Setting Up an Cisco Application Policy Infrastructure Controller Container

This chapter contains the following sections:

Cisco UCS Director and Cisco Application Centric Infrastructure

Cisco UCS Director is a unified infrastructure management solution that provides management from a single interface for compute, network, storage, and virtualization layers. Cisco UCS Director uses a workflow orchestration engine with workflow tasks that support the compute, network, storage, and virtualization layers. Cisco UCS Director supports multitenancy, which enables policy-based and shared use of the infrastructure.

Cisco UCSD 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 application-centric infrastructure.

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

Cisco Application Policy Infrastructure Controller

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

The orchestration feature allows you to automate APIC configuration and management tasks in workflows. A complete list of the APIC orchestration tasks is available in the Workflow Designer, and in the Task Library. For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide for this release.

APIC Application Containers

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

- Establish networks in a VMware environment.
- Provision multiple VMs from a network.
- Provide a way to isolate those networks using gateways (for example, ASAv).

- Allow load balancing the container network using VPX or SDX load balancers.
- Use a Cisco Application Centric Infrastructure Controller (APIC).
- 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

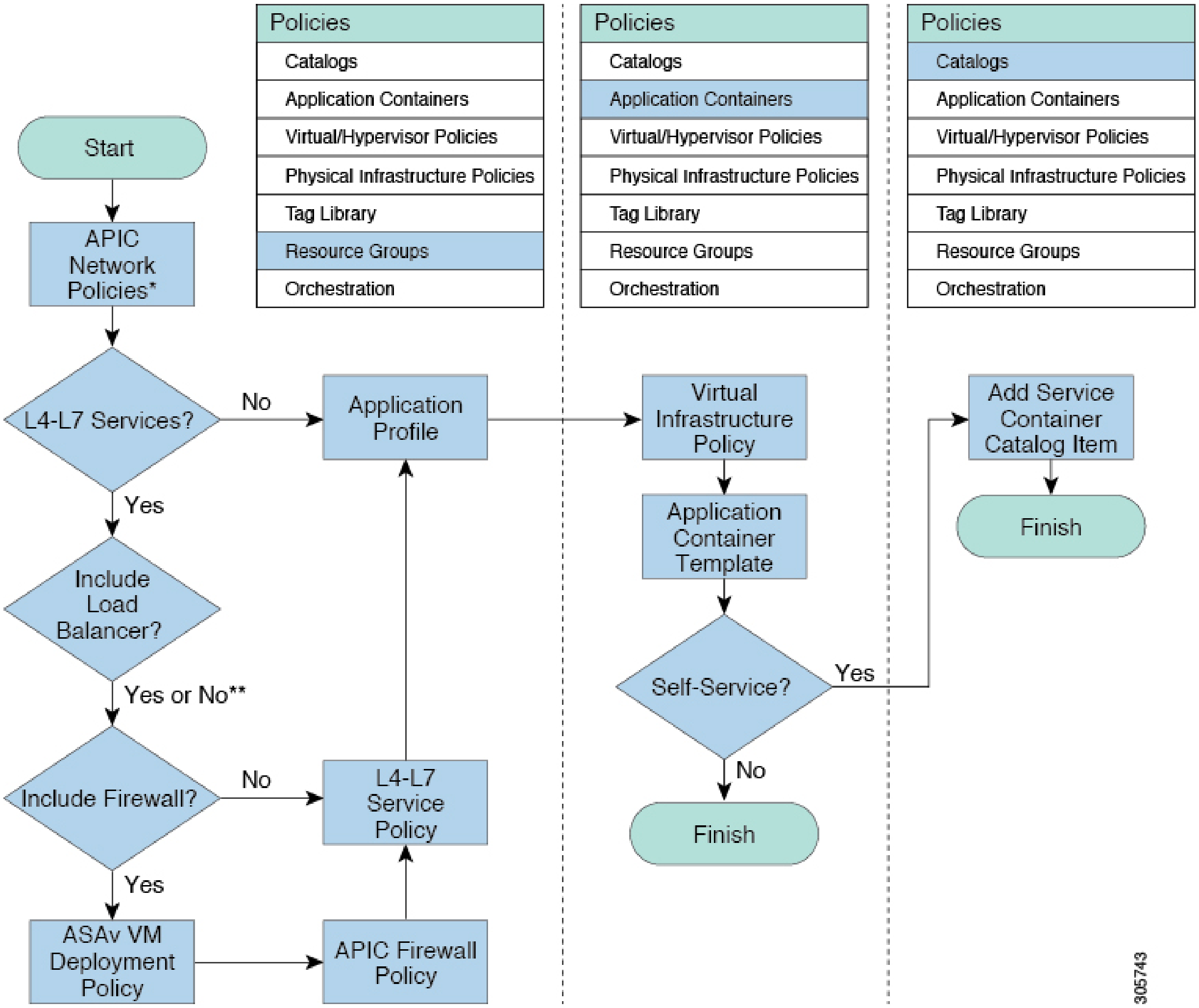
Cisco UCS Director APIC application containers have the following limitations:

- 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 require 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 1: 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 ASAv brings full firewall functionality to virtualized environments in order to secure data center traffic and multi-tenant environments. The ASAv VM deployment policy is used in the **Deploy ASAv VM from OVF** task.

Adding an ASAv VM Deployment Policy

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

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

Step 3 Click **Add**.

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

Name	Description
Policy Name field	The name of the ASAv VM deployment policy.
ASAv OVF field	Click **Select** and choose a template file in the open virtualization format (OVF).
VM Name field	The name for the ASAv virtual machine (VM) instance. The policy will automatically prefix this VM name with the container name.
Port field	The port number of the firewall appliance. We recommend using port 443.
Username field	The username that is used to access the firewall appliance.
Password field	The password that is used to access the firewall appliance.
Disk Format drop-down list	Choose the virtual disk format. The available formats for provisioning are **Thick Provision Lazy Zeroed**, **Thick Provision Eager Zeroed**, and **Thin Provision**.

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

Step 5 Click **Submit**.

APIC Firewall Policy

You can 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 On the menu bar, choose **Policies** > **Resource Groups**.

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

Step 3 Click **Add**.

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

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

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

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

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

Step 5 Click **Submit**.

APIC Network Policy

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

Adding an APIC Network Policy

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

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

Step 3 Click **Add**.

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

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

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

Step 5 Click **Submit**.

Layer 4 to Layer 7 Service Policy

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

Adding a Layer 4 to Layer 7 Service Policy

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

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

Step 3 Click **Add**.

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

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

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

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

Step 5 Click **Submit**.

Network Device System Parameters Policy

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

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

Adding a Network Device System Parameters Policy

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

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

Step 3 Click **Add**.

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

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

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

Step 5 Click **Submit**.

