Balancing is also supported on Fabric Containers.

Creating Fabric Application Container Policies

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

Step 2 On the **Application Containers** page, click **Virtual Infrastructure Policies**.

Step 3 Click **Add Policy**.

Step 4 On the **Virtual Infrastructure Policy Specification** screen, 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 **Fabric** and click **Next** to confirm your selection and follow the wizard prompts. **Note** For Cisco Dynamic Fabric Automation environment, the creation of a gateway is optional.
Select Virtual Account drop-down list	The chosen virtual account (the cloud on which the gateway VM is created).

Step 5 Click **Next**.

Step 6 On the **Virtual Infrastructure Policy - Fabric Information** screen, complete the following fields:

Name	Description
With VSG check box	Check the check box for VSG support. If checked, enter the information for the **Service Network Configuration** and **Host Network Configuration**.
Fabric account drop-down list	Choose a fabric account.
Switch Type drop-down list	Choose a switch type.
Switch Name drop-down list	Choose a switch.
Alternate Switch Namedrop-down list	Choose an alternate switch name.
Service Network Configuration	

Name	Description
Layer 3 check box	This field appears only when the **With VSG** check box is checked. Check the check box for Layer 3 support. **Note** You must complete the required pre-deployment 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	This field appears only when the **Layer 3** check box is checked. Choose the fabric organization.
Fabric Partition drop-down list	This field appears only when the **Layer 3** check box is checked. Choose the fabric partition.
Fabric Service Network field	This field appears only when the **Layer 3** check box is checked. Expand the fabric service network list and select a fabric service network.
Mobility Domain Id (HA) field	This field is auto-populated when the **Auto Select Mobility Domain Id** check box is checked. If the check box is unchecked, expand the **Mobility Domain ID** list and select a mobility domain ID.
Auto Select Mobility Domain Id check box	Check this box to select a mobility domain ID automatically.
Host Network Configuration	

Name	Description
Mobility Domain Id(Service Network + HA) field	This field is auto-populated when the **Auto Select Mobility Domain Id** check box is checked. If the check box is unchecked, expand the **Mobility Domain ID** list and select a 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.
Auto Select Mobility Domain Id check box	Check this box to select a mobility domain ID automatically.
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.
Multi Cast Group Address field	Enter the multi-cast group address.
Profile Name field	Exapand the profile name list and select a profile name.

Step 7 Click **Next**.

Step 8 On the **Virtual Infrastructure Policy - Gateway** screen, check the **Gateway Required** check box if you want to add a gateway for the container.

Step 9 Click **Next**.

Step 10 On the **Virtual Infrastructure Policy - Fencing Load Balancing** screen, check the **F5 Load Balancer Required** check box if you want to add a load balancer for the container.

Step 11 On the **Summary** screen, view the configuration summary and click **Submit**.

Creating Fabric Application Container Template

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

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.

Before You Begin

Create an application container policy.

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

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

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

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

Step 4 Click **Next**.

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

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

Step 6 Click **Next**.

Step 7 On the **Application Container Template - Fabric Networks** screen, click **Add (+)** to add a fabric network. Complete the following fields:

Name	Description
External Partition check box	This field appears only when the gateway is selected in the chosen virtual infrastructure policy. 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 drop-down list	Choose a network role.
Description field	The description of the network.
Multicast Group Address field	The multicast group address.

Name	Description
Profile Name field	Expand the profile name list and select a profile.
Gateway IP Address field	The IP address of the default gateway for the network.
Network Mask field	The network mask (for example, 255.255.255.0).
DHCP Server Address field	The IP address of the DHCP server.
vrfdhcp field	The IP address of the VRF DHCP server.
mtuvalue field	The maximum transmission unit (MTU) value.
dhcpServerv6Address field	The IPv6 address of the DHCP server.
vrfv6dhcp field	The IPv6 address of VRF DHCP server.
Gateway IP v6Address field	The IPv6 address of gateway.
Prefix Length field	The prefix length used by the IPv6 address.
DHCP Scope	
DHCP Enabled check box	Check the check box to enable DHCP.
Service Configuration Parameters	
Start IP field	The starting IP address of the network.
End IP field	The ending IP address of the network.
Secondary Gateway field	The IP address of secondary gateway.

Step 8 Click **Submit**.

Step 9 Click **Next**.

Step 10 On the **Application Container Template - VMs** screen, click **Add (+)** 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.
Provision VM using Content Library Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.

Name	Description
Content Library VM Template field	This field appears only when the **Provision VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image drop-down list	This field appears only when the **Provision VM using Content Library Template** check box is unchecked. Choose the image to be deployed.
Number of Virtual CPUs drop-down list	The number of virtual CPUs to be allocated to the VM.
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	Expand the VM network interfaces and select a VM network interface.
Maximum Quantity field	The maximum number of instances that can be added in this container after it is created.
Initial Quantity field	The number of VM instances to provision when the container is created.

Step 11 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 or ASA the network policy should use a Static IP Pool only. The VSG or ASA VM requires IP addresses as input. There is no current provision to specify DHCP for deploying a VSG or ASA 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 12 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:

Field	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.
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 13 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, none of the workflow is 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 14 Click **Next**. The **Application Container Template - Summary**screen appears, displaying your current settings.

Step 15 Click **Submit** to complete the creation of the application container template.

CHAPTER 8

Setting Up a Cisco Application Policy Infrastructure Controller Container

This chapter contains the following sections:

- Adding Bare Metal Servers to an Existing Container, page 127

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 UCS Director also supports the ability to define contracts between different container tiers, enabling you to apply rules between tiers.

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 an 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 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 a 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, ASAv).

- Allow load balancing the container network using VPX or SDX load balancers.
- Use a Cisco Application Centric Infrastructure (ACI).
- Provision a bare metal 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 resource group.
- 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 firewall policy (optional).

