Configuring Cisco UCS Service Profile Templates for Big Data

This chapter contains the following sections:

Cisco UCS Service Profile Templates for Big Data

Cisco Unified Computing System (Cisco UCS) service profiles are a powerful means for streamlining the configuration and management of Cisco UCS servers. They provide a mechanism for rapidly provisioning servers and their associated network connections with consistency in all details of the environment. They can be set up in advance before physically installing the servers.

Service profiles are built on policies—Administrator-defined sets of rules and operating characteristics such as the server identity, interfaces, and network connectivity. Every active server in your Hadoop cluster must be associated with a service profile.

The Cisco UCS service profile template for the Big Data enables you to set up the configuration for the servers in your Hadoop cluster. The service profile template for Big Data is included in a cluster deploy template. When the cluster deploy template is applied to the servers, the service profile template configures one or more service profiles that are applied to the servers.

Note The service profile template for Big Data wizard gathers the information required to create a service profile template. You can only apply this service profile template through the cluster deploy template.

For more information about service profiles and service profile templates, see the Cisco UCS Manager configuration guides.

Creating a Cisco UCS Service Profile Template for Big Data

Before you begin

Add a Cisco UCS Manager account.

Step 1 Choose **Solutions** > **Big Data** > **Containers**.

Step 2 Click **UCS SP Templates**.

Step 3 Click **Add (+)**.

Step 4 On the **UCS SP Template Specification** page of the **Create UCS SP Template for Big Data** wizard, complete the following fields:

Name	Description
Template Name field	A unique name for the template.
Template Description field	The description of the template.
Template Type drop-down list	Choose a service profile template. Service profiles created from an initial template inherit all the properties of the template. However, changes to the initial template do not automatically propagate to the bound service profiles. If you want to propagate changes to bound service profiles, unbind and rebind the service profile to the initial template.
Container Type drop-down list	The type of container for the cluster. Choose one of the following: • Hadoop • Splunk • Baremetal OS
Use vNIC Bonding check box	Check the check box to use vNIC bonding. Eight vNICs are available in the **Create vNIC Policy** page of the **Create UCS SP Template for Big Data** wizard.
Use Multiple vNIC check box	Check the check box to have more than one vNIC interface and the required polices for creating a template. This option is only available when you select **Hadoop** or **Splunk** in the **Container Type** drop-down list. It is not displayed for **Baremetal OS**.

Step 5 Click **Next**.

What to do next

Create a QoS policy.

Creating a QoS Policy

The quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters, you can also specify more controls on the outgoing traffic, such as burst and rate.

Step 1 On the **Create QoS Policy** page of the **Create UCS SP Template for Big Data** wizard, do one of the following:

- To accept the default QoS policies, click **Next**.
- To create one or more custom QoS policies, click **Add (+)** and continue with Step 2.
- To review or modify one of the default QoS policies, choose the policy in the table and click **Edit**. For information about the fields on the **Edit QoS Policy Entry** screen, see Step 2.

Step 2 On the **Add Entry to QoS Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Priority drop-down list	Choose the priority assigned to this QoS policy. Choose one of the following: • **Fc**—Use this priority for QoS policies that control only vHBA traffic. • **Platinum**—Use this priority for QoS policies that control only vNIC traffic. • **Gold**—Use this priority for QoS policies that control only vNIC traffic. • **Silver**—Use this priority for QoS policies that control only vNIC traffic. • **Bronze**—Use this priority for QoS policies that control only vNIC traffic. • **Best Effort**—It is reserved for the Basic Ethernet traffic lane. If you assign this priority to a QoS policy and configure another system class as CoS 0, Cisco UCS does not default to this system class. It defaults to the priority with CoS 0 for that traffic.
Burst(Bytes) field	The normal burst size for servers that use this policy. This field determines the maximum size of traffic bursts beyond which the traffic is considered to exceed the rate limit. The default is 10240. The minimum value is 0, and the maximum value is 65535. This setting is not applicable to all adapters.

