Configuring Storage Connections

This chapter contains the following sections:

VSANs

In Cisco UCS, a VSAN, also known as a named VSAN, creates a connection to a specific external SAN. The VSAN isolates traffic to that external SAN, including broadcast traffic. The traffic on one VSAN knows that the traffic on another VSAN exists but cannot read or access that traffic.

The name that you assign to a VSAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the VSAN. You do not need to reconfigure the servers individually to maintain communication with the external SAN. You can create more than one named VSAN with the same VSAN ID.

For more information about VSANs in Cisco UCS, including guidelines and recommendations, see the Cisco UCS Manager configuration guides.

Named VSANs in Cluster Configurations

In a cluster configuration, a VSAN can be configured to be accessible only to the Fibre Channel uplink ports on one fabric interconnect or to the Fibre Channel uplink ports on both fabric interconnects.

Named VSANs and the FCoE VLAN ID

Configure each VSAN with an FCoE VLAN ID. This property determines which VLAN is used for transporting the VSAN and its Fibre Channel packets.

For FIP-capable, converged network adapters, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the VSAN must be configured with a VLAN that is not the native VLAN for the FCoE VLAN ID. This configuration ensures that FCoE traffic can pass through these adapters.

In the following sample configuration, a service profile with a vNIC and vHBA mapped to fabric A is associated with a server that has FIP capable, converged network adapters:

- The vNIC is configured to use VLAN 10.

- VLAN 10 is also designated as the native VLAN for the vNIC.

- The vHBA is configured to use VSAN 2.

- Therefore, VSAN 2 cannot be configured with VLAN 10 as the FCoE VLAN ID. VSAN 2 can be mapped to any other VLAN configured on fabric A.

Creating a VSAN

Note Fibre Channel over Ethernet (FCoE) VLANs in the SAN cloud and VLANs in the LAN cloud must have different IDs. Using the same ID for an FCoE VLAN in a VSAN and a VLAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that FCoE VLAN. Ethernet traffic is dropped on any VLAN that has an ID that overlaps with an FCoE VLAN ID.

Step 1 On the menu bar, choose **Physical** > **Compute**.

Step 2 In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3 In the right pane, click the **VSANs** tab.

Step 4 Click **Add**.

Step 5 In the **Add VSAN** dialog box, complete the following fields:

Name	Description
VSAN Name field	A unique name for the VSAN.
VSAN ID field	The unique identifier assigned to the network.
Type drop-down list	Choose the type of VSAN. This can be one of the following: • **SAN Cloud** • **Storage Cloud** If you are creating a VSAN for Fibre Channel zoning, we recommend that you choose **Storage Cloud**.

Name	Description
Fabric ID drop-down list	Choose how to configure the VSAN. This can be one of the following: • **Common/Global**—The VSAN maps to the same VSAN ID in all available fabrics. • **Fabric A**—The VSAN maps to a VSAN ID that exists only in fabric A. • **Fabric B**—The VSAN maps to a VSAN ID that exists only in fabric B.
FCoE VLAN field	The unique identifier assigned to the VLAN used for Fibre Channel connections. For FCoE Initialization Protocol (FIP)-capable, converged network adapters, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the named VSAN must be configured with a named VLAN that is not the native VLAN for the FCoE VLAN ID. This configuration ensures that FCoE traffic can pass through these adapters.

Step 6   Click **Submit**.

What to Do Next

If you plan to use this VSAN for Fibre Channel zoning, see Configuring a VSAN for Fibre Channel Zoning, on page 19.

WWN Pools

WWNN Pools

A WWNN (World Wide Node Name) pool is a WWN (World Wide Name) pool that contains only WW (World Wide) node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool. You can view the WWN blocks and initiators in a WWNN pool by double-clicking the pool in the **WWNN Pools** tab.

Creating a WWNN Pool

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **Organizations** tab.

Step 4   Click the organization in which you want to create the pool and then click **View Details**.

Step 5   Click the **WWNN Pools** tab.

Step 6   Click **Add**.

Step 7   In the **Add WWNN Pool** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the pool.
Description field	A description for the pool.
From field	The first WWNN address in the block.
Size field	The number of WWNN addresses in the block.