APIC Application Container Limitations

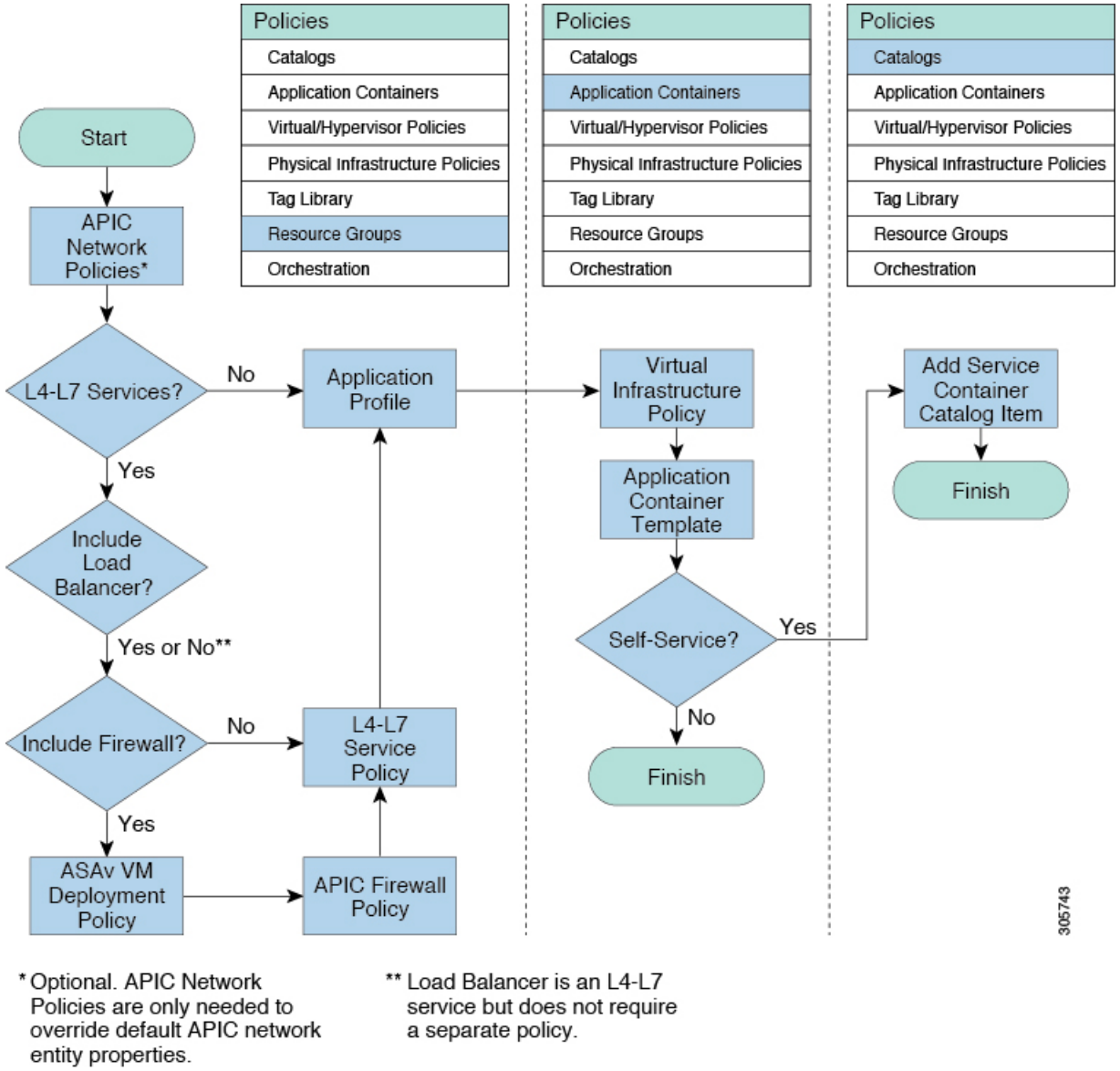
Cisco UCS Director APIC application containers have the following limitations:

- 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.
- For application container configuration that requires physical servers, only UCS managed servers are currently supported.

APIC Application Container Creation Process

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

Figure 3: Process for Creating an APIC Application Container



* Optional. APIC Network Policies are only needed to override default APIC network entity properties.

** Load Balancer is an L4-L7 service but does not require a separate policy.

ASAv VM Deployment Policy

The Adaptive Security Virtual Appliance (ASAv) brings full firewall functionality to virtualized environments 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 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **ASAv VM Deployment Policy**.

Step 3 Click **Add**.

Step 4 On the **ASAv VM Deployment Policy** screen, complete the following fields:

Name	Description
Policy Name field	Enter the name of the ASAv VM deployment policy.
ASAv OVF list	Expand the list to choose a template file in the open virtualization format (OVF) and click **Select**.
VM Name field	Enter the name for the ASAv virtual machine (VM) instance. The policy automatically prefixes this VM name with the container name.
Port field	Enter the port number of the firewall appliance. We recommend using port **443**.
Username field	Enter the username that is used to access the firewall appliance.
Password field	Enter 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** Until the release of version ASAv 9.5.2, the OVA file was provided for ASAv deployment for a VMware environment. Starting with version ASAv 9.5.2, 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 optionally 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 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **APIC Firewall Policy**.

Step 3 Click **Add**.

Step 4 On the **Create Firewall Policy** screen, complete the following fields:

Name	Description
Policy Details	
Name field	Enter the name of the firewall policy.
Description field	Enter the description of the firewall policy.
ACL(s) Details	

Name	Description
ACL(s) list	Expand the list to choose the access control lists (ACLs) defined for the firewall policy. Click + to define an ACL. On the **Add Entry to ACL(s)** screen, 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—Check this box if you want to create a new ACL. • **New ACL List Name** field—This field appears when you check the **New ACL list?** check box. Enter the name of the ACL that you want to create. • **ACE 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—Check this box to permit or deny any source host or network. By default, this check box is checked. • **Source Address** field—This field appears when you uncheck the **Source Any** check box. Enter 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—Check this box to apply the ACL entry statement on any destination address. By default, this check box is checked. • **Destination Address** field—This field appears when you uncheck the **Destination Any** check box. Enter 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—Enter the sequence in which permit statements or deny statements need to be executed.

Name	Description
Bridge Group Interface Details—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	Enter the bridge group interfaces defined for the firewall policy. Expand the bridge group interface(s) list, and click + to define a bridge group ID. On the **Add Entry to Bridge Group Interface(s)** screen, complete the following fields: • **Bridge Group ID** field—Enter the unique ID of a bridge group. The value of bridge group ID is an integer between 1 and 100. • **IPv4 Address Value** field—Enter the management IP address of the bridge group.
Interface Details	

Name	Description
Interface(s) field	Enter the interfaces defined for the firewall policy. Expand the interface(s) list and click + to define an interface. On the **Add Entry to Interface(s)** screen, complete the following fields: • **Interface Name** field—Enter 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—Enter the IP pool from which you want to choose the unreserved virtual IP address for the interface. • **Security Level** field—Enter 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	
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 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **APIC Network Policy**.

Step 3 Click **Add**.

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

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

Name	Description
EPG Specification	
QOS field	Enter the QOS name that needs to be assigned to EPG.
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—**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—**Policies are pushed to leaf nodes only upon attaching a physical NIC and associating a virtual NIC with a port group (an EPG). • **Pre-provision—**Specifies that a policy (for example, VLAN, VXLAN binding, contracts, or filters) is downloaded to a leaf switch even before a VM controller is attached to the virtual switch (for example, VMware VDS) thereby pre-provisioning the configuration on the switch.
Bridge Domain Specification	
Forwarding drop-down list	Choose the forwarding method of the bridge domain: **Optimize** or **Custom**.
L2 Unknown Unicast drop-down list	Choose the forwarding method for unknown layer destinations. This drop-down list appears when you choose **Custom** in the **Forwarding** drop-down list.
Unknown Multicast Flooding drop-down list	Choose the forwarding method for multicast traffic for unknown layer destinations. This drop-down list appears when you choose **Custom** in the **Forwarding** drop-down list.
ARP Flooding check box	Check this box to enable ARP flooding. If ARP flooding is disabled, unicast routing is performed on the target IP address. This check box appears when you choose **Custom** in the **Forwarding** drop-down list.

Name	Description
Unicast Routing check box	Check this box to enable unicast routing. Unicast routing is the forwarding method based on predefined forwarding criteria (IP or MAC address). This check box appears when you choose **Custom** in the **Forwarding** drop-down list. This check box is checked by default.

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 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **L4-L7 Service Policy**.

Step 3 Click **Add**.

