Cisco CloudCenter Solution with Cisco ACI: Deployment Topologies and Requirements

Overview

This document describes how a Cisco CloudCenter™ dedicated deployment can easily be configured to work with Cisco® Application Centric Infrastructure (Cisco ACI™) northbound APIs without plug-ins or any other additional software required. It summarizes four deployment topologies: single pod, multipod, stretched network, and multicloud. It presents configuration and network requirements for the Cisco CloudCenter and Cisco ACI solution using VMware vSphere as the virtual machine platform.

Contents

Audience

This document is written for Cisco ACI customer IT managers and architects and for Cisco and partner sales engineers, field consultants, and professional services staff who want to understand Cisco CloudCenter and Cisco ACI deployment considerations for both single-pod and stretched application deployments.

Introduction

Cisco is the market leader for Software-Defined Networking (SDN). Cisco ACI is a holistic SDN architecture that introduces hardware and software innovations built on the new Cisco Nexus® 9000 Series Switches. Cisco ACI provides a centralized policy-based application deployment architecture that is managed through the Cisco Application Policy Infrastructure Controller (APIC).

The Cisco CloudCenter solution is a hybrid cloud management platform that securely provisions infrastructure resources and deploys application components and data to more than 19 data center, private cloud, and public cloud environments. Cisco CloudCenter application-centric hybrid cloud management is an excellent fit for Cisco ACI and policy-based network management.

IT organizations pursuing a hybrid IT strategy need flexibility in the ways and locations in which applications are deployed in data center and private and public cloud environments. Cisco CloudCenter users can use self-service technology to deploy applications on demand in any environment. But when they deploy an entire application or even just a single tier in an environment with a Cisco ACI managed network, they get public cloud agility with greater network security and more cost-effective deployment options than with a public cloud alone.

You can use the Cisco CloudCenter and Cisco ACI solution to provision and secure infrastructure and deploy applications based on the desired end state and needs of the application. The Cisco CloudCenter platform automates the entre application deployment process and communicates directly with the Cisco ACI API to automate creation of Cisco ACI policy objects, including application network profiles (ANPs), endpoint groups (EPGs), contracts, filters, and any other objects required by an application.

IT gets optimal network security and operational efficiency to meet the needs of the application, without the need for users to have any knowledge of network policies and without the need for the network team to manually set policies. Scaling and end-of-life actions are automated as well, providing automatic updates and termination of network policies.

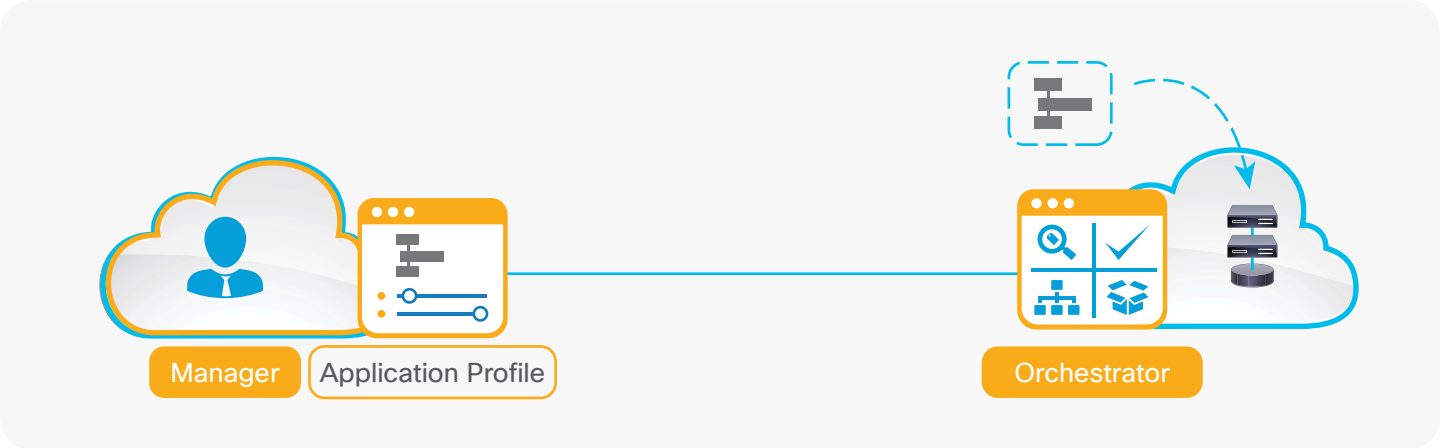
Cisco CloudCenter components

The power of the Cisco CloudCenter solution comes from its unique and patented technology. The solution combines a cloud-independent application profile, which defines deployment and management requirements for the full application stack, with a cloud-specific orchestrator, which abstracts the unique aspects of the environment, provisions infrastructure, and deploys and configures application components using the infrastructure and services available (Figure 1).

- **Cisco CloudCenter manager** is a centralized management portal that allows users to quickly and easily model, deploy, and manage applications. It also gives administrators enterprise-class visibility and governance control of applications, clouds, and users.
- **Cisco CloudCenter application profile** is a user-created model of an application's deployment and management requirements in a portable and cloud-independent format. Each application profile is easily created with a simple, visual, drag-and-drop topology modeler using either preconfigured or customized services, images, and containers.
- **Cisco CloudCenter orchestrator** is a cloud-specific, multitenant orchestration tier that is transparent to users and is installed in each data center private cloud or public cloud environment. It interprets the needs of the application, provisions infrastructure resources, deploys the application components and, optionally, data, manages the deployment including run-time policies, and aggregates usage and cost information.

