Tenant Onboarding

- Tenant Onboarding Overview, page 1
- Tenant Onboarding with Virtual Data Centers, page 1
- Tenant Onboarding with Resource Groups, page 5

Tenant Onboarding Overview

In Cisco UCS Director, tenants enable you to securely control and allocate the virtual and physical infrastructure of your data center to the different user groups, organizations, and customers. Your IT teams no longer need to manually provision infrastructure for users to deploy virtual machines (VMs) to run end user applications. Instead, you can configure tenant onboarding through Cisco UCS Director to define the infrastructure boundaries and resource limits that are applied automatically when a user makes a service request to provision a VM or an application.

Depending upon the infrastructure in your data center, you can use one of the following configurations for tenant onboarding:

- Resource groups for systems that include an integration with Cisco Application Centric Infrastructure (Cisco ACI) and Cisco Application Policy Infrastructure Controller (Cisco APIC)
- Virtual data centers for systems that does not include Cisco ACI or Cisco APIC

Cisco UCS Director tenants are essentially customers that share the compute, network, and storage resources that is configured for ACI in Cisco UCS Director.

Tenant Onboarding with Virtual Data Centers

Virtual data centers (vDCs) in Cisco UCS Director enable you to securely create and onboard tenants that represent user groups or customer organizations. For each tenant, the vDCs define the boundaries of the infrastructure that your user groups or customer organizations can access and use.

You can also use vDCs to control the VMs and infrastructure resources that user groups can view in the End User Portal. When users log in to request or manage VMs, those users can only see the vDCs assigned to their user group and the VMs that have been provisioned from those vDCs. The users cannot see the VMs or vDCs assigned to other user groups or customer organizations.

You can assign more than one vDC to a user group. This configuration enables you to set different approvers and/or different resources for VMs, based upon the type of application that the end user requests. If you assign multiple vDCs to a user group or customer organization, you can allow your users to choose the vDC where the VM should be created.

Note You cannot configure tenant onboarding with vDCs if your system includes an integration between Cisco UCS Director and Cisco Application Policy Infrastructure Controller (APIC).

For more information about tenant onboarding with vDCs, see the Cisco UCS Director Administration Guide.

Virtual Data Centers

A Virtual Data Center (VDC) is a logical grouping that combines virtual resources, operational details, rules, and policies to manage specific group requirements.

A group or organization can manage multiple VDCs, images, templates, and policies. Organizations can allocate quotas and assign resource limits for individual groups at the VDC level.

You can also define approvers specific to a VDC. The approvers assigned to a particular VDC must approve all service requests from users for VM provisioning.

Note There is a default VDC in Cisco UCS Director, and all discovered VMs are part of this default VDC. Discovered VMs are VMs that are created outside of Cisco UCS Director or were already created on VMware vCenter before Cisco UCS Director was installed. Cisco UCS Director automatically discovers such VMs and adds them to the default VDC.

A VM that is provisioned using a service request can be associated with a specific VDC. When you create a service request, you can choose the VDC on which this VM is provisioned. You can view a list of the VDCs that are available for a particular group and choose the required VDC when provisioning VMs.

Policies for Virtual Data Centers

You specify the infrastructure allocations in a vDC through a set of policies and configuration options. Each policy defines a subset of resources that the associated user group or customer organization can use and view. These policies include the following:

- System policy—System specific information, including which template to use, time zone, and OS specific information.
- Computing policy—Available compute resources, including the host or cluster, number of vCPUs, CPU configuration, and memory configuration.
- Network policy—Available network resources, including IP address configuration (DHCP or static IP address) and the option for the end user to choose vNICs for any VM.
- Storage policy—Available storage resources, including the datastore scope, type of storage to use, minimum conditions for capacity, and latency.
- Approvers—Names and contact email addresses of the required approvers for VMs provisioned from the vDC resources. By default, you can configure a maximum of two approvers per vDC

- Cost model—Cost and chargeback policy for all VMs provisioned from the vDC resources.
- ISO image mapping policy—ISO images available for VMs provisioned from the vDC resources.
- End user self-service policy—Actions or tasks that a user can perform on VMs provisioned from the vDC resources.