Step 4 On the **Add L4-L7 Service Policy** screen, complete the following fields:

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

Name	Description
Allow Firewall check box	

Name	Description
	Check this box if the firewall service is applicable for the Layer 4 to Layer 7 service policy. When you choose **Allow Firewall**, the following additional fields appear: • **Firewall Type** drop-down list—Choose the firewall type. • **Device Package** field—Expand the list to choose the correct device package based on the supported APIC version. • **Firewall Policy** field—Expand the list to choose a firewall policy. Click + to add a firewall policy. For more information about how to add a firewall policy, see Adding an APIC Firewall Policy, on page 69. • **Multi Context Enabled** check box—Check this box to identify if a multiple security context enabled ASA is used for firewall configuration. This check box appears only when **PHYSICAL** firewall type is selected. 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 box to enable high availability for the firewall service. • **Enable Stateful Failover** drop-down list—This field appears if you check **Enable Firewall HA**. Choose to enable or disable the stateful failover for ASA in high availability mode. 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 box to run transparent firewall mode. This check box appears only when **VIRTUAL** firewall type is selected.

Name	Description
	Note This feature is supported in VDC with managed network services.
Allow Load Balancer check box	Check this box if the load balancer service is applicable for the Layer 4 to Layer 7 service policy. When you choose **Allow Load Balancer**, the following additional fields appear: • **Load Balancer Type** drop-down list—Choose the load balancer type. • **Device Package** field—Expand the list to choose a device package from the list. • **Enable Load Balancer HA** check box—Check this box to enable high availability for the load balancer service. • **Network Setting** check box—Check this check box to set the NTP and SNMP configuration for the load balancer device. • **NTP and SNMP Configuration** field—This field appears when the **Network Setting** check box is checked. Expand the list to choose a network device policy. The NTP and SNMP configuration set in the selected network device policy is applied to the load balancer device. **Note** The load balancer service is the only supported service for a tenant with multiple private networks.
Summary—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 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Network Device System Parameters Policy**.

Step 3 Click **Add**.

Step 4 On the **Create Network Device System Parameters Policy** screen, complete the following fields:

Name	Description
Parameters Policy Specification	
Policy Name field	Enter the name of the network device system parameters policy.
Description field	Enter the description of the network device system parameters policy.
NTP Parameters	
NTP Server field	Enter comma separate IP addresses or host names of the NTP servers.
SNMP Parameters	
Trap Class drop-down list	Choose one of the following as the trap class: • **Specific—**To use the device-specific trap. • **Generic—**To implement the pre-defined traps such as cold start, warm start, link down, link up, authentication failure, and EGP neighbor loss.
Trap Destination field	Enter the IP address of the system to which the appliance forwards traps received by managed devices.
Community Name field	Enter 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.

Name	Description
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	Enter the name of the SNMP user.
Group field	Enter the 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.
Authentication Password field	Enter 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	Enter 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.

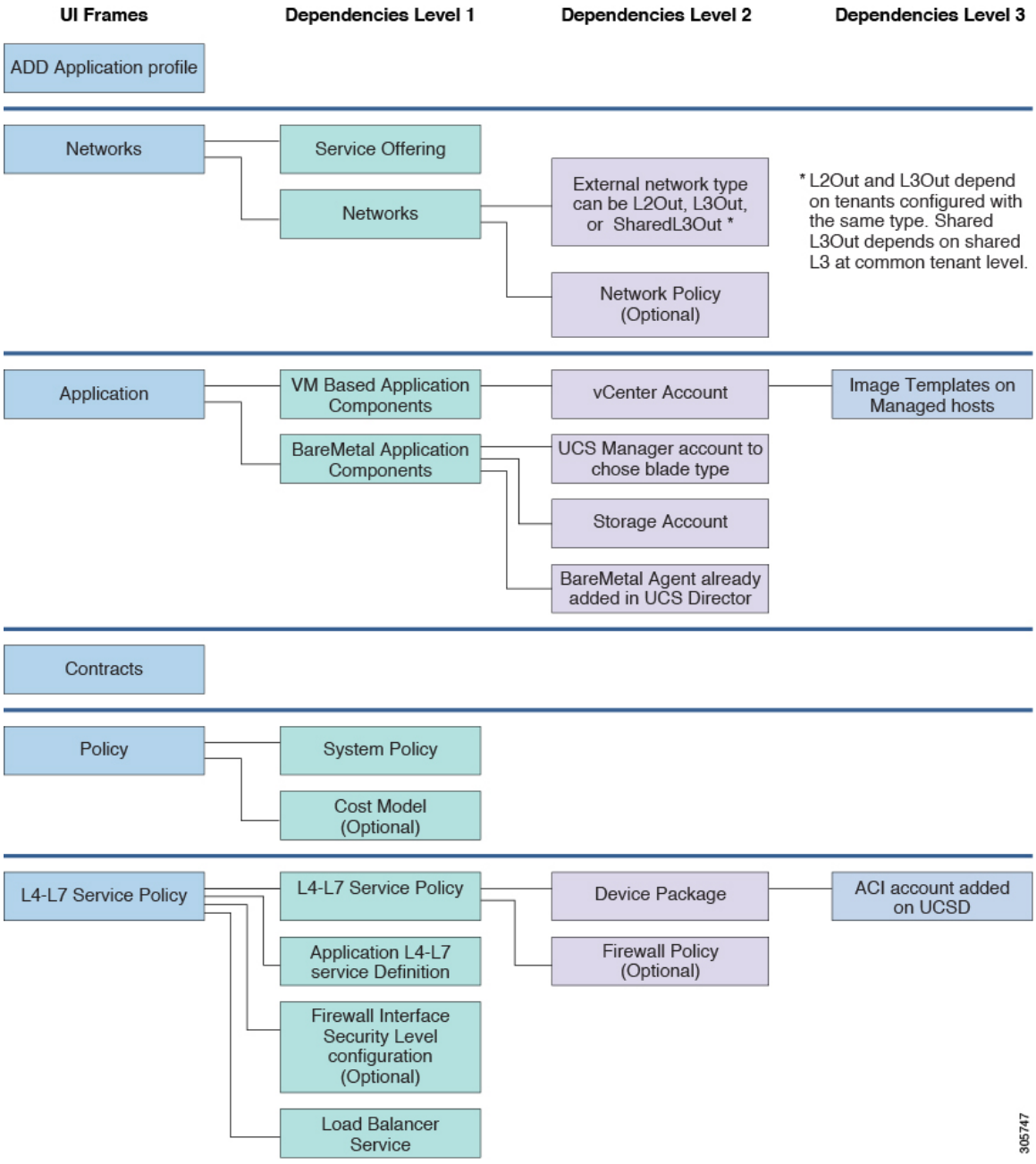
Application Profiles

An application profile is a description of the infrastructure required for the deployment of an application. These infrastructure requirements include bare metal 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 4: Application Profile — Dependencies



Adding an Application Profile

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Application Profile**.

Step 3 Click the row with the application profile and choose **View** from the **More Actions** drop-down list to view the name, description, and service offering of the application profile, or, choose **View Details** to see the following:

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 4 Click **Add**.

Step 5 On the **Profile Specification** screen, complete the following fields:

Name	Description
Name field	Enter the name of the application profile. The name must be alphanumeric, not greater than 32 characters, and can include the following special characters: _, -, ., :. The name cannot be modified after it is added.
Description field	Enter the description of the application profile.

