



# Configuring Storage-Related Policies

---

This chapter includes the following sections:

- [Configuring vHBA Templates, page 1](#)
- [Configuring Fibre Channel Adapter Policies, page 4](#)

## Configuring vHBA Templates

### vHBA Template

This template is a policy that defines how a vHBA on a server connects to the SAN. It is also referred to as a vHBA SAN connectivity template.

You need to include this policy in a service profile for it to take effect.

### Creating a vHBA Template

#### Before You Begin

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

- Named VSAN
- WWNN pool or WWPN pool
- SAN pin group
- Statistics threshold policy

#### Procedure

---

- Step 1** In the **Navigation** pane, click the **SAN** tab.
- Step 2** On the **SAN** tab, expand **SAN ► 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 **vHBA Templates** node and choose **Create vHBA Template**.

**Step 5** In the **Create vHBA Template** dialog box, complete the following fields:

Name	Description
Name field	The name of the virtual HBA template. 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 user-defined description of the template.
Fabric ID field	The name of the fabric interconnect that vHBAs created with this template are associated with.
Select VSAN drop-down list	The VSAN to associate with vHBAs created from this template.
Create VSAN link	Click this link if you want to create a VSAN.
Template Type field	This can be: <ul style="list-style-type: none"> <li>• <b>Initial Template</b>—vHBAs created from this template are not updated if the template changes.</li> <li>• <b>Updating Template</b>—vHBAs created from this template are updated if the template changes.</li> </ul>
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.
WWN Pool drop-down list	The WWN pool that a vHBA created from this template uses to derive its WWN address.
QoS Policy drop-down list	The QoS policy that is associated with vHBAs created from this template.
Pin Group drop-down list	The LAN pin group that is associated with vHBAs created from this template.
Stats Threshold Policy drop-down list	The statistics collection policy that is associated with vHBAs created from this template.

**Step 6** Click **OK**.

### What to Do Next

Include the vHBA template in a service profile.

## Deleting a vHBA Template

### Procedure

---

- Step 1** In the **Navigation** pane, click the **SAN** tab.
  - Step 2** On the **SAN** tab, expand **SAN > Policies > Organization\_Name**.
  - Step 3** Expand the **vHBA Templates** node.
  - Step 4** Right-click the vHBA template that you want to delete and choose **Delete**.
  - Step 5** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
- 

## Binding a vHBA to a vHBA Template

You can bind a vHBA associated with a service profile to a vHBA template. When you bind the vHBA to a vHBA template, Cisco UCS Manager configures the vHBA with the values defined in the vHBA template. If the existing vHBA configuration does not match the vHBA template, Cisco UCS Manager reconfigures the vHBA. You can only change the configuration of a bound vHBA through the associated vHBA template. You cannot bind a vHBA to a vHBA template if the service profile that includes the vHBA is already bound to a service profile template.



---

**Important** If the vHBA is reconfigured when you bind it to a template, Cisco UCS Manager reboots the server associated with the service profile.

---

### 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 node for the organization that includes the service profile with the vHBA you want to bind. If the system does not include multi-tenancy, expand the **root** node.
  - Step 4** Expand **Service\_Profile\_Name > vHBAs**.
  - Step 5** Click the vHBA you want to bind to a template.
  - Step 6** In the **Work** pane, click the **General** tab.
  - Step 7** In the **Actions** area, click **Bind to a Template**.
  - Step 8** In the **Bind to a vHBA Template** dialog box, do the following:
    - a) From the **vHBA Template** drop-down list, choose the template to which you want to bind the vHBA.
    - b) Click **OK**.
  - Step 9** In the warning dialog box, click **Yes** to acknowledge that Cisco UCS Manager may need to reboot the server if the binding causes the vHBA to be reconfigured.
-

## Unbinding a vHBA from a vHBA Template

### 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 node for the organization that includes the service profile with the vHBA you want to unbind. If the system does not include multi-tenancy, expand the **root** node.
- Step 4** Expand *Service\_Profile\_Name* ► **vHBAs**.
- Step 5** Click the vHBA you want to unbind from a template.
- Step 6** In the **Work** pane, click the **General** tab.
- Step 7** In the **Actions** area, click **Unbind from a Template**.
- Step 8** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
- 

## Configuring Fibre Channel Adapter Policies

### Ethernet and Fibre Channel Adapter Policies

These policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

**Note**

For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.

### Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

**Important**

We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), you must use the following formulas to calculate values that work with Windows:

$$\text{Completion Queues} = \text{Transmit Queues} + \text{Receive Queues}$$
$$\text{Interrupt Count} = (\text{Completion Queues} + 2) \text{ rounded up to nearest power of } 2$$

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

$$\text{Completion Queues} = 1 + 8 = 9$$
$$\text{Interrupt Count} = (9 + 2) \text{ rounded up to the nearest power of } 2 = 16$$

## Creating a Fibre Channel Adapter Policy

**Tip**

If the fields in an area are not displayed, click the **Expand** icon to the right of the heading.

## 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 **Fibre Channel Policies** and choose **Create Fibre Channel Adapter Policy**.
- Step 5** Enter a name and description for the policy in 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.