What to Do Next

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

Application Profiles

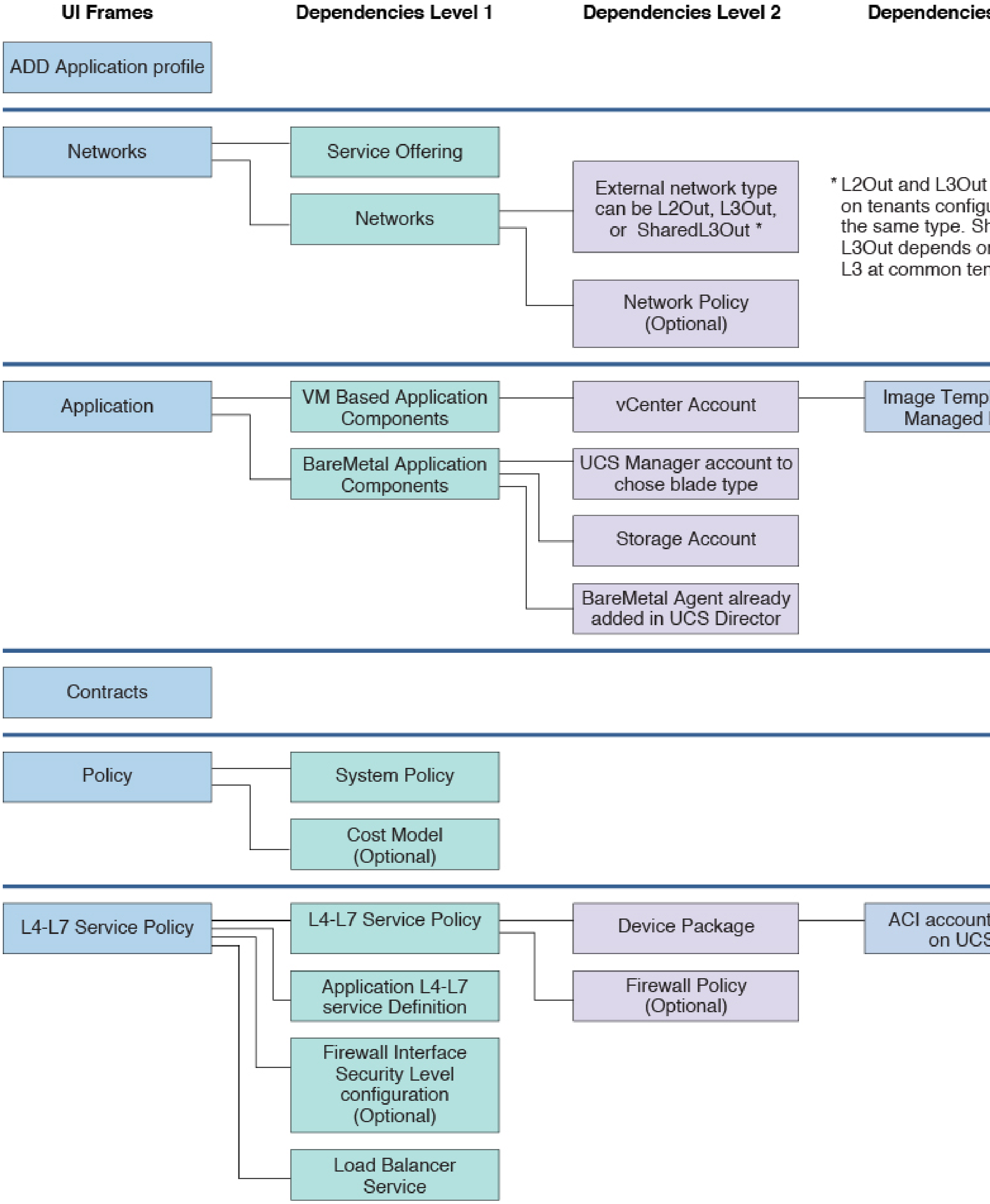
An application profile is a description of the infrastructure required for the deployment of an application. These infrastructure requirements include bare metal configurations, virtual machines (VMs), L4-L7 policies, and connection policies.

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:

305747 Application Profile – Dependencies

Figure 2: Application Profile — Dependencies


UI Frames
Dependencies Level 1
Dependencies Level 2
Dependencies
ADD Application profile
Networks
Service Offering
Networks
External network type can be L2Out, L3Out, or SharedL3Out *
Network Policy (Optional)
* L2Out and L3Out
on tenants configu
the same type. Sh
L3Out depends o
L3 at common te
Application
VM Based Application Components
vCenter Account
Image Temp
Managed
BareMetal Application Components
UCS Manager account to chose blade type
Storage Account
BareMetal Agent already added in UCS Director
Contracts
Policy
System Policy
Cost Model (Optional)
L4-L7 Service Policy
L4-L7 Service Policy
Device Package
ACI account
on UCS
Firewall Policy (Optional)
Application L4-L7 service Definition
Firewall Interface Security Level configuration (Optional)
Load Balancer Service

Adding an Application Profile

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

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

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

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

Step 3 Click **Add**.

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

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

Step 5 Click **Next**.

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

Name	Description
Service Offering drop-down list	Click **Select** and choose a service offering from the list. The service offering must belong to the tenant for which you will create containers with this application profile. Click the + icon to add a service offering. For more information about how to add a service offering, see the Cisco UCS Director APIC Management Guide.

Name	Description
Networks field	Define the network types and the number of networks that are needed in the application. For more information on how to configure a network, see the *next Step*.