Unlike other infrastructure-focused cloud management solutions, the Cisco CloudCenter solution is cloud independent. You don't need to write cloud-specific scripts or orchestration workflows or to modify application code. There also is no cloud lock-in. And with a single platform, IT doesn't need to invest in multiple cloud-specific management stacks and teams.

Figure 1. Cisco CloudCenter components



Joint solution

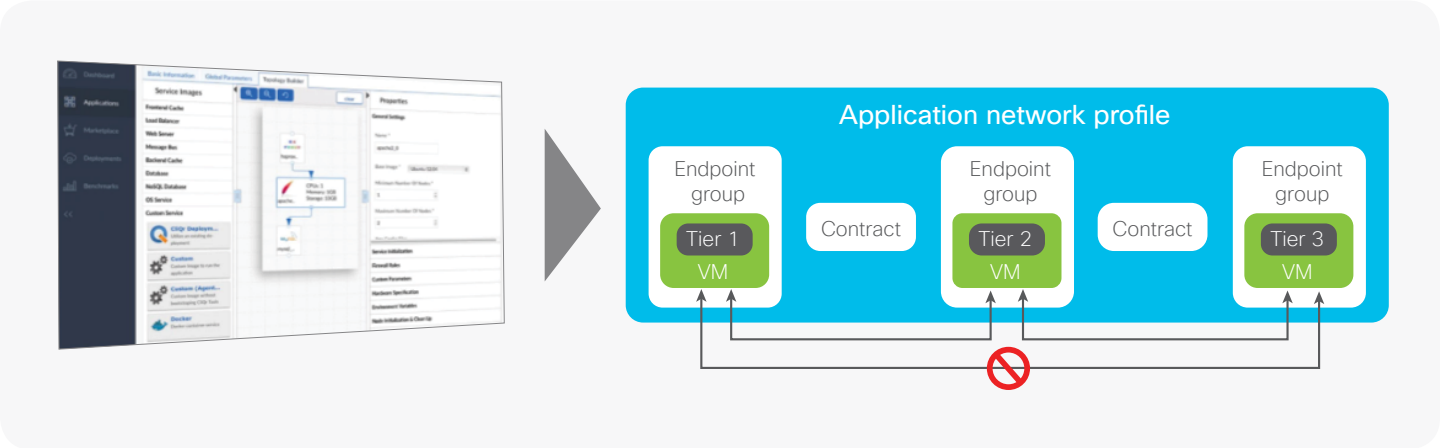
The Cisco CloudCenter and Cisco ACI platforms work together transparently. When a user initiates deployment of the Cisco CloudCenter application profile, as shown in Figure 2, the orchestrator uses topology and network settings in the application profile to automate creation of policy objects for Cisco ACI. The orchestrator calls the local APIC API to instantiate the Cisco ACI ANP, the EPGs, and the consumer and provider contracts based on the topology and security requirements of the application profile. Each application tier is placed in a unique and isolated application tier network. The connectivity between the application tier networks is automatically guided by the application topology.

Users get the flexibility of self-service on-demand deployment. But network administrators can control port settings and other security configuration parameters that are included in each Cisco CloudCenter application profile that is published or shared for the user's on-demand, self-service use. The Cisco CloudCenter and Cisco ACI platforms work together without the need to install plug-ins, create environment-specific scripts, or modify any application code.

Cisco CloudCenter includes the following workflows:

- **Model an application profile:** A service manager can use the Cisco CloudCenter GUI to create a cloud-independent application profile and then share it with specific users or publish it in a marketplace.
- **Perform self-service deployment:** Role- and user-based access controls, paired with tag-based governance, help users choose an appropriate deployment environment that optionally includes Cisco ACI.

Figure 2. Cisco CloudCenter application profile determines Cisco ACI application network profile objects



- **Create and deploy APIC policy objects:** If a user chooses an environment that is part of a Cisco ACI fabric, Cisco CloudCenter automates creation of the appropriate policy objects and calls the APIC northbound Representational State Transfer (REST) API to consume networks services and deploy policy objects created for that specific application deployment.
- **Provision infrastructure:** Cisco CloudCenter calls infrastructure APIs (for example, OpenStack or VMware vCenter) to provision computing, memory, and storage resources in the appropriate network segments.
- **Deploy application tiers:** Cisco CloudCenter deploys and orchestrates all application components based on the topology and dependencies modeled in the application profile.
- **Perform ongoing management:** Both users and administrators can review the deployment progress and settings to help ensure proper configuration.
- **Block east-west traffic**: If a tier is autoscaled, Cisco CloudCenter updates Cisco ACI contract policies to block east-west traffic and confine breaches to a single machine if a system is compromised.
- **Perform end-of-life management:** Infrastructure and network policy objects are automatically deleted, preserving the integrity of the network and conserving infrastructure resources.

