Managing Policies

This chapter contains the following sections:

Policies

Cisco UCS Director provides an End User Portal in which resources, such as virtual machines (VMs) or bare metal servers, are provisioned from a pool of assigned resources using predefined policies set by administrators.

A policy is a group of rules that determine where and how a new resource, be it a virtual machine or a bare metal server, is provisioned within the infrastructure, based on available system resources.

Cisco UCS Director requires that you set up the following policies to provision resources:

- Computing
- Storage
- Network
- System
- Bare Metal

Important Create a cloud account prior to setting up policies to provision VMs.

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.

Creating a Computing Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Computing**.

Step 2 On the **Computing** page, click **VMware Computing Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Computing Policy** screen, complete the following fields:

Name	Description
Policy Name field	The name of the policy. **Note** This name is used during catalog definition.
Policy Description field	The description of the policy.
Cloud Name drop-down list	Choose the cloud where resource allocation occurs.
Host Node/Cluster Scope drop-down list	Choose the scope of deployment. **Note** You can narrow the scope of deployment by specifying whether to use all, include chosen, or exclude chosen options. Depending on the choices, a new field appears where the required hosts or clusters can be chosen.
Resource Pool drop-down list	Choose the resource pool.
ESX Type drop-down list	Choose the ESX installation type: **ESX**, **ESXi**, or **both**.

Name	Description
ESX Version drop-down list	Choose the version of ESX.
Filter Conditions check boxes	Check one or more conditions that should match. Any hosts that do not meet these criteria are excluded from consideration. If more than one condition is chosen, all of the chosen conditions must match.
Deployment Options	
Override Template check box	Check to override the template properties. You are provided with options to enter custom settings for CPU and memory.
Number of vCPUs field	A custom number of vCPUs. The specified number of vCPUs for a VM should not exceed the total cores for the chosen scope of host nodes or clusters. **Note** This option appears if you checked **Override Template**.
CPU Reservation (MHz) field	The CPU reservation for the VM. The reservation depends upon the number of vCPUs specified. **Note** This option appears if you checked **Override Template**.
CPU Limit (MHz) field	The CPU limit for the VM. The CPU limit is based on the chosen scope of host nodes or clusters.
CPU Shares drop-down list	Choose the CPU shares: low, normal, or high. The CPU shares determine which VM gets CPU resources when there is competition among VMs. **Note** This option appears if you checked **Override Template**.
Memory field	The custom memory for the VM. **Note** This option appears if you checked **Override Template**.
Memory Reservation (MB) field	The memory reservation for the VM. The reservation depends upon the memory specified. **Note** This option appears if you checked **Override Template**.
Memory Limit (MB) field	The memory limit for the VM. The memory limit is based on the chosen scope of host nodes or clusters. **Note** This option appears if you checked **Override Template**.

Name	Description
Memory Shares drop-down list	Choose the memory shares: low, normal, or high.1 Memory shares determine which VM gets memory resources when there is competition among VMs. **Note** This option appears if you checked **Override Template**.
Resizing Options	
Allow Resizing of VM check box	Check to allow VM resizing before provisioning or to resize an existing VM.
Permitted Values for vCPUs field	The range of vCPUs to use while provisioning a VM or resizing an existing VM. A range of more than 8 is visible during VM provisioning or resizing only if the chosen cloud (vCenter) is 5 or above and has VM version 8. Only the values specified in the box are visible. **Note** This option appears if you checked **Allow Resizing of VM**.
Permitted Values for cores per socket	The number of permitted cores per socket. The number of cores per socket can be configured when creating a service request, deploying a VM, cloning a VM, or provisioning a VM using an orchestration workflow. If this field is empty, you will not have the option to specify the cores per socket while provisioning a VM and other actions.
Permitted Values for Memory in MB field	The range of memory to use while provisioning a VM or resizing an existing VM. For example: 512, 768, 1024, 1536, 2048, 3072, 4096, and so on. Only the values specified in the box are visible. **Note** This option appears if you checked **Allow Resizing of VM**.

Step 5 Click **Submit**.

Configuring a Bare Metal Server Provisioning Policy

Before You Begin

- A Bare Metal Agent (BMA) account must be added and configured with Bare Metal OS images.
- A Cisco UCS Manager account must be added.

- A Cisco UCS Central account must be added.
- If you need a specific cost associated with the bare metal server, then you must create a bare metal server cost model prior to creating this policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Bare Metal Servers**.

Step 2 On the **Bare Metal Servers** page, click **Bare Metal Server Provisioning Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Bare Metal Server Provisioning Policy** screen, complete the required fields, including the following:

Name	Description
Policy Name field	Enter a unique name for the policy.
Policy Description field	Enter a description for the policy.
Account Type drop-down list	Choose an account type from the drop-down list. It can be one of the following: • UCS Central • UCS Manager
UCS Central Account Name drop-down list	Choose a Cisco UCS Central account name. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list.
Account Name drop-down list	Choose an account name from the drop-down list.
Server Selection Scope drop-down list	Choose the scope for the policy. It can be one of the following: • **Include Servers** • **Include Server Pools**
Domain Group(s) list	Expand the list to check the UCS domain groups to be included in this policy. After checking the domain groups, click **Validate**. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list.