Step 8   Click **Submit**.

Adding an Initiator to a WWNN Pool

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **Organizations** tab.

Step 4   Click the organization in which you want to modify the pool and then click **View Details**.

Step 5   Click the **WWNN Pools** tab.

Step 6   Click the pool to which you want to add an initiator.

Step 7   Click **Create WWNN Initiator**.

Step 8   In the **Create WWNN Initiator** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the initiator.
Description field	A description for the initiator.

Name	Description
World Wide Name field	The WWN for the initiator.

Step 9   Click **Submit**.

WWPN Pools

A WWPN (World Wide Port Name) pool is a WWN pool that contains only WW port names. If you include a pool of WWPNs in a service profile, the port on each vHBA of the associated server is assigned a WWPN from that pool. You can view the WWN blocks and initiators in a WWPN pool by double-clicking the pool in the **WWPN Pools** tab.

Creating a WWPN Pool

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **Organizations** tab.

Step 4   Click the organization in which you want to create the pool and then click **View Details**.

Step 5   Click the **WWPN Pools** tab.

Step 6   Click **Add**.

Step 7   In the **Add WWPN Pool** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the pool.
Description field	A description for the pool.
From field	The first WWPN address in the block.
Size field	The number of WWPN addresses in the block.

Step 8   Click **Submit**.

Adding an Initiator to a WWPN Pool

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **Organizations** tab.

Step 4   Click the organization in which you want to modify the pool and then click **View Details**.

Step 5   Click the **WWPN Pools** tab.

Step 6   Click the pool to which you want to add an initiator.

Step 7   Click **Create WWPN Initiator**.

Step 8   In the **Create WWPN Initiator** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the initiator.
Description field	A description for the initiator.
World Wide Name field	The WWN for the initiator.

Step 9   Click **Submit**.

Adding a WWN Block

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **Organizations** tab.

Step 4   Click the organization in which you want to modify the pool and then click **View Details**.

Step 5   Click one of the following tabs:

- **WWNN Pools** tab

- **WWPN Pools** tab

Step 6   Click the pool to which you want to add a WWN block.

Step 7   Click **Create WWN Block**.

Step 8   In the **Create WWN Block** dialog box, complete the following fields:

Name	Description
From field	The first WWNN or WWPN address in the block.

Name	Description
Size field	The number of WWN or WWPN addresses in the block.

Step 9   Click **Submit**.

vHBAs

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

One or more of the following resources must already exist:

- VSAN
- WWPN pool
- SAN pin group
- Statistics threshold policy

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **Organizations** tab.

Step 4   Click the organization in which you want to create the policy and then click **View Details**.

Step 5   Click the **vHBA Templates** tab.

Step 6   Click **Add**.

Step 7   In the **Add vHBA Template** dialog box, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.

Name	Description
Fabric ID drop-down list	Choose the fabric interconnect that vHBAs created with this template are associated with.
VSAN drop-down list	Choose the VSAN that you want to associate with vHBAs created from this template.
Template Type drop-down list	Choose the type of template that you want to use. This can be one of the following: **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	Choose the WWPN pool that a vHBA created from this template uses to derive its WWPN address.
QoS Policy drop-down list	Choose the QoS policy that is associated with vHBAs created from this template.
Pin Group drop-down list	Choose the SAN pin group that is associated with vHBAs created from this template.
Stats Threshold Policy drop-down list	Choose the statistics threshold policy that is associated with vHBAs created from this template.

Step 8   Click **Submit**.

What to Do Next

Include the vHBA template in a storage policy.

Creating a vHBA

Step 1   On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2   Click the **vHBA** tab.

Step 3   Click **Add**.

Step 4   In the **Create vHBA** dialog box, complete the following fields to specify the Cisco UCS connections for the vHBA:

Name	Description
vHBA Name field	A unique name for the vHBA.
UCS Account Name drop-down list	Choose the Cisco UCS Manager account to which you want to add this vHBA.
UCS Organization Name drop-down list	Choose the Cisco UCS organization to which you want to add this vHBA.
vHBA Template drop-down list	Choose the vHBA template that you want to assign to this vHBA.
Adapter Policy drop-down list	Choose one of the following Ethernet adapter policies: • **Default** • **Windows** • **VMware** • **Linux**

Step 5   Click **Submit**.

