Cisco CloudCenter Solution: Multitenancy

Contents

Executive Summary

The Cisco CloudCenter™ hybrid cloud management platform securely provisions infrastructure resources and deploys application components and data across more than 19 data center, private cloud, and public cloud environments.

It offers exceptional multitenant management capabilities that deliver complete isolation for peer tenants, partial isolation for parent-child tenants, and flexible sharing options for users within a tenant.

With an enterprise-class multitenant solution, IT can avoid the need to deploy multiple management tools for multiple tenants. At the same time, IT can simplify and reduce its service delivery footprint and can gain central governance capabilities that cross the boundaries of applications, clouds, and users.

The Cisco CloudCenter solution delivers multitenant capabilities that are powerful enough for many cloud service providers that deliver hybrid cloud services to fully isolated customers. Yet the solution is also simple enough for enterprise IT to configure a variety of deployment models to meet the isolation and sharing needs of any organization, simple or complex.

This document presents three basic multitenant models and describes tenant administrator functions. It also provides some basic deployment considerations.

Multitenancy Overview

The Cisco CloudCenter solution is a hybrid cloud management platform purposely built to manage multiple applications deployed in multiple clouds for multiple groups of users.

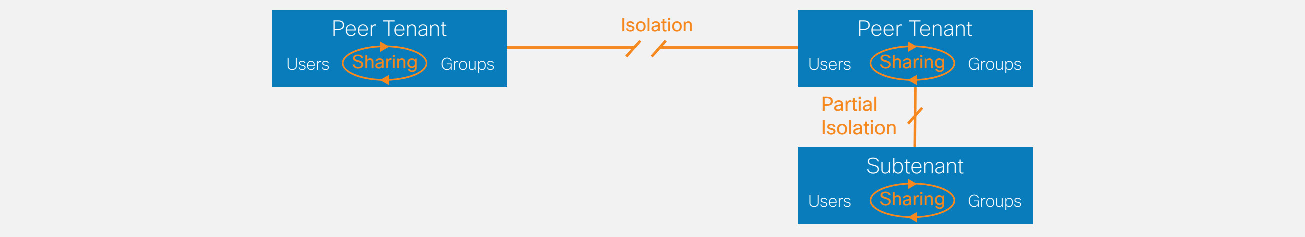
It supports a wide range uses for enterprise IT organizations, including simple application migration, DevOps and continuous-delivery automation across various cloud environments, and dynamic capacity augmentation within or between clouds. It is the foundation for a comprehensive hybrid IT-as-a-service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

To support the complexity and broad range of hybrid-cloud use cases, the Cisco CloudCenter solution offers several multitenant deployment models that give IT architects and administrators a range of options, from simple to complex, for configuring and controlling both isolation and sharing within or between groups of users (Figure 1).

Enterprise IT customers can easily use multitenant capabilities to implement powerful isolation when needed. But the Cisco CloudCenter solution also provides easy-to-configure detailed control over the sharing that occurs among users and groups within a tenant and between tenants and subtenants.

A flexible mix of isolation and sharing allows IT to balance user agility with administrative visibility and control.

Figure 1. Cisco CloudCenter Tenant Isolation, Partial Isolation, and Sharing



Powerful Isolation

With the Cisco CloudCenter solution, 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 being completely isolated from each other.

Many cloud service providers already rely on Cisco CloudCenter as the backbone of their multicloud service delivery systems, offering shared services to multiple completely isolated customers who are tenants in a single Cisco CloudCenter deployment.

From a technical perspective, an enterprise IT organization needs to enable tenancy only if the organization has more than one authentication source. But from a business perspective, a company may want to enable tenancy for many reasons:

- Multiple independent business units have independent IT departments.
- A common central IT organization delivers some common services to multiple IT subdepartments that also have autonomous service delivery portfolios.
- Some groups require a custom user interface with a unique brand or logo.
- Responsibilities need to be segregated to meet regulatory requirements.
- Strictly isolated tenancy is needed to help ensure the highest level of information security.

This powerful multitenancy capability allows multiple business groups to securely use one installation of Cisco CloudCenter to reduce costs and increase operational efficiency, while implementing various degrees of isolation or sharing.

Other cloud management solutions require a separate installation for each tenant. Separate installations increase rollout and maintenance costs, reduce IT's ability to centrally deliver services, and restrict central governance and control capabilities.

Flexible Sharing

The Cisco CloudCenter solution facilitates sharing within each tenant. Powerful features for sharing application profiles, application services, deployment environments multiply the speed and agility benefits of an application-defined management solution.

