



Configuring Storage-Related Policies

This chapter includes the following sections:

- [Configuring vHBA Templates, page 1](#)
- [Configuring Fibre Channel Adapter Policies, page 5](#)
- [Configuring the Default vHBA Behavior Policy, page 11](#)
- [Configuring SAN Connectivity Policies, page 12](#)

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 must 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 multitenancy, 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 other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Description field	A user-defined description of the template. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
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 one of the following: <ul style="list-style-type: none"> • Initial Template—vHBAs created from this template are not updated if the template changes. • Updating Template—vHBAs created from this template are updated if the template changes.
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.
WWPN Pool drop-down list	The WWPN pool that a vHBA created from this template uses to derive its WWPN address.
QoS Policy drop-down list	The QoS policy that is associated with vHBAs created from this template.

Name	Description
Pin Group drop-down list	The SAN 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.

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 the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

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 the 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 multitenancy, 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	<p>The name of the policy.</p> <p>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.</p>
Description field	<p>A description of the policy. We recommend that you include information about where and when the policy should be used.</p> <p>Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).</p>

Name	Description
Owner field	This can be one of the following: <ul style="list-style-type: none"> • Local—This policy is available only to service profiles and service profile templates in this Cisco UCS domain. • Pending Global—Control of this policy is being transferred to Cisco UCS Central. Once the transfer is complete, this policy will be available to all Cisco UCS domains registered with Cisco UCS Central. • Global—This policy is managed by Cisco UCS Central. Any changes to this policy must be made through Cisco UCS Central.

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. This parameter applies to Extended Link Services (ELS) and Common Transport (CT) fibre channel frames for generic services. It does not affect adapter performance. Enter an integer between 64 and 128. The default is 64.
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. This parameter applies to Extended Link Services (ELS) and Common Transport (CT) fibre channel frames for generic services. It does not affect adapter performance. Enter an integer between 64 and 128. The default is 64.
SCSI I/O Queues field	The number of SCSI IO queue resources the system should allocate. Enter an integer between 1 and 8. The default is 1. Note At this time, the Cisco UCS M81KR Virtual Interface Card adapter supports only 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. The default is 512. Note The number of descriptors can affect the performance of the adapter, so we recommend that you do not change the default value.

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

Name	Description
FCP Error Recovery field	<p>Whether the system uses FCP Sequence Level Error Recovery (FC-TAPE) protocol for sequence level error recovery with tape devices. This enables or disables the Read Exchange Concise (REC) and Sequence Retransmission Request (SRR) functions on the VIC firmware. This can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—This is the default. • Enabled—You should select this option if your system is connected to one or more tape drive libraries. <p>Note This parameter only applies to a server with a Virtual Interface Card (VIC) adapter, such as the Cisco UCS M81KR Virtual Interface Card.</p>
Flogi Retries 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 in this field. We recommend you consult your storage array documentation for the optimal value for this parameter.</p> <p>Note This parameter only applies to a server with a VIC adapter, or a converged network adapter such as the Cisco UCS M71KR-E Emulex Converged Network Adapter.</p>
Flogi Timeout 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. The default is 4,000. We recommend you consult your storage array documentation for the optimal value for this parameter.</p> <p>Note This parameter only applies to a server with a VIC adapter or a converged network adapter.</p>
Plogi Retries 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. The default is 8. We recommend you consult your storage array documentation for the optimal value for this parameter.</p> <p>Note This parameter only applies to a server with a VIC adapter.</p>