What to Do Next

Include this vHBA in a storage policy.

Fibre Channel Adapter Policy

By default, Cisco UCS provides a set of 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 nondefault adapter settings. You can find the details of these required settings on the support list provided by those vendors.

Note   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 TAC.

Creating a Fibre Channel Adapter Policy

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **Organizations** tab.

Step 4   Click the organization in which you want to create the policy and then click **View Details**.

Step 5   Click the **FC Adapter Policies** tab.

Step 6   Click **Add**.

Step 7   In the **Create Fibre Channel Adapter Policy** dialog box, enter a name and description for the policy.

Step 8   In the **Resources** area, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Ring Size field for transmit queues	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 the performance of the adapter. Enter an integer between 64 and 128. The default is 64.
Ring Size field for receive queues	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 the performance of the adapter. Enter an integer between 64 and 128. The default is 64.
Ring Size field for SCSI I/O queues	The number of descriptors in each SCSI I/O queue. Enter an integer between 64 and 512. The default is 512. The number of descriptors can affect the performance of the adapter, so we recommend that you do not change the default value.

Step 9   In the **Options** area, complete the following fields:

Name	Description
FCP Error Recovery drop-down list	Choose 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: • **Disabled**—This is the default. • **Enabled**—You should select this option if your system is connected to one or more tape drive libraries. **Note** This parameter applies only to a server with a Virtual Interface Card (VIC) adapter, such as the Cisco UCS M81KR Virtual Interface Card.
Flogi Retries field	The number of times that the system tries to log in to the fabric after the first failure. Enter any integer. To specify that the system is to continue to try indefinitely, enter infinite in this field. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter or a converged network adapter such as the Cisco UCS M71KR-E Emulex Converged Network Adapter.
Flogi Timeout field	The number of milliseconds that the system waits before it tries to log in again. Enter an integer between 1000 and 255000. The default is 4,000. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter or a converged network adapter.
Plogi Retries field	The number of times that the system tries to log into a port after the first failure. Enter an integer between 0 and 255. The default is 8. We recommend that you consult your storage array documentation for the optimal value for this parameter. **Note** This parameter applies only to a server with a VIC adapter.

Name	Description
Plogi Timeout field	The number of milliseconds that the system waits before it tries to log in again.
	Enter an integer between 1000 and 255000. The default is 20,000. We recommend that you consult your storage array documentation for the optimal value for this parameter.
	Note This parameter applies only to a server with a VIC adapter.
Port Down Timeout field	The number of milliseconds that 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 multipathing drivers and it is one of the key indicators used for error processing.
	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.
	We recommend that you consult your storage array documentation for the optimal value for this parameter.
	Note This parameter applies only to a server with a VIC adapter.
Port Down IO Retry field	The number of times that an IO request to a port is returned because the port is busy before the system decides the port is unavailable.
	Enter an integer between 0 and 255. The default is 8. We recommend that you consult your storage array documentation for the optimal value for this parameter.
	Note This parameter applies only to a server with a VIC adapter running Windows.
Link Down Timeout field	The number of milliseconds that 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. The default is 30,000. We recommend that you consult your storage array documentation for the optimal value for this parameter.
	Note This parameter applies only to a server with a VIC adapter running Windows.

Name	Description
IO Throttle Count field	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.
	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.
	Enter an integer between 1 and 1024. The default is 16. We recommend that you consult your storage array documentation for the optimal value for this parameter.
	Note This parameter applies only to a server with a network adapter such as the Cisco UCS M71KR-E Emulex Converged Network Adapter or the Cisco UCS M71KR-Q QLogic Converged Network Adapter. Servers with a VIC adapter ignore this parameter.
Max LUNs Per Target field	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.
	Enter an integer between 1 and 1024. The default value is 256. For servers running ESX or Linux, the recommended value is 1024.
	We recommend that you consult your operating system documentation for the optimal value for this parameter.
	Note This parameter applies only to a server with a VIC adapter or a network adapter.
Interrupt Mode drop-down list	Choose the method used to send interrupts to the operating system from the driver. This can be one of the following:
	• **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.
	Note This parameter applies only 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.

