Configuring Server-Related Policies

This chapter includes the following sections:

Configuring Boot Policies

Boot Policy

The boot policy determines the following:

- Configuration of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can choose to have associated servers boot from a local device, such as a local disk or CD-ROM (VMedia), or you can select a SAN boot or a LAN (PXE) boot.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, the server uses the default settings in the BIOS to determine the boot order.

Important Changes to a boot policy may be propagated to all servers created with an updating service profile template that includes that boot policy. Reassociation of the service profile with the server to rewrite the boot order information in the BIOS is auto-triggered.

Guidelines

When you create a boot policy, you can add one or more of the following to the boot policy and specify their boot order:

Boot type	Description
SAN boot	Boots from an operating system image on the SAN. You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary. We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN, when you move a service profile from one server to another, the new server boots from the exact same operating system image. Therefore, the new server appears to be the exact same server to the network.
LAN boot	Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server.
Local disk boot	If the server has a local drive, boots from that drive.
Virtual media boot	Mimics the insertion of a physical CD-ROM disk (read-only) or floppy disk (read-write) into a server. It is typically used to manually install operating systems on a server.

Note The default boot order is as follows:

1. Local disk boot
2. LAN boot
3. Virtual media read-only boot
4. Virtual media read-write boot

Creating a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, we recommend that you create a global boot policy that can be included in multiple service profiles or service profile templates.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Boot Policies** and select **Create Boot Policy**.
The **Create Boot Policy** wizard displays.

Step 5 Enter a unique name and description for the policy.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Step 6 (Optional) To reboot all servers that use this boot policy after you make changes to the boot order, check the **Reboot on Boot Order Change** check box.

Step 7 (Optional) To ensure that Cisco UCS Manager uses any vNICs or vHBAs in the order shown in the **Boot Order** table, check the **Enforce vNIC/vHBA Name** check box.
If you do not check this check box, Cisco UCS Manager uses the priority specified in the vNIC or vHBA.

Step 8 To add a local disk, virtual CD-ROM, or virtual floppy to the boot order:

a) Click the down arrows to expand the **Local Devices** area.

b) Click one of the following links to add the device to the **Boot Order** table:

- **Add Local Disk**
- **Add CD-ROM**
- **Add Floppy**

c) Add another boot device to the **Boot Order** table or click **OK** to finish.

Step 9 To add a LAN boot to the boot order:

a) Click the down arrows to expand the **vNICs** area.

b) Click the **Add LAN Boot** link.

c) In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.

d) Add another device to the **Boot Order** table or click **OK** to finish.

Step 10 To add a SAN boot to the boot order:

a) Click the down arrows to expand the **vHBAs** area.

b) Click the **Add SAN Boot** link.

c) In the **Add SAN Boot** dialog box, complete the following fields, then click **OK**:

Name	Description
vHBA field	Enter the name of the vHBA you want to use for the SAN boot.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location.

d) If this vHBA points to a bootable SAN image, click the **Add SAN Boot Target** link and, in the **Add SAN Boot Target** dialog box, complete the following fields, then click **OK**:

Name	Description
Boot Target LUN field	The LUN that corresponds to the location of the boot image.
Boot Target WWPN field	The WWPN that corresponds to the location of the boot image.
Type field	This can be: • **primary**—If the server boots using a SAN WWN address, this is the first address it tries. Each boot policy can have only one primary SAN boot location. • **secondary**—If the server cannot boot from the primary SAN location, it attempts to boot from this location. Each boot policy can have only one secondary SAN boot location.

e) Add another boot device to the **Boot Order** table or click **OK** to finish.

What to Do Next

Include the boot policy in a service profile and/or template.

Deleting a Boot Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.

Step 3 Expand the **Boot Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Configuring Chassis Discovery Policies

Chassis Discovery Policy

This discovery policy determines how the system reacts when you add a new chassis. If you create a chassis discovery policy, the system does the following:

- Automatically configures the chassis for the number of links between the chassis and the fabric interconnect specified in the policy.
- Specifies the power policy to be used by the chassis.

