Cisco CloudCenter Solution: Architecture Overview

Contents

Executive Summary

The Cisco CloudCenter™ hybrid cloud management platform has a simple architecture, with two primary software components that support a wide range of use cases:

- **Cisco CloudCenter Manager:** The interface in which users model, deploy, and manage applications on and between a data center and a cloud infrastructure, and in which administrators control clouds, users, and governance rules.
- **Cisco CloudCenter Orchestrator:** Resident in every data center or cloud region; automates application deployment along with infrastructure (computing, storage, and networking) provisioning and configuration based on the application's requirements.

The Cisco CloudCenter solution includes a number of additional architectural features, such as cloud-independent application profiles, that improve speed and flexibility while offering comprehensive administrator visibility and control that spans the boundaries of applications, clouds, and users.

This document summarizes the main architectural features that make the Cisco CloudCenter solution a unique and powerful choice for any IT organization or service provider seeking to deploy and manage applications in a mix of data center and cloud environments.

Introduction

The Cisco CloudCenter solution is a hybrid cloud management platform that securely provisions infrastructure resources and deploys application components and data in more than 19 data center and private and public cloud environments.

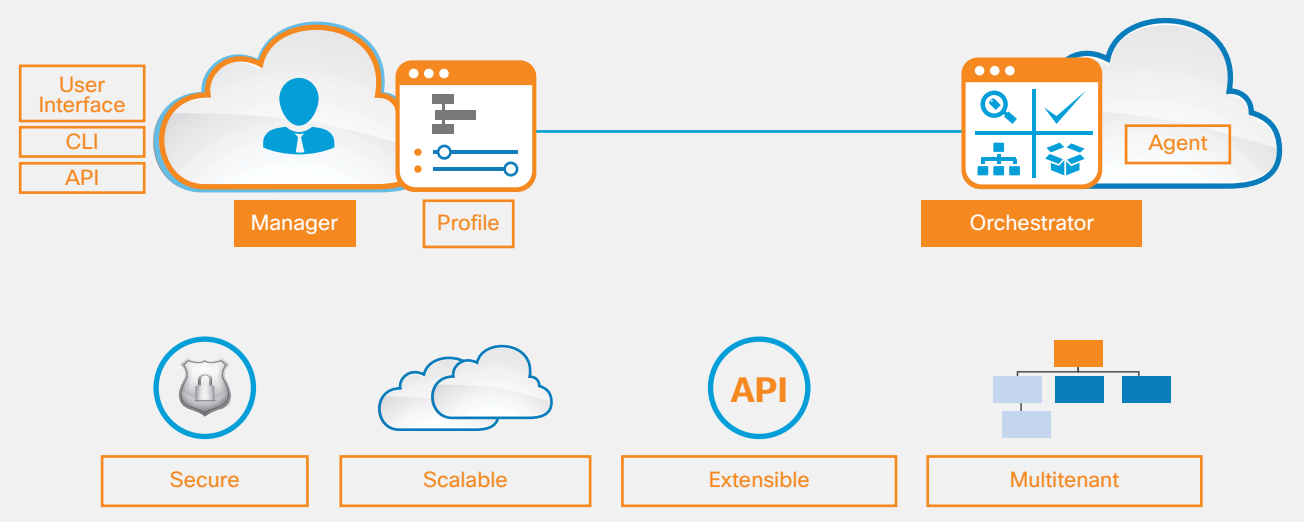
The solution supports a wide range of uses in enterprise IT organizations, including application migration, DevOps automation across various cloud environments, and dynamic capacity augmentation within or between clouds. It also can serve as the foundation for a comprehensive hybrid IT-as-a-service (ITaaS) delivery strategy.

With its simple two-part architecture, the Cisco CloudCenter solution delivers fast time-to-value, and deployment does not require a major professional services project.

This enterprise-class solution offers a secure, scalable, extensible, and multitenant solution that meets the needs of the most demanding IT organizations and cloud service providers. Or department level deployments make it easy for IT and users to deploy and manage applications in any data center or cloud environment.

