Overview of Application Containers

This chapter contains the following sections:

Application Containers

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

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

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

- Physical server or virtual machine
- Amount of reserved storage
- Maximum available CPU
- Maximum available memory
- Version of operating system
- Range of VLANs
- Gateway or firewall, if desired

- Load balancer, if desired
- Required approvals, if desired
- Access Control List (ACL) rules or other L3 services, if desired
- Costs associated with the application container, if desired

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

Types of Application Containers

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

- Fenced Virtual—A fenced virtual container is a collection of VMs with an internal private network that is based on rules specified by the administrator. The fenced container can have one or more VMs that are guarded by a fencing gateway to the public or external cloud. This is the most common type of application container for use with VMs. For more information, see the Setting Up a Fenced Virtual Container chapter in this guide.
- Virtual Secure Gateway (VSG)—A Cisco Virtual Secure Gateway (VSG) container is used to provide enhanced security in virtual environments. You can use Cisco UCS Director to configure a Prime Network Services Controller (PNSC) in addition to its internal firewall (Cisco Virtual Security Gateway), which is then integrated into an application container. For more information, see the Setting Up a Virtual Secure Gateway Container chapter in this guide.
- Application Centric Infrastructure Controller (APIC) container—The APIC container is used in the Cisco APIC deployments. APIC is the unified point of automation, management, monitoring, and programmability for the Cisco Application Centric Infrastructure (ACI). The APIC supports the deployment, management, and monitoring of any application anywhere, with a unified operations model for physical and virtual components of the infrastructure. It is the central control engine for a broader cloud network. The APIC programmatically automates network provisioning and control, based on user-defined application requirements and policies. Cisco UCS Director lets you create application containers that support Cisco APIC. For more information about the APIC container, see the Setting Up an Cisco Application Policy Infrastructure Controller Container chapter in this guide, and the Cisco UCS Director APIC Management Guide for this release.
- Fabric—The fabric application container is used in Dynamic Fabric Automation (DFA) network deployments. Cisco Unified Fabric Automation is a multistage, switching network in which every connected device is reachable through the same number of hops. Cisco Unified Fabric Automation Organization fabric enables the use of a scale-out model for optimized growth. For more information on application containers in a DFA network, see the Setting Up a Fabric Container chapter in this guide, and the Cisco UCS Director Unified Fabric Automation Management Guide.

Viewing Application Containers

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

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

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

Supported Layer 4 to Layer 7 Services

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

Firewall

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

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

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

Load Balancer

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

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