Configuring a Chassis Discovery Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** node, select the **Global Policies** tab in the **Work** pane.

Step 3 From the **Action** drop-down list, select the number of links to be used by the chassis.

Step 4 In the **Redundancy** field of the **Power Policy** area, select one of the following options:

- **non-redundant**
- **n+1**
- **grid**

Step 5 Click **Save Changes**.

Configuring IPMI Profiles

IPMI Access Profile

This policy allows you to determine whether IPMI commands can be sent directly to the server, using the IP address. For example, you can send commands to retrieve sensor data from the BMC. This policy defines the IPMI access, including a username and password that can be authenticated locally on the server, and whether the access is read-only or read-write.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating an IPMI Profile

Before You Begin

An IPMI profile requires that one or more of the following resources already exist in the system:

- Username with appropriate permissions that can be authenticated by the operating system of the server
- Password for the username
- Permissions associated with the username

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **IPMI Profiles** and select **Create IPMI Profiles**.

Step 5 In the **Create IPMI Profile** dialog box:

a) Enter a unique name and description for the profile.
b) Click **OK**.

Step 6 In the **IPMI Profile Users** area of the navigator, click +.

Step 7 In the **User Properties** dialog box:

a) Complete the following fields:

Name	Description
Name field	The username to associate with this IPMI profile.
Password field	The password associated with this username.
Confirm Password field	The password a second time for confirmation purposes.

Name	Description
Role field	This can be: • **admin** • **Read Only**

b) Click **OK**.

Step 8 Repeat Steps 6 and 7 to add another user.

Step 9 Click **OK** to return to the IPMI profiles in the **Work** pane.

What to Do Next

Include the IPMI profile in a service profile and/or template.

Deleting an IPMI Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 In the **Servers** tab, expand **Servers ➤ Policies ➤** ***Organization_Name***

Step 3 Expand the **IPMI Profiles** node.

Step 4 Right-click the profile you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Configuring Local Disk Configuration Policies

Local Disk Configuration Policy

This policy configures any optional SAS local drives that have been installed on a server through the onboard RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy. The local disk modes include the following:

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No Local Storage**—For a diskless workstation or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.

- **RAID Mirrored**—For a 2-disk RAID 1 server configuration.
- **RAID Stripes**—For a 2-disk RAID 0 server configuration.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

Creating a Local Disk Configuration Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Local Disk Config Policies** and select **Create Local Disk Configuration Policy**.

Step 5 In the **Create Local Disk Configuration Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used.
Mode drop-down list	This can be one of the following local disk policy modes: • **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes. • **No Local Storage**—For a diskless workstation or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk. • **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered. • **RAID Mirrored**—For a 2-disk RAID 1 server configuration. • **RAID Stripes**—For a 2-disk RAID 0 server configuration.

Name	Description
	Note If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences after you apply the **No RAID** mode. To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.

Step 6 Click **OK**.

Changing a Local Disk Configuration Policy

This procedure describes how to change a local disk configuration policy from an associated service profile. You can also change a local disk configuration policy from the **Policies** node of the **Servers** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Service Profiles**.

Step 3 Expand the organization that includes the service service profile with the local disk configuration policy you want to change.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Click the service profile that contains the local disk configuration policy you want to change.

Step 5 In the **Work** pane, click the **Policies** tab.

Step 6 In the **Actions** area, click **Change Local Disk Configuration Policy**.

Step 7 In the **Change Local Disk Configuration Policy** dialog box, choose one of the following options from the **Select the Local Disk Configuration Policy** drop-down list.

Option	Description
Use a Disk Policy	Select an existing local disk configuration policy from the list below this option. Cisco UCS Manager assigns this policy to the service profile.
Create a Local Disk Policy	Enables you to create a local disk configuration policy that can only be accessed by the selected service profile.