Computing Policies

Computing policies determine the compute resources that can be used during provisioning to satisfy group or workload requirements.

As an administrator, you can define advanced policies by mixing and matching various conditions in the computing policy.

Note We recommend that you thoroughly understand all the fields in the computing policy. Some combinations of conditions can result in no host machines being available during self-service provisioning.

Network Policies

The network policy includes resources such as network settings, DHCP or static IP, and the option to add multiple vNICs for VMs provisioned using this policy.

Storage Policies

A storage policy defines resources such as the datastore scope, type of storage to use, minimum conditions for capacity, latency, and so on.

The storage policy also provides options to configure additional disk policies for multiple disks, and to provide datastore choices for use during a service request creation.

Note Cisco UCS Director supports datastore choice during a service request creation for VM provisioning. You can enable or disable datastore choices for the end user during service request creation. The datastores listed depend upon the scope conditions specified in the storage policy that is associated with the VDC during the service request creation.

To use the datastore selection feature while creating a service request, the template for VM provisioning must have the disk type assigned as **System**. This is applicable for templates with single or multiple disks.

End User Self-Service Policy

An End User Self-Service Policy controls the actions or tasks that a user can perform on a VDC. The starting point for creating this policy is to specify an account type (for example, VMware). After you specify an account type, you can continue with creating the policy. After you create the policy, you must assign the policy to a vDC that is created with the same account type. For example, if you have created an end user

policy for VMware, then you can specify this policy when you create a VMware vDC. You cannot view or assign policies that have been created for other account types.

In addition to creating an end user self-service policy, Cisco UCS Director allows you to perform the following tasks:

- View—Displays a summary of the policy.
- Edit—Opens the **End User Policy** screen from which you can modify the description or the end user self-service options.
- Clone—Opens the **End User Policy** screen through which you can create an additional policy using the parameters defined in an existing end user self-service policy.
- Delete—Deletes the policy from the system. You cannot delete a policy that has a VDC assigned to it.

Important The tasks that a user can perform on a VDC are defined by the role that the user is mapped to and by the end user self-service policy assigned to the VDC. If you have upgraded to the current release, then the permissions to perform VM management tasks are retained in any pre-existing end user self-service policy. However, the permissions defined in the user role to which the user belongs takes precedence.

Resource Limits

If you want to ensure that a user group or customer organization does not exceed specific compute, network, or storage resource thresholds, you can add resource limits to the user group that apply across all vDCs assigned to that group. If you use resource limits, even if one or more vDCs assigned to the user group have resources available, Cisco UCS Director will reject service requests that exceed the resource limits.

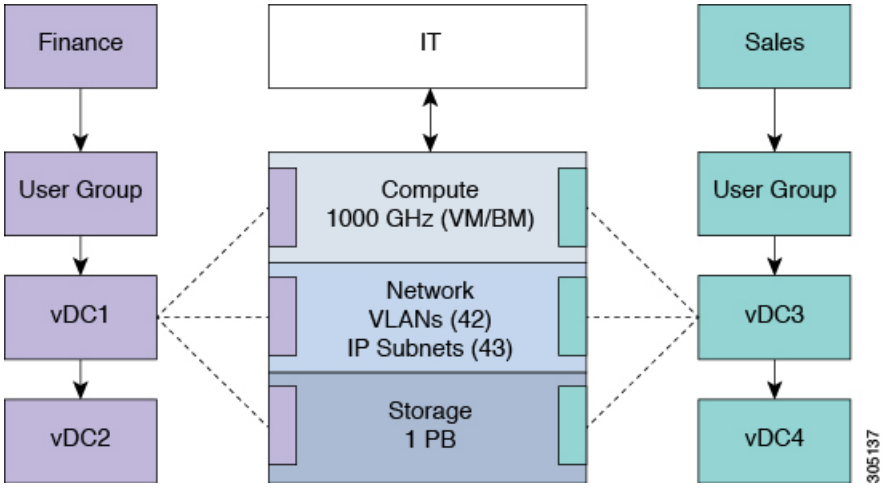
For example, if you have a data center that includes the following resources:

- ESXi cluster with 10 hosts
- Compute resources that total 1,000 GHz
- Network resources with all the required network portgroups, IP subnets, and VLANs
- Storage resources of 100 datastores
- User groups for Finance, Sales, and Development
- Resource limits for the Finance user group of 300GHz compute and 20 datastores.
- Three vDCs assigned to the Finance user group, each with 100 GHz compute and 10 datastores

With this configuration, users in the Finance group can log into the End User Portal and view their available resource limits, the vDCs that are associated with their user group, and other information about their available resources, and deployed applications. If they have deployed applications across all 20 datastores in their resource limits, they cannot make any further service requests without first requesting an additional resource allocation.

As you can see from the following illustration, the combination of user groups, vDCs, policies, and resource limits determine the boundaries of the compute, network, and storage infrastructure that is available to each of the Finance and Sales organizations for application provisioning.

Figure 1: Example: Resource Limits for Finance and Sales Organizations



Tenant Onboarding with Resource Groups

Resource groups enable you to securely onboard resources for tenants that represent user groups and customer organizations. Each resource group is a pool of physical and/or virtual resources with specific capacities and capabilities. Based on the specific resource requirements, resources are assigned to a tenant (user groups or organizations) from this pool. You can share resources in a resource group across tenants or you can dedicate them to a specific tenant.

When you onboard a tenant through a resource group, you need to do the following:

1. Create one or more resource tags, if desired.
2. If you created resource tags, tag the physical and virtual resources that you want to make available to the tenant. If you did not create resource tags, you can allocate resources to a tenant based on the required capacity and capability.
3. Create a resource group.
4. Add infrastructure resources (devices) to the resource group, either manually or through associating resource tags with the group.

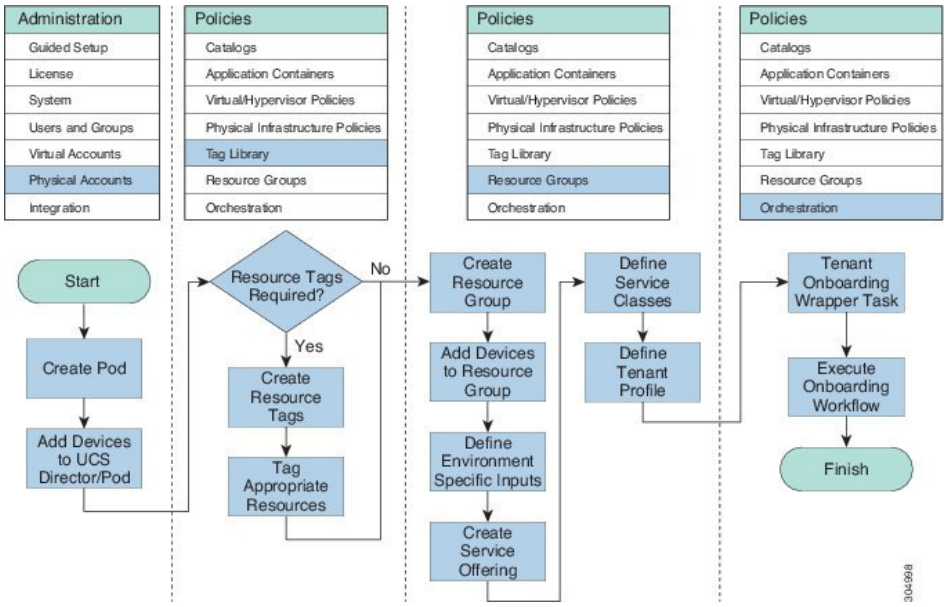
   You can add physical infrastructure resources, virtual infrastructure resources, or a combination of physical and virtual infrastructure resources to the group.
5. Define the environment specific inputs for each type of infrastructure resource associated with the resource group. These inputs can include domain and other information required to identify and assign the resources.
6. Create one or more service offerings to describe the requirements of a particular application that a user can provision.