Name	Description
Include Ungrouped Domains check box	Check this check box to populate the **Domain Name(s)** list with ungrouped domains along with the domain names included in the selected domain groups. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list and if you have selected a domain group from the **Domain Group(s)** list.
Domain Name(s) list	Expand the list to check the UCS domain names to be included in this policy. After checking the domain name, click **Validate**. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list.
Servers field	Check the servers for this policy. This field is visible only if you selected **Include Servers** in the **Server Selection Scope** drop-down list.
Server Pools field	Check the server pools for this policy. This field is visible only if you selected **Include Server Pools** in the **Server Selection Scope** drop-down list.
Service Profile Template drop-down list	Choose a service profile template.
Use for SAN Boot check box	Check to include servers that contain at least one FCoE capable interface card.
Minimum Number of CPUs field	Specify the minimum number of CPUs that the server must contain.
Minimum Amount of Memory (MB) field	Specify the minimum amount of memory that must be available on the server.
Minimum Number of Cores Enabled field	Specify the number of cores that must be enabled on the server.
Allow User to Choose Servers check box	Check to allow users to select servers while using this policy to provision bare metal servers. If you do not check this check box, a bare metal server is provisioned based on the parameters you specify in this policy.

Name	Description
Show Server Resources to User check box	Check to have the system resources displayed when provisioning bare metal servers. You can choose any of the following resources: • **CPU** • **Memory** • **Storage**
Target BMA drop-down list	Select a bare metal agent for the PXE setup.
Use Windows Images check box	Check this check box to view a list of Windows images that you can select.
OS Image Selection	Check the check boxes of the OS images. If you checked **Use Windows Images**, then a list of Windows images are displayed. If you did not check **Use Windows Images**, then a list of Windows and CentOS images are displayed. While creating a service request for provisioning bare metal servers, you are prompted to select a Windows image.
Network Boot Manager drop-down list	Choose a boot manager from the drop-down list. It can be one of the following: • PXE • iPXE-BIOS • iPXE-EUFI
IP Configuration Type drop-down list	Choose the type of IP configuration from the drop-down list. It can be one of the following: • DHCP • Static

Name	Description
Domain Mapping list	Expand this list to map a domain to a specific BMA, or OS image. Click + to add a domain mapping. You will need to specify information for the following fields: • Domain Name—check the names of the domains that you want to map. • Target BMA—Choose a target BMA from the drop-down list. • OS Image—Check an OS image. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list.
Network Management	
Use Static IP Pool Policy check box	Check to select a static IP pool policy for provisioning a bare metal server. If you check this check box, an IP address is automatically assigned to the bare metal server from the IP range provided in the static IP pool policy.
Server IP Address field	Specify an IP address range.
Server Netmask field	Specify the server netmask.
Server Gateway field	Specify the server gateway IP address
Name Server field	Specify the name server IP address
Management VLAN field	Specify the management VLAN. By default, it is set to 0.
System Parameters	
Server Host Name field	Specify the server host name.
Host Name Validation Policy drop-down list	Choose a policy from the drop-down list. The server host name is validated against the policy that you select in this field before it is applied on the bare metal server.
Password field	Specify the password for the server host name.
Confirm Password field	Confirm the password for the server host name.

Name	Description
Timezone drop-down list	Set the time zone for the servers.
Cost Model drop-down list	Choose a cost model for the servers.

Step 5 Click **Submit**.

What to Do Next

You can validate the policy.

Validating a Bare Metal Server Provisioning Policy

To ensure that the parameters specified in the bare metal server provisioning policy are accurate, you can run this validation process on the policy.

Before You Begin

You should have created a bare metal server provisioning policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Bare Metal Servers**.

Step 2 On the **Bare Metal Servers** page, click **Bare Metal Server Provisioning Policy**.

Step 3 Choose a policy from the list of policies.

Step 4 From the **More Actions** drop-down list, choose **Validate**.
The validation process is initiated, and the results are displayed in the **Status** column on the **Bare Metal Server Provisioning Policy** screen.

Data Collection Policy

A data collection policy can be created to control the parameters that can be retrieved from the vCenter server for each VMware account. Each of the parameters mentioned in a data collection policy is collected and used in specific trend reports in Cisco UCS Director.

Note VMware is the only supported virtual account type. When a VMware account is added, it is automatically associated with the **default-data-collection-policy**.

Configuring a Data Collection Policy for a Virtual Account

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Data Collection Policy**.

Step 3 Click **Add**.

Step 4 On the **Add** screen, complete the following fields:

Name	Description
Name field	The name of the data collection policy. **Note** This name is used during catalog definition.
Description field	The description of the policy.
Account Type drop-down list	The VMware virtual account is selected.

Name	Description
Resource window	Choose a data collection group containing vCenter parameters. For example: CPU. Click the pencil icon to edit the data collection group. On the **Edit Resource Entry** screen, you can enable or disable data collection by checking or unchecking **Enable Collection**. To view the datastore-specific performance data in the Cisco UCS Director GUI, select the following resources: • Datastore throughput in kilobytes per second • Datastore number of read average • Datastore number of write average • Disk total latency in milliseconds For a Disk Latency report, in addition to selecting the resources listed above, set the vCenter Server performance data statistics collection level to 3. For a Throughput report, in addition to selecting the resources listed above, set the vCenter Server performance data statistics collection level to 4. **Important** Increasing the statistics collection to level 2 and above in the vCenter server could have an impact on the performance of the vCenter server and of Cisco UCS Director. For more information, see https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2003885.