Deployment topologies

A dedicated Cisco CloudCenter deployment with Cisco ACI uses four main topologies:

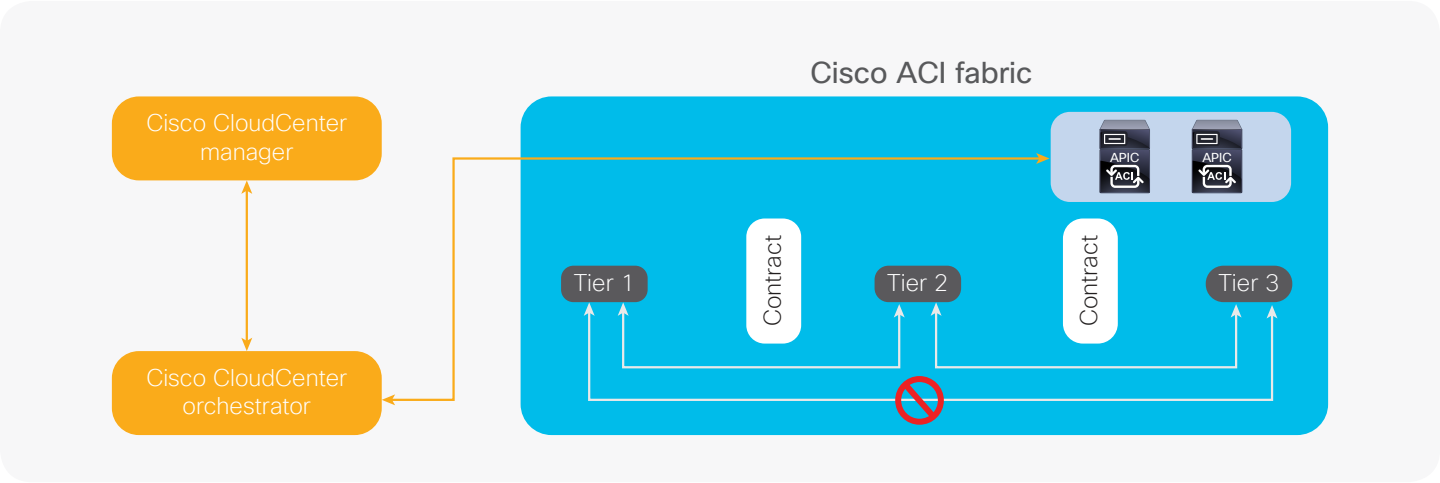
- Single pod
- Multipod
- Stretched fabric
- Multicloud

Single pod

Cisco CloudCenter can deploy and manage an N-tier application in a single Cisco ACI pod (Figure 3). Cisco CloudCenter automates Cisco ACI policy object creation that guides network placement with whitelisted communication between tiers. Users don't need any knowledge about SDN technology or underlying network configuration or policies to implement a highly secure and fully automated deployment.

The unique Cisco ACI label-based dynamic directional routing helps ensure that only the consumer virtual machines can connect to the provider virtual machines with matching labels. This approach provides a truly isolated network for each application deployment. Additional firewall rules are automatically assigned to the application deployment based on tag-based governance rules applied for each application deployment.

Figure 3. Single-pod topology



Users get the flexibility of self-service on-demand deployment. But network administrators can control port settings and other security configuration parameters that are included in each Cisco CloudCenter application profile that is published or shared for the user's on-demand, self-service use. Different tiers of an enterprise web application can be placed in different networks with different VLANs.

Multipod topology

Cisco CloudCenter can deploy N-tiered applications in a data center with multiple Cisco ACI pods. In this scenario, the application can be distributed across different pods in a single data center (Figure 4).

The multi-pod topology provides key benefits, including deploying various application tiers in different availability zones. You may have persistent database tier in product, and want to deploy a dev or test application server in non-production zone. This topology supports needs where various tiers are placed in different ACI fabrics.

Stretched fabric

Cisco CloudCenter can deploy N-tiered applications in a Cisco ACI fabric that is stretched across geographically dispersed sites and over long distances. In this scenario, the application can be distributed to different pods in separate data centers while taking advantage of the network services provided by the single fabric (Figure 5).

The stretched fabric topology provides important benefits, including workload portability and virtual machine mobility, and extends the capabilities of Cisco ACI integration with Layer 4 through Layer 7 (L4-L7) services. Future Cisco CloudCenter releases will enable automated disaster-recovery and high-availability workflows, in which an application can be deployed in a cross-site, cross-pod manner with the database tier being automatically placed in a master-slave or master-master replication scheme.