Figure 1 shows the primary software components of the solution: Cisco CloudCenter Manager and Cisco CloudCenter Orchestrator. The solution also offers various other architectural features such as application profile that give Cisco CloudCenter customers a significant advantage when implementing their cloud strategies.

Figure 1. Cisco CloudCenter Software Components and Main Architectural Features



This document provides an introduction to the Cisco CloudCenter software components and main architectural features.

Cisco CloudCenter Manager

Cisco CloudCenter Manager serves as the primary interface for users and administrators. Only one manager is required for each Cisco CloudCenter installation, and the manager can be used with multiple fully or partially isolated tenants as needed. A manager is linked to one or many orchestrators and can simultaneously support thousands of applications. Additional managers can be added to meet disaster-recovery or high-availability requirements.

For a traditional on-premises configuration, the manager is delivered as a preinstalled virtual appliance. The multitenant SaaS version of the manager can be linked to customer-installed orchestrators.

The manager includes user functions for modeling, deploying, and managing applications, and administrator functions that deliver visibility and control that spans the boundaries of applications, users, and clouds.

Cisco CloudCenter users and administrators access the manager through a web browser user interface, command-line interface (CLI), or representational state transfer (REST) API.

- **Browser-based user interface:** The manager coordinates application deployment, lifecycle management, administration, and governance activities for each data center or cloud environment. Cisco CloudCenter supports Security Assertion Markup Language 2.0 (SAML 2.0)–based integration with an existing user directory (such as Lightweight Directory Access Protocol [LDAP] or Microsoft Active Directory). The solution supports indirect Active Directory authentication using single sign-on (SSO) access between Cisco CloudCenter as a service provider and the customer's identity provider (IDP), such as Active Directory Federation Services (ADFS). See the product documentation for a quick user interface tour.
- **Command-line interface:** Experienced administrators can perform a wide range of common functions from the Cisco CloudCenter CLI. This interface is based on the rerun Bash framework, a modular shell automation framework for Cisco CloudCenter scripts that call APIs. See the product documentation for common CLI use cases.
- **REST API:** Cisco CloudCenter has a mature and well-documented API. Solution users and administrators can use the solution's REST API to run most Cisco CloudCenter functions. Login credentials determine which APIs can be run. See the product documentation for more information about the Cisco CloudCenter REST API.

Application Profile

The application profile, a critical feature of the unique Cisco CloudCenter hybrid cloud management solution, is a cloud-independent and portable model that defines each application's deployment and management requirements.

Each application profile combines infrastructure automation and application automation layers in a single deployable blueprint. With an application profile, one Cisco CloudCenter platform can be used to deploy and manage any modeled application in any data center or cloud environment.

The solution's cloud-independent application profile coupled with its cloud-specific orchestrator abstracts the application from the cloud, interprets the needs of the application, and translates these needs to cloud-specific services and APIs. It thus eliminates the need for cloud-specific scripting and cloud lock-in.

Each application profile is an XML and JavaScript Object Notation (JSON) metadata description that includes:

- Descriptions of application topology and dependencies
- Infrastructure resource and cloud service requirements
- Descriptions of deployment artifacts, including packages, binaries, scripts, and, optionally, data
- Orchestration procedures needed to deploy, configure, and secure all application components
- Run-time policies that guide ongoing lifecycle management

Each application profile can also provide details such as upgrade information and backup and restore information that is needed when migrating an application from cloud to cloud.

Most important, an application profile does not require a user to provide any environment-specific scripts that would otherwise hard-wire the profile to a single cloud infrastructure.

Behind the scenes, each application profile is created, stored, shared, or accessed through the Cisco CloudCenter Manager. It is then interpreted by the orchestrator to provision infrastructure resources and deploy application components according to the unique API and best practices of each runtime environment.

