Storage Policies

This chapter includes the following sections:

Fibre Channel Adapter Policy

Fibre channel adapter 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 Central may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in possible mismatch between SANsurfer and Cisco UCS Central:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Central 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 Central, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Central displays as 5 s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Central allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Central displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

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 non-default 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 Technical Support.

Creating or Editing a Fibre Channel Adapter Policy

Step 1 In the **Actions** bar, type **Create Fibre Channel Adapter Policy** and press Enter.

Step 2 In the **Fibre Channel Adapter Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create this policy.

Step 3 Enter a **Name** and optional **Description**
The policy name is case sensitive.

Step 4 In **Resources**, complete the fields as necessary.

Step 5 In **Settings**, complete the fields as necessary.

Step 6 Click **Create**.

SAN Connectivity Policy

SAN connectivity policies determine the connections and the network communication resources between the server and the SAN 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 These policies are included in service profiles and service profile templates, and can be used to configure multiple servers. So, using static IDs in connectivity policies is not recommended.

Creating or Editing a SAN Connectivity Policy

Step 1 In the **Actions** bar, type **Create SAN Connectivity Policy** and press Enter.

Step 2 In the **SAN Connectivity Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.
The name is case sensitive.

Step 4 In **Identifiers**, choose the WWNN pool.
For more information, see Creating and Editing a WWN Pool.

Step 5 In **vHBAs**, create one or more vHBAs and select the properties.
You can manually create the vHBA, use a vHBA template, or create a redundancy template pair. For more information, see Creating or Editing a vHBA Template.

Step 6 Click **Create**.

Storage Connection Policy

The storage connection policy contains a collection of target storage ports on storage array that you use to configure fibre channel zoning.

From Cisco UCS Central you can create a storage connection policy in an organization.

Creating or Editing a Storage Connection Policy

Step 1 In the **Actions** bar, type **Create Storage Connection Policy** and press Enter.

Step 2 In the **Storage Connection Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

a) Enter a **Name** and an optional **Description** for this policy.
b) Select a **Zoning Type**. This can be one of the following:

- **None—**FC zoning is not configured.
- **Single Initiator Single Target—**The system 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.

  This is the default.
- **Single Initiator Multiple Targets—**The system 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 3 Click **Endpoints** and click the plus sign to add a **WWPN**.
The WWPN is 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.

a) In the **FC Target Endpoints** > **Basic** tab, enter an optional description and select the fabric interconnect in the **Path** field.
   By default, fabric interconnect A is used for communications with the target endpoint.
b) In the **FC Target Endpoints** > **VSAN** tab, select the VSAN associated with the FI port and target endpoint.

Step 4 Click **Create**.

Fibre Channel Zoning

Fibre Channel (FC) zoning allows you to partition the Fibre Channel fabric into one or more zones. Each zone defines the set of FC initiators and FC targets that can communicate with each other in a VSAN.

The access and data traffic control provided by zoning does the following:

- Enhances SAN network security
- Helps prevent data loss or corruption
- Reduces performance issues

Cisco UCS Central FC zoning combines direct attach storage with local zoning. Fibre Channel or FCoE storage is directly connected to the fabric interconnects, and zoning is performed in Cisco UCS Central, using Cisco UCS local zoning.

Configuring Zoning

Note This dialog box is read-only if the global service profile or service profile template you select already has a SAN connectivity policy associated with it.

Step 1 From the **Service Profile** or **Service Profile Template** page, click the **Tools** icon and choose **Configuring Zoning**.

Step 2 In the **Configure Zoning** dialog box, click the plus icon to add a new vHBA Initiator Group, and type the name that you want to use for the group.

Step 3 In **Basic**, enter the optional description.

Step 4 In **vHBA Initiators**, select the vHBA initiators that you want to add.

Step 5 In **Storage Connection Policy**, select the policy that you want to use.

Step 6 Click **Save**.

Direct-Attached Storage

Direct-attached storage (DAS) uses FC storage ports to connect an FC storage device to a port on the fabric interconnect.

Configuring Direct-Attached Storage

Step 1 Ensure that the FI is configured in FC Switch Mode.

Step 2 Create a VSAN in the Storage cloud.

Step 3 Set the port role to FC Switch Mode.

Step 4 Perform the following steps to confirm that the storage port WWPN is logged into the fabric interconnect.

a) Log in through the secure shell (SSH), or establish a Telnet connection to the UCS Virtual IP (VIP) on the primary FI.

b) Enter the connect nxos { a | b } command, where a | b represents FI A or FI B.

c) Enter the **show flogi database vsan** *vsan ID* command, where *vsan ID* is the identifier for the VSAN.

Step 5 Create a storage connection policy.

Step 6 Create a service profile that uses the storage connection policy you just created.

Step 7 Associate the service profile with the server.