Option	Description
No Disk Policy	Does not use a local disk configuration policy for the selected service profile.

Step 8 Click **OK**.

Step 9 (Optional) Expand the **Local Disk Configuration Policy** area to confirm that the change has been made.

Deleting a Local Disk Configuration Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.

Step 3 Expand the **Local Disk Config Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Configuring Scrub Policies

Scrub Policy

This policy determines what happens to local data on a server during the discovery process and when the server is disassociated from a service profile. This policy can ensure that the data on local drives is erased at those times.

Creating a Scrub Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Scrub Policies** and select **Create Scrub Policy**.

Step 5 In the **Create Scrub Policy** wizard, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used.
Disk Scrub field	If this field is set to **yes**, when a service profile containing this scrub policy is associated with a server, the disks on that server are completely erased. If this field is set to **no**, the contents of the disks are preserved.
BIOS Settings Scrub field	If this field is set to **yes**, when a service profile containing this scrub policy is associated with a server, the BIOS settings on that server are reset to the defaults. If this field is set to **no**, the BIOS settings are preserved.

Step 6 Click **OK**.

Deleting a Scrub Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.

Step 3 Expand the **Scrub Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Configuring Serial over LAN Policies

Serial over LAN Policy

This policy sets the configuration for the serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

If you implement a serial over LAN policy, we recommend that you also create an IPMI profile.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating a Serial over LAN Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Serial over LAN Policies** and select **Create Serial over LAN Policy**.

Step 5 In the **Create Serial over LAN Policy** wizard, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used.
Admin State field	This can be: • **enabled** • **disabled**
Speed drop-down list	This can be: • **115200** • **19200** • **38400** • **57600** • **9600**

Step 6 Click **OK**.

Deleting a Serial over LAN Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.
Step 3 Expand the **Serial over LAN Policies** node.
Step 4 Right-click the policy you want to delete and select **Delete**.
Step 5 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Configuring Server Autoconfiguration Policies

Server Autoconfiguration Policy

This policy determines whether one or more of the following is automatically applied to a new server:

- A server pool policy qualification that qualifies the server for one or more server pools
- An organization
- A service profile template that associates the server with a service profile created from that template

Creating an Autoconfiguration Policy

Before You Begin

This policy requires that one or more of the following resources already exist in the system:

- Server pool policy qualifications
- Service profile template
- Organizations, if a system implements multi-tenancy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 Click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Autoconfig Policies** subtab.
Step 5 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 6 In the **Create Autoconfiguration Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used.
Qualification drop-down list	If you want to associate this policy with one or more specific server pools, choose the server pool qualification policy that identifies these pools from the drop-down list.
Org drop-down list	If you want to associate an organization with this policy, or if you want to change the current association, choose the desired organization from the drop-down list.
Service Profile Template Name drop-down list	The service profile template associated with this policy.

Step 7 Click **OK**.

Deleting an Autoconfiguration Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **Autoconfig Policies** subtab.

Step 5 Right-click the autoconfiguration policy that you want to delete and choose **Delete**.

Step 6 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Configuring Server Discovery Policies

Server Discovery Policy

This discovery policy determines how the system reacts when you add a new server. If you create a server discovery policy, you can control whether the system conducts a deep discovery when a server is added to a chassis, or whether a user must first acknowledge the new server. By default, the system conducts a full discovery.

With this policy, an inventory of the server is conducted, then server pool policy qualifications are run to determine whether the new server qualifies for one or more server pools.

Creating a Server Discovery Policy

Before You Begin

If you plan to associate this policy with a server pool, create server pool policy qualifications.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 Click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **Server Discovery Policies** subtab.

Step 5 Click the + icon on the table icon bar to open the **Create Server Discovery Policy** dialog box.

Step 6 In the **Description** field, enter a description for the discovery policy.