Step 6 Click **Next**.

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

Name	Description
Service Offering list	Expand service offerings, check the service offering that you want to use, and then click **Validate**. The service offering must belong to the tenant for which you will create containers with this application profile. Click **Add** to add a service offering. See the Cisco UCS Director APIC Management Guide.
Networks list	Expand the list and click **Add** to configure a newtork. For more information on how to configure a network, see the *next Step*.

Step 8 Click **Add** to configure the tier for application.
On the **Add Entry to Networks** screen, 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 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.

Name	Description
Interested Tag Value list	Expand Interested Tag Values and check the tag values that you want to use, and then click **Validate**, to choose the tag values for each tier. During container provisioning, a resource is selected based on the tag associated with the tier. This field appears only when **Network Type** is **Internal**. **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	Choose the APIC network policy from the list. This field appears only when **Network Type** is **Internal**, **Infrastructure**, or **Failover**. Click + to add an APIC network policy. See Adding an APIC Network Policy, on page 73.
L2/L3 Selection drop-down list	By default, **L2Out** is selected to integrate the ACI fabric with external Layer 2 network. This field appears only when **Network Type** is **External**. You can choose one of the following: • **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	By default, the box is checked to use the L2/L3 out configuration defined in the tenant while creating a container. This field appears only when **Network Type** is **External**. **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 **Submit**.

Step 10 Click **Next**.

Step 11 On the **Application** screen, do the following:

a) Expand **VM Based Application Components** and click +.

b) On the **Add Entry to VM Based Application Components** screen, 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** list appears. Click + to add a tag.
Provision new VM using Content Library VM Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision new VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.

Name	Description
VM Image list	This field appears only when the **Provision new VM using Content Library VM Template** check box is unchecked. Expand VM Image, click a VM image that you want to use, and then click **Validate**. The list varies according to the option selected in the **Image Selection Type** drop-down list. **Note** All the VM images are listed from the 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.
Use Linked Clone check box	This check box is enabled only when you choose a VM template with a snapshot. Check this box to deploy new VMs using linked clone feature which enables them to be provisioned faster and storage efficient.
Snapshot field	This field appears only when the **Use Linked Clone** check box is checked. Click **Select** to choose a snapshot that need to be used to provision a new VM using linked clone feature.
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 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 list	Expand the list and click + to add a VM network interface.

Name	Description
Maximum Quantity field	Enter 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	Enter the number of VM instances to be provisioned when the application is created.

c) Click **Submit**.

Step 12 On the **Application** screen, do the following:

a) Expand the **Bare Metal Application Components** list and click +.

b) On the **Add Entry to Bare Metal Application Components** screen, complete the following fields:

Name	Description
Instance Name field	Enter the name of the bare metal instance.
Description field	Enter the description of the bare metal instance.
Boot Lun Size (GB) field	Recommended LUN size for booting.
Network drop-down list	Choose a network.
Target BMA drop-down list	Choose the bare metal agent (BMA) for PXE setup.
Bare Metal Image drop-down list	Choose the bare metal 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 13 Click **Next**.

Step 14 On the **Contracts** screen, 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 unidirectional 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.

Step 15 Expand Contracts and click + to add the communication protocol details.

a) On the **Add Entry to Contracts** screen, 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 box to apply the same contract for traffic from source to destination, or from destination to source.
The following fields appear only if TCP or UDP protocol is selected:	
Source Port Start field	Enter the starting range of the source port number.

Name	Description
Source Port End field	Enter the ending range of the source port number.
Destination Port Start field	Enter the starting range of the destination port number.
Destination Port End field	Enter the ending range of the destination port number.
Stateful check box	This check box appears when you choose TCP protocol. Check the box to enable stateful connection.
Action drop-down list	Choose the action to be taken for the communication: • **Accept** • **Drop** • **Reject**

b) Click **Submit**.

Step 16 Click **Next**.

Step 17 On the **Policy** screen, do the following:

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

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

c) On the **System Policy Information** screen, 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	Enter the template to use for the VM name. **Note** If the name template is not specified, the name provided by the user is used as the VM name.
Disable VM Name Uniqueness Check check box	Check this check box to skip the VM name uniqueness validation.
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 box to allow the user to specify the name or prefix for the VM.
Power On after deploy check box	Check the box to power on the VM after provisioning.
Host Name Template field	Enter the template of the host name.

Name	Description
Disable Host Name Uniqueness Check check box	Check this check box to skip the host name uniqueness validation.
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	Enter the name of the DNS domain.
DNS Suffix List field	Enter the list of domain name suffixes that get appended to DNS.
DNS Server List field	Enter 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	An annotation states that the app/web tier allows the subnet to be created as Shared and Public through the APIC network policy. Check the box to define the VM annotation.
VM Annotation field	This field appears when the **Define VM Annotation** check box is selected. Enter the annotation note for the VM.
Custom Attributes field	This field appears when the **Define VM Annotation** check box is selected. Expand Custom Attributes and click + to add a custom attribute.

d) Click **Submit**.
e) From the **Cost Model** drop-down list, choose a cost model to compute the chargeback.
f) Expand **HyperV Deployment Policy** and check the HyperV deployment policy for the HyperV container provision.
g) Click **Next**.

Step 18 On 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, complete the following fields:

a) **L4-L7 Service Policy** drop-down list—Choose the Layer 4 to Layer 7 service policy from the list. Click + to add a Layer 4 to Layer 7 service policy. See Adding a Layer 4 to Layer 7 Service Policy, on page 75.

b) **Application L4-L7 Service Definition** list—Expand Application L4-L7 Service Definition and click +. On the **Add Entry to Application L4-L7 Service Definition** screen, complete the following fields:

Name	Description
Service Name field	Enter the name of the service.
Consumer drop-down list	Choose the internal tier. **Note** When you are deploying ASA/ASAv between the tiers, you can create a VDC with the shared Layer 3 network without any dependency on the tenant with the Layer 2 network.
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	Choose the port number of the selected protocol. **Note** This field appears only for the load balancer service.

Name	Description
Services list	Expand the list to choose the service type by checking one of the following boxes: • **FIREWALL—**To provide firewall service between consumer and provider. • **LB_SINGLE_ARM—**To configure the 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. • **LB_DUAL_ARM—**To configure the load balancer service between consumer and provider in the dual-arm mode. In the dual-arm mode, the load balancer is connected to the consumer and provider with two different interfaces. • **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** box to customize the firewall security for the network tiers in the application profile.
d) Expand Firewall Security Levels that appears when the **Customize Firewall Security For Tiers** check box is selected. Choose a tier and click edit to change the security level.

Step 19 Click **Submit**.

Cloning an Application Profile

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Application Profile**.

Step 3 Click the row with the application profile that you want to clone.

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

Step 5 On the **Profile Specification** screen, complete the following fields:

Name	Description
Name field	Enter the name of the application profile. The name must be alphanumeric, not greater than 32 characters, and can include the following special characters: _, -, ., :. The name cannot be modified after it is added.
Description field	Enter the description of the application profile.

Step 6 Click **Next**.