Step 10   Click **Submit**.

SAN Connectivity Policy

SAN connectivity policies determine the connections and the network communication resources between the server and the LAN on the network. These policies use pools to assign WWNs and WWPNs to servers and to identify the 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.

Creating a SAN Connectivity Policy

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **Organizations** tab.

Step 4   Click the organization in which you want to create the policy and then click **View Details**.

Step 5   Click the **SAN Connectivity Policies** tab.

Step 6   Click **Add**.

Step 7   In the **SAN Connectivity Policy** dialog box, enter a name and description for the policy.

Step 8   From the **WWNN Pool** drop-down list, choose the WWNN pool that you want to associate with this policy.

Step 9   In the **vHBAs** table, click **Add** and do the following:

a) Enter a name for the vHBA.

b) To use a vHBA template to create the vHBA, check the **Use vHBA Template** check box and choose the appropriate template from the drop-down list that is displayed.

c) To create a new vHBA without a template, do not check the **Use vHBA Template** check box and complete the fields that are displayed.
For more information about these fields, see Creating a vHBA, on page 9.

d) Click **Submit**.

Repeat this step if you want to add additional vHBAs to the policy.

Step 10   After you have created all vHBAs required for the policy, click **Submit**.

Storage Policy

The storage policy is a Cisco UCS Director policy that configures the connections between a server and SAN storage, including the World Wide Node Name (WWNN) assigned to the server and the virtual host bus adapters (vHBAs) used by the server. Depending upon the configuration you choose, this policy can be used to configure two or more vHBAs for the server. You can choose to create the vHBAs in this policy or use a SAN connectivity policy to determine the vHBA 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 Storage Policy

Step 1 On the menu bar, choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2 Click the **Storage Policy** tab.

Step 3 Click **Add**.

Step 4 enter a name and description for the policy.

Step 5 In the **Add Storage Policy** dialog box, complete the following fields to specify the Cisco UCS connections for the storage policy:

Name	Description
Policy Name field	A unique name for the storage policy.
Policy description field	The description for the storage policy.
UCS Account Name drop-down list	Choose the Cisco UCS Manager account to which you want to add this storage policy.
UCS Organization Name drop-down list	Choose the Cisco UCS organization to which you want to add this storage policy.
Local Disk Configuration Policy drop-down list	Choose the local disk configuration policy that you want to include in this storage policy.

Name	Description
SAN Connectivity Type drop-down list	Choose one of the following connectivity types: • **Expert**—Allows you to create up to 10 vHBAs that the server can use to access SAN storage. • **Simple**—Allows you to create a maximum of two vHBAs that the server can use to access SAN storage. • **No vHBAs**—Does not allow you to create any vHBAs. If you choose this option, any server associated with a service profile that includes this policy is not connected to the SAN. • **Hardware Inherited**—Uses the vHBAs assigned to the Fibre Channel adapter profile associated with the server. • **Use SAN Connectivity Policy**—Uses a SAN connectivity policy to determine the SAN connectivity for the server.

Step 6   If you chose the **Expert** SAN storage option, do the following:

a) From the **WWNN Pool** drop-down list, choose the WWNN pool that you want to assign to this policy.
The WWNN pool must contain a sufficient number of WWNNs to assign a WWNN to each server that is associated with the service profile that uses this storage policy.

b) In the **Add vHBA** drop-down, choose the number of vHBAs (up to 10) that you want to add to the storage policy.

c) From the **Template For vHBA1 .....vHBA10** list, choose a vHBA template for each vHBA.

d) Go to Step 9.

Step 7   If you chose the **Simple** SAN storage option, do the following:

a) From the **WWNN Pool** drop-down list, choose the WWNN pool that you want to assign to this policy.
The WWNN pool must contain a sufficient number of WWNNs to assign a WWNN to each server that is associated with the service profile that uses this storage policy.

b) In the **vHBA0 (Fabric A)** area, complete the following fields:

• In the **vHBA0 Name** field, enter a unique name for the vHBA.