Figure 4. Multipod topology with one Cisco CloudCenter orchestrator

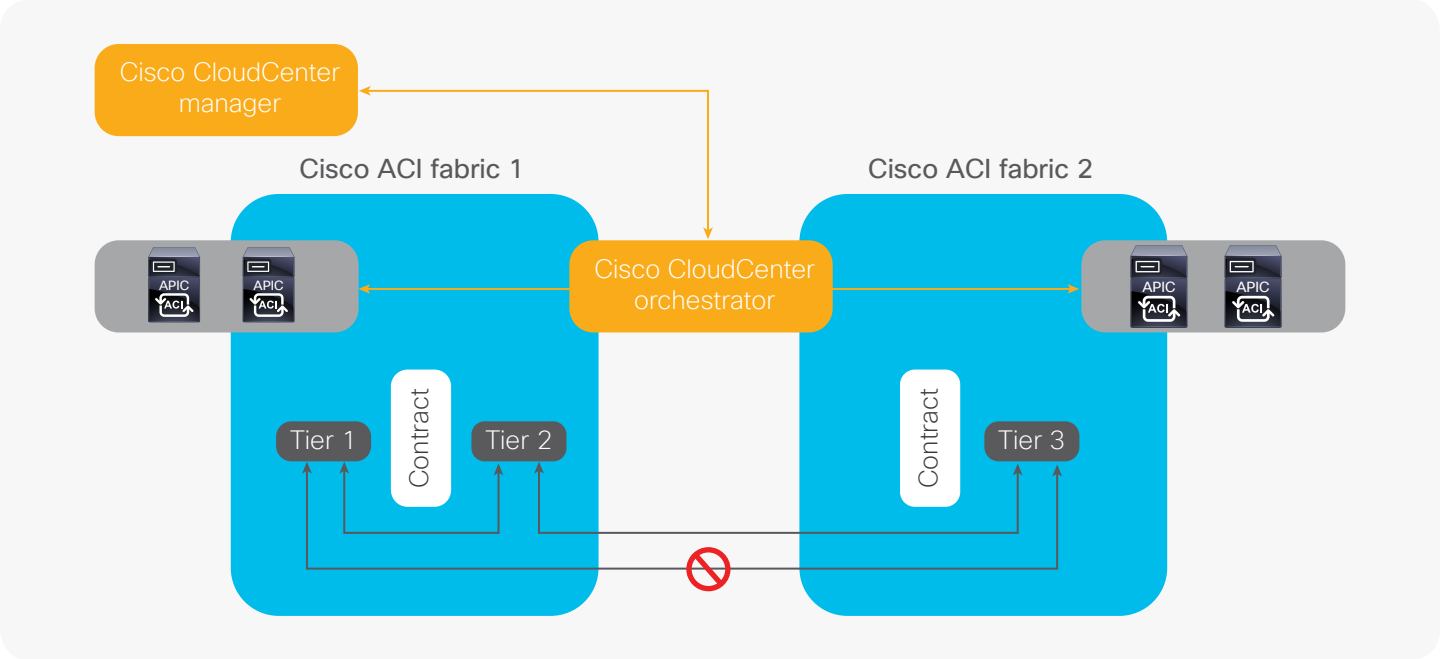


Figure 5. Stretched fabric topology with two Cisco CloudCenter orchestrators

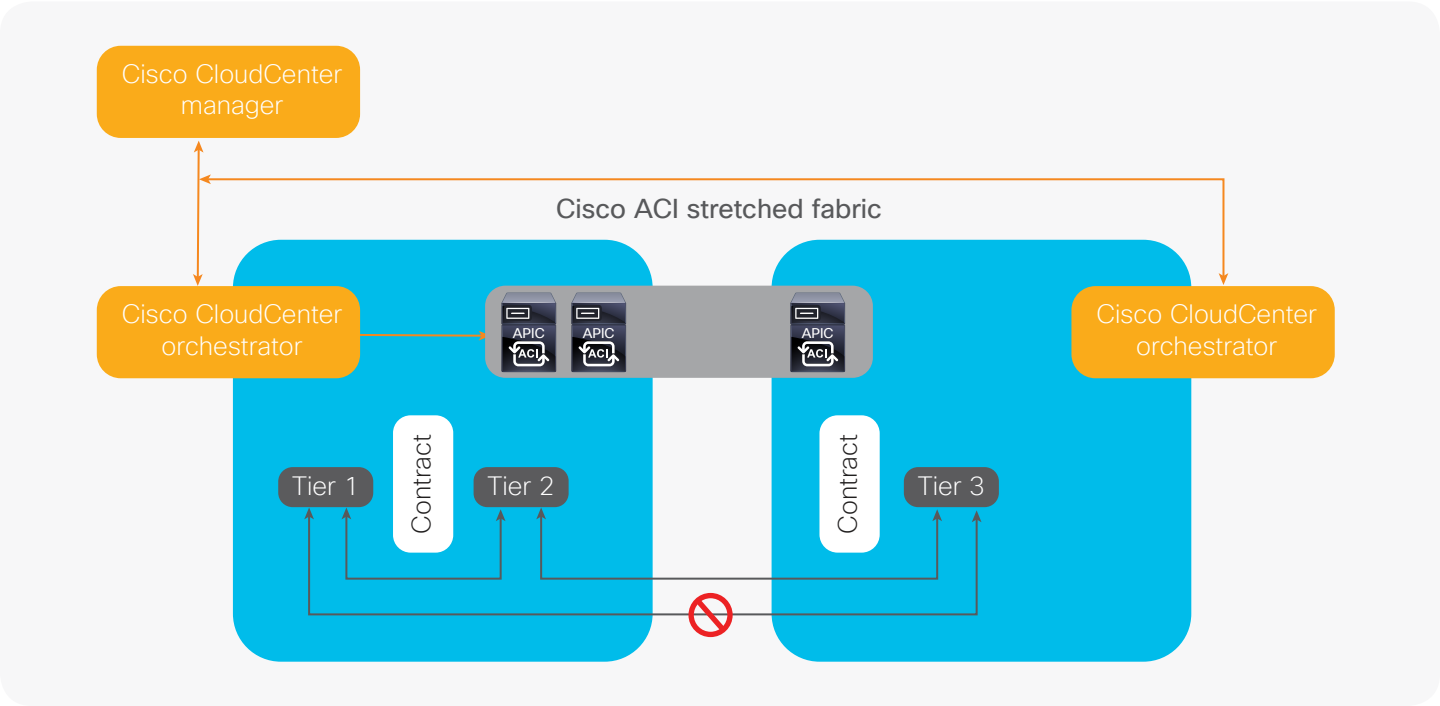
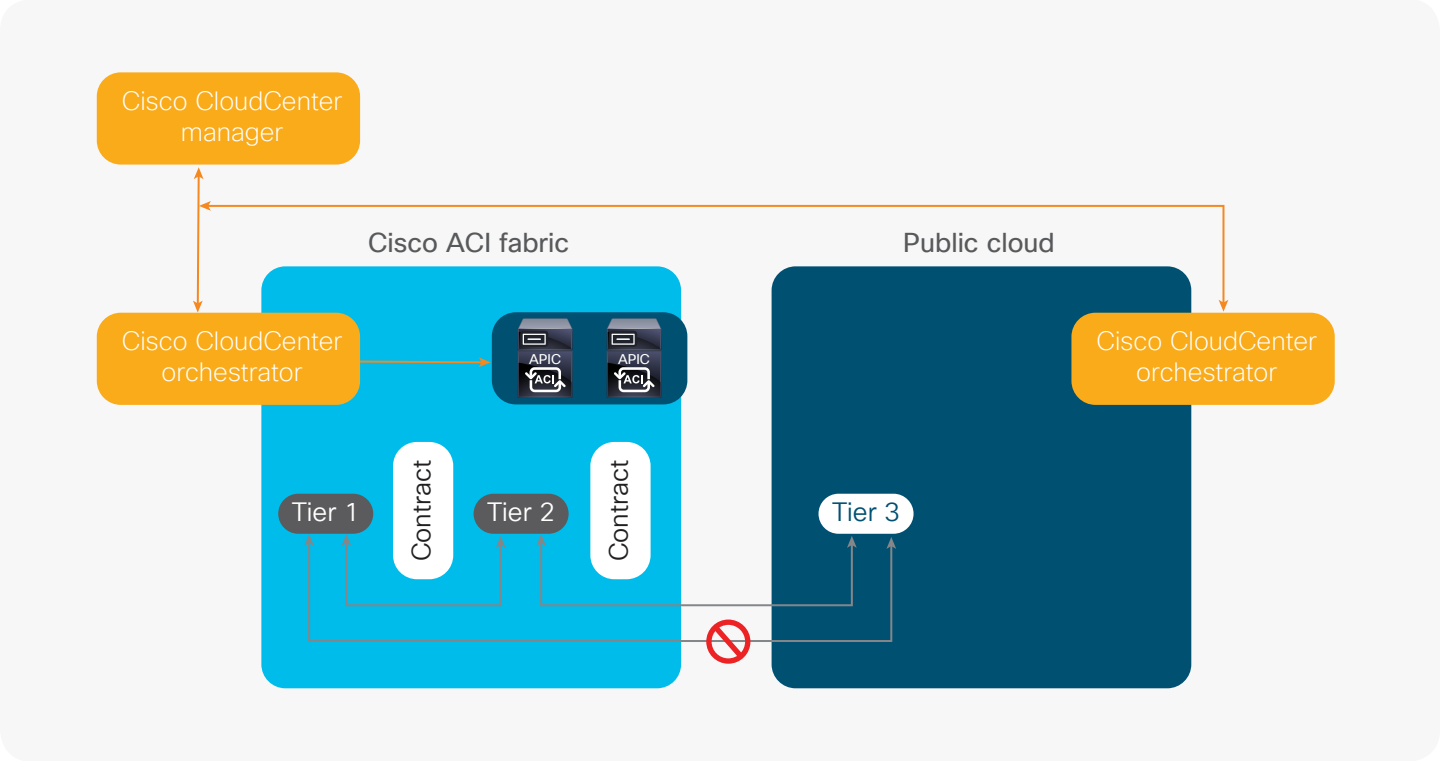


Figure 6. Multicloud topology with two Cisco CloudCenter orchestrators



Multicloud

Cisco CloudCenter can deploy N-tiered applications across a Cisco ACI pod and public cloud. In this scenario, the database tier and application server tier can reside in a highly secure and controlled Cisco ACI managed environment, while the web or mobile application tier can take advantage of the pay-per-use and highly scalable public cloud environment (Figure 6).