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

Name	Description
Service Offering list	Expand service offerings, check the service offering that you want to use, and then click **Validate**. The service offering must belong to the tenant for which you will create containers with this application profile. Click **Add** to add a service offering. See the Cisco UCS Director APIC Management Guide.
Networks list	Expand the list and click **Add** to configure a newtork. For more information on how to configure a network, see the *next Step*.

Step 8 Click **Add** to configure the tier for application.
On the **Add Entry to Networks** screen, 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 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 list	Expand Interested Tag Values and check the tag values that you want to use, and then click **Validate**, to choose the tag values for each tier. During container provisioning, a resource is selected based on the tag associated with the tier. This field appears only when **Network Type** is **Internal**. **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	Choose the APIC network policy from the list. This field appears only when **Network Type** is **Internal**, **Infrastructure**, or **Failover**. Click + to add an APIC network policy. See Adding an APIC Network Policy, on page 73.

Name	Description
L2/L3 Selection drop-down list	By default, **L2Out** is selected to integrate the ACI fabric with external Layer 2 network. This field appears only when **Network Type** is **External**. You can choose one of the following: • **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	By default, the box is checked to use the L2/L3 out configuration defined in the tenant while creating a container. This field appears only when **Network Type** is **External**. **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 On the **Application** screen, add VM-based application components:

a) Click +.

b) On the **Add Entry to VM Application Components** screen, 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** list appears. Click + to add a tag.

Name	Description
Provision new VM using Content Library VM Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision new VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image list	This field appears only when the **Provision new VM using Content Library VM Template** check box is unchecked. Expand VM Image, click a VM image that you want to use, and then click **Validate**. The list varies according to the option selected in the **Image Selection Type** drop-down list. **Note** All the VM images are listed from the 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.
Use Linked Clone check box	This check box is enabled only when you choose a VM template with a snapshot. Check this box to deploy new VMs using linked clone feature which enables them to be provisioned faster and storage efficient.
Snapshot field	This field appears only when the **Use Linked Clone** check box is checked. Click **Select** to choose a snapshot that need to be used to provision a new VM using linked clone feature.
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 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 list	Expand the list and click + to add a VM network interface.
Maximum Quantity field	Enter 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	Enter the number of VM instances to be provisioned when the application is created.

c) Click **Submit**.

Step 11 On the **Application** screen, add bare metal application components:

a) Click +.

b) On the **Add Entry to Bare Metal Application Components** screen, complete the following fields:

Name	Description
Instance Name field	Enter the name of the bare metal instance.
Description field	Enter the description of the bare metal instance.
Boot Lun Size (GB) field	Recommended LUN size for booting.
Network drop-down list	Choose a network.
Target BMA drop-down list	Choose the bare metal agent (BMA) for PXE setup.
Bare Metal Image drop-down list	Choose the bare metal 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 On the **Contracts** screen, click + to add the communication protocol details.

a) On the **Add Entry to Contracts** screen, 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 box to apply the same contract for traffic from source to destination, or from destination to source.
The following fields appear only if TCP or UDP protocol is selected:	
Source Port Start field	Enter the starting range of the source port number.

Name	Description
Source Port End field	Enter the ending range of the source port number.
Destination Port Start field	Enter the starting range of the destination port number.
Destination Port End field	Enter the ending range of the destination port number.
Stateful check box	This check box appears when you choose TCP protocol. Check the box to enable stateful connection.
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 On the **Policy** screen, do the following:

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

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

c) On the **System Policy Information** screen, 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	Enter the template to use for the VM name. **Note** If the name template is not specified, the name provided by the user is used as the VM name.
Disable VM Name Uniqueness Check check box	Check this check box to skip the VM name uniqueness validation.
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 box to allow the user to specify the name or prefix for the VM.
Power On after deploy check box	Check the box to power on the VM after provisioning.
Host Name Template field	Enter the template of the host name.

Name	Description
Disable Host Name Uniqueness Check check box	Check this check box to skip the host name uniqueness validation.
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	Enter the name of the DNS domain.
DNS Suffix List field	Enter the list of domain name suffixes that get appended to DNS.
DNS Server List field	Enter 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	An annotation states that the app/web tier allows the subnet to be created as Shared and Public through the APIC network policy. Check the box to define the VM annotation.
VM Annotation field	This field appears when the **Define VM Annotation** check box is selected. Enter the annotation note for the VM.
Custom Attributes field	This field appears when the **Define VM Annotation** check box is selected. Expand Custom Attributes and click + to add a custom attribute.

d) Click **Submit**.
e) From the **Cost Model** drop-down list, choose a cost model to compute the chargeback.
f) Expand **HyperV Deployment Policy** and check the HyperV deployment policy for the HyperV container provision.
g) Click **Next**.

Step 16 On 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, complete the following fields:

a) **L4-L7 Service Policy** drop-down list—Choose the Layer 4 to Layer 7 service policy from the list. Click + to add a Layer 4 to Layer 7 service policy. See Adding a Layer 4 to Layer 7 Service Policy, on page 75.

b) **Application L4-L7 Service Definition** list—Expand Application L4-L7 Service Definition and click +. On the **Add Entry to Application L4-L7 Service Definition** screen, complete the following fields:

Name	Description
Service Name field	Enter the name of the service.
Consumer drop-down list	Choose the internal tier. **Note** When you are deploying ASA/ASAv between the tiers, you can create a VDC with the shared Layer 3 network without any dependency on the tenant with the Layer 2 network.
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	Choose the port number of the selected protocol. **Note** This field appears only for the load balancer service.

Name	Description
Services list	Expand the list to choose the service type by checking one of the following boxes: • **FIREWALL—**To provide firewall service between consumer and provider. • **LB_SINGLE_ARM—**To configure the 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. • **LB_DUAL_ARM—**To configure the load balancer service between consumer and provider in the dual-arm mode. In the dual-arm mode, the load balancer is connected to the consumer and provider with two different interfaces. • **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** box to customize the firewall security for the network tiers in the application profile.
d) Expand Firewall Security Levels that appears when the **Customize Firewall Security For Tiers** check box is selected. Choose a tier and click edit to change the security level.

Step 17 Click **Submit**.

Editing an Application Profile

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Application Profile**.

Step 3 Click the row with the application profile that you want to edit.

Step 4 Click **Edit**.

Step 5 On the **Profile Specification** screen, complete the following fields:

Name	Description
Name field	Enter the name of the application profile. The name must be alphanumeric, not greater than 32 characters, and can include the following special characters: _, -, ., :. The name cannot be modified after it is added.
Description field	Enter the description of the application profile.

Step 6 Click **Next**.

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

Name	Description
Service Offering field	Displays the service offering chosen when the application profile was created. It cannot be changed.
Networks field	Expand the list to define the network type 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 Click **Add** to configure the tier for application.
On the **Add Entry to Networks** screen, 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 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 list	Expand Interested Tag Values and check the tag values that you want to use, and then click **Validate**, to choose the tag values for each tier. During container provisioning, a resource is selected based on the tag associated with the tier. This field appears only when **Network Type** is **Internal**. **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	Choose the APIC network policy from the list. This field appears only when **Network Type** is **Internal**, **Infrastructure**, or **Failover**. Click + to add an APIC network policy. See Adding an APIC Network Policy, on page 73.