Examples of information that can be shared within a tenant include:

- Cloud accounts
- Deployment environments
- Application profiles
- Application services
- Application marketplace
- Artifact repositories
- Tags and rules
- Policies

User groups provide a powerful sharing feature. Each user can belong to one or more groups, and different user groups, such development, testing, and production, can be supported by a single tenant. Users within a tenant can share application profiles, images, and services to provide a transparent and automated systems development lifecycle (SDLC). However, as part of specific groups, users can access only specific cloud accounts, controlled by use plans or bundles and different chargeback or showback mechanisms. They also may be limited in their capability to promote a deployment from the test environment to the staging and production environments.

In addition, roles can be assigned to both users and user groups. A role is a named collection of global privileges or permissions related to Cisco CloudCenter functions. Roles can be used to govern the functions that a user can perform (for example, the capability to create application profiles or add a cloud account) and support an effective scheme for the segregation of duties.

In addition to user roles, the Cisco CloudCenter solution provides detailed access control lists (ACLs) and sharing permissions to objects within Cisco CloudCenter. Sharing permissions include the capability to view a specific deployment environment, share a specific application profile with other users or user groups, and so on.

Parent-Child Partial Isolation

In addition to strict isolation between peer tenants and flexible sharing within each tenant, Cisco CloudCenter offers an option for partial isolation between parent and child tenants.

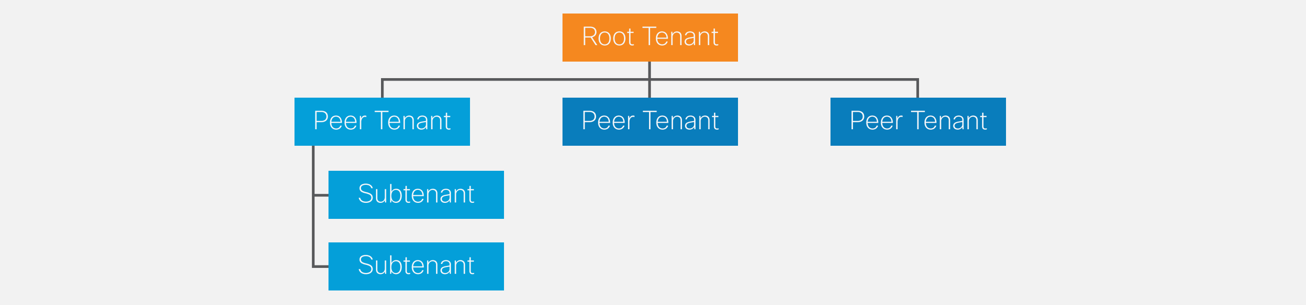
In some cases, a central IT organization offers shared services, delivered either on the premises or through cloud service provider, that are consumed by various business units that are otherwise independent. For otherwise-independent IT departments, the central IT organization may want to enforce OS image standards, require the use of specific artifact repositories, or have a common rules-based governance framework. In addition, IT may offer shared services that are funded by a collection of business units. Those business units many also have IT organizations that deliver other IT or cloud services that are separately funded. Partial isolation that is controlled through the tenant parent-child relationship enables these scenarios.

Parent-child sharing is limited to:

- Cloud accounts
- Application services
- Artifact repositories
- Tags and rules
- Policies

By enforcing the separation of various tenants and offering one platform and shared governance for applications, clouds, and users, parent-child partial isolation reduces costs and optimizes efficiency.

Figure 2. Cisco CloudCenter Tenancy Model



Initial Setup Considerations

When the Cisco CloudCenter solution is first installed, it is set up with one root tenant and with one root tenant administrator who acts as the overall platform administrator. The root administrator is responsible for setting up clouds, configuring initial cloud accounts, creating users, and (optionally) creating additional tenants.

With the hosted delivery software-as-a-service (SaaS) model, Cisco is the root tenant and serves the role of root administrator. In this model, Cisco creates additional tenants for each customer who uses the SaaS version of the Cisco CloudCenter solution. This model is also used by cloud service providers who use a single Cisco CloudCenter installation to deliver shared services to fully isolated customers.

For dedicated Cisco CloudCenter installations, customers designate a root administrator. As shown in Figure 2, the root administrator can add multiple layers of tenants to meet the isolation and sharing requirements of an organization.

The root tenant can optionally create one or more peer tenants. Peer tenants might be customer organizations or business units that require tenant-level isolation and their own user interface customization, cloud management, user management, application marketplace, governance models, and so on.