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

Name	Description
Network field	Enter the name of the network.
Description field	Enter the description of the network.
Network Type drop-down list	Choose one of the following as the network type: • **Internal** • **External** • **Infrastructure** • **Failover** **Note** When a tenant needs multiple private networks, you need to define only **Internal** and **External** network types.
Interested Tag Value field	Click **Select** and choose the tag values for each tier. During container provisioning, resource is selected based on the tag associated with the tier. **Note** You can select more than one tag (the tag that is used for VMware cluster or datastore cluster). For example, if you select a datastore tag (ds tag - gold) and a VMware cluster tag (cluster tag - ESXi cluster tag), during the datastore selection, the datastore tagged with the gold value is selected. **Note** To avail shared L3Out support, choose the tag value that is used for tagging the external network and contract of a common tenant.
APIC Network Policy drop-down list	This field appears only when you choose network type as **Internal**. Choose the APIC network policy from the list. Click the + icon to add an APIC network policy. For more information about how to add an APIC network policy, see Adding an APIC Network Policy, on page 11.

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

Step 8 Click **Next**.

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

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

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

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

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

c) Click **Submit**.

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

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

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

Name	Description
Instance Name field	Enter the name of the bare metal instance.
Description field	Enter the description of the bare metal instance.
Network drop-down list	Choose the 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 11 Click **Next**.

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

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

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

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

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

Click the + icon to add the communication protocol details:

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

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

b) Click **Submit**.

Step 13 Click **Next**.

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

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

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

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

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

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

a) **L4-L7 Service Policy** drop-down list—Choose the Layer 4 to Layer 7 service policy from the list. Click the + icon to add a Layer 4 to Layer 7 service policy. For more information about how to add a Layer 4 to Layer 7 service policy, see Adding a Layer 4 to Layer 7 Service Policy, on page 13.

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

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

Name	Description
Services field	Choose the service type by checking one of the following check boxes: • **FIREWALL—**To provide firewall service between consumer and provider. • **LB_SINGLE_ARM—**To configure 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** check box to customize the firewall security for the network tiers in the application profile. The **Firewall Security Levels** field displays the security level configured for the tiers. Choose a tier and click the edit icon to edit the security level.

Step 16 Click **Submit**.

Cloning an Application Profile

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

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

Step 3 Choose an application profile.

Step 4 Click **Clone**.

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

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

Step 6 Click **Next**.

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

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

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

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

Name	Description
Network Type drop-down list	Choose one of the following as the network type: • **Internal** • **External** • **Infrastructure** • **Failover** **Note** When a tenant needs multiple private networks, you need to define only **Internal** and **External** network types.
Interested Tag Value field	Click **Select** and choose the tag values for each tier. During container provisioning, resource is selected based on the tag associated with the tier. **Note** You can select more than one tag (the tag that is used for VMware cluster or datastore cluster). For example, if you select a datastore tag (ds tag - gold) and a VMware cluster tag (cluster tag - ESXi cluster tag), during the datastore selection, the datastore tagged with the gold value is selected. **Note** To avail shared L3Out support, choose the tag value that is used for tagging the external network and contract of a common tenant.
APIC Network Policy drop-down list	This field appears only when you choose network type as **Internal**. Choose the APIC network policy from the list. Click the + icon to add an APIC network policy. For more information about how to add an APIC network policy, see Adding an APIC Network Policy, on page 11.
L2/L3 Selection drop-down list	This field appears only when you choose network type as **External**. By default, **L2Out** is selected to integrate the ACI fabric with external Layer 2 network. • **L2Out—**To integrate the ACI fabric with external Layer 2 network. • **L3Out—**To integrate the ACI fabric with external Layer 3 network. • **SharedL3Out—**To integrate the ACI fabric with shared external Layer 3 network. The network must be tagged and updated on Tenant vPOD in advance and the same tag must be selected for the external network in case of shared L3Out.

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

Step 9 Click **Next**.

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

a) Click the + icon.

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

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

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

c) Click **Submit**.

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

a) Click the + icon.

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

Name	Description
Instance Name field	Enter the name of the bare metal instance.
Description field	Enter the description of the bare metal instance.
Network drop-down list	Choose the 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 the + icon to add the communication protocol details.

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

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

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

b) Click **Submit**.

Step 14 Click **Next**.