Step 5 Click **Submit**.

Associating the Data Collection Policy for a Virtual Account

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Data Collection Policy Association**.

Step 3 Choose the **Data Collection Policy Association** tab.

Step 4 Click the row with the virtual (VMware) account for which you want to associate the data collection policy, and click **Edit**.

Step 5 In the **Edit** dialog box, choose the data collection policy from the **Policy** drop-down list that you configured.

Step 6 Click **Submit**.
The VMware account is now associated with the data collection policy.

About Group Share Policy

A group share policy provides more control to the users on resources and on what they can share with other users. With this policy, users can view resources that are currently assigned only to them or can view resources that are assigned to all groups that the users are part of.

While you are creating a group, you can define a group share policy and determine which groups have read/write permissions. Later, when users are added to this group, their access to resources is defined by the group share policy.

Creating a Group Share Policy

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Group Share Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Group Share Policy** screen, complete the following fields:

Name	Description
Policy Name field	The name of the group share policy.
Policy Description field	The description of the policy.
MSP Group Share Policy check box	Check to apply this policy to one or more MSP organizations.

Name	Description
MSP Organizations field	Click **Select** to choose the MSP organizations that have read/write permissions for the resources defined with this policy. This file is only available if you check **MSP Group Share Policy**.
Customer Organizations field	Click **Select** to choose the organizations that have read/write permissions for the resources defined with this policy.

Step 5 Click **Submit**.

What to Do Next

You can associate this group share policy with user groups in the system. Based on the permissions, users within those groups inherit read/write permissions to resources.

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.

Storage Policies for Multiple VM Disks

Cisco UCS Director supports VM provisioning with multiple disks on multiple datastores.

Disks are classified into five types: system, data, database, swap, and log. The system disk policy is configured first, and the other disks can be configured depending on requirements. You can configure the disk policy individually for each disk type or choose the default system disk policy for each disk.

Note For information on creating a storage policy for a template with multiple disks, see Multiple Disk VM Provisioning.

Adding and Configuring a Storage Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Storage**.

Step 2 On the **Storage** page, click **VMware Storage Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Storage Resource Allocation Policy** screen, complete the following fields:

Name	Description
Storage Policy - System Disk Policy	
Policy Name field	Enter the cloud in which resource allocation occurs.
Policy Description field	Enter the description of the policy. If you want to narrow the scope of deployment, choose whether to use all data stores, include selected data stores, or exclude selected data stores.
Cloud Name drop-down list	Choose the cloud account for this resource allocation. If you choose an SRM account, the **Enable Protection** check box is displayed. For more information about how to enable protection groups for Site Recovery Manager, see the Cisco UCS Director VMware Management Guide.
Use ReadyClone check box	Check to ensure that VMs are deployed using ReadyClones. This option is available only if the cloud account you chose is an HX cloud.
System Disk Scope	
Use Linked Clone check box	Check if you want to use a linked clone. If you do not check this box, the configuration uses a full clone.
Storage Profile drop-down list	Choose a storage profile if you want to provision one or more VMs with the associated storage profile.

Name	Description
Data Stores/Datastore Clusters Scope drop-down list	To define the scope of deployment, choose one of the following options: • **All** • **Include Selected Datastores** • **Exclude Selected Datastores** • **Include Selected Datastore Clusters** • **Exclude Selected Datastore Clusters** Depending on which option you choose, additional fields may display. **Note** The option that you choose determines which datastores or datastore clusters are available when you create a VM disk.
Selected Data Stores field	If you chose **Include Selected Datastores** or **Exclude Selected Datastores**, expand **Selected Data Stores** to choose the appropriate datastores.
Use Shared Data Store only check box	Check to use only shared datastores. This option is available only if you chose to include or exclude selected datastores.
Selected Datastore Clusters field	If you chose **Include Selected Datastore Clusters** or **Exclude Selected Datastore Clusters**, expand **Selected Datastore Clusters** to choose the appropriate datastore clusters.
Select SDRS Rule Type drop-down list	If you chose to include or exclude selected datastore clusters, choose one of the following SDRS rule types: • **Keep VMDKs Together—**You need to select an existing rule on the filtered clusters. The newly provisioned VM is added to the VM anti-affinity rule. • **Separate VMDKs—**If the newly provisioned VM contains more than one disk, a new VM affinity rule is created on the datastore cluster.
Select SDRS Rule field	If you chose **Keep VMDKs Together**, you must choose the VMs to which you want to apply the rule.
Storage Options	
Use Local Storage check box	By default, the option is checked. Uncheck if you do not want to use local storage.

Name	Description
Use NFS check box	By default, the option is checked. Uncheck if you do not want to use NFS storage.
Use SAN check box	By default, the option is checked. Uncheck if you do not want to use SAN storage.
Filter Conditions check boxes	To add one more conditions to filter the datastores, do the following for each desired condition: • Check the appropriate box. • Choose the desired option from the drop-down list. • Enter the criteria by which you want to filter the datastores. Any datastores that do not meet these criteria are excluded from consideration. If more than one condition is chosen, all conditions must match.
Override Template check box	Check to override the template properties. You are provided with options to enter custom settings, such as using thin provisioning or setting a custom disk size.
Use Thin Provisioning check box	Check to use thin provisioning during VM storage provisioning. Thin provisioning enables dynamic allocation of physical storage capacity to increase VM storage utilization. This option is available only if you choose **Override Template**.
Manual Disk Size check box	Check to use a custom disk size that overrides the disk size of the template used for VM provisioning. This option is available only if you choose **Override Template**.
Resizing Options for VM Lifecycle	
Allow Resizing of Disk check box	Check to provide the end user with an option to choose the VM disk size before provisioning.