Name	Description
Plogi Timeout 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. The default is 20,000. We recommend you consult your storage array documentation for the optimal value for this parameter.</p> <p>Note This parameter only applies to a server with a VIC adapter.</p>
Error Detect Timeout 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>
Port Down Timeout 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. This parameter is important for host multi-pathing drivers and it is one of the key indicators used for error processing.</p> <p>Enter an integer between 0 and 240000. The default is 30,000. For a server with a VIC adapter running ESX, the recommended value is 10,000.</p> <p>We recommend you consult your storage array documentation for the optimal value for this parameter.</p> <p>Note This parameter only applies to a server with a VIC adapter.</p>
Port Down IO Retry 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> <p>Enter an integer between 0 and 255. The default is 8. We recommend you consult your storage array documentation for the optimal value for this parameter.</p> <p>Note This parameter only applies to a server with a VIC adapter running Windows.</p>
Link Down Timeout field	<p>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.</p> <p>Enter an integer between 0 and 240000. The default is 30,000. We recommend you consult your storage array documentation for the optimal value for this parameter.</p> <p>Note This parameter only applies to a server with a VIC adapter running Windows.</p>
Resource Allocation Timeout field	<p>The number of milliseconds to wait before the system assumes that a resource cannot be properly allocated.</p> <p>This value cannot be changed.</p>

Name	Description
IO Throttle Count field	<p>The maximum number of data or control I/O operations that can be pending in the vHBA at one time. If this value is exceeded, the additional I/O operations wait in the queue until the number of pending I/O operations decreases and the additional operations can be processed.</p> <p>Note This parameter is not the same as the LUN queue depth, which is controlled by Cisco UCS Manager based on the operating system installed on the server.</p> <p>Enter an integer between 1 and 1024. The default is 16. We recommend you consult your storage array documentation for the optimal value for this parameter.</p>
Max LUNs Per Target field	<p>The maximum number of LUNs that the Fibre Channel driver will export or show. The maximum number of LUNs is usually controlled by the operating system running on the server.</p> <p>Enter an integer between 1 and 1024. The default value is 256. For servers running ESX or Linux, the recommended value is 1024.</p> <p>We recommend you consult your operating system documentation for the optimal value for this parameter.</p> <p>Note This parameter only applies to a server with a VIC adapter or a network adapter.</p>
Interrupt Mode field	<p>The method used to send interrupts to the operating system from the driver. This can be one of the following:</p> <ul style="list-style-type: none"> • MSI-X—Message Signaled Interrupts (MSI) with the optional extension. We recommend that you select this option if the operating system on the server supports it. • MSI—MSI only. • INTx—PCI INTx interrupts. <p>Note This parameter only applies to a server with a VIC adapter or a network adapter running an operating system other than Windows. The Windows operating system ignores this parameter.</p>

Step 8 Click **OK**.

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

Configuring the Default vHBA Behavior Policy

Default vHBA Behavior Policy

Default vHBA behavior policy allow you to configure how vHBAs are created for a service profile. You can choose to create vHBAs manually, or you can allow them to be created automatically.

You can configure the default vHBA behavior policy to define how vHBAs are created. This can be one of the following:

- **None**—Cisco UCS Manager does not create default vHBAs for a service profile. All vHBAs must be explicitly created.
- **HW Inherit**—If a service profile requires vHBAs and none have been explicitly defined, Cisco UCS Manager creates the required vHBAs based on the adapter installed in the server associated with the service profile.



Note If you do not specify a default behavior policy for vHBAs, **none** is used by default.

Configuring a Default vHBA Behavior 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 **root** node.
You can configure only the default vHBA behavior policy in the root organization. You cannot configure the default vHBA behavior policy in a sub-organization.

Step 4 Click **Default vHBA Behavior**.

Step 5 On the **General Tab**, in the **Properties** area, click one of the following radio buttons in the **Action** field:

- **None**—Cisco UCS Manager does not create default vHBAs for a service profile. All vHBAs must be explicitly created.
- **HW Inherit**—If a service profile requires vHBAs and none have been explicitly defined, Cisco UCS Manager creates the required vHBAs based on the adapter installed in the server associated with the service profile.

Step 6 Click **Save Changes**.

Configuring SAN Connectivity Policies

LAN and SAN Connectivity Policies

Connectivity policies determine the connections and the network communication resources between the server and the LAN or SAN on the network. These policies use pools to assign MAC addresses, WWNs, and WWPNS to servers and to identify the vNICs and vHBAs that the servers use to communicate with the network.