An end user sees the application profile as a button or catalog item that, with one click, can be deployed to any supported environment. A developer or application owner sees it as a simple topology, modeled with visual drag-and-drop components, that incorporates security, compliance, and other configuration settings approved by various teams as part of the service lifecycle before the application is released for use. To the orchestrator, the application profile is a JSON file that includes information that is interpreted by the orchestrator when the application is deployed.

Application Profile Creation and Sharing

Several main architectural features help simplify the modeling of each application profile:

- **Templates:** Cisco CloudCenter provides more than 12 of ready-to-use, reusable templates to that are starting points for modeling each application profile. The topology modeled in the profile directs deployment-time orchestration and eliminates the need to write workflows. Templates are available for common application types, including batch and parallel processing, endpoint services, and clusters, as well as for single virtual machine virtual machine, multitier, and loosely coupled containerized topologies. Templates are also available for many popular application technologies, including Java, .NET, LAMP, Ruby on Rails, and Hadoop. See the product documentation for more information about templates.
- **Topology Modeler:** Users open templates and model each application profile in the Topology Modeler. Figure 2 shows the visual drag-and-drop environment used to model a simple three-tier application.
- **Service library:** Cisco CloudCenter provides common OS images and application services that customers can use to quickly model an application profile. The solution includes more than 30 of the most popular operating systems, databases, middleware, load balancers, message busses, application servers, and front-end caches. Customers can also easily customize and extend the service library by adding other OS images, adding their own services, or importing applications from other widely used formats such as Amazon Web Services (AWS) CloudFormation, OpenStack Heat templates, and OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA).

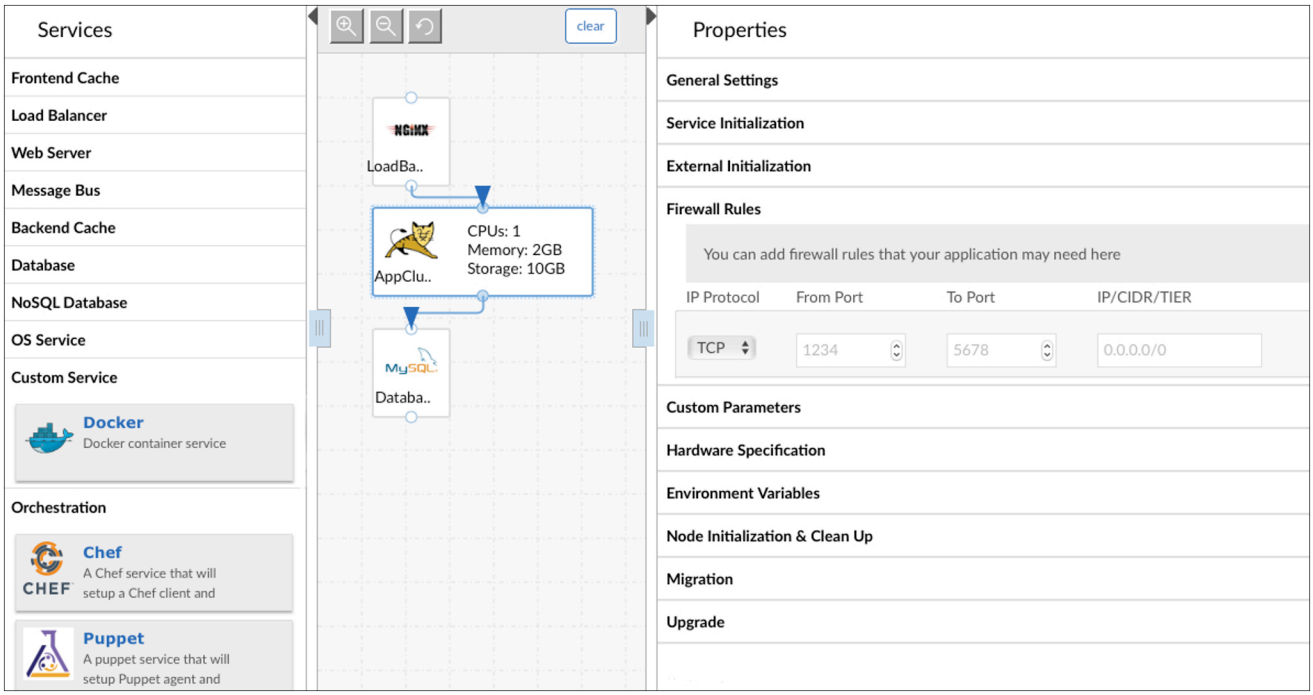
See the product documentation for more information about ready-to-use supported Base OS images and application services, as well as for more information about how to create new services and how to manage services.