Step 7 In the **Action** field, select one of the following options:

- **immediate**—The system attempts to discover new servers automatically
- **user-acknowledged**—The system waits until the user tells it to search for new servers
- **diag**—Reserved for diagnostic use

Step 8 (Optional) To associate this policy with a server pool, select server pool policy qualifications from the **Qualification** drop-down list.

Step 9 (Optional) To include a scrub policy, select a policy from the **Scrub Policy** drop-down list.

Step 10 Click **OK**.

What to Do Next

Include the server discovery policy in a service profile and/or template.

Deleting a Server Discovery Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 Click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Server Discovery Policies** subtab.
Step 5 Right-click the server discover policy that you want to delete and choose **Delete**.
Step 6 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Configuring Server Inheritance Policies

Server Inheritance Policy

This policy is invoked during the server discovery process to create a service profile for the server. All service profiles created from this policy use the values burned into the blade at manufacture. The policy performs the following:

- Analyzes the inventory of the server
- If configured, assigns the server to the selected organization
- Creates a service profile for the server with the identity burned into the server at manufacture

You cannot migrate a service profile created with this policy to another server.

Creating a Server Inheritance Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 Click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Server Inheritance Policies** subtab.
Step 5 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.
Step 6 In the **Create Server Inheritance Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used.
Qualification drop-down list	If you want to associate this policy with one or more specific server pools, choose the server pool qualification policy that identifies these pools from the drop-down list.
Org drop-down list	If you want to associate an organization with this policy, or if you want to change the current association, choose the desired organization from the drop-down list.

Step 7 Click **OK**.

Deleting a Server Inheritance Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 Click the **Equipment** node.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the **Server Inheritance Policies** subtab.
Step 5 Right-click the server inheritance policy that you want to delete and choose **Delete**.
Step 6 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Configuring Server Pool Policies

Server Pool Policy

This policy is invoked during the server discovery process. It determines what happens if server pool policy qualifications match a server to the target pool specified in the policy.

If a server qualifies for more than one pool and those pools have server pool policies, the server is added to all those pools.

Creating a Server Pool Policy

Before You Begin

This policy requires that one or more of the following resources already exist in the system:

- A minimum of one server pool
- Server pool policy qualifications, if you choose to have servers automatically added to pools

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click **Server Pool Policies** and select **Create Server Pool Policy**.

Step 5 In the **Create Server Pool Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend including information about where and when the policy should be used.
Target Pool drop-down list	If you want to associate this policy with a server pool, select that pool from the drop-down list.
Qualification drop-down list	If you want to associate this policy with one or more specific server pools, choose the server pool qualification policy that identifies these pools from the drop-down list.

Step 6 Click **OK**.

Deleting a Server Pool Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.

Step 3 Expand the **Server Pool Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Configuring Server Pool Policy Qualifications

Server Pool Policy Qualifications

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

Depending upon the implementation, you may include server pool policy qualifications in the following policies:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

Creating Server Pool Policy Qualifications

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi-tenancy, expand the **root** node.

Step 4 Right-click the **Server Pool Policy Qualifications** node and select **Create Server Pool Policy Qualification**.

Step 5 In the **Create Server Pool Policy Qualification** dialog box, enter a unique name and description for the policy.

Step 6 (Optional) To use this policy to qualify servers according to their adapter configuration:

a) Click **Create Adapter Qualifications**.

b) In the **Create Adapter Qualifications** dialog box, complete the following fields:

Name	Description
Type drop-down list	Choose the adapter type from the drop-down list. This can be: • **fcoe**—Fibre Channel over Ethernet • **non-virtualized-eth-if** • **non-virtualized-fc-if** • **path-encap-consolidated** • **path-encap-virtual** • **protected-eth-if** • **protected-fc-if** • **protected-fcoe** • **virtualized-eth-if** • **virtualized-fc-if** • **virtualized-scsi-if**
Maximum Capacity field	Enter the maximum capacity for the selected type.

c) Click **OK**.