Note

We do not recommend that you use static IDs in connectivity policies, because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

Privileges Required for LAN and SAN Connectivity Policies

Connectivity policies enable users without network or storage privileges to create and modify service profiles and service profile templates with network and storage connections. However, users must have the appropriate network and storage privileges to create connectivity policies.

Privileges Required to Create Connectivity Policies

Connectivity policies require the same privileges as other network and storage configurations. For example, you must have at least one of the following privileges to create connectivity policies:

- **admin**—Can create LAN and SAN connectivity policies
- **ls-server**—Can create LAN and SAN connectivity policies
- **ls-network**—Can create LAN connectivity policies
- **ls-storage**—Can create SAN connectivity policies

Privileges Required to Add Connectivity Policies to Service Profiles

After the connectivity policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create connectivity policies.

Interactions between Service Profiles and Connectivity Policies

You can configure the LAN and SAN connectivity for a service profile through either of the following methods:

- LAN and SAN connectivity policies that are referenced in the service profile
- Local vNICs and vHBAs that are created in the service profile
- Local vNICs and a SAN connectivity policy
- Local vHBAs and a LAN connectivity policy

Cisco UCS maintains mutual exclusivity between connectivity policies and local vNIC and vHBA configuration in the service profile. You cannot have a combination of connectivity policies and locally created vNICs or vHBAs. When you include a LAN connectivity policy in a service profile, all existing vNIC configuration is erased, and when you include a SAN connectivity policy, all existing vHBA configuration in that service profile is erased.

Creating a SAN Connectivity 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 multitenancy, expand the **root** node.
- Step 4** Right-click **SAN Connectivity Policies** and choose **Create SAN Connectivity Policy**.
- Step 5** In the **Create SAN Connectivity Policy** dialog box, enter a name and description for the policy in the following fields:

Name	Description
Name field	<p>The name of the policy.</p> <p>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.</p>

Name	Description
Description field	<p>A description of the policy. We recommend that you include information about where and when the policy should be used.</p> <p>Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).</p>
Owner field	<p>This can be one of the following:</p> <ul style="list-style-type: none"> • Local—This policy is available only to service profiles and service profile templates in this Cisco UCS domain. • Pending Global—Control of this policy is being transferred to Cisco UCS Central. Once the transfer is complete, this policy will be available to all Cisco UCS domains registered with Cisco UCS Central. • Global—This policy is managed by Cisco UCS Central. Any changes to this policy must be made through Cisco UCS Central.

Step 6 From the **WWNN Assignment** drop-down list in the **World Wide Node Name** area, choose one of the following:

- Choose **Select (pool default used by default)** to use the default WWN pool.
- Choose one of the options listed under **Manual Using OUI** and then enter the WWN in the **World Wide Node Name** field.

You can specify a WWNN in the range from 20:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF. You can click the **here** link to verify that the WWNN you specified is available.

- Choose a WWN pool name from the list to have a WWN assigned from the specified pool. Each pool name is followed by two numbers in parentheses that show the number of WWNs still available in the pool and the total number of WWNs in the pool.

Step 7 In the **vHBAs** table, click + on the table icon bar and complete the following fields in the **Create vHBA** dialog box:

- a) Complete the following fields to specify the identity information for the vHBA:

Name	Description
Name field	<p>The name of this vHBA.</p> <p>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.</p>