Name	Description
Permitted Values for Disk in GB field	Specify the custom range of disk size values that are chosen while provisioning a VM. For example: 1, 5, 10, 50, 100, 500, 1024, 5120, 10240, and so on. This option is available only if you choose **Allow Resizing of Disk**.
Allow user to select datastores from scope check box	Check to provide the end user with an option to choose the datastore during the service request creation.

Note If you use this storage policy for OVF deployment, then the deployed OVF VM is created without thin provisioning.

Step 5 Click **Next**.

Step 6 On the **Additional Disk Policies** screen, do one of the following:

- Expand **Disk Policies** to choose a disk type to configure if you do not want to use the same disk policy for that disk type as you configured in the System Disk Policy.
- Click **Next** if you want to use the System Disk Policy options for all disk types.

Note By default, the disk policy for the disk is the same as in the System Disk Policy that you configured on the **Add Storage Resource Allocation Policy** screen.

Step 7 If you chose to configure a custom system disk policy for a specific disk type, do the following:

a) Click **Edit** to edit the disk type.
b) On the **Edit Disk Policies Entry** screen, uncheck **Same As System Disk Policy**.
c) On the**Edit Entry** screen, complete the fields.
All the fields displayed here are the same as the fields displayed on the **Add Storage Resource Allocation Policy** screen.

Note This configuration determines which datastores are available for the disk type when you create a VM disk.

d) Click **Submit**.
e) Repeat these steps to configure the other disk types, if desired.

Note To use the storage policy created with additional disk policies, you must associate the policy with the VDC that is used for the VM provisioning

Step 8 Click **Next**.

Step 9 On the **Hard Disk Policy** screen, specify the number of physical disks that you want to create during VM provisioning.

a) Expand **Disks** to add a disk by completing the following fields:

Field	Description
Disk Label field	Enter a descriptive label for the disk you are adding.
Disk Size (GB) field	Enter the size of the disk.

Field	Description
Disk Type drop-down list	Choose the disk type. The options that you see in this drop-down list depends on whether you checked **Same as System Policy** earlier in this procedure.
Controller Options	
Controller Type drop-down list	Choose a controller type from the drop-down list. Based on the availability of ports, a controller is mapped to the VM disks.
Create Disk on new Controller check box	Check this box to create a new controller. The type of controller that is created is based on the selection you made in the **Controller Type** drop-down list.
Disk Provisioning Options	
Disk Provisioning Options radio buttons	Click the radio button of the type of provisioning you want to specify. You can specify one of the following: • **Thin Provision** • **Thick Provision lazy zeroed** • **Thick Provision eager zeroed**
Resizing Options for VM Lifecycle	
Allow Resizing of Disk check box	Check to enable editing of the VM disk size before provisioning.
Permitted Values for Disk in GB field	Specify the custom range of disk size values that are chosen while provisioning a VM. For example: 1, 5, 10, 50, 100, 500, 1024, 5120, 10240, and so on. This option appears if **Allow Resizing of Disk** is checked.
Allow user to select datastores from scope check box	Check to provide the user with an option to choose the datastore during the service request creation.

Step 10 Click **Submit**.

Note

- If you use a storage policy for OVF deployment, then the deployed OVF VM is created without thin provisioning.
- To use the storage policy created with additional disk policies, you need to associate the policy with the VDC that is used for the VM provisioning.
- When using the Additional Disks Policies configured in a policy, make sure to uncheck **Provision all disks in a single database** during catalog creation for the multiple disk template. For more information about catalog creation, see Managing Catalogs.

Virtual Storage Catalogs

You can use a virtual storage catalog to customize storage policies. Using the virtual storage catalog, you can choose more than one storage policy and give it a custom storage entry name.

You map a storage catalog to a catalog by enabling it during catalog creation. When you raise a service request using the catalog, you are provided with the **Storage Tier** choice.

Configuring a Virtual Storage Catalog

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Storage**.

Step 2 On the **Storage** page, click **Virtual Storage Catalog**.

Step 3 Click **Add**.

Step 4 On the **Add Catalog** screen, complete the following fields:

Name	Description
Catalog Name field	The name of the catalog. This name is used during catalog custom actions definition.
Catalog Description field	The description of the catalog.
Cloud Name drop-down list	Select the cloud account.
Choose No of Entries drop-down list	Choose the number of entries. The range is from 1 to 10. Depending on the choice, storage entry options are provided in the subsequent dialog box.

Step 5 Click **Next**.

Step 6 On the **Add Entries** screen, complete the following fields:

Name	Description
Storage Entry #1	
Storage Entry Name field	The name of the storage entry.
Storage Policy drop-down list	Choose the storage policy.
Storage Entry # 2	
Storage Entry Name field	The storage entry name of the second policy.
Storage Policy drop-down list	Choose the storage policy.