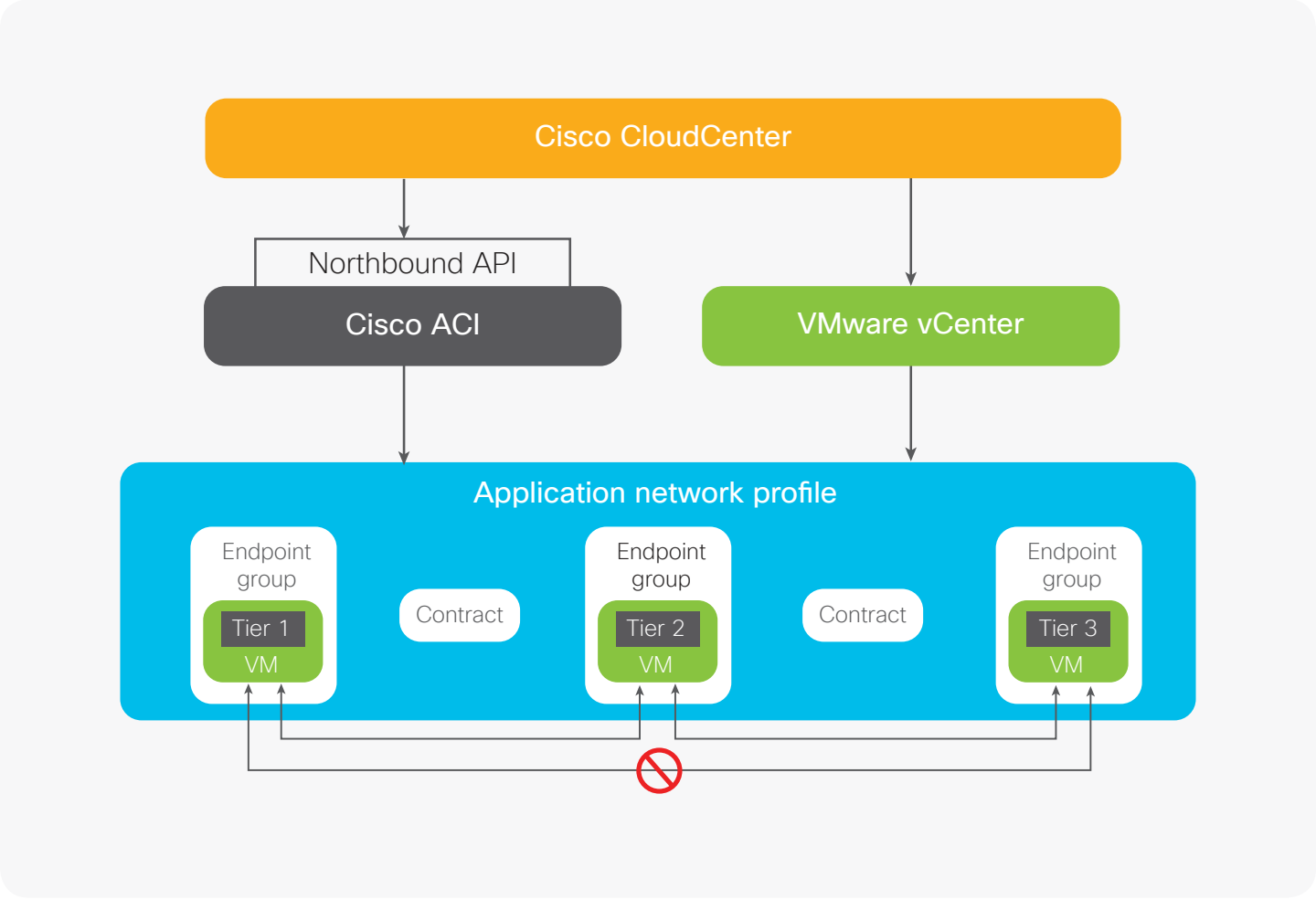
The multicloud topology provides important benefits, including greater security for the database tier, a lower-cost private cloud environment for longer-running workloads, and scalability and pay-per-use for highly variable workloads in the public cloud. The combination of cost efficiency and security for some tiers and scalability and pay-per-use economics for other tiers can provide an optimal mix of deployment options.

Configuration requirements

A common configuration for a Cisco CloudCenter and Cisco ACI solution includes a dedicated Cisco CloudCenter Manager and Orchestrator deployment in a Cisco ACI environment with VMware vCenter to provision infrastructure resources, as shown in Figure 7.

- Cisco CloudCenter provides hybrid orchestration.
- Cisco ACI provides SDN.
- VMware vCenter provides the hypervisor and the VMware vCenter API that is called to provision infrastructure resources.

Figure 7. Cisco CloudCenter with Cisco ACI and VMware vCenter



Cisco ACI requirements

The Cisco ACI fabric consists of three major components:

- The APIC
- Spine switches
- Leaf switches

Cisco CloudCenter interacts directly with the APIC. Table 1 summarizes the high-level Cisco ACI requirements for this joint solution.

Table 1. Cisco ACI requirements for Cisco CloudCenter solution

Requirement	Details
Set up a working Cisco ACI environment.	Verify that the following components have passed all checks to provide end-to-end connectivity: • Leaf switch profiles, switch selectors, interface profile, and policy groups • VLAN pool • VMware Virtual Machine Manager (VMM) domain • Routable IP subnet to a new tenant and bridge domain configured with a Layer 3 Outside (L3Out) interface for external Internet connectivity • Routing protocols • Virtual Routing and Forwarding (VRF)
Accept the API call that directs fulfillment of network policy objects.	Cisco CloudCenter creates an XML file and calls the APIC API that provides details of the following Cisco ACI policy objects: • ANP • EPG • Contracts • Subjects and filters
Either associate a valid APIC SSL certificate with the host name or enable HTTP access.	By default, the APIC listens only to HTTPS for both the GUI and REST APIs. For Cisco ACI integration to work with the APIs, the following criteria must be met: • The APIC SSL certificate is valid for the APIC host name. • No valid certificate exists in the APIC. • The APIC is accessible using an IP address. • HTTP access is enabled for the APIC.
Using the APIC GUI, manually add a new ANP with one EPG. **Verify that the APIC provisions a new vSphere Distributed Switch (vDS) port group for the EPG.** **Using the vCenter user interface, provision or clone a new virtual machine with the network pointing to the created port group.**	Cisco CloudCenter requires access credentials for the APIC, the tenant name, and a VMM domain name.
Use Secure Shell (SSH) at the console for the new virtual machine and verify that outbound Internet access works.	For example, enter curl -L http://google.com (with or without a proxy).