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

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

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

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

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

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

a) **L4-L7 Service Policy** drop-down list—Choose the Layer 4 to Layer 7 service policy from the list. Click the + icon to add a Layer 4 to Layer 7 service policy. For more information about how to add a Layer 4 to Layer 7 service policy, see Adding a Layer 4 to Layer 7 Service Policy, on page 13.
b) **Application L4-L7 Service Definition** field—Click the + icon. In the **Add Entry to Application L4-L7 Service Definition** dialog box, complete the following fields:

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

Name	Description
Services field	Choose the service type by checking one of the following check boxes: • **FIREWALL—**To provide firewall service between consumer and provider. • **LB_SINGLE_ARM—**To configure 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** check box to customize the firewall security for the network tiers in the application profile. The **Firewall Security Levels** field displays the security level configured for the tiers. Choose a tier and click the edit icon to edit the security level.

Step 17 Click **Submit**.

Editing an Application Profile

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

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

Step 3 Choose an application profile.

Step 4 Click **Edit**.

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

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

Step 6 Click **Next**.

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

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

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

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

Name	Description
Network Type drop-down list	Choose one of the following as the network type: - **Internal** - **External** - **Infrastructure** - **Failover** **Note** When a tenant needs multiple private networks, you need to define only **Internal** and **External** network types.
Interested Tag Value field	Click **Select** and choose the tag values for each tier. During container provisioning, resource is selected based on the tag associated with the tier. **Note** You can select more than one tag (the tag that is used for VMware cluster or datastore cluster). For example, if you select a datastore tag (ds tag - gold) and a VMware cluster tag (cluster tag - ESXi cluster tag), during the datastore selection, the datastore tagged with the gold value is selected. **Note** To avail shared L3Out support, choose the tag value that is used for tagging the external network and contract of a common tenant.
APIC Network Policy drop-down list	This field appears only when you choose network type as **Internal**. Choose the APIC network policy from the list. Click the + icon to add an APIC network policy. For more information about how to add an APIC network policy, see Adding an APIC Network Policy, on page 11.
L2/L3 Selection drop-down list	This field appears only when you choose network type as **External**. By default, **L2Out** is selected to integrate the ACI fabric with external Layer 2 network. - **L2Out**—To integrate the ACI fabric with external Layer 2 network. - **L3Out**—To integrate the ACI fabric with external Layer 3 network. - **SharedL3Out**—To integrate the ACI fabric with shared external Layer 3 network. The network must be tagged and updated on Tenant vPOD in advance and the same tag must be selected for the external network in case of shared L3Out.

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

Step 9 Click **Next**.

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

a) Click the + icon.

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

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

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

c) Click **Submit**.

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

a) Click the + icon.

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

Name	Description
Instance Name field	Enter the name of the bare metal instance.
Description field	Enter the description of the bare metal instance.
Network drop-down list	Choose the 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 the + icon to add the communication protocol details.

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

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

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

b) Click **Submit**.

Step 14 Click **Next**.

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

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

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

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

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

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

Step 17 Click **Submit**.

Deleting an Application Profile

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

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

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

Step 3 Choose an application profile from the table.

Step 4 Click **Delete**.

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

Creating a Virtual Infrastructure Policy

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

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

Step 3 Click **Add Policy**.

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

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

Step 5 Click **Next**.

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

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

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

Step 7 Click **Next**.

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

Step 9 Click **Submit**.

Creating an Application Container Template

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

Before You Begin

Create a virtual infrastructure policy.

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

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

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

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

Step 4 Click **Next**.

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

Name	Description
Select Virtual Infrastructure Policy drop-down list	Choose an APIC policy.
+	Click the + icon to create a new infrastructure policy. See Creating a Virtual Infrastructure Policy , on page 44.

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

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

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

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

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 Click the **Application Container Templates** tab.

Step 3 Choose an **APIC** template.

Step 4 Click **Create Container**.

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

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

Step 6 Click **Submit**. The **Submit Result** dialog box appears.

Note Make a note of the service request ID presented in the **Submit Result** prompt.

Step 7 Click **OK**.

Note You can view the progress of the created container by viewing the details of the service request.

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

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

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 13 .

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

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

Step 3 Click on an existing application container.

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

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

Name	Description
Service Type drop-down list	Choose any one of the following service types: • **Firewall**. • **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	Select 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.