Step 7 Click **Submit**.

What to Do Next

- You can map the virtual storage catalog during catalog creation.

  See Managing Catalogs.
- You can view the storage tier options during the Service request creation.

  See Using Self-Service Provisioning.

Credential Policies

A policy comprises a set of rules that controls access to a system or network resource. A credential policy defines password requirements and account lockouts for user accounts. Credential policies that are assigned to user accounts control the authentication process in Cisco UCS Director. After you add a credential policy, you can assign the new policy as the default policy for a credential type or to an individual application.

Configuring a Credential Policy

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Credential Policies**.
Step 2 On the **Credential Policies** page, click **Credential Policies**.
Step 3 Click **Add**.
Step 4 On the **Add Credential Policy** screen, check the check the account type.
Step 5 Click **Select**.
Step 6 On the **Add Credential Policy** screen, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Description field	A description for the policy.
Username field	The user name for the account.
Password field	The password for the user account.
Protocol drop-down list	Select the protocol.
Port field	The port number.

The fields displayed in this screen vary depending on the type of account that you are creating the policy for.

Step 7 Click **Submit**.
At a later point in time, if you modify the credentials in this policy, the changes are automatically applied to accounts configured with the policy. These changes are applied when Cisco UCS Director attempts to connect with these accounts.

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.

Adding a Static IP Pool Policy

You can optionally configure a static IP pool policy that can be used with a network policy.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.
Step 2 On the **Network** page, click **Static IP Pool Policy**.
Step 3 Click **Add**.
Step 4 On the **Static IP Pool Policy Information** screen, complete the following fields:

Name	Description
Policy Name field	Name of the IP pool policy.
Policy Description field	Description of the IP pool policy.

Name	Description
Allow IP Overlap drop-down list	Indicate whether IP overlap is allowed or not. By default, overlapping IP is not enabled. Enabling overlapping of IP implies the following: • You can create an IP pool and have IP addresses overlap within that pool. • You can create two static IP pools and have the IP addresses overlap between the pools.
Scope drop-down list	The scope of the IP pool overlap. The options are: • MSP Organization This option is visible only if you have enabled MSP. • Group/Customer Organization • Container **Note** This option is visible only if you select Yes in the **Allow IP Overlap** drop-down list.
User Group ID field	Choose **Select** to check the user group for the policy. All the user groups created in the system are displayed.
Container ID field	Choose **Select** to check the container.

Step 5 Expand the **Static IP Pools** section section and click **(+)** to add and configure multiple static IP pools.

Step 6 On the **Add Entry to Static IP Pools** screen, complete the following fields:

Name	Description
Static IP Pool field	The static IP pool. For example: 10.5.0.1 - 10.5.0.50, 10.5.0.100, 10.5.1.20 -10.5.1.70.
Subnet Mask field	The subnetwork mask for the pool. For example: 255.255.255.0.
Gateway IP Address field	The IP address of the default gateway for this network.
VLAN ID field	The VLAN ID to be used for the network. Enter a valid VLAN ID range.

Step 7 Click **Submit**.

Step 8 Click **Submit** on the **Static IP Pool Policy Information**screen.

Configuring a IP Subnet Pool Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **IP Subnet Pool Policy**.

Step 3 Click **Add**.

Step 4 On the **IP Subnet Pool Policy Information** screen, complete the following fields:

Field	Description
Policy Name field	The name of the policy.
Policy Description field	The description of the policy.
Network Supernet Address field	The network supernet address.
Network Supernet Mask field	The network supernet mask.
Number of Subnets Required drop-down list	Choose the number of subnets required for your configuration.
Gateway Address drop-down list	Choose a gateway address index:
Allow IP Overlap drop-down list	Indicate whether IP overlap is allowed or not. By default, overlapping IP is not enabled. Enabling overlapping of IP implies the following: • You can create an IP pool and have IP addresses overlap within that pool. • You can create two IP subnet pools and have the IP addresses overlap between the pools.

Field	Description
Scope drop-down list	The scope of the IP subnet pool overlap. The options are: • MSP Organization This option is visible only if you have enabled MSP. • Group/Customer Organization • Container **Note** This option is visible only if you select Yes in the **Allow IP Overlap** drop-down list.

Important While creating a policy with overlapping IP enabled, you must first determine if there are any other IP subnet pool policies created with the same IP range. If those other policies also have overlapping IP enabled, then you can create an additional policy with no errors. However, if a previously created IP subnet pool policy, which uses the same IP range that you want to specify for the policy you are creating, does not have overlapping IP enabled, then you cannot proceed. The same behavior holds true in the case of creating a policy without enabling overlapping IP.

While creating this policy without enabling overlapping IP, you must first determine if there are any other policies that are created with the same IP range. If previously created pool policies have overlapping IP enabled, then you cannot specify the same IP range to create another policy with overlapping IP disabled.

Step 5 Click **Submit**.

Adding a Network Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **VMware Network Policy**.

Step 3 Click **Add**.

Step 4 On the **Network Policy Information** screen, complete the following fields:

Name	Description
Policy Name field	The name of the network policy.
Policy Description field	The description of the network policy.
Cloud Name drop-down list	Choose the cloud account to which the policy applies.