Name	Description
L2/L3 Selection drop-down list	By default, **L2Out** is selected to integrate the ACI fabric with external Layer 2 network. This field appears only when **Network Type** is **External**. You can choose one of the following: • **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	By default, the box is checked to use the L2/L3 out configuration defined in the tenant while creating a container. This field appears only when **Network Type** is **External**. **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 On the **Application** screen, add VM-based application components:

a) Click +.

b) On the **Add Entry to VM Application Components** screen, 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** list appears. Click + to add a tag.

Name	Description
Provision new VM using Content Library VM Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision new VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image list	This field appears only when the **Provision new VM using Content Library VM Template** check box is unchecked. Expand VM Image, click a VM image that you want to use, and then click **Validate**. The list varies according to the option selected in the **Image Selection Type** drop-down list. **Note** All the VM images are listed from the 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.
Use Linked Clone check box	This check box is enabled only when you choose a VM template with a snapshot. Check this box to deploy new VMs using linked clone feature which enables them to be provisioned faster and storage efficient.
Snapshot field	This field appears only when the **Use Linked Clone** check box is checked. Click **Select** to choose a snapshot that need to be used to provision a new VM using linked clone feature.
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 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 list	Expand the list and click + to add a VM network interface.
Maximum Quantity field	Enter 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	Enter the number of VM instances to be provisioned when the application is created.

c) Click **Submit**.

Step 11 On the **Application** screen, add bare metal-based application components:

a) Click +.

b) On the **Add Entry to Bare Metal Application Components** screen, complete the following fields:

Name	Description
Instance Name field	Enter the name of the bare metal instance.
Description field	Enter the description of the bare metal instance.
Boot Lun Size (GB) field	Recommended LUN size for booting.
Network drop-down list	Choose a network.
Target BMA drop-down list	Choose the bare metal agent (BMA) for PXE setup.
Bare Metal Image drop-down list	Choose the bare metal 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 + to add the communication protocol details:

a) On the **Add Entry to Contracts** screen, 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 box to apply the same contract for traffic from source to destination, or from destination to source.
The following fields appear only if TCP or UDP protocol is selected:	
Source Port Start field	Enter the starting range of the source port number.

Name	Description
Source Port End field	Enter the ending range of the source port number.
Destination Port Start field	Enter the starting range of the destination port number.
Destination Port End field	Enter the ending range of the destination port number.
Stateful check box	This check box appears when you choose TCP protocol. Check the box to enable stateful connection.
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 On the **Policy** screen, do the following:

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

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

c) On the **System Policy Information** screen, 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	Enter the template to use for the VM name. **Note** If the name template is not specified, the name provided by the user is used as the VM name.
Disable VM Name Uniqueness Check check box	Check this check box to skip the VM name uniqueness validation.
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 box to allow the user to specify the name or prefix for the VM.
Power On after deploy check box	Check the box to power on the VM after provisioning.
Host Name Template field	Enter the template of the host name.

Name	Description
Disable Host Name Uniqueness Check check box	Check this check box to skip the host name uniqueness validation.
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	Enter the name of the DNS domain.
DNS Suffix List field	Enter the list of domain name suffixes that get appended to DNS.
DNS Server List field	Enter 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	An annotation states that the app/web tier allows the subnet to be created as Shared and Public through the APIC network policy. Check the box to define the VM annotation.
VM Annotation field	This field appears when the **Define VM Annotation** check box is selected. Enter the annotation note for the VM.
Custom Attributes field	This field appears when the **Define VM Annotation** check box is selected. Expand Custom Attributes and click + to add a custom attribute.

d) Click **Submit**.
e) From the **Cost Model** drop-down list, choose a cost model to compute the chargeback.
f) Expand **HyperV Deployment Policy** and check the HyperV deployment policy for the HyperV container provision.
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 Choose **Policies** > **Resource Groups**.
Step 2 On the **Resource Groups** page, click **Application Profile**.
Step 3 Click the row with the application profile that you want to delete.
Step 4 Click **Delete**.
Step 5 On the **Application Profile** confirmation screen, click **Delete**.

Creating a Virtual Infrastructure Policy

Step 1 Choose **Policies** > **Application Containers**.
Step 2 On the **Application Containers** page, click **Virtual Infrastructure Policies**.
Step 3 Click **Add Policy**.
Step 4 On 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 On 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.

Name	Description
+	Click 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 Choose **Policies** > **Application Containers**.

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

Step 3 Click **Add Template**.

Step 4 On the **Add Application Container Template** screen, 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 5 Click **Next**.

Step 6 On the **Application Container Template - Select a Virtual infrastructure policy** screen, complete the following selections:

Name	Description
Select Virtual Infrastructure Policy drop-down list	Choose an APIC policy.
+	Click to create a new infrastructure policy. See Creating a Virtual Infrastructure Policy , on page 111.

Step 7 Click **Next**.

Step 8 On the **Application Container Template - Options** screen, complete the following fields:

Name	Description
End User Self-Service Policy drop down list	Choose an end-user policy. See Configuring Options on the End User Portal, on page 141
Enable Self-Service Deletion of Containers check box	Check this box to allow the user to delete the application container.
Enable VNC Based Console Access check box	Check this box to allow the 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 persons.

Step 9 Click **Next**.

Step 10 On the **Application Container Template - Setup Workflows** screen, select a workflow from the container setup workflow list.

Step 11 Click **Next** to view the **Summary** screen.

Step 12 Click **Submit** to complete the creation of the application container template.

Note The workflow creation of the application container template is automatically fetched for the VMware-based container even when it is not defined. You need to design and select the specific workflow for the HyperV based container.

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

Step 3 Choose an **APIC** template.

Step 4 Click **Create Container**.

Step 5 On the **Create container from template** screen, complete the following fields:

Name	Description
Container Name field	Enter the name of the container. This name must be unique.

Name	Description
Container Label field	Enter the label for the container.
Tenant list	Expand Tenant, check the tenant that you want to use, and then click **Validate**. **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	(Optional). Choose an organization within the tenant.
Enable Resource Limits check box	Check this check box to enable the resource limit. On choosing this check box, you will get additional fields to specify the number of vCPUs, memory, maximum storage size, maximum number of half-width physical servers, and maximum number of full-width physical servers for the container
Enable Network Management check box	Check this check box to put the container under APIC management.
Network Throughput drop-down list	Choose the network throughput from the drop-down list.
Tier Label Customization area	The customized name of the tier label. This area does not appear for a tenant with multiple private networks.

Step 6 Click **Submit**.

Note Make a note of the service request ID presented in the **Submit Result** prompt. You can view the progress of the created container by viewing the details of the service request.

Step 7 Click **Application Containers**.

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.

Supported Layer 4 to Layer 7 Devices

The APIC application container supports the following Layer 4 to Layer 7 devices:

- **Firewall—**Physical ASA and Cisco ASAv.
- **Load Balancer—**VPX or SDX load balancers.

For information about supported firewalls and load balancers, see the Cisco UCS Director Compatibility Matrix.

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 75 .

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

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

Step 3 Choose an application container in which you want to configure L4-L7 service.

Step 4 From the **More Actions** drop-down list, choose **Configure L4-L7 Services**.

