Creating Application Containers

This chapter contains the following sections:

General Application Container Creation Process

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

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

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

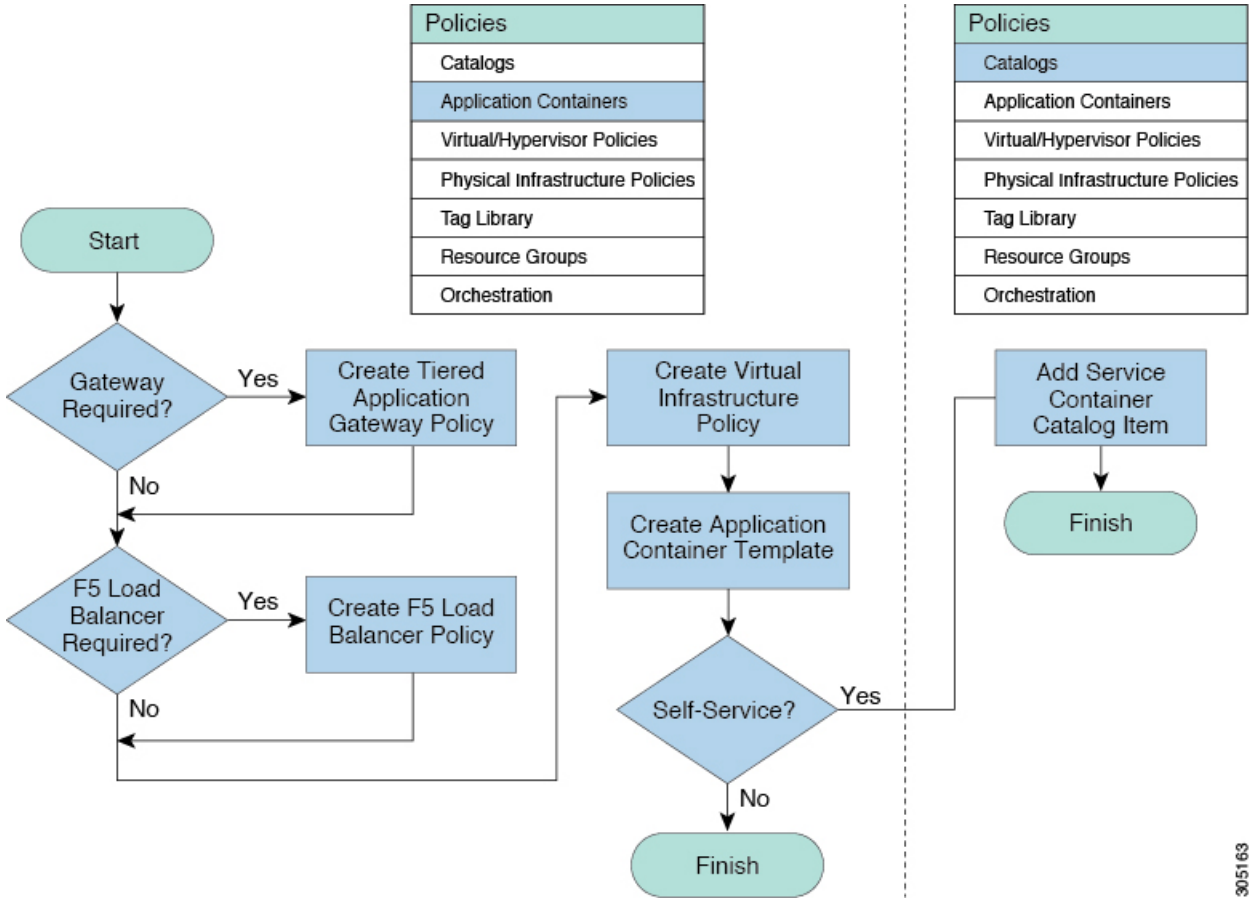
d Add an end user self-service policy and configure the self-service options.

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

5 Create a container based on the container template.

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

Figure 1: Process for Creating a General Application Container Template



Creating Application Container Policies

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

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

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

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

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

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

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

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

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

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

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

Step 7 Click **Next**.

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

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

Step 9 Click **Next**.

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

Step 11 Click **Next**.

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

Step 13 Click **Next**.

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

About Application Container Templates

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

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

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

Creating Application Container Templates

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

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

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

Before You Begin

Create a virtual infrastructure policy. See Creating Application Container Policies, on page 2.

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

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

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

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

Step 4 Click **Next**.

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

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

Step 6 Click **Next**.

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

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

Step 8 Click **Submit**.

Step 9 Click **Next**.

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

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

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

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

Step 13 Click **OK**.

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

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

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

Step 15 Click **Next**.

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

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

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

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

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

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

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

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

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

Complete the following fields:

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

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

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

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

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

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

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

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

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

What to Do Next

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

Creating a Custom Workflow for Application Containers

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

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

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

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

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

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

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

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

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

  6 Specify the primary DVSwitch and alternate DVSwitch names.

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

Managing Application Containers

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

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

Viewing Container Actions

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

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

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

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

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

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

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

Adding VMs

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

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

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

Step 3 Choose a container.

Step 4 Click **Add VMs**.

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

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

Step 7 Define the Virtual Machine:

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

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

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

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

Skip to Step 10.

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

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

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

Step 10 Click **Submit**.

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

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

Deleting VMs

Before You Begin

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

- Power off the VMs you want to delete.

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

Step 2 Choose an application container.

Step 3 Click **Decommission Container**.

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

Note The list shows only VMs that are powered off.

Step 5 Click **Submit**.

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

Accessing a VM Console

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

Before You Begin

Enable access for VMs that you want to access using VNC. See Enabling VNC Console Access, on page 17.

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

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

Step 3 Choose a container.

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

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

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

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

Enabling VNC Console Access

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

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

Cloning an Existing Container

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

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

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

Step 5 Click **Submit**.

Managing Container Power

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

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

Deleting Application Containers

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

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

Viewing Reports

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

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

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

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

Step 4 Click **View Reports**.

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

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

A dialog appears with a report detailing the application container.

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

Viewing Application Container Information

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

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

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

Step 3 Click **View Details**.

Step 4 You can view the following information:

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

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