Name	Description
Allow end user to select optional NICs check box	Check if you want to provide vNICs selection during the creation of a service request-deployment configuration.
VM Networks field	Expand the **VM Networks** table to add a new entry to the VM network.

Step 5 Click **Add** in the VM Networks section to add and configure multiple vNICs. These vNICs are applicable to the VM that is provisioned using this policy.

Note To add or replace vNICs for provisioned or discovered VMs using VM actions, you must configure the vNICs.

Step 6 On the **Add Entry to VM Networks** screen, complete the following fields:

Name	Description
NIC Alias field	The name for the new NIC
Mandatory check box	If **Allow end user to select optional NICs** is checked on the **Network Policy Information** screen, this box is pre-selected. If the **Allow end user to select optional NICs** box was not checked, and this check box is not selected, then the **NIC Alias** field is optional. **Note** At least one of the NICs should have the **Mandatory** option selected. The NICs that have the **Mandatory** option selected are used in VM provisioning and there will be no option for the user during VM service request creation.
Allow end user to choose portgroups check box	Check to allow the end user to choose port groups during provisioning.
Show policy level portgroups check box	Checking this check box along with the **Allow end user to choose portgroups** check box lists all the selected portgroups of NICs in the policy.
Copy Adapter from Template check box	Check if you do not need custom settings. Clear this check box for custom settings. The **Adapter Type** drop-down list is not visible when you check this check box.
Allow the end user to override IP Address check box	Check to allow users to override the IP address.

Name	Description
Adapter Type drop-down list	Choose the adapter type. Select this option if the user wants to have the same Adapter Type that is available in the template. **Note** This option is not visible if the **Copy Adapter from Template** option is chosen.

Step 7 Click **Add (+)** in the **Port Groups** section. The **Add Entry to Port Groups** screen appears.

Step 8 Click **Select** to choose the port group name.

Step 9 From the **Select IP Address Type** drop-down field, choose **DHCP** (default) or **Static**.

a) If you choose **Static**, you must choose **IP Pool Policy** (default) or **Inline IP Pool**.
If you choose **IP Pool Policy**, click **Select to choose a static IP pool**. On the **Select** screen, choose from the list of preconfigured static IP pool(s). If no preconfigured static IP pools exist, see Adding a Static IP Policy for more information.

b) If you choose **Inline IP Pool**, complete the following fields:

Name	Description
Static IP Pool field	The static IP pool. For example: 10.5.0.1 - 10.5.0.50, 10.5.0.100, 10.5.1.20-10.5.1.70
Subnet Mask field	The subnetwork mask for the pool. For example: 255.255.255.0
Gateway IP Address field	The IP address of the default gateway for this network.
Allow IP Overlap drop-down list	Indicate whether IP overlap is allowed or not. By default, overlapping IP is not enabled. Enabling overlapping of IP implies the following: • You can create an IP pool and have IP addresses overlap within that pool. • You can create two static IP pools and have the IP addresses overlap between the pools
Scope drop-down list	The scope of the IP pool overlap. The options are: • MSP Organization This option is visible only if you have enabled MSP. • Group/Customer Organization • Container **Note** This option is visible only if you select Yes in the **Allow IP Overlap** drop-down list.

Name	Description
User Group ID field	Choose **Select** to check the user group. All the user groups created in the system are displayed.
Container ID field	Choose **Select** to check the container.

Step 10 Check **IPv6** to configure IPv6.
You must configure the identical fields that you specified for IPv4 configuration.

Step 11 Click **Submit**.

Step 12 Click **Submit** on the **Add Entry to VM Networks** screen.

Step 13 Click **Submit** on the **Network Policy Information** screen.

Networking Provisioning Policies

A network provisioning policy is used during orchestration workflow tasks. This policy defines Layer 2 network configuration and access control lists (ACLs) for switches in the network.

Configuring a Network Provisioning Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **Network Provisioning Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Policy** screen, complete the following fields:

Name	Description
General Information	
Policy Name field	The name of the policy.
Policy Description field	The description of the policy.
L2 Network Configuration VLAN	

Name	Description
Use Private VLAN check box	If checked, the following fields are automatically populated: • Private VLAN Type: community • Primary VLAN ID: 0 • Secondary VLAN Range—Starting ID 500 • Secondary VLAN Range—Ending ID 1000
VLAN Range - Starting ID field	A starting ID for the VLAN range. 500 is the default ID start range.
VLAN Range - Ending ID field	An ending ID for the VLAN range. 1000 is the default ID end range.
Base Profile Name field	The VLAN base profile name. This is the profile that contains one or more nested profile assignments.
Access Control List	
ACL Type drop-down list	By default, it is set to **Simple**. This is the only option available currently.
Allow ICMP check box	Check to allow ICMP on the VLAN.
Permit Incoming Traffic to TCP Ports field	The following options are available: • FTP • SSH • Telnet • SMTP • POP3 • HTTP • HTTPS • MySQL
Permit Incoming Traffic to UDP Ports field	The following options are available: • SNMP • Syslog

Step 5 Click **Submit**.

VLAN Pool Policies

A VLAN pool policy defines the VLAN range for a pod. This policy is used in the orchestration workflow for generating a free VLAN ID from the defined range specified in the policy.