Each tenant is assigned a tenant administrator who has access to all global permissions and privileges at the tenant level. At this level, tenant administrators can create users and user groups, and they can create subtenant organizations as isolated tenants. Subtenants can add their own subtenants. There is no limit to the number of subtenant hierarchies that can be created.

Tenant Administrator Functions

A root administrator can create tenant organizations and assign a tenant administrator for each one.

When creating a tenant, the root administrator can:

- Label the tenant user interface with a tenant logo
- Change the tenant user interface look and feel (colors and fonts)
- Enable all or a subset of parent tenant clouds for the tenant

The root administrator controls the following global permissions for each tenant organization and tenant administrator:

- The root administrator can allow the tenant administrator to add tenant-specific orchestrators. If this permission is not granted, tenant organizations can access clouds only through orchestrators that are set up by the platform administrator.
- The root administrator can allow tenant administrators to set up their own cloud accounts. If this permission is not granted, tenants can use only the cloud accounts that are set up and shared by the root administrator.
- The root administrator can allow the tenant administrator to create and maintain a private application marketplace.
- The root administrator can set permissions for publishing application profiles to the platform public marketplace.

Tenants are treated as independent "customer" organizations, and tenant administrators have complete independence in managing their users and user groups. Each tenant administrator can perform the following user management functions:

- Create, deactivate, or delete a user.
- Change a user password.
- Create and assign groups.
- Create and assign roles.

Authenticating Users within Tenants

An important aspect of a multitenant setup is user authentication. Authentication is configured and managed at the tenant level. Each tenant can use a personal authentication scheme.

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 also supports indirect Active Directory authentication using single sign-on (SSO) access between Cisco CloudCenter as a service provider and a customer's identity provider (IDP) such as Active Directory Federation Services (ADFS).

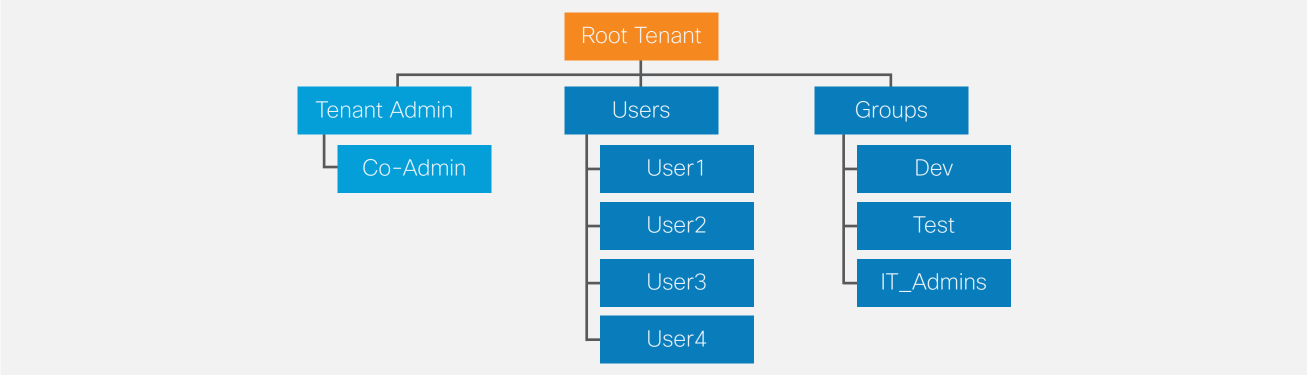
Activation profiles offer a fast and easy way to add new users. Activation profiles are predefined mappings of Cisco CloudCenter groups, roles, and cloud settings to Cisco CloudCenter role-based access control (RBAC) settings. Mappings can be created based on properties that are associated with users in an LDAP or Active Directory server. When a directory is imported into Cisco CloudCenter, the appropriate activation profile is used to activate that user in Cisco CloudCenter.

Model 1: Single Tenant

In the single-tenant deployment model, the root tenant is the only tenant for all users and groups. This model is appropriate for a centralized organization that doesn't need isolation between users and user groups.

In this model, shown in Figure 3, all users who log in to the system come from one SAML SSO authentication source. These users can be mapped to zero, one, or many groups.