• From the **Select VSAN** drop-down list, choose the name of the VSAN with which this vHBA should be associated.

c) In the **vHBA1 (Fabric B)** area, complete the following fields:

• In the **vHBA1 Name** field, enter a unique name for the vHBA.

• From the **Select VSAN** drop-down list, choose the name of the VSAN with which this vHBA should be associated.

d) Go to Step 9.

Step 8   If you chose the **Use SAN Connectivity Policy** option, choose the policy that you want to associate with the server from the **SAN Connectivity Policy** drop-down list.

Step 9   Click **Submit**.

What to Do Next

Include the storage policy in a service profile.

Fibre Channel Zoning

Support for Fibre Channel Zoning in Cisco UCS

Cisco UCS supports switch-based Fibre Channel zoning and Cisco UCS local Fibre Channel zoning (also known as Cisco UCS Manager-based Fibre Channel zoning). You cannot configure a combination of zoning types in the same Cisco UCS domain. You can configure a Cisco UCS domain with one of the following types of zoning:

  • No zoning

  • Cisco UCS local Fibre Channel zoning—This configuration combines direct attach storage with local zoning. Fibre Channel or FCoE storage is directly connected to the fabric interconnects and zoning is configured in Cisco UCS, using local zoning. Any existing Fibre Channel or FCoE uplink connections must be disabled. Cisco UCS does not currently support active Fibre Channel or FCoE uplink connections that coexist with the utilization of the Cisco UCS local zoning feature.

  • Switch-based Fibre Channel zoning—This configuration combines direct attach storage with uplink zoning. The Fibre Channel or FCoE storage is directly connected to the fabric interconnects and zoning is performed externally to the Cisco UCS domain through a Cisco MDS or Nexus 5000 Series switch. This configuration does not support local zoning in the Cisco UCS domain.

Note   Zoning is configured on a per-VSAN basis. You cannot enable zoning at the fabric level.

For more information about Fibre Channel zoning, including guidelines for implementing it, see the Cisco UCS Manager configuration guides.

Storage Connection Policy

The storage connection policy contains a collection of target storage ports on storage arrays that you use to configure Cisco UCS local Fibre Channel zoning. You can create this policy underneath an organization or an initiator group. This policy is known as a Fibre Channel storage connection policy in Cisco UCS Manager.

You add vHBA initiator groups to a storage connection policy through the Fibre Channel target endpoints.

The storage arrays in these zones must be directly connected to the fabric interconnects. The target storage ports on these arrays that you include in the storage connection policy can be either Fibre Channel storage ports or FCoE storage ports. You use the WWN of a port to add it to the policy and to identify the port for the Fibre Channel zone.

> **Note** Cisco UCS does not create Fibre Channel storage by default.

Configuring Fibre Channel Zoning in Cisco UCS

> **Note** This procedure provides a high-level overview of the steps required to configure a Cisco UCS domain for Cisco UCS local Fibre Channel zoning. Ensure that you complete all of the following steps.

DETAILED STEPS

	Command or Action	**Purpose**
Step 1	If you have not already done so, disconnect the fabric interconnects in the Cisco UCS domain from any external Fibre Channel switches, such as an MDS.	If the Cisco UCS domain still includes zones that were managed by the external Fibre Channel switch, enter the **clear-unmanaged-fc-zone-all** command on every affected VSAN to remove those zones. You must perform this step in the Cisco UCS Manager CLI.
Step 2	Configure the Fibre Channel switching mode for both fabric interconnects in Fibre Channel switch mode.	You cannot configure Fibre Channel zoning in end-host mode. See Changing Fibre Channel Switching Mode.
Step 3	Configure the Fibre Channel and FCoE storage ports that you require to carry traffic for the Fibre Channel zones.	See Configuring Fabric Interconnects and Ports.
Step 4	Create one or more VSANs and enable Fibre Channel zoning on all VSANs that you require to carry traffic for the Fibre Channel zones.	For a cluster configuration, we recommend that you create the VSANs that you intend to include in a storage zone and use the common or global configuration to ensure that they are accessible to both fabric interconnects. See Creating a VSAN, on page 2 and Configuring a VSAN for Fibre Channel Zoning, on page 19.
Step 5	Create a LAN connectivity policy.	See Creating a LAN Connectivity Policy.
Step 6	Create a network policy and add the LAN connectivity policy to it.	See Creating a Network Policy.
Step 7	Create a SAN connectivity policy.	See Creating a SAN Connectivity Policy, on page 14.
Step 8	Create a storage policy and add the SAN connectivity policy to it.	See Creating a Storage Policy, on page 15.