Configuring a VLAN Pool Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **VLAN Pool Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Policy** screen, complete the following fields:

Name	Description
Pod drop-down list	Allows you to choose the pod.
Policy Name field	The policy name. This policy name is used in orchestration workflows.
Policy Description field	The description of the policy.
VLAN Range field	The VLAN range. For example: 1,3, 5—15.

Step 5 Click **Submit**.

System Policies

A system policy defines system-specific information, such as the template to use, time zone, OS-specific information, and so on.

Configuring a System Policy

Note When you use the system policy to provision virtual machines by deploying an OVF, enter only the **VM Name Template** and the **Host Name Template** fields. The remaining fields in the system policy are not applicable.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **VMware System Policy**.

Step 3 Click **Add**.

Step 4 On the **System Policy Information** screen, complete the following fields:

Name	Description
Policy Name field	The name of the policy. This name is used during catalog definition.
Policy Description field	The description of the policy.
VM Name Template field	The VM name template to use. Cisco UCS Director allows automatic creation of VM names. VM names can be automatically created using a set of variable names. Each variable must be enclosed in ${VARIABLE_NAME}. For example: vm-${GROUP_NAME}-SR${SR_ID}.
Disable VM Name Uniqueness Check check box	Check to disable the VM name uniqueness check when the VM is provisioned. Disabling the VM name uniqueness check allows you to disable the VM name validation across Cisco UCS Director and use the same VM name in a multi-tenant and multi-domain environment. If this field is unchecked, the VM name uniqueness check runs and only allows the same VM name if it is provisioned in a different folder or datacenter.
VM Name Validation Policy drop-down list	Allows you to choose a VM name validation policy. This list is populated with the policies that you created previously.

Step 5 Choose from the following optional **VM Name Template** features:

Name	Description
End User VM Name or VM Prefix check box	Check to allow the user to add a VM name or VM prefix during a service request creation for VM provisioning.
Power On after deploy check box	Check to automatically power on all VMs deployed using this policy.
Host Name Template field	The VM hostnames that can be automatically created using set of variable names. Each variable must be enclosed in **${VARIABLE}**.
Disable Host Name Uniqueness Check check box	Check to disable the host name uniqueness check when the VM is provisioned with guest OS customizations. Disabling the host name uniqueness check allows you to disable the host name validation across Cisco UCS Director and use the same host name in a multi-tenant and multi-domain environment. If this field is unchecked, the host name uniqueness check runs and only allows the same host name if the VM is going to be provisioned in a different tenant, domain, or workgroup.
Host Name Validation Policy drop-down list	Choose a host name validation policy. This list is populated with the policies that you created earlier on.

Step 6 Complete the following fields:

Name	Description
Linux Time Zone drop-down list	Choose the time zone.
Linux VM Max Boot Wait Time drop-down list	Choose the maximum waiting period for the Linux VM to boot.
DNS Domain field	The IP domain to use for the VM.
DNS Suffix List field	The DNS suffixes to configure for the DNS lookup. Use commas to separate multiple entries.
DNS Server List field	The list of DNS server IP addresses. Use commas to separate multiple entries.

Name	Description
VM Image Type drop-down list	Choose the OS of the image that is installed on the VM. You can choose between: • Windows and Linux • Linux Only
Windows	
Product ID field	The Windows product ID or license key. The product ID or license key can be provided here or at the OS license pool. The key entered in the OS license pool overrides the key provided here.
License Owner Name field	The Windows license owner name.
Organization field	The organization name to configure in the VM.
License Mode drop-down list	Choose per-seat or per-server.
Number of License Users	The number of license users or connections.
WINS Server List field	The WINS server IP addresses. Use commas to separate multiple entries.
Windows VM Max Boot Wait Time drop-down list	Choose the maximum waiting period for the Windows VM to boot.
Create a unique SID check box	Check to create a unique SID for the system.
Auto Logon check box	Check to enable auto logon.
Auto Logon Count field	The number of times to perform auto logon.
Administrator Password field	The password for the administrator's account.
Windows Time Zone drop-down list	Choose the time zone that must be set for the Windows VM.
Domain/Workgroup drop-down list	Choose either **Domain** or **Workgroup**.
Workgroup field	The name for the workgroup. This option appears if **Workgroup** is chosen as the value in the **Domain/Workgroup** drop-down list.

Name	Description
Domain field	The name of the Windows domain. **Note** This option appears if **Domain** is chosen as the value in the **Domain/Workgroup** drop-down list.
Domain Username field	The Windows domain administrator's username. **Note** This option appears if **Domain** is chosen as the value in the **Domain/Workgroup** drop-down list.
Domain Password field	The Windows domain administrator's password. **Note** This option appears if **Domain** is chosen as the value in the **Domain/Workgroup** drop-down list.