7 Create one or more service classes within that service offering to define the requirements for a particular type of infrastructure resource required for the service offering. If you use resource tags, you can associate a service class with a particular resource tag.

8 Define a tenant profile to associate one or more service offerings with the resource group.

9 Develop the orchestration workflow required to deliver the service offering to the user as part of a service request.

Figure 2: Tenant Onboarding with Resource Groups Process Flow



Note Resource groups support tenant onboarding only for systems that include Cisco Application Centric Infrastructure (ACI) and Cisco Application Policy Infrastructure Controller (APIC).

For more information about tenant onboarding with resource groups, including specific examples, see the Cisco UCS Director APIC Management Guide.

Resource Tags

Resource tags are an optional component that allow you to assign a label to a physical or virtual infrastructure resource or to a category of infrastructure resources. Each resource tag is a name-value pair that identifies the resource or category of resources in a way that is meaningful to your data center.

When you tag an object, you can also define applicability rules that determine how the tags are filtered and displayed. You can also organize your resource tags into tag libraries, which allow you to determine how you want to categorize the resources that have that tag applied. For example, you can create one or more tag libraries based on the following criteria:

- Resource type

- Capacity
- Quality
- Capability

You can use resource tags to identify specific resources that should be used by a tenant or to identify resources that are appropriate for a specific tier of service. For example, you can create a tag with a name of tier and a value of gold. The resources that you associate this tag are then identified as appropriate for the gold tier of service, whether they are compute, storage, or network infrastructure devices.

Once you have tagged a set of resources, you can associate those resources with resource groups. The resource tags enable you to easily identify how the infrastructure resources should be grouped. They also define the boundaries of the infrastructure resources that are available to a particular resource group.

Resource Groups

You can use a resource group to select the appropriate resources for a tenant based on the requirements of an application. Additional concepts, such as a service offering, tenant profile, application profile, and resource group, are all required. Using these resource group concepts, you can onboard tenants and deploy applications based on a dynamic selection of resources. You can share resources in a resource group across tenants or you can dedicate them to a specific tenant.

A resource group is a pool of resources. Each group can contain physical infrastructure resources, virtual infrastructure resources, or a combination of physical and virtual infrastructure resources. Resource groups enable you to onboard tenants into Cisco UCS Director with minimum intervention.

As an infrastructure administrator or system administrator, you can add physical or virtual accounts to a resource group one at a time. Also, you can assign a pod to a resource group where all the accounts in the pod are added to the resource group.

When an account is added to a resource group, the resource group by default announces all the capabilities and capacities for objects for that account as resource group entity capacities and capabilities. With Cisco UCS Director, you can selectively disable certain capacities or capabilities from the resource group.

Service Offerings

A service offering defines the resources required to provision an application. Each service offering must include one or more service classes that represents the capacity and capability needed for the following resource layers:

- Virtual Compute
- Virtual Storage
- Virtual Network
- Physical Compute
- Physical Storage
- Physical Network
- Layer 4 to Layer 7 Services

When you define a service offering, you can specify the usage of resource groups as one of the following:

- Shared—The resources are shared among the applications or tenants.
- Dedicated —The resources are dedicated to a single application or tenant.

Based on the capacity, capability, and resource tags defined in the service offering, the resource groups are filtered and the matching resource groups are selected for further processing in the tenant onboarding and application deployment.

Tenant Profiles

Tenant profiles represent the pairing of one or more service offerings with one or more resource groups. Each tenant profile defines the characteristic of infrastructure requirements and application requirements.

You can create a tenant profile to meet each possible combination of customer and application. You can associate a tenant profile with multiple service offerings and choose a resource group for each service offering. A tenant profile can be shared by more than one tenant.