Cisco CloudCenter requirements

Cisco CloudCenter consists of two major installed components:

- Cisco CloudCenter manager
- Cisco CloudCenter orchestrator

The orchestrator is the fabric-resident component that calls infrastructure APIs (vCenter) to provision infrastructure resources, and calls APIC APIs to fulfill network policy objects. The orchestrator includes RabbitMQ and an image repository to enable transparent interaction with Cisco ACI and vSphere.

Table 2 summarizes the requirements and prerequisites for a dedicated Cisco CloudCenter installation that works with Cisco ACI and vCenter.

Table 2. Requirements for a dedicated Cisco CloudCenter installation

VMware Requirements	Details
Dedicated deployment models require four virtual appliances: - **Cisco CloudCenter Manager appliance: Manages clouds, environments, and applications (user interface and REST)** - **Cisco CloudCenter orchestrator appliance: Provisions computing, storage, networking, and security resources for virtual and physical environments** - **Advanced Message Queuing Protocol (AMQP) appliance (RabbitMQ): Brokers communication between the application virtual machines and the orchestrator** - **Application virtual machine Base OS images: Uses CentOS or Ubuntu Linux (or Microsoft Windows)**	Cisco CloudCenter requires: - IP address for the Cisco CloudCenter Managerand Orchestrator and AMQP servers - HTTP/HTTPS proxy address if HTTP proxy isused for external Internet access - OVA files if you are using your own application virtual machine images (Cisco CloudCenterneeds to install the management agent on each virtual machine)
Virtual machines distributed as single Open Virtualization Archive (OVA) files must be imported into the VMware data center.	Cisco CloudCenter requires access credentials to the vCenter setup.
Install Base OS images.	Cisco CloudCenter provides both CentOS 6.5 and Ubuntu 12.04 Base OS images for application virtual machines. However, customers can use their own CentOS, Red Hat Enterprise Linux (RHEL), or Ubuntu image. For Windows workloads, customers can use a Windows 2008 or 2012 image.

VMware Requirements	Details
Cisco CloudCenter also provides IP Address Management (IPAM).	Worker virtual machines can receive IP addresses in three ways: ▪ Infoblox (Cisco CloudCenter requires access credentials to the Infoblox setup) ▪ Dynamic Host Configuration Protocol (DHCP) server ▪ Customizable script-based IP assignment (need IP address, subnet, and ranges)
The application virtual machines require external internet access to download middleware services.	For example, enter **apt-get install mysql/yum install mysql**.

VMware vCenter requirements

Cisco CloudCenter provisions infrastructure through an infrastructure-as-a-service (IaaS) layer API in a data center such as OpenStack or Cisco UCS Director, or often through a vSphere or vCenter API (Table 3).

Table 3. VMware vSphere Requirements Cisco CloudCenter Solution

VMware Requirements	Details
A working vCenter 5.0 or 5.5 environment is required.	The minimum version is vCenter 5.0, but Cisco recommends vSphere 5.5 U2.
Cisco CloudCenter automates the provisioning of virtual machines through the vCenter API.	Access credentials to the vCenter setup are required.
All VMware ESX hosts must be physically connected to the Cisco ACI leaf switches.	The minimum requirements are: ▪ Physical ESX host capable of running at least 10 medium-sized instances ▪ ESX cluster (cluster can consist of just one host) ▪ Data store (or data-store cluster for vSphere Distributed Resource Scheduler (DRS) support) with at least 100 GB of free space
If the VMware ESXi hosts are based on Cisco Unified Computing System™ (Cisco UCS®), certain configurations are required.	The VLANs for the Cisco CloudCenter Manager must be mapped to the virtual network interface card (vNIC) template. Uplinks from the fabric must connect trunking VLANs to the leaf switches.

Networking requirements

Be sure to address all network considerations for each main component. Although this section lists all the ports for each component, several ports are optional and their use depends on your deployment requirements. Tables 4, 5, and 6 list the ingress and egress ports for Cisco CloudCenter components.

Table 4. Cisco CloudCenter manager network requirements

Port	Direction	Remote source	Notes
80	Ingress (optional)	Browser IP address	From the client browser to HTTP/HTTPS if autoredirection is required
443	Ingress	0.0.0.0/0	From the client browser to access the Cisco CloudCenter manager user interface or REST API
22	Egress or ingress (optional)	Allowed SSH source IP address	Remote troubleshooting (optional)
8443	Egress or ingress	Cisco CloudCenter Orchestrator IP addresses	Two-way communication with the orchestrator virtual machine
	Egress or ingress (optional)	Health monitor IP address	From Cisco CloudCenter manager to communicate with the health monitor

Table 5. Cisco CloudCenter orchestrator network requirements

Port	Direction	Remote source	Notes
8443	Egress or ingress	Cisco CloudCenter Manager IP address	Two-way communication with the Cisco CloudCenter Manager virtual machine
22	Ingress (optional)	Allowed SSH source IP addresses	To the orchestrator for remote troubleshooting (optional)
7789	Ingress	Application virtual machine IP addresses	Required for remote access reverse connection ▪ If port 7789 is not open, all reverse connections from the application virtual machines (SSH and VNC communication) will fail.