Name	Description
Define VM Annotation check box	

Name	Description
	Check to specify annotations to the VM. You can specify a note and custom attributes as part of the annotation. After you select this check box, complete the following fields: • **VM Annotation** field Enter a description for the VM. • **Custom Attributes** Click **Add (+)** to specify the **Name**, **Type**, and **Value**. Following are some of the **Custom Attributes** that you can add: • ${VM_HOSTNAME} • ${VM_HOSTNAME_SHORT} • ${VM_HOSTNAME_DOMAIN} • ${VM_IPADDRESS} • ${VM_ID} • ${VM_NAME} • ${VM_STATE} • ${VM_STATE_DETAILS} • ${VM_PARENT} • ${VM_CLOUD} • ${VM_GROUP_NAME} • ${VM_GROUP_ID} • ${VM_VDC_NAME} • ${VM_VDC_ID} • ${VM_SR_ID} • ${VM_SCHED_TERM} • ${VM_TYPE} • ${VM_COMMENTS} • ${VM_CATALOG_ID} • ${ INITIATING_USER} • ${SUBMITTER_EMAIL} • ${SUBMITTER_FIRSTNAME}

Name	Description
	• ${SUBMITTER_LASTNAME} • ${SUBMITTER_GROUPNAME} • Variables for VM creation: ◦ ${SR_ID} ◦ ${GROUP_NAME} ◦ ${USER} ◦ ${APPCODE} ◦ ${COST_CENTER} ◦ ${UNIQUE_ID} ◦ ${LOCATION} ◦ ${PROFILE_NAME} ◦ ${COMMENTS} ◦ ${CATALOG_NAME} ◦ ${CLOUD_NAME} **Note** The information that you add as part of the VM Annotation is displayed for the VM in the **VM Details** page.

Step 7 Click **Submit**.

OS Licenses

Cisco UCS Director provides an option for users to add Windows OS licenses. These licenses are mapped to Windows images during the creation of a catalog. You have an option to provide the Windows OS license for a Windows image in VMware System Policy or choose the key from the OS version field during catalog creation.

Adding an OS License

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **OS License**.

Step 3 Click **Add**.

Step 4 On the **Add License Details** screen, complete the following fields:

Name	Description
Windows Version Name field	The Windows version name.
License field	The Windows product ID or license key. This field accepts KMS client set-up keys.
License Owner Name field	The Windows license owner name.
Organization field	The organization name to configure in the VM.
License Mode drop-down list	Allows you to choose per-seat or per-server.
Number of Licensed Users field	The number of license users or connections.

Step 5 Click **Submit**.

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.

Creating an End User Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **End User Self-Service Policy**.

Step 3 Click **Add**.

Step 4 On the **Add End User Policy** screen, select an account type from the drop-down list.

Step 5 Click **Submit**.

Step 6 On the **End User Policy** screen, complete the following fields:

Name	Description
Policy Name field	The name of the policy.
Policy Description field	The description for the policy.
End User Self-Service Options field	A list of tasks that a user can perform on a VDC that is assigned with this policy. The list of tasks varies according to the **Account Type**.

Step 7 Click **Submit**.

What to Do Next

Assign this end-user policy to a VDC. For more information, see Adding a Virtual Data Center.

Configuring a VM Management Policy

This policy defines how VMs are managed in the VDC.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **VM Management Policy**.

Step 3 Click **Add**.

Step 4 On the **Add VM Management Policy** screen, complete the following fields:

Field	Description
Policy Name field	A unique name for the policy.
Policy Description field	A description for the policy.
VM Lease Expiry Notification Settings	
Configure VM Lease Notification check box	Check to set notification parameters for VMs configured with lease time.
How many days before VM Lease expiry should notifications be sent field	Enter a number. This number indicates the number of days prior to VM lease expiry that an email notification is sent to the VM owner.
How many notifications should be sent field	Enter a number. This number indicates the number of email notifications that will be sent informing the user of the VM lease expiration.
Interval between notifications drop-down list	Choose a number from the drop-down list. This number defines the time gap or interval between the notification emails that are sent.
Inactive VM Management Settings	
Delete after inactive VM days field	Enter a number. This number indicates the number of days after which an inactive VM is deleted from the system. **Note** Inactive VMs are deleted only if the **Delete Inactive VMs Based on vDC Policy** option is selected in the Properties pane. This option is displayed when you select **Administration** > **System** > **Advanced Controls**.

Field	Description
Additional grace period for deleting expired VMs field	Enter a number. This number indicates the number of days that the system waits before deleting an inactive VM from the system. **Note** When the time period specified in the **Delete after inactive VM days** and **Additional grace period for deleting expired VMs** fields elapse, VMs discovered through Cisco UCS Director are deleted, and service requests for VMs provisioned through Cisco UCS Director are rolled back. A new email template for rolled back Service Requests (SR) for these system—provisioned VMs has been introduced.
Action to be taken when a service request (SR) roll back task fails for VMs provisioned through Cisco UCS Director drop-down list	Select an action to be taken when a service request (SR) roll back task fails for VMs provisioned through Cisco UCS Director. You can choose one of the following options: • Send notification and delete the VM • Send notification and do not delete the VM **Note** In the VM Automatic Deletion email template, a new field titled **Rollback SR ID** has been introduced. This field is populated for VMs provisioned through Cisco UCS Director and is blank for VMs discovered through Cisco UCS Director.
Configure VM Delete Notification check box	Check to set notification parameters for VMs that are to be deleted.
How many days before VM deletion should notifications be sent field	Enter a number. This number indicates the number of days prior to VM deletion that an email notification is sent to the user.
How many notifications should be sent field	Enter a number. This number indicates the number of notification emails that are sent to the user.
Interval between notifications drop-down list	Choose a number from the drop-down list. This number defines the time gap or interval between the notification emails that are sent.

Step 5 Click **Submit**.

What to Do Next

You can map this policy to a virtual data center.