Figure 3. Single Tenant with Sharing between Users and Groups

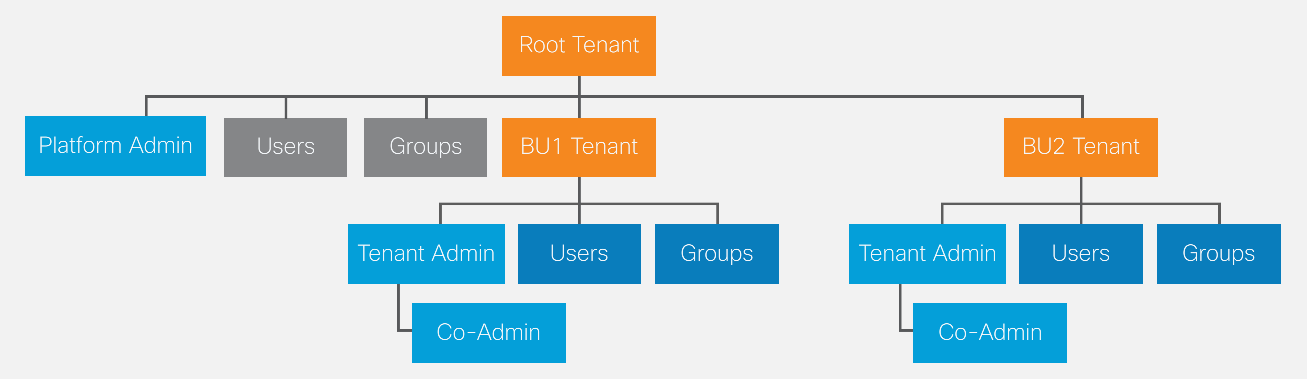


The main benefit of deploying Cisco CloudCenter with the single-tenant model is that all users and objects can be managed collectively. Role-based access, object-level sharing, and control across the tenant provide the following capabilities:

- RBAC
  - Set access for users for specific applications.
  - Apply roles to any user or group.
  - Enforce least-restrictive aggregated permissions.
- Object-level sharing and permission control within the tenant
  - Set access for users to perform actions such as deploying applications to specific clouds.
  - Create and share deployment environments with specific users. (A deployment environment is a specific cloud, cloud region, and cloud account combination.)
  - Make all services available to users to model application profiles in the topology modeler.
  - Share code repositories when deploying application profiles.
  - Share application profiles with other uses.
  - Allow users to publish applications to their tenant private marketplaces.

The disadvantage of the single-tenant model is that administrators have access to every user, cloud, and governance policy. This access may not be appropriate in larger organizations that have multiple IT teams with resources that they pay for and manage independently.

Figure 4. No Sharing between Independent Peer Tenants



Model 2: Peer Tenant

In the peer-tenant deployment model, the root tenant's only role is administering the platform. Individual tenant administrators are fully responsible for configuring and supporting their own tenant environment and delivering IT services.

This model is appropriate for an enterprise IT organization that:

- Has a decentralized IT structure and wants to gain cost and operational efficiencies by using one platform to manage applications, clouds, and users
- Doesn't need sharing between tenants that each independently manage their own service portfolio or has a compelling reason to prohibit sharing between tenants for reasons such as regulatory compliance

In this model, shown in Figure 4, all users who log in to the system authenticate against different SAML SSO sources. These users can be mapped to zero, one, or many groups within their tenants.

The main benefit of deploying a Cisco CloudCenter solution with multiple peer tenants is that one platform can be used for managing applications, clouds, and users, but each tenant can be managed independently as a completely separate entity. RBAC and object-level sharing are restricted to users within each tenant and provide the following capabilities:

- RBAC
  - Limit user access to specific application profiles within the tenant.
  - Apply unique roles to any user or group within the tenant.
  - Enforce least-restrictive aggregated permissions.
- Object-level sharing and permission control
  - No object-level sharing and permissions between tenants is allowed.

Model 3: Multiple Tenants with Subtenants

The multiple tenants with subtenants deployment model provides a mix of the benefits of the other two models. With this model, the root tenant can either just administer the platform or administer shared services.

This model supports a shared-service approach in which one central IT group may offer shared services to other subtenants. Those subtenants also have the flexibility to offer additional IT services to their respective organizations. But because the subtenants are peers, they are otherwise isolated.

In this model, shown in Figure 5, all users who log in to the system authenticate against different SAML SSO sources. These users can be mapped to zero, one, or many groups within their own tenants or subtenants.

