Overview

This chapter contains the following sections:

Application Containers

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

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

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

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

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

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

Types of Application Containers

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

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

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

Viewing Application Containers

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

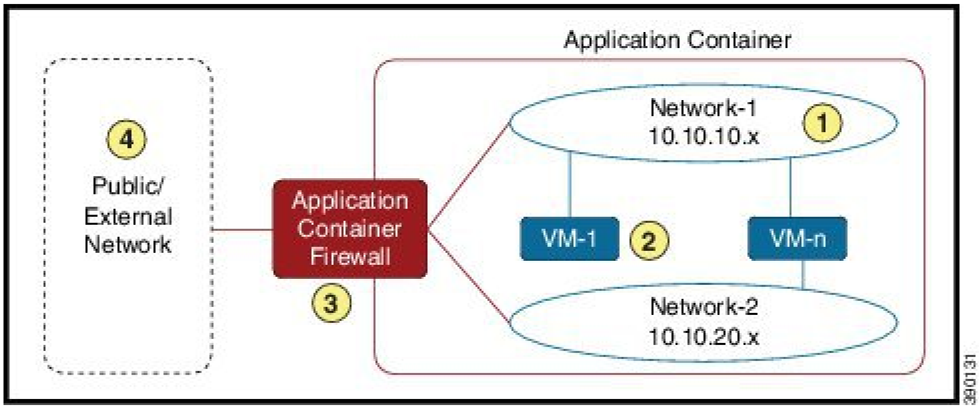
From the menu bar, choose **Policies** > **Application Containers**.
Application containers use a color scheme to identify the container's status:

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

Securing a Container Using an ASA Gateway

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

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



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

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

1. **Define gateway policy**—In the gateway policy, you must define the gateway type for the container and on which cloud account (vCenter) the gateway gets deployed.
2. **Define an application container template**—You must define the cloud account on which the container is created, as well as, performing several other tasks:

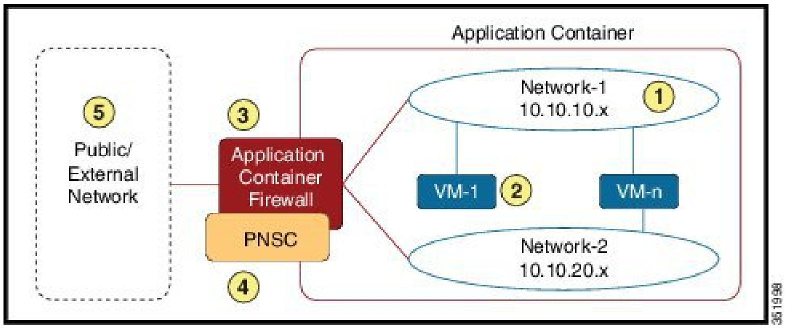
Note The steps are different for creation of an APIC container. See APIC Application Container Creation Process.

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

3. **Create an application container from the defined container template**—An application container is created from the template defined in step 2. You must choose a group for which the container is created.
4. **Application container**—After creating the application container, you can do various management actions, such as power management of the container, adding VMs to a container, cloning or deleting the container, and opening a console for VMs and viewing the reports.

Securing a Container Using a Cisco Virtual Security Gateway

Figure 2: Example Application Container Using a Cisco VSG



Region	Description

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

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

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

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

1. **Create a PNSC account**
2. **View PNSC reports**
3. **Create a PNSC firewall policy**
4. **Integrate a Cisco VSG into a application container—**This process involves several tasks:
    - Upload an OVF file
    - Deploy an OVF file
    - Create an application container template for a Cisco VSG

Orchestration Tasks for Network Device Management

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

A complete list of the network device orchestration tasks is available in the Workflow Designer and in the Task Library.

For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.

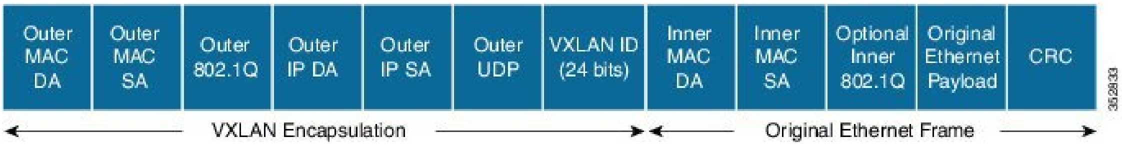
Application Container Support for Cisco VXLANs

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

Note APIC containers do not support VXLANs.

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

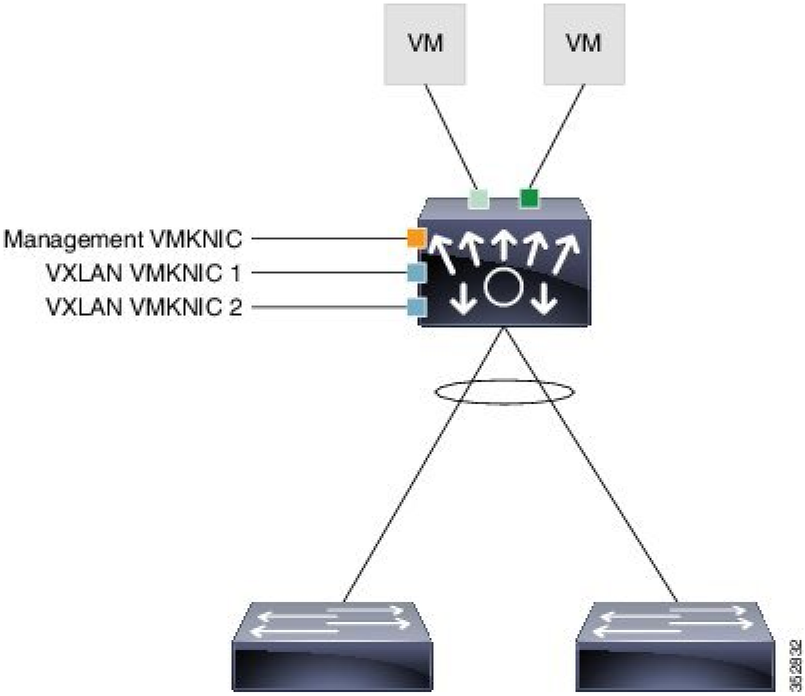
Figure 3: VXLAN encapsulated frame format



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

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

Figure 4: VEM VMKNIC interface with VXLAN Capability



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

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

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

ASAv Gateway

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

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

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