Configuring Storage Connections

This chapter contains the following sections:

- Global VSANs, on page 1
- WWN Pools, on page 2
- IQN Pools, on page 5
- vHBA Template, on page 6
- Creating a vHBA Policy, on page 7
- SAN Connectivity Policy, on page 8
- Storage Policy, on page 9
- ID Range Qualification Policy, on page 10

Global VSANs

You can define global VSANs in the domain group root, or a domain group below the root. Global VSANs are fabric-interconnect specific and can be created for either Fabric A or Fabric B. A global VSAN cannot be a common VSAN.

Resolution of global VSANs takes place prior to the deployment of global service profiles. If a global service profile references a global VSAN, and that VSAN does not exist, deployment of the global service profile fails due to insufficient resources. All global VSANs created in a Cisco UCS Central account must be resolved before deploying the global service profile.

A global VSAN is not deleted when you delete a global service profile that references it. Delete the global VSAN from the Cisco UCS Central account.

A global VSAN is visible to a Cisco UCS Manager account only if you deploy a global service profile that references the VSANs. Once a VSAN that is deployed with a global service profile becomes available in a Cisco UCS Manager account, you can include it in a local service profile and policy. You cannot turn a global VSAN into a local VSAN.

Creating a Global VSAN

You can create a global VSAN with IDs from 1 to 4093, except for those in the following reserved ranges:

- If you plan to use FC switch mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3040 to 4078.

- If you plan to use FC end-host mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3840 to 4079.

Note 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 for a VLAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE VLAN ID.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **VSANs**.

Step 6 Click **Add**.

Step 7 On the **Add VSAN** screen, do the following:

a) In the **VSAN Name** field, enter a unique name for the VSAN. The VSAN name is case-sensitive.
b) In the **VSAN ID** field, enter a unique identifier to be assigned to the network.
c) In the **Domain Group** field, check the check box for the domain group in which you want to create the global VSAN.
d) From the **Fabric ID** drop-down list, choose the fabric interconnect where you want to create the global VSAN.
e) In the **FCOE VLAN** field, enter the ID for the VLAN to be used for transporting the VSAN and its Fibre Channel packets.
f) Click **Submit**.

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 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **WWNN Pools**.

Step 8 Click **Add**.

Step 9 On the **Add WWNN Pool** screen, 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.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 10 Click **Submit**.

WWXN Pools

A WWXN pool is a WWN pool that contains both WW node names and WW port names.

Creating a WWXN Pool

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **WWXN Pools**.

Step 8 Click **Add**.

Step 9 On the **Add WWXN Pool** screen, 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 WWXN address in the block.
Size field	The number of WWXN addresses in the block.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 10 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 **Multi-Domain Managers**.
Step 3 In the left pane, expand **UCS Central Accounts** and then click the Cisco UCS Central account.
Step 4 In the right pane, click the **Organizations** tab.
Step 5 Click the organization in which you want to create the pool and then click **View Details**.
Step 6 Click the **WWPN Pools** tab.
Step 7 Click **Add**.
Step 8 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.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 9 Click **Submit**.

Adding a WWN Block

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, expand **Multi-Domain Managers**.
Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.
Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.
Step 5 Click **Organizations**.
Step 6 Click the organization in which you want to modify the pool and then click **View Details**.

Step 7 Click one of the following tabs:

- **WWNN Pools**
- **WWPN Pools**
- **WWXN Pools**

Step 8 Click the pool to which you want to add a WWN block.

Step 9 Click **Create WWN Block**.

Step 10 On the **Create WWN Block** screen, complete the following fields:

Name	Description
Description field	Type a description.
From field	The first WWNN, WWPN, or WWXN address in the block.
Size field	The number of WWNN, WWPN, or WWXN addresses in the block.
ID Range Qualification Policy drop-down list	Choose the ID Range Qualification Policy.

Step 11 Click **Submit**.

IQN Pools

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs in a Cisco UCS domain. IQN pools created in Cisco UCS Central can be shared between Cisco UCS domains. IQN pool members are of the form **prefix:suffix:number**, where you can specify the prefix, suffix, and a block (range) of numbers. An IQN pool can contain more than one IQN block, with different number ranges and different suffixes, but sharing the same prefix

Creating an IQN Pool

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the pool and then click **View Details**.

Step 7 Click **IQN Pools**.

Step 8 Click **Add**.

Step 9 On the **IQN Pool** screen, enter a name, description, and prefix for the IQN pool.

Step 10 In the **IQNPool Block**, enter Suffix, From, Size, and ID Range Qualification Policy information.

Step 11 Click **Submit**.

vHBA Template

This template is a policy that defines how a vHBA (virtual Host Bus Adapter) 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

One or more of the following resources must already exist:

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

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **vHBA Templates**.

Step 8 Click **Add**.