Step 7 (Optional) To use this policy to qualify servers according to their physical location:

a) Click **Create Chassis and Server Qualifications**.

b) In the **Create Chassis and Server Qualifications** dialog box, click **Add**.

c) In the first page of the **Create Server Qualifications** wizard, enter the range of server slot numbers where the server should be located in the **From** field and the **To** field, then click **Finish Stage**.

Example:
For example, if you want to include all servers in slots 3 through 5 in all chassis in the policy, enter 3 in the **From** field and 5 in the **To** field. However, if you want to include all servers in slots 3 and 5, enter 3 in the **From** field and 3 **To** field to create an entry for slot 3. You will need to create another server qualification entry for slot 5.

d) In the second page of the **Create Server Qualifications** wizard, enter the range of chassis numbers where the server should be located in the **From** field and the **To** field, then click **Finish**.

Example:

For example, if you want to include all servers in chassis 1 through 4 in the policy, enter 1 in the **From** field and 4 in the **To** field. However, if you want to include all servers in chassis 1 and 4, enter 1 in the **From** field and 1 **To** field to create an entry for chassis 1. You will need to create another server qualification entry for chassis 4.

Step 8 (Optional) To use this policy to qualify servers according to their memory configuration:

a) Click **Create Memory Qualifications**.

b) In the **Create Memory Qualifications** dialog box, complete the following fields:

Name	Description
Clock field	The minimum clock speed required, in megahertz.
Latency field	The maximum latency allowed, in nanoseconds.
Min Cap field	The minimum CPU capacity required, in megabytes.
Max Cap field	The maximum CPU capacity allowed, in megabytes.
Width field	The minimum width of the data bus.
Units field	The unit of measure to associate with the value in the **Width** field.

c) Click **OK**.

Step 9 (Optional) To use this policy to qualify servers according to their CPU/Cores configuration:

a) Click **Create CPU/Cores Qualifications**.

b) In the **Create CPU/Cores Qualifications** dialog box, complete the following fields:

Name	Description
Processor Architecture drop-down list	The CPU architecture to which this policy applies.
Min Number of Cores field	The minimum number of CPU cores required.
Max Number of Cores field	The maximum number of CPU cores allowed.
Min Number of Threads field	The minimum number of CPU threads required.
Max Number of Threads field	The maximum number of CPU threads allowed.
CPU Speed field	The minimum CPU speed required.
CPU Stepping field	The minimum CPU version required.

c) Click **OK**.

Step 10 (Optional) To use this policy to qualify servers according to their storage configuration and capacity:

a) Click **Create Storage Qualifications**.

b) In the **Create Storage Qualifications** dialog box, complete the following fields:

Name	Description
Number of Blocks field	The minimum number of blocks required.
Block Size field	The minimum block size required, in bytes.
Min Cap field	The minimum storage capacity required, in megabytes.
Max Cap field	The maximum storage capacity allowed, in megabytes.
Per Disk Cap field	The minimum storage capacity per disk required, in gigabytes.
Units field	The number of units.

c) Click **OK**.

Step 11 Verify the qualifications in the table and correct if necessary.

Step 12 Click **OK**.

Deleting Server Pool Policy Qualifications

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.

Step 3 Expand the **Server Pool Policy Qualifications** node.

Step 4 Right-click the policy qualifications you want to delete and select **Delete**.

Step 5 If Cisco UCS Manager displays a confirmation dialog box, click **Yes**.

Deleting Qualifications from Server Pool Policy Qualifications

Use this procedure to modify Server Pool Policy Qualifications by deleting one or more sets of qualifications.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers ➤ Policies ➤ *Organization_Name***.

Step 3 Expand the **Server Pool Policy Qualifications** node.

Step 4 Choose the policy you want to modify.

Step 5 In the **Work** pane, choose the **Qualifications** tab.

Step 6 To delete a set of qualifications:

a) In the table, choose the row that represents the set of qualifications.

b) Right-click the row and select **Delete**.

Step 7 Click **Save Changes**.