- Step 6** (Optional) In the **Resources** area, adjust the following values:

Name	Description
Transmit Queues field	The number of transmit queue resources to allocate.  This value cannot be changed.
Ring Size field	The number of descriptors in each transmit queue.  Enter an integer between 64 and 128.
Receive Queues field	The number of receive queue resources to allocate.  This value cannot be changed.
Ring Size field	The number of descriptors in each receive queue.  Enter an integer between 64 and 128.
SCSI I/O Queues field	The number of SCSI IO queue resources the system should allocate.  Enter an integer between 1 and 8.  <b>Note</b> At this time, the Cisco M81KR VIC adapter only supports one SCSI I/O queue.
Ring Size field	The number of descriptors in each SCSI I/O queue.  Enter an integer between 64 and 512.

- Step 7** (Optional) In the **Options** area, adjust the following values:

Name	Description
<b>FCP Error Recovery</b> field	<p>Whether the system uses FCP Sequence Level Error Recovery protocol (FC-TAPE). This can be:</p> <ul style="list-style-type: none"> <li>• <b>disabled</b></li> <li>• <b>enabled</b></li> </ul> <p><b>Note</b> This option only applies to a server with the Cisco M81KR VIC adapter running Windows or Linux.</p>
<b>Flogi Retries</b> field	<p>The number of times that the system tries to log in to the fabric after the first failure.</p> <p>Enter any integer. To specify that the system continue to try indefinitely, enter infinite or -1 in this field.</p> <p><b>Note</b> This option only applies to a server with the Cisco M81KR VIC adapter running Windows.</p>
<b>Flogi Timeout</b> field	<p>The number of milliseconds that the system waits before it tries to log in again.</p> <p>Enter an integer between 1000 and 255000.</p> <p><b>Note</b> This option only applies to a server with the Cisco M81KR VIC adapter running Windows.</p>
<b>Plogi Retries</b> field	<p>The number of times that the system tries to log into a port after the first failure.</p> <p>Enter an integer between 0 and 255.</p> <p><b>Note</b> This option only applies to a server with the Cisco M81KR VIC adapter running Windows or Linux.</p>
<b>Plogi Timeout</b> field	<p>The number of milliseconds that the system waits before it tries to log in again.</p> <p>Enter an integer between 1000 and 255000.</p> <p><b>Note</b> This option only applies to a server with the Cisco M81KR VIC adapter running Windows.</p>
<b>Error Detect Timeout</b> field	<p>The number of milliseconds to wait before the system assumes that an error has occurred.</p> <p>This value cannot be changed.</p>
<b>Port Down Timeout</b> field	<p>The number of milliseconds a remote Fibre Channel port should be offline before informing the SCSI upper layer that the port is unavailable.</p> <p>Enter an integer between 0 and 240000.</p> <p><b>Tip</b> For to a server with the Cisco M81KR VIC adapter running the ESX host, the recommended value is 10000.</p>
<b>Port Down IO Retry</b> field	<p>The number of times an IO request to a port is returned because the port is busy before the system decides the port is unavailable.</p>

Name	Description
	Enter an integer between 0 and 255. <b>Note</b> This option only applies to a server with the Cisco M81KR VIC adapter running Windows.
<b>Link Down Timeout</b> field	The number of milliseconds the uplink port should be offline before it informs the system that the uplink port is down and fabric connectivity has been lost. Enter an integer between 0 and 240000. <b>Note</b> This option only applies to a server with the Cisco M81KR VIC adapter running Windows.
<b>Resource Allocation Timeout</b> field	The number of milliseconds to wait before the system assumes that a resource cannot be properly allocated. This value cannot be changed.
<b>IO Throttle Count</b> field	The number of I/O operations that can be pending in the vHBA at one time. Enter an integer between 1 and 1024. <b>Note</b> This option only applies to a server with the Cisco M81KR VIC adapter running Windows.
<b>Max LUNs Per Target</b> field	The maximum number of LUNs that the driver will export. This is usually an operating system platform limitation. Enter an integer between 1 and 1024. The recommended value is 1024. <b>Note</b> This option only applies to a server with the Cisco M81KR VIC adapter running Linux or ESX host.
<b>Interrupt Mode</b> field	The preferred driver interrupt mode. This can be: <ul style="list-style-type: none"> <li>• <b>MSI-X</b>—Message Signaled Interrupts(MSI) with the optional extension. This is the recommended option.</li> <li>• <b>MSI</b>—MSI only.</li> <li>• <b>INTx</b>—PCI INTx interrupts.</li> </ul> <b>Note</b> This option is not used by the Cisco M81KR VIC adapter.

**Step 8** Click **OK**.

**Step 9** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.



## Deleting a Fibre Channel Adapter Policy

### Procedure

---

- Step 1** In the **Navigation** pane, click the **SAN** tab.
  - Step 2** On the **SAN** tab, expand **SAN ► Policies ► *Organization\_Name***.
  - Step 3** Expand the **Fibre Channel Policies** node.
  - Step 4** Right-click the policy you want to delete and choose **Delete**.
  - Step 5** If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