Step 9 On the **Add vHBA Template** screen, enter a unique name and description for the policy.

Step 10 From the **Fabric ID** drop-down list, choose the fabric interconnect that you want to associate with vHBAs created from this template.

Step 11 From the **VSAN** drop-down list, choose the VSAN that you want to associate with vHBAs created from this template.

Step 12 From the **Template Type** drop-down list, choose 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.

Step 13 In the **Max Data Field Size** field, enter 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.

Step 14 To associate policies with vNICs created from this template, complete the following fields:

Name	Description
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 15 Click **Submit**.

What to do next

Include the vHBA template in a vHBA policy.

Creating a vHBA Policy

Before you begin

Make sure that at least one of the following exists in the Cisco UCS Central account and organization to which this policy applies:

- vHBA template
- Fibre Channel adapter policy

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Central**.

Step 2 Click **vHBA**.

Step 3 Click **Add**.

Step 4 On the **Create UCS Central vHBA Policy** screen, do the following:

a) In the **vHBA Name** field, enter a unique name for the policy.
b) From the **Account Name** drop-down list, choose a Cisco UCS Central account to which this policy applies.
c) From the **Organization** drop-down list, choose the organization to which this policy applies.
d) From the **vHBA Template** drop-down list, choose a vHBA template.
e) From the **Adapter Policy** drop-down list, choose an adapter policy.

f) Click **Submit.**

What to do next

Include the vHBA policy in a storage policy.

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 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organizations**.

Step 6 Click the organization in which you want to create the policy and then click **View Details**.

Step 7 Click **SAN Connectivity Policies**.

Step 8 Click **Add**.

Step 9 On the **SAN Connectivity Policy** screen, enter a name and description for the policy.

Step 10 From the **WWNN Pool** drop-down list, choose the WWNN pool that you want to associate with this policy.

Step 11 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 Template, on page 6.

d) Click **Submit**.

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

Step 12 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 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Central**.

Step 2 Click **Storage Policy**.

Step 3 Click **Add**.

Step 4 On the **Create UCS Central Storage Policy** screen, enter a name and description for the policy.

Step 5 Complete the following fields to specify the Cisco UCS Central connections for the policy:

- **UCS Account Name** drop-down list—Choose the Cisco UCS Central account to which you want to add this policy.
- **UCS Organization Name** drop-down list—Choose the Cisco UCS Central organization to which you want to add this policy.

Step 6 From the **Local Disk Configuration Policy** drop-down list, choose the local disk configuration policy that you want to include in this storage policy.

Step 7 From the **SAN Connectivity Type** drop-down list, choose one of the following connectivity types:

Option	Description
Expert	Allows you to create up to 10 vHBAs that the server can use to access SAN storage. Continue with Step 8.
Simple	Allows you to create a maximum of two vHBAs that the server can use to access SAN storage. Continue with Step 9.
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 SAN. Continue with Step 11.
Hardware Inherited	Uses the vHBAs assigned to the Fibre Channel adapter profile associated with the server. Continue with Step 11.
Use SAN Connectivity Policy	Uses a SAN connectivity policy to determine the SAN connectivity for the server.

Option	Description
	Continue with Step 10.

Step 8 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 enough of WWNNs to assign a WWNN to each server that is associated with a 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) Continue with Step 11.

Step 9 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 enough of WWNNs to assign a WWNN to each server that is associated with a 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 is to 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 is to be associated.

d) Continue with Step 11.

Step 10 If you chose the SAN connectivity policy option, choose the policy that you want to associate with the server from the **SAN Connectivity Policy** drop-down list.

Step 11 Click **Submit**.

What to do next

Include the storage policy in a service profile.

ID Range Qualification Policy

ID range qualification policies allow you to create policies and assign them to qualified domain groups and domain IP addresses. The ID range qualification policy is then visible to those domain groups and domain IP addresses. You can also create ID range qualification policies without assigning qualified domain groups or IP addresses. If you do not set qualifiers, the policy is available to all domain groups. ID resolution occurs hierarchically in the organization structure in the same manner as other global policies.

The ID Range Qualification Policy can be associated to:

- MAC Pool

- WWNN Pool
- WWPN Pool
- WWXN Pool
- IP Pools
- IQN Pools.

After you create an ID range qualification policy, you can apply it to a block in a new pool or an existing pool.

Creating an ID Range Qualification Policy

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **ID Range Qualification Policies**.

Step 6 Click **Add**.

Step 7 On the **Create a ID Range Qualification Specification** screen, enter a name and description for the policy.

Step 8 In the **Domain Group** table, click the check box for the appropriate Domain Group or groups.

Step 9 Expand the **IPv4 Addresses** field, to select or add addresses.

Step 10 Expand the **IPv6 Addresses** field, to select or add addresses.

Step 11 Click **Submit**.