Name	Description
Protocol drop-down list	Choose a protocol. Available protocols are: • FTP • RDP • HTTP • DNS
Port field	This field does not appear if the container for a tenant with multiple private networks is selected. The port number of the selected protocol.
The following fields appear only if the **Load Balancer (One Arm, SSL Offload)** is chosen from the **Service Type** drop-down list.	
SSL Port field	The port number of the SSL enabled vServer.
Certificate field	A valid SSL certificate.
Key field	Unique key for the SSL certificate.
The following fields appear only if the container for the tenant with multiple private networks is selected.	
Front End Port	The front end port number.
Back End Port	The back end port number.
CookieName	Enter the name of the cookie.
LB Method	Choose the load balancer method.
PersistenceType	Choose the persistence type.

Step 6 Click **Submit**.

Adding Firewall Rules

Before You Begin

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

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

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

Step 3 Click an existing application container.

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

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

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

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

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

Step 7 Click **Submit**.

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

Adding Real Servers to Load Balancer Service

Before You Begin

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

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

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

Step 3 Click an existing application container.

Step 4 Choose any L4-L7 service with Load Balancer service type.
The **LB Servers** screen appears.

Step 5 In the **Add Servers** dialog box, choose any VM(s) from the table.

Step 6 In the **Port** field , enter the port number.
The selected VMs are configured with this port number.

Step 7 Click **Submit**.

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

Deleting L4-L7 Services

Before You Begin

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

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

Step 2 Choose an application container.

Step 3 Click **L4 L7 Services**.

Step 4 From the list of L4-L7 services, choose the service that you want to delete.

Step 5 Click **Delete**.

Step 6 In the confirmation dialog, click **Delete**.

Adding Contracts

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

Before You Begin

Create an APIC application container.

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

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

Step 3 Click an existing application container.

Step 4 Click the **Contracts** tab.

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

Step 6 In the **Add Entry to Contracts** dialog box, complete the following fields:

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

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

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

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

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

Adding Security Rules

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

Before You Begin

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

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

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

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

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

Deleting Security Rules

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

Before You Begin

Create an APIC application container.

Step 1 Choose any existing security rule that you want to delete.

Step 2 Click **Delete** to delete the selected security rule.
A confirmation dialog box appears.

Step 3 Click **Delete**.
The security rule is deleted.

Service Chaining

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

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

- Create the service chain in an existing container. See Configuring L4-L7 Services, on page 47.
- 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 20 and Adding a Layer 4 to Layer 7 Service Policy, on page 13.

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.

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

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

Before You Begin

Create an APIC application container.

Adding Tier/Network

Before You Begin

Create an APIC application container.

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

Step 2 Choose an existing application container.

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

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

Name	Description
Tier/Network Name field	The name of the tier or network.
Tier Label field	The label for the tier.

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

Adding a Virtual Network Interface Card to a VM

Before You Begin

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

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

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

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

Step 4 Click **Add vNICs**.

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

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

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

Deleting a Virtual Network Interface Card

Before You Begin

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

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

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

Step 3 Click the **Virtual Machines** tab.
From the list of VMs, select a VM of the vNIC that you want to delete.

Step 4 Click **Delete vNICs**.

Step 5 In the **Delete VM vNICs** dialog box, choose the vNIC that you want to delete.

Step 6 Click **Submit**.
The VM vNIC is deleted.

Adding 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 Click the **Application Containers** tab.

Step 3 Choose a container.

Step 4 Click **Add BMs**.

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

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

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

Step 7 Click **Submit**.

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

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

Adding a Disk

Before You Begin

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

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

Step 2 Choose an application container.

Step 3 Click **Bare Metals**.

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

Step 5 Click **Add Disk**.

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

Step 7 Click **Submit**.

Deleting a Disk

Before You Begin

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

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

Step 2 Choose an application container.

Step 3 Click **Bare Metals**.

Step 4 Choose the bare metal server from which the disk is to be deleted .

Step 5 Click **Delete Disk**.

Step 6 Choose the BM LUNs identity number that you want to delete from the table.

Step 7 Click **Submit**.

Step 8 In the confirmation dialog box, click **OK**.

Deleting Bare Metal Servers

Before You Begin

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

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

Step 2 Choose an application container.

Step 3 Click **Bare Metals**.

Step 4 From the list of the bare metal servers, choose the bare metal server that you want to delete.

Step 5 Click **Delete BM**.
The bare metal server and the associated disks are deleted.