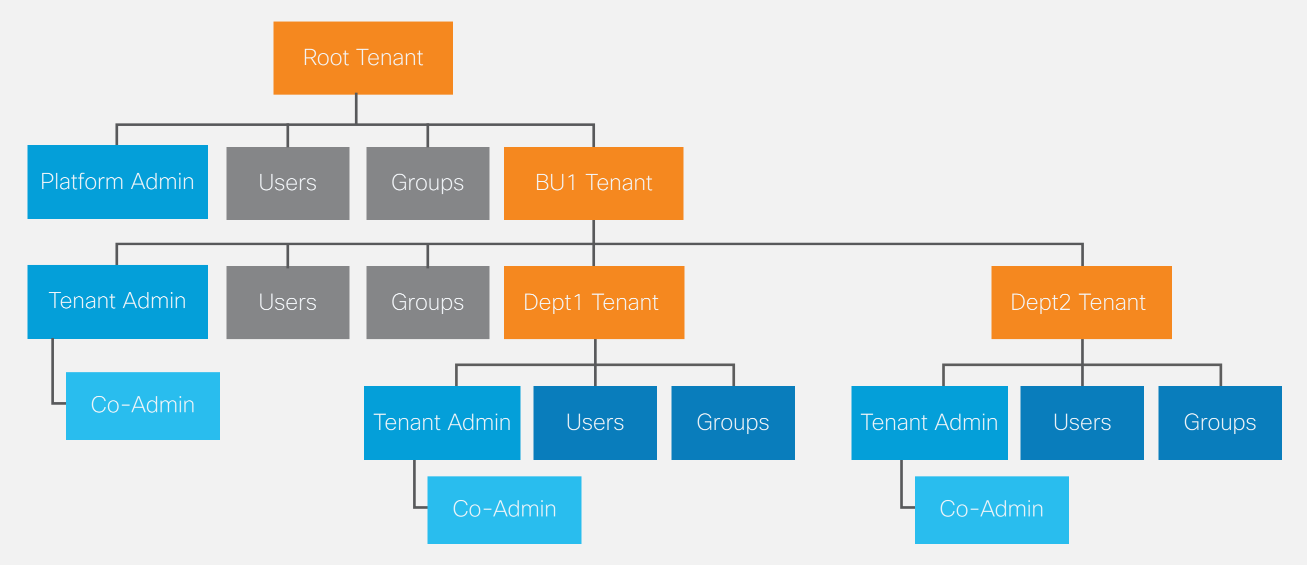
The main benefit of deploying Cisco CloudCenter using the multiple tenants with subtenants model is that each tenant can be managed independently, but still share both centrally managed cloud accounts and rolled-up cost reporting from all tenants lower in the hierarchy.

For example, a banking conglomerate may have multiple divisions that follow enterprise architecture standards and consume shared IT services, but within the investment banking tenant, sell-side and buy-side resources, applications, and users are strictly segregated and isolated in subtenant organizations.

In this model, RBAC and object-level sharing and control are blends of the functions of the other two models and provide the following capabilities:

- RBAC
  - Set access for users to access specific applications within the tenant.
  - Apply roles to any user or group within the tenant.
  - Enforce least-restrictive aggregated permissions.
- Object-level sharing and permission control
  - Share common code repositories for modeling applications.
  - Create and share cloud accounts with users of a tenant and subtenants.
  - Make services available to users of both a tenant and subtenants to model applications in the topology modeler.

Figure 5. Limited Sharing Between Business Unit and Department Tenants



Comparison of Deployment Models

Table 1 provides a comparison of the three Cisco CloudCenter multitenancy deployment models.

Table 1. Comparison of Multitenancy Deployment Models

Feature	Single Tenant	Multiple Tenants	Multiple Tenants with Subtenants
Sample use cases	· Centralized IT · One organization	· Decentralized IT · Each IT department manages its own resources	· Centralized IT delivers shared services · Each IT department offers additional services
Separated SSO	No	Yes	Yes
Separated groups	No	Yes	Yes
RBAC	Across tenant	Within tenant	Within tenant
Sharing	Within tenant	· Within tenant · None between peer tenants	· Within tenant · Parent-to-child sharing · None between peer tenants
Application profile sharing	Yes	Only with command-line interface (CLI) import and export or through public marketplace	Only with CLI import and export or through public marketplace
Advantages	· All objects and users in one tenant · Can easily share cloud accounts and applications	Users, applications, cloud accounts, and so on are completely separate	Shared service delivery with additional tenant autonomy
Disadvantages	· Administrators cannot independently manage the infrastructure or cloud accounts they own	Cannot share with other tenants	· Cannot share with peer tenants · Can share only with child tenants

Conclusion

With Cisco CloudCenter IT can simplify and centralize an IT service delivery strategy while giving various tenant organizations flexibility to add their own services. The solution provides powerful isolation when needed. But also provides easy-to-configure control over the sharing within and between tenants and subtenants.

For More Information

www.cisco.com/go/cloudcenter