- **Containers:** Cisco CloudCenter supports containers, such as Docker, that can be easily modeled as part of any application profile and then deployed and managed in any data center or cloud environment. Users can drag and drop the Docker service into an application profile that contains single or multiple Docker containers. Cisco CloudCenter supports composite application topologies using containers mixed with other application and cloud services. The solution adds management and governance to container deployments.

  See the product documentation for more information about Docker and for a blog about how Cisco CloudCenter uses Weave to manage multiple-host and cross-host topologies.

- **Marketplace:** Users can share application profiles in several ways. Users can share application profiles directly with other users, or they can publish profiles to either public or private Cisco CloudCenter marketplaces. Application profiles also can be added to third-party service catalogs for broad availability. Access to profiles is based on user credentials and on governance rules related to such factors as intended use, geographic location, security levels, and compliance requirements. See the product documentation for more information about marketplaces.

Figure 2. Topology Modeler Showing Service Library, Three-Tier Application, and Properties



Cisco CloudCenter Orchestrator

Cisco CloudCenter Orchestrator is a patented technology that decouples applications from underlying infrastructure and hides the complexity of underlying cloud resources.

One orchestrator is deployed locally in each data center, private cloud, and public cloud region and orchestrates the initial deployment of the application profile and all ongoing management requests that come from Cisco CloudCenter Manager.

The orchestrator receives information and instructions from the manager, including application profiles, runtime policies, and application lifecycle management commands such as deploy, start, stop, and remove. The orchestrator runs those commands and sends a status update back to the manager.

- **Secure connection to the manager:** The orchestrator uses a REST API to connect with Cisco CloudCenter Manager. The manager does not communicate directly with the cloud infrastructure management endpoint. The orchestrator abstracts the unique API and services offered by each cloud, and it uses the same communication mechanism back to the manager regardless of the cloud on which the orchestrator is installed.

  The distributed architecture makes a clear separation between security boundaries. The manager and the orchestrator use only a single port to communicate securely over HTTPS with mutual certificate-based authentication.

- **Functions during deployment:** When deploying an application profile, the orchestrator first rules out clouds that may be inappropriate options based on the needs of the application. The orchestrator then interprets the deployment and management requirements of the application profile and sends cloud-specific API commands to the underlying cloud to install required infrastructure to meet the needs of the application.

  The orchestrator then performs additional actions need to fill in gaps in cases in which functions may not be directly supported by the underlying cloud infrastructure. For example, microsegmentation or elastic load balancing may not be available in the cloud infrastructure directly.

- **Functions during management:** Every cloud behaves in a different way. Cisco CloudCenter helps ensure that a request from the manager is interpreted as that it has the same outcome across all clouds, regardless of the capabilities of the underlying cloud. For example, the **suspend** command in one cloud may be called the **power off** command in another. The orchestrator determines the correct command mapping for each cloud so that users don't need expertise in the underlying cloud environment commands.

  Importantly, the orchestrator does not lie in the application's execution path. Instead, it sits to the side and orchestrates the provisioning and application deployment. The orchestrator does not add any performance overhead and can provide better application performance through optimal placement and instance configuration choices.