Name	Description
Use vHBA Template check box	<p>Check this check box if you want to use a template to create the vHBA. The Cisco UCS Manager GUI displays the vHBA Template drop-down list from which you can choose the appropriate template and the Adapter Performance Profile area from which you can choose an adapter profile.</p> <p>Note You can choose this option only if one or more vHBA templates exist in the system.</p>
Create vHBA Template link	Click this link if you want to create a vHBA template.
WWPN Assignment drop-down list	<p>How Cisco UCS assigns the World Wide Port Node to the vHBA. If you want Cisco UCS to:</p> <ul style="list-style-type: none"> • Use the default WWPN pool, leave this field set to Select (pool default used by default). • Use the WWPN assigned to the server by the manufacturer, select Derived. • Use a specific WWPN, select 20:00:00:25:B5:00:00:00, 20:XX:XX:XX:XX:XX:XX:XX, or 5X:XX:XX:XX:XX:XX:XX:XX and enter the WWPN in the WWPN field. <p>If you want the WWPN to be compatible with Cisco MDS Fibre Channel switches, use the WWPN template 20:00:00:25:B5:XX:XX:XX.</p> <ul style="list-style-type: none"> • Use a WWPN from a pool, choose the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available addresses in the pool and the second is the total number of addresses in the pool. <p>If this Cisco UCS domain is registered with Cisco UCS Central, there may be two pool categories. Domain Pools are defined locally in the Cisco UCS domain and Global Pools are defined in Cisco UCS Central.</p>
Create WWPN Pool link	Click this link if you want to create a new WWPN pool that will be available to all objects in the Cisco UCS domain.
WWPN field	<p>The manually-assigned WWPN if the WWPN Assignment drop-down list is set to one of the manual templates.</p> <p>You can specify a WWPN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF.</p> <p>To make sure the WWPN is available, click the corresponding link.</p>

b) In the **VSAN** area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component.
Select VSAN drop-down list box	The VSAN with which this vHBA is associated.
Create VSAN link	Click this link if you want to create a VSAN.
Pin Group drop-down list box	The SAN pin group with which this vHBA is associated.
Create SAN Pin Group link	Click this link if you want to create a pin group.
Persistent Binding field	This can be one of the following: <ul style="list-style-type: none"> • Disabled • Enabled
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.
Operational Parameters Section	
Stats Threshold Policy drop-down list box	The statistics threshold policy with which this vHBA is associated.

c) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list box	The Fibre Channel adapter policy with which this vHBA is associated.
Create Fibre Channel Adapter Policy link	Click this link if you want to create a Fibre Channel adapter policy.
QoS drop-down list box	The quality of service policy with which this vHBA is associated.
Create QoS Policy link	Click this link if you want to create a QoS policy.

d) Click **OK**.

Step 8 After you have created all the vHBAs you need for the policy, click **OK**.

What to Do Next

Include the policy in a service profile or service profile template.

Creating a vHBA for a SAN Connectivity 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** Choose the policy for which you want to create a vHBA.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** In the table icon bar, click the + button.
- Step 6** In the **Create vHBA** dialog box, do the following:
- a) Complete the following fields to specify the identity information for the vHBA:

Name	Description
Name field	<p>The name of this vHBA.</p> <p>This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.</p>
Use vHBA Template check box	<p>Check this check box if you want to use a template to create the vHBA. The Cisco UCS Manager GUI displays the vHBA Template drop-down list from which you can choose the appropriate template and the Adapter Performance Profile area from which you can choose an adapter profile.</p> <p>Note You can choose this option only if one or more vHBA templates exist in the system.</p>
Create vHBA Template link	Click this link if you want to create a vHBA template.

Name	Description
WWPN Assignment drop-down list	<p>How Cisco UCS assigns the World Wide Port Node to the vHBA. If you want Cisco UCS to:</p> <ul style="list-style-type: none"> Use the default WWPN pool, leave this field set to Select (pool default used by default). Use the WWPN assigned to the server by the manufacturer, select Derived. Use a specific WWPN, select 20:00:00:25:B5:00:00:00, 20:XX:XX:XX:XX:XX:XX:XX, or 5X:XX:XX:XX:XX:XX:XX:XX and enter the WWPN in the WWPN field. <p>If you want the WWPN to be compatible with Cisco MDS Fibre Channel switches, use the WWPN template 20:00:00:25:B5:XX:XX:XX.</p> <ul style="list-style-type: none"> Use a WWPN from a pool, choose the pool name from the list. Each pool name is followed by a pair of numbers in parentheses. The first number is the number of available addresses in the pool and the second is the total number of addresses in the pool. <p>If this Cisco UCS domain is registered with Cisco UCS Central, there may be two pool categories. Domain Pools are defined locally in the Cisco UCS domain and Global Pools are defined in Cisco UCS Central.</p>
Create WWPN Pool link	Click this link if you want to create a new WWPN pool that will be available to all objects in the Cisco UCS domain.
WWPN field	<p>The manually-assigned WWPN if the WWPN Assignment drop-down list is set to one of the manual templates.</p> <p>You can specify a WWPN in the range from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF.</p> <p>To make sure the WWPN is available, click the corresponding link.</p>

b) In the VSAN area, complete the following fields:

Name	Description
Fabric ID field	The fabric interconnect associated with the component.
Select VSAN drop-down list box	The VSAN with which this vHBA is associated.
Create VSAN link	Click this link if you want to create a VSAN.
Pin Group drop-down list box	The SAN pin group with which this vHBA is associated.

Name	Description
Create SAN Pin Group link	Click this link if you want to create a pin group.
Persistent Binding field	This can be one of the following: <ul style="list-style-type: none"> • Disabled • Enabled
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.
Operational Parameters Section	
Stats Threshold Policy drop-down list box	The statistics threshold policy with which this vHBA is associated.

- c) In the **Adapter Performance Profile** area, complete the following fields:

Name	Description
Adapter Policy drop-down list box	The Fibre Channel adapter policy with which this vHBA is associated.
Create Fibre Channel Adapter Policy link	Click this link if you want to create a Fibre Channel adapter policy.
QoS drop-down list box	The quality of service policy with which this vHBA is associated.
Create QoS Policy link	Click this link if you want to create a QoS policy.

- d) Click **OK**.

Step 7 Click **Save Changes**.

Deleting a vHBA from a SAN Connectivity 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** Choose the policy from which you want to delete the vHBA.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** In the **vHBAs** table, do the following:
- Click the vHBA that you want to delete.
 - On the icon bar, click **Delete**.
- Step 6** If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Creating an Initiator Group for a SAN Connectivity 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** Choose the policy for which you want to create an initiator group.
- Step 4** In the **Work** pane, click the **vHBA Initiator Groups** tab.
- Step 5** In the table icon bar, click the + button.
- Step 6** In the **Create vHBA Initiator Group** dialog box, complete the following fields:

Name	Description
Name field	The name of the vHBA initiator group. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Description field	A description of the group. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Select vHBA Initiators table	Check the check box in the Select column for each vHBA that you want to use.

Name	Description
Storage Connection Policy drop-down list	<p>The storage connection policy associated with this vHBA initiator group. If you want to:</p> <ul style="list-style-type: none"> • Use an existing storage connection policy, then choose that policy from the drop-down list. The Cisco UCS Manager GUI displays information about the policy and its FC target endpoints in the Global Storage Connection Policy area. <p>Create a new storage connection policy that will be globally available, then click the Create Storage Connection Policy link.</p> <ul style="list-style-type: none"> • Create a local storage connection policy that is available only to this vHBA initiator group, then choose the Specific Storage Connection Policy option. The Cisco UCS Manager GUI displays the Specific Storage Connection Policy area that allows you to configure the local storage connection policy.
Create Storage Connection Policy link	<p>Click this link to create a new storage connection policy that will be available to all service profiles and service profile templates.</p>

Step 7 Click **OK**.

Deleting an Initiator Group from a SAN Connectivity 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** Choose the policy from which you want to delete the initiator group.
- Step 4** In the **Work** pane, click the **vHBA Initiator Groups** tab.
- Step 5** In the table, do the following:
- Click the initiator group that you want to delete.
 - On the icon bar, click **Delete**.
- Step 6** If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-

Deleting a SAN Connectivity Policy

If you delete a SAN connectivity policy that is included in a service profile, you will delete all vHBAs from that service profile and disrupt SAN data traffic for the server associated with the service profile.

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 **SAN Connectivity Policies** node.
 - Step 4** Right-click the policy that you want to delete and choose **Delete**.
 - Step 5** If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
-