Step 5 On the **L4-L7 Configuration** screen, complete the following fields:

Name	Description
Service Type drop-down list	Choose any one of the following service types which are displayed based on the application container configuration: • **Firewall**. • **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. • **Load Balancer (Two Arm)** • **Firewall and Single Arm Load Balancer** • **Firewall and Load Balancer (One Arm, with SSL Offload)** **Note** If the **Configure L4-L7 Service** check box is checked in the application profile, corresponding service types are listed under the following conditions: • If the **Allow Firewall** check box is checked in the **Add L4-L7 Service Policy** dialog box, the firewall service type is only listed. • If the **Allow Load Balancer** check box is checked in the **Add L4-L7 Service Policy** dialog box, the load balancer service type is only listed. • If the **Allow Firewall** check box and **Allow Load Balancer** are checked in the **Add L4-L7 Service Policy** dialog box, the firewall and load balancer service types are listed. **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.
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	Expand LB Servers, and choose the server that needs to be load-balanced. 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.

Name	Description
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 Choose **Policies** > **Application Containers**.

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

Step 3 Double-click an existing application container.

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

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

Step 6 On the **Add Firewall Rule** screen, complete the following fields:

Name	Description
Interface Name drop-down list	Choose the name of the interface.

Name	Description
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.
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 Choose **Policies** > **Application Containers**.
Step 2 On the **Application Containers** page, click **Application Containers**.
Step 3 Double-click an existing application container.
Step 4 Choose any L4-L7 service with Load Balancer service type.
The **LB Servers** screen appears.
Step 5 Click **Add Servers**.
Step 6 On the **Add Servers** screen, expand **VMs** and check the VM(s) that you want to use.
Step 7 In the **Port** field, enter the port number.
The selected VMs are configured with this port number.
Step 8 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 Choose **Policies** > **Application Containers**.
Step 2 On the **Application Containers** page, click **Application Containers**.
Step 3 Double-click an application container.
Step 4 Click **L4 L7 Services**.
Step 5 From the list of L4-L7 services, choose the service that you want to delete.
Step 6 Click **Delete**.
Step 7 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 Choose **Policies** > **Application Containers**.

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

Step 3 Double-click an existing application container.

Step 4 Click **Contracts**.

Step 5 Click **Add Contract (+)** to add a new contract.

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

Name	Description
Select Source Network field	Expand **Select Source Network**, check the source network in the source/destination container to which you want to apply the contract, and then click **Validate**.
Select Destination Network field	Expand **Select Destination Network**, choose the destination network in the source/destination container to which you want to apply the contract, and then click **Validate**.
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.	
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.

Name	Description
The following fields appear only if TCP or UDP protocol is selected:	
Source Port Start field	Enter the starting range of the source port number.
Source Port End field	Enter the ending range of the source port number.
Destination Port Start field	Enter the starting range of the destination port number.
Destination Port End field	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**
Stateful check box	This check box appears when you choose TCP protocol. Check the box to enable stateful connection.

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 Choose **Policies** > **Application Containers**.

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

Step 3 Double-click an application container.

Step 4 Click **Contracts**.

Step 5 Click the row with the contract to which you want to add security rule, and click **View Details**.

Step 6 Click **Security Rules**.

Step 7 Click **Add** to add a security rule.

Step 8 On the **Add Contract** screen, complete the following fields:

Name	Description
Select Source Network field	Displays the source network of the contract.
Select Destination Network field	Displays the destination network of the contract.
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 from destination to source.
The following fields appear only if TCP or UDP protocol is selected:	
Source Port Start field	Enter the starting range of the source port number.
Source Port End field	Enter the ending range of the source port number.
Destination Port Start field	Enter the starting range of the destination port number.
Destination Port End field	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**
Stateful check box	This check box appears when you choose TCP protocol. Check the box to enable stateful connection.

Step 9 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 in Cisco UCS Director. See Adding Security Rules, on page 121.

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 115.
- 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 82 and Adding a Layer 4 to Layer 7 Service Policy, on page 75.

Note A service chain cannot be created in an application container that uses both physical and virtual gateways.

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 132.

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 Choose **Policies** > **Application Containers**.

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

Step 3 Choose an application container.

Step 4 From the **More Actions** drop-down list, choose **Add Tier/Network**.

Step 5 On the **Add Tier/Network** screen, 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.

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

Step 6 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 Choose **Policies** > **Application Containers**.
Step 2 On the **Application Containers** page, click **Application Containers**.
Step 3 Double-click an application container.
Step 4 Click **Virtual Machines**.
Step 5 Click the row with the VM to which you want to add vNIC.
Step 6 From the **More Actions** drop-down list, choose **Add vNICs**.
Step 7 On the **Add vNIC to Container Network** screen, 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 8 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 Choose **Policies** > **Application Containers**.
Step 2 On the **Application Containers** page, click **Application Containers**.
Step 3 Double-click an application container.
Step 4 Click **Virtual Machines**.
Step 5 Click the row with the VM of the vNIC that you want to delete.
Step 6 Click **Delete vNICs**.
Step 7 On the **Delete VM vNICs** screen, choose the vNIC that you want to delete.
Step 8 Click **Delete**.
The VM vNIC is deleted.

Adding Bare Metal Servers to an Existing Container

Note Bare metal servers are supported only in APIC containers.

Before You Begin

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

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

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

Step 3 Choose a container to which you want to add BM.

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

Step 5 On the **Add BMs** screen, expand **Bare Metal Application Components** and click **Add (+)** to add a new BM.

Step 6 On the **Add Entry** screen, 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 drop-down list	Choose the network (tier) to which you want to add the BM component.
Bare Metal Image drop-down list	The BM image to use. This list is retrieved from the Bare Metal Agent.
Blade Type drop-down list	Choose one of the following as the blade type for the container: • Half Width • Full Width
Boot Lun Size (GB) field	Recommended LUN size for booting.

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** screen.

Adding a Disk

Before You Begin

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

Step 1 Choose **Policies** > **Application Containers**.
Step 2 On the **Application Containers** page, click **Application Containers**.
Step 3 Double-click an application container.
Step 4 Click **Bare Metals**.
Step 5 Choose any bare metal server to which the disk is to be added.
Step 6 Click **Add Disk**.
Step 7 On the **Add Disk to BM** screen, enter the disk size in GB.
Step 8 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 Choose **Policies** > **Application Containers**.
Step 2 On the **Application Containers** page, click **Application Containers**.
Step 3 Double-click an application container.
Step 4 Click **Bare Metals**.
Step 5 Choose the bare metal server from which the disk is to be deleted .
Step 6 Click **Delete Disk**.
Step 7 Choose the BM LUNs identity number that you want to delete from the table.
Step 8 Click **Submit**.
Confirm the deletion in the conformation screen.