	Command or Action	**Purpose**
Step 9	Create one or more storage connection policies and include one or more Fibre Channel target endpoints to serve as vHBA initiator groups.	See Creating a Storage Connection Policy, on page 20.
Step 10	Create a service profile and add the network policy and storage policy to it.	See Creating a Service Profile.
Step 11	Associate the service profile with a server.	
Step 12	View and generate reports for the Fibre Channel zones through a service profile and/or organization.	(Optional) See Viewing Fibre Channel Zones, on page 21.
Step 13	If you modify the LAN and/or SAN connectivity policies, which causes the server to reboot, request inventory collection for the service profile and the server.	(Optional) See Requesting Inventory Collection for a Service Profile and Requesting Inventory Collection for a Server.

Configuring a VSAN for Fibre Channel Zoning

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **VSANs** tab.

Step 4   Click the VSAN that you want to configure for Fibre Channel zoning.

Step 5   Click **FC Zoning Settings**.

Step 6   In the **FC Zoning Settings** dialog box, check the **Enable FC Zoning** check box.

Step 7   Click **Save**.

Creating a Storage Connection Policy

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   In the right pane, click the **Organizations** tab.

Step 4   Click the organization in which you want to create the policy and then click **View Details**.

Step 5   Click the **Storage Connection Policies** tab.

Step 6   Click **Add**.

Step 7   In the **Storage Connection Policy** dialog box, enter a name and description for the policy.

Step 8   In the **Zoning Type** drop-down list, choose one of the following options:

- **None**—No Fibre Channel zoning.

- **Single Initiator Single Target**—Cisco UCS Director automatically creates one zone for each vHBA and storage port pair. Each zone has two members. We recommend that you configure this type of zoning unless you expect the number of zones to exceed the maximum supported.

- **Single Initiator Multiple Targets**—Cisco UCS Director automatically creates one zone for each vHBA. We recommend that you configure this type of zoning if you expect the number of zones to reach or exceed the maximum supported.

Step 9   In the **FC Target Endpoints** table, click **Add** and do the following:

a) Complete the following fields:

Name	Description
WWPN field	The WWPN (WWN) assigned to the physical target port on the Fibre Channel or FCoE storage array that the server uses to access the LUNs configured on the storage array.
Fabric ID drop-down list	Choose the fabric interconnect used for communications with the target endpoint.
VSAN drop-down list	Choose the VSAN used for communications with the target endpoint.

b) Click **Submit**.

Repeat this step until you have created all desired target endpoints.

Step 10   Click **Submit**.

Viewing Fibre Channel Zones

Before You Begin

You must have Fibre Channel Zoning configured to view any Fibre Channel zones.

Step 1   On the menu bar, choose **Physical** > **Compute**.

Step 2   In the left pane, expand the pod and then click the Cisco UCS Manager account.

Step 3   Click one of the following tabs:

- **Organizations**

- **Service Profiles**

Step 4   Click the **FC Zones** tab.

Step 5   (Optional) To customize the columns that you see in the table and any report that you generate, do the following:

a) On the table menu bar, click the **Customize Table Columns** button.

b) In the **Customize Report Table** dialog box, check or uncheck the check boxes to determine which elements you see in the report and click **Save**.

Step 6   (Optional) To export a report of what you see in the tab, do the following:

a) On the table menu bar, click **Export Report**.

b) In the **Export Report** dialog box, select a report format and click **Generate Report**.

c) When the report has generated, click **Download**.

d) If the report opens in a separate tab, use the download button from your browser to download the report.

e) In the **Export Report** dialog box, click **Close**.