Orchestrator Agent

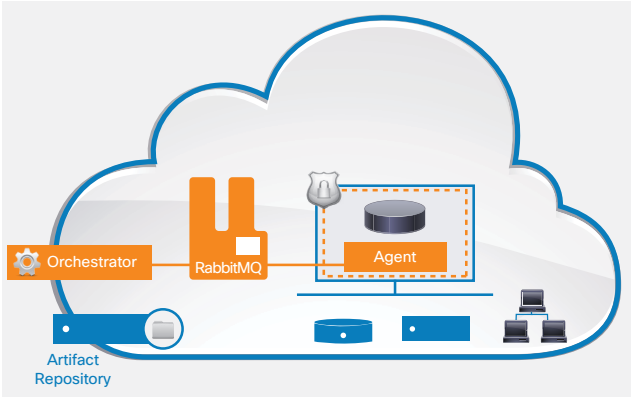
Cisco CloudCenter manages each provisioned application tier with an orchestrator agent that is installed in each virtual machine. The agent receives commands from the orchestrator to complete application deployment or enforce ongoing management actions and automation policies. The agent sends back monitoring information collected from underlying cloud APIs.

The agent is included in Cisco CloudCenter preconfigured shared virtual machine images. For customer-provided custom virtual machine images, Cisco CloudCenter detects whether the agent is present, and if it is missing, the solution automatically installs the agent in each virtual machine after it is deployed.

Applications can be run without an agent, and they can have the agent removed at any time, without affecting the running application. However, if you run without an agent, some capabilities, such as autoscaling, are not available for those applications.

The orchestrator communicates with the orchestrator agent through RabbitMQ queueing services that run on provisioned virtual machines, as shown in Figure 3.

Figure 3. Agent in Each Virtual Machine Communicates with Orchestrator



The constant exchange of messages between these two components guides the orchestration and ongoing management of worker virtual machines in a cloud environment. Advanced Message Queuing Protocol (AMQP)-based communication is used between the orchestrator and the agent. The Cisco CloudCenter solution uses RabbitMQ as the open-source message broker to implement AMQP.

The orchestrator sends requests to the agent, including requests to:

- Perform certain tasks such as running configuration scripts during deployment
- Run custom cleanup scripts during deprovisioning or shutdown
- Collect system metrics based on policy enforcement requirements
- Perform actions that may be required to enforce policies, such as reconfiguring middleware service during autoscaling

The agent sends the following information to the orchestrator:

- Monitoring data, such as system metrics
- Status information
- Heartbeat information to indicate that the system is alive

Artifact Repositories

Typically, enterprises maintain application packages, data, and scripts in multiple repositories of their choice. Use the artifact repository to link to an existing repository to store and access files and to point to application binaries, scripts, and shared files. Use the preconfigured Cisco CloudCenter Network File System (NFS) options to mount storage with multiple disks and encryption.

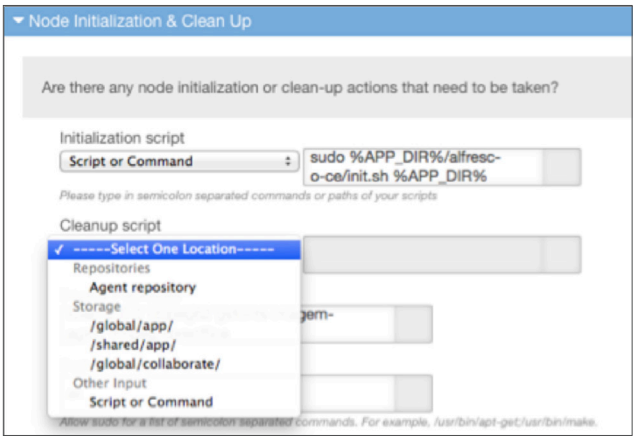
Administrators can make the artifact repository (or multiple artifact repositories) specific to a user, a tenant, or a cloud, or any combination of these resources, based on deployment requirements. Cisco CloudCenter provides a Repositories tab in the manager user interface for this purpose. Administrators can enforce access permissions for each repository. Tenant users can view repositories that are specific to their tenant.