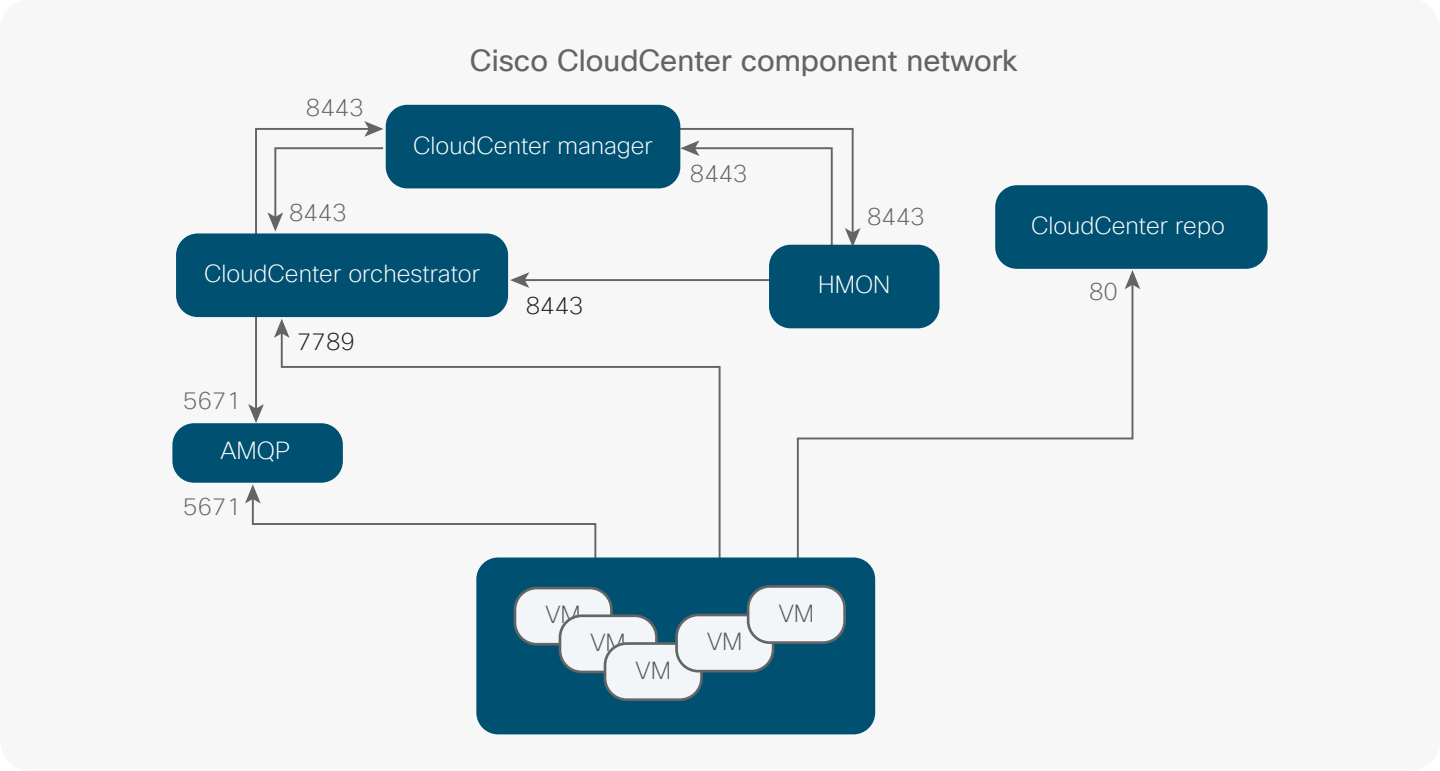
Port	Direction	Remote source	Notes
7788	Egress or ingress Guacamole is a clientless remote desktop gateway that supports protocols such as Virtual Network Computing (VNC) and Remote Discovery Protocol (RDP) and is used to allow users to access their cloud resources without requiring VPN and site-to-site connections.	Cisco CloudCenter Orchestrator (Guacamole)	Required for remote access reverse connection between the Guacamole gateway and the connection broker (both these services exist in the orchestrator instance) ▪ Effective starting with Cisco CloudCenter 4.1.0, ports 7788 and 7789 both must be open if you need to use the Cisco CloudCenter web-based remote-access gateway (Guacamole server). ▪ If ports 7789 and 7789 are not open, all reverse connections from the application virtual machines (SSH and VNC communication) will fail. ▪ You can restrict the source for port 7788 to just the orchestrator's IP address.
443	Ingress	0.0.0.0/0	Browser-level SSH, VNC, and RDP access to application virtual machines

Table 6. Cisco CloudCenter AMQP Network Requirements

Port	Direction	Remote source	Notes
5671	Ingress	Cisco CloudCenter orchestrator IP address Virtual machine application IP address	AMQP over Transport Layer Security (TLS) is used for the orchestrator and the application virtual machines to communicate with the AMQP server.

Figure 8 provides a graphical view of the ports and the main components of the Cisco CloudCenter solution.

Figure 8. Ports and Main components of Cisco CloudCenter solution



Conclusion

Cisco CloudCenter architectural flexibility in combination with the comprehensive SDN framework of Cisco ACI greatly increases business agility and security while accelerating application delivery. With Cisco CloudCenter application-centric hybrid cloud management and Cisco ACI as the policy enforcement engine, both simple and complex applications can be deployed in their entirety in minutes.

For more information

www.cisco.com/go/cloudcenter

C11-737225-01 07/17