Deleting Bare Metal Servers

Before You Begin

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

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

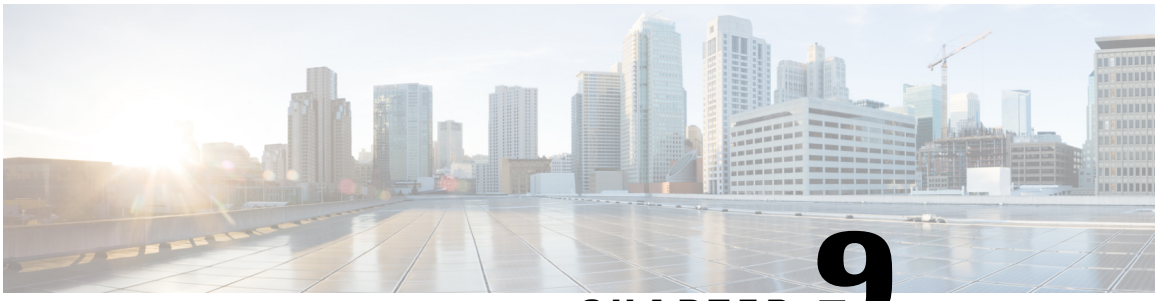
Step 2 On the **Application Containers** page, click **Application Containers**.

Step 3 Double-click an application container.

Step 4 Click **Bare Metals**.

Step 5 From the list of the bare metal servers, choose the bare metal server that you want to delete.

Step 6 Click **Delete BM**.
The bare metal server and the associated disks are deleted.



CHAPTER 9

Managing Application Containers

This chapter contains the following sections:

Managing Application Containers

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

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

Viewing Container Actions

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

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

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

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

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

Adding VMs

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

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

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

Step 3 Choose an application container.

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

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

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

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

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

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

Skip to Step 8.

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

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

Step 8 Click **Submit**.

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

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

Deleting VMs from an Application Container

Before You Begin

- Create and deploy an existing application container with one or more VMs.
- Power off the VMs that you want to delete.

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

Step 2 Choose an application container.

Step 3 From the **More Actions** drop-down list, choose **Decommission Container**.

Step 4 From the list of VMs, click the rows with the VMs that you want to delete.

Note The list shows only VMs that are powered off.

Step 5 Click **Submit**.

The VM is deleted from the selected container.

Accessing a VM Console

Before You Begin

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

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

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

Step 3 Choose an application container.

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

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

Step 6 Click **Submit**.

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

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

Enabling VNC Console Access

You can enable console access on an individual VM.

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **VMs**.
Step 3 Click the row with the VM for which to enable console access.
Step 4 From the **More Actions** drop-down list, choose **Configure VNC**.
Step 5 On the **Configure VNC Request** screen, from the **Key Board Mapping** drop-down list, choose a mapping.
Step 6 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 Choose **Policies** > **Application Containers**.
Step 2 On the **Application Containers** page, click **Application Containers**.
Step 3 Choose an application container.
Step 4 Click **Clone Container** and complete the following fields:

Name	Description
Container Name field	Enter the name of the container.
Container Label field	Enter a unique container label.
Tenant list	Expand the list to choose a tenant and click **Select**.

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 On the **Application Containers** page, click **Application Containers**.
Step 3 Choose an application container.
Step 4 Click **Power On Container** or **Power Off Container**.
Step 5 From the list, select the VMs to power on or off.
Step 6 Click **Submit**.

Viewing Application Containers

To view application containers in Cisco UCS Director, choose **Policies** > **Application Containers**.

Choose **Policies** > **Application Containers**.
Application containers use a color scheme to identify the container's status:

- Green—All VMs and bare metal servers (BMs) are powered on, including the gateway (GW) if the container configuration includes a GW.
- Yellow—Any of the requested BMs are still in progress/failed or any of the application VMs are down.
- Blue—Container provisioning is in progress.
- Grey—VMs and BMs are not present in the container.
- Red—All VMs and BMs, including the GW, are powered off.

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 Choose **Policies** > **Application Containers**.

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

Step 3 Choose an application container.

Step 4 From the **More Actions** drop-down list, choose **Delete Container**.

Note If you choose to delete an application container with associated L4-L7 services, 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 with the container, click **Submit**.
A notice appears confirming that a service request was generated.

Step 6 Choose **Organizations** > **Service Requests**.

Step 7 On the **Service Requests** page, click **Service Requests**.

Step 8 Click the row with the deletion service request.

Step 9 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 Choose **Policies** > **Application Containers**.

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

Step 3 Choose an application container.

Step 4 Click **View Reports**.

Step 5 On the **View Container Reports** screen, 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.

Step 6 Click **Submit**.
The report displays the ID of the Service Request used to create the application container in the report header.

Viewing Application Container Information

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

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

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

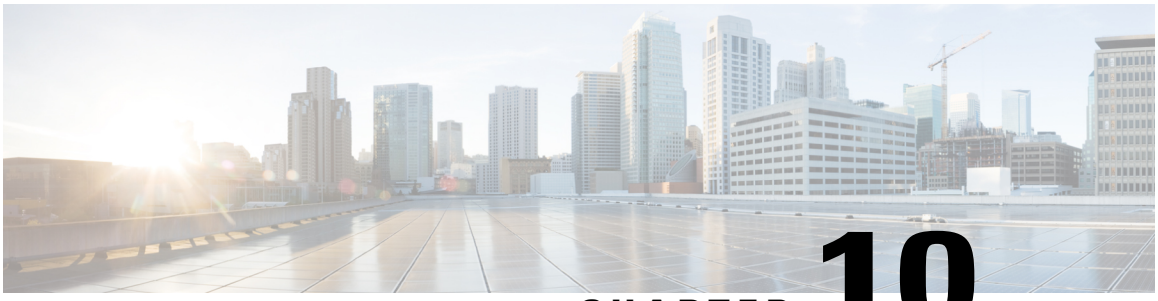
Step 3 Choose an application container.

Step 4 Click **View Details**.

Step 5 You can view the following information:

Page	Description
Summary	• **Overview—**Displays a summary of the application container, such as: container name and ID; if DR is enabled; group name; application profile; application container template used; if there are managed network services; number of tiers, VMs, and BMs; and resource pool. • **Resource Limits—**Displays a summary of the available resources and limits for resources, such as: CPUs; memory; datastore size; network throughput; and servers.
Virtual Machines	Displays details about the VMs provisioned for the application container, such as: VM ID, name, and type; status; IP address; guest OS; and the time when the VM was provisioned. **Note** Specific naming conventions are followed for 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	Displays details about bare metals, such as the bare metal name, OS type, IP address, and Service Request (SR) ID. Bare metals are physical servers provisioned as part of the application container.

Page	Description
Tier Mapping	Displays information about the tiers, such as: the VMs and BMs in each tier; resource name and type; and IP address. Tiers correspond to the networks that 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.
L4 L7 Services	Displays information about L4-L7 services, such as: Service Request (SR) ID; service name; primary IP address; service type; device type; consumer and provider tiers; load balancer VIP and SNIP; service chain flag and type; protocol; port; and if SSL is enabled. **Note** You can drill down the service name to view the list of real servers.
Contracts	Displays the information about the contracts that define the rule for communication in multi-tier applications, such as: contract; source container and network; and destination container and network. **Note** You can drill down each contract to view the security rules.



CHAPTER 10

Self Service Management Options

This chapter contains the following sections:

Configuring Options on the End User 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 End User Portal Guide to obtain information on how to manage application containers using the end user portal.

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **End User Self-Service Policy**.

Step 3 Click **Add**.

Step 4 On the **Add End User Policy** screen, in **Account Type** choose a cloud type.

Step 5 Click **Submit**.

Step 6 On the **End User Policy** screen, complete the following fields:

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

Step 7 Click **Submit**.