When modeling an application or application profiles, users can select the relevant repository to provide the relative path to the application packages, scripts, or files. The list of available repositories is displayed for user selection. Figure 4 shows an example.

When users select a repository, the endpoint URL is appended automatically to the user-provided name of the folder in which the packages, scripts, or files are located.

Cisco CloudCenter supports HTTP, HTTPS, and FTP including Amazon Simple Storage Service (S3), Chef, Puppet, and Artifactory. For an external repository, such as S3 for Amazon storage, enter the host name with the endpoint URL of the repository. See the product documentation for more information about supported artifact repositories.

Figure 4. Selecting the Artifact Repository for a Cleanup Script



Enterprise-Class Solution

The Cisco CloudCenter enterprise-class solution offers a secure, scalable, and extensible multitenant solution. It can start simple and scale to meet the needs of the most demanding IT organizations and cloud service providers.

Secure

The Cisco CloudCenter solution is uniquely designed with security at its core to span the boundaries of applications, clouds, and users. It encrypts data at rest and in motion and offers a range of critical management, authentication, and authorization features that don't just secure the Cisco CloudCenter solution, but also the clouds to which it connects.

- Identity management and authentication
  - Support for SAML 2.0 based SSO with optional multifactor authentication
  - LDAP and Active Directory support through a SAML 2.0 SSO IDP such as Ping Identity, ADFS, or Shibboleth
  - SHA-256-based password hash with random salt to protect against reverse engineering
  - Randomly generated REST API keys

  - Virtual machine and cloud storage access through a user-specific, unique RSA-2048 public key infrastructure (PKI)–based Secure Shell (SSH) key pair
  - Detailed role-based access control (RBAC) for global permissions at the user and user-group levels
  - Object-level permissions shared within tenants to control access to a wide range of features, such as the application profiles, deployment environment, and service library
- Key management
  - Compliant with FIPS Java Cryptography Architecture (JCA)
  - Encrypts key pairs using AES-256
  - Allows users to specify public or private key at deployment time, which helps ensure that Cisco has no possession of user keys
  - Use of transparent browser-based SSH and secure VNC with key management, so if a key pair is managed by Cisco CloudCenter, you don't need to specify keys for an authorized user
  - Secure database vault fully encrypted using a key stored in a different security domain, such as a hardware security module (HSM)
  - Support for AWS CloudHSM
- Network security
  - Communication over a two-way trusted HTTPS connection by all Cisco CloudCenter components
  - Microsegmented application communication through Cisco® Application Centric Infrastructure (Cisco ACI™) or VMware NSX
- Data security and protection
  - Block-level AES-256 encryption of Cisco CloudCenter deployed storage
  - Consolidated audit logs for all user activity

Scalable

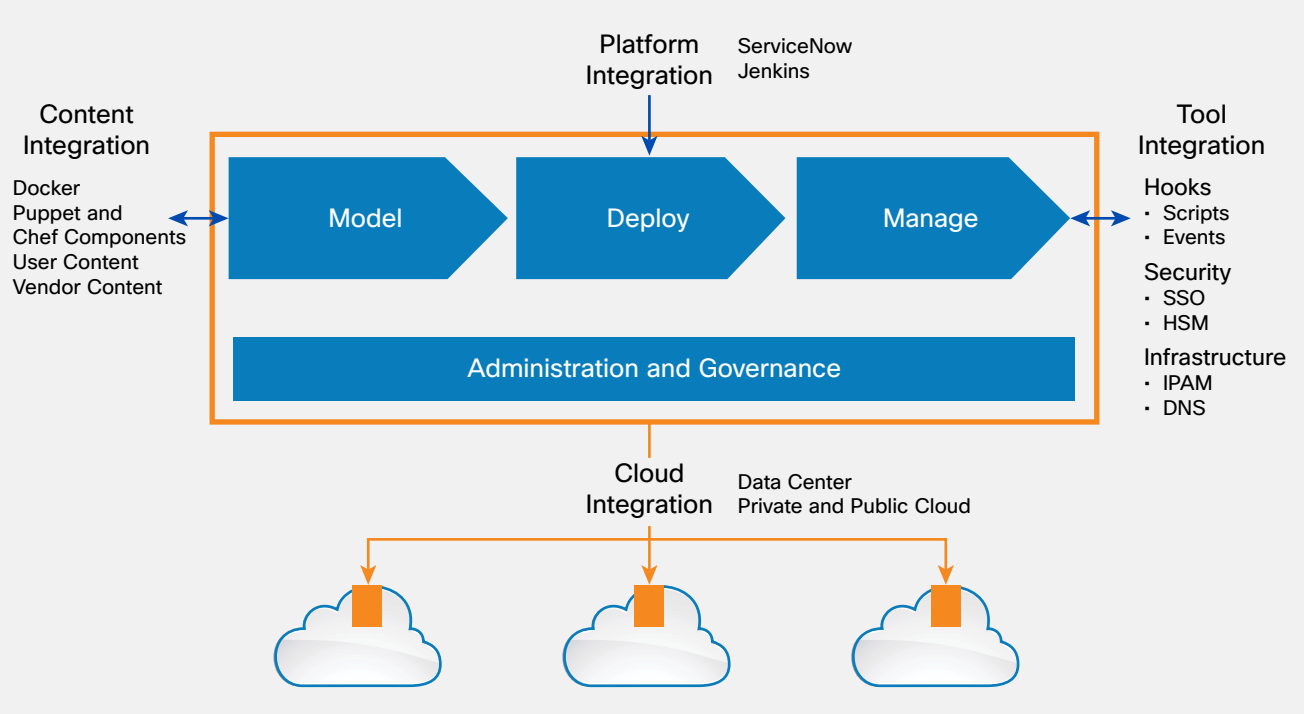
Cisco CloudCenter uses an architecture that is simple enough for a single application in a single cloud, but that can scale to meet the needs of the world's largest cloud service providers, which have many isolated tenants, each with multiple applications deployed.

- **One manager:** Only one manager is required for each Cisco CloudCenter installation. The manager can be used with multiple fully or partially isolated tenants and can support thousands of applications. The manager is linked to one or many orchestrators. Additional managers can be added to meet disaster-recovery or high-availability requirements. Most virtual machine status information, messages, and policies are managed at the orchestrator and do not require communication with the manager. With this architecture, the manager is not a bottleneck, and the manager and the orchestrator can scale independently.
- **Multiple orchestrators:** A single multitenant orchestrator is deployed in each public cloud region, data center, or private cloud. Each orchestrator can support a single tenant or multiple tenants. In either scenario, one orchestrator can manage up to 10,000 virtual machines. The orchestrator also can be deployed as a cluster to provide additional scalability and avoid creation of a single point of failure.
- **Orchestrator agent communication:** Orchestrator scalability is enhanced by AMQP-based communication between the agent and orchestrator. Cisco CloudCenter uses RabbitMQ as the open-source message broker to implement AMQP, and it requires the RabbitMQ AMQP server to be co-located with each orchestrator server. Message exchange is performed by one network port on RabbitMQ. Both the orchestrator and the agent must be able to connect to RabbitMQ's port 5671.

Extensible

As an enterprise-class hybrid cloud management platform, Cisco CloudCenter is built to integrate with and extend a wide range of other data center and cloud management platforms and tools that are found in the typical IT enterprise (Figure 5). See the product documentation and search for "integrations."

Figure 5. North, South, East, and West Extensibility Model

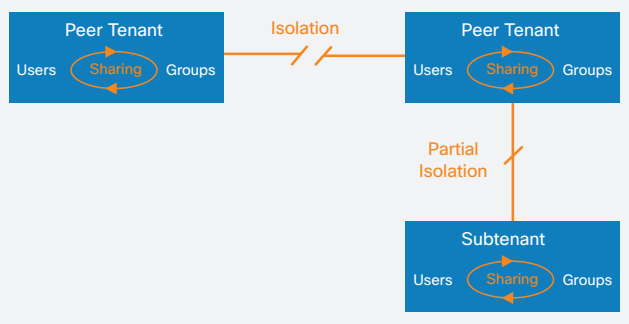


- **Content integration:** A wide range of content sources can be tapped when modeling application profiles. Application profiles contain images, application and cloud services, and containers. Users can import images, share completed application profiles directly with other users, and import or export application profiles to the Cisco CloudCenter private or public application marketplace. Application profiles can be modeled tapping configuration management tools like Chef, Puppet, and SaltStack to deploy individual tiers. Users can modify preconfigured services or add their own custom services. Vendors can add content to the Cisco CloudCenter service library that customers can use to model application profiles. Unique platform-as-a-service (PaaS) offerings such as AWS Relational Database Service (RDS) are treated as services (content), not integration points.
- **Platform integration:** Northbound REST APIs expose Cisco CloudCenter actions to other platforms. Each application profile has a unique ID and can be deployed through the API. For example, you can integrate Cisco CloudCenter with Jenkins, ServiceNow, your own front end, or other solutions to automate application stack deployment and management. See the product documentation for more information about the API.
- **Tool integration:** See the product documentation for the growing list of preconfigured integration capabilities for Cisco ACI, ServiceNow, Docker, Jenkins, Infoblox, and more. Also see the product documentation for information about callout scripts.
- **Cloud integration:** Cisco CloudCenter offers preconfigured integrations that support more than 19 data center, private, and public cloud environments. Southbound integration includes orchestrators that work in all supported environments. There is no further integration beyond setup and configuration. Cisco CloudCenter does not expose the southbound integration interface. If needed, customers and partners can request support for additional clouds. See the product documentation for information about supported data center and private clouds and public clouds.

Multitenant

Cisco CloudCenter offers various multitenant models to support typical enterprise IT hybrid-cloud use cases, as shown in Figure 6. These models give IT architects and administrators a range of options, from simple to complex, for configuring and controlling isolation and sharing within or between groups of users.

Figure6. Multitenant Isolation, Partial Isolation, and Sharing



- **Full isolation:** With Cisco CloudCenter, each tenant can be fully isolated from other peer tenants. In this way, two completely independent business units can use a single Cisco CloudCenter instance while strictly separating tenants.
- **Flexible sharing:** Cisco CloudCenter facilitates sharing within each tenant. Powerful features for sharing application profiles, application services, deployment environments, and more multiply the speed and agility benefits of an application-defined management solution.
- **Partial isolation:** Cisco CloudCenter offers an option for partial isolation between parent and child tenants. In some cases, a central IT organization may offer shared services, delivered either on the premises or through cloud service provider, that are consumed by various business units that are otherwise independent. For otherwise independent IT departments, the central IT organization may want to enforce OS image standards, require use of specific artifact repositories, or require a common rules-based governance framework.

Conclusion

The Cisco CloudCenter solution employs a two-part architecture that simplifies deployment, enables fast time-to-value, and allows users to start small and scale as needed. The solution works for one application in one cloud, as well as for a full multitenant cloud service provider at scale and everything in between.

The unique Cisco CloudCenter architecture delivers management capabilities that span the boundaries of applications, clouds, and users. It is designed to abstract applications from the cloud, and it reduces the need for users to understand the details underlying cloud-specific APIs and services. It also includes a wide range of architectural features that enable comprehensive application and cloud management within enterprise IT ecosystems.

The Cisco CloudCenter solution offers compelling benefits for modern IT organizations whether they are just starting with user self-service in a data center, migrating their first application to the cloud, or running the second or third iteration of a hybrid IT strategy that includes a portfolio of data center and private and public cloud processing services.

For More Information

www.cisco.com/go/cloudcenter

C11-737224-00 05/16