Name	Description
Rate drop-down list	Choose the expected average rate of traffic. Choose one of the following: • **Line-rate**—Equals a value of 0 and specifies no rate limiting. This is the default value. • **Specify Manually**—Enables you to specify the rate in a field. The minimum value is 0, and the maximum value is 40,000,000. The granularity for rate limiting on a Cisco UCS M81KR Virtual Interface Card adapter is 1 Mbps. The adapters treat the requested rate as a "not-to-exceed" rate. Therefore, a value of 4.5 Mbps is interpreted as 4 Mbps. Any requested rate of more than 0 and less than 1 Mbps is interpreted as 1 Mbps, which is the lowest supported hardware rate limit. Rate limiting is not applicable to all adapters. For example, this setting is not supported on the Cisco UCS VIC-1240 Virtual Interface Card.
Host Control drop-down list	Determines whether Cisco UCS controls the class of service (CoS) for a vNIC. This setting has no effect on a vHBA. The default setting is **None**. Cisco UCS uses the CoS value associated with the priority regardless of the CoS value assigned by the host.

Step 3 Click **Submit**.

Step 4 Click **Next**.

What to do next

Create a VLAN policy.

Creating a VLAN Policy

The VLAN policy creates a connection to a specific external LAN in the underlying infrastructure of a Hadoop cluster that is within a single Cisco UCS domain. The VLAN isolates traffic to that external LAN, including broadcast traffic.

Step 1 On the **Create VLAN Policy** page of the **Create UCS SP Template for Big Data** wizard, do one of the following:

- To accept the default VLAN policies, click **Next**.
- To create one or more custom VLAN policies, click **Add (+)** and continue with Step 2.
- To review or modify one of the default VLAN policies, choose the policy in the table and click **Edit**. For information about the fields on the **Edit VLAN Policy Entry** screen, see Step 2.

Step 2 On the **Add Entry to VLAN Policy** screen, complete the following fields:

Name	Description
VLAN Name field	The name of the VLAN policy.
Fabric ID drop-down list	Choose how to configure the VLAN. The setting can be one of the following: • **Common or Global**—The VLAN maps to the same VLAN ID in all available fabrics. • **Fabric A**—The VLAN maps to a VLAN ID that exists only in fabric A. • **Fabric B**—The VLAN maps to a VLAN ID that exists only in fabric B.
Sharing drop-down list	The default setting is **None**.

Step 3 Click **Submit**.

Step 4 Click **Next**.

What to do next

Create a vNIC policy.

Creating a vNIC Policy

The vNIC policy defines how a vNIC on a server connects to the LAN. Each server in a Hadoop cluster requires a vNIC policy for each of the following NICs:

- MGMT
- DATA

Note In addition to MGMT NIC, DATA NIC is available if you have checked **Multiple vNIC** in the **Create UCS SP Template for Big Data** wizard.

Step 1 On the **Create vNIC Policy** page of the **Create UCS SP Template for Big Data** wizard, do one of the following:

- To accept the default vNIC policies, click **Next**.
- To create one or more custom vNIC policies, click **Add (+)** and continue with Step 2.
- To delete a vNIC policy, choose a policy in the table and click **Delete**.

  Note When you delete the vNICs, ensure that at least one vNIC is available per fabric interconnect.

- To review or modify one of the default vNIC policies, choose the policy in the table and click **Edit**. For information about the fields on the **Edit vNIC Policy Entry** screen, see Step 2.

Step 2 On the **Add Entry to vNIC Policy** screen, complete the following fields:

Name	Description
vNIC Name field	Name of the vNIC.
Fabric ID drop-down list	Choose the fabric interconnect with which the vNICs created with this policy are associated. If you want vNICs created from this policy to access the second fabric interconnect when the default choice is unavailable, check the **Enable Failover** check box. When the **Use vNIC Bonding** check box is checked in the **UCS SP Template Specification** page of the **Create UCS SP Template for Big Data** wizard, the **Enable Failover** check box is disabled. Do not enable vNIC fabric failover under the following circumstances: **Note** • If the Cisco UCS domain is running in Ethernet Switch Mode, vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to other fabric interconnect. • If you associate one or more vNICs created from this template and associate the service profile with the server that has an adapter without the fabric failover support (For example, Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter) Cisco UCS Manager generates a configuration fault.
VLANs area	In the VLANs area, do the following to select the VLAN to be assigned to vNICs created from this policy: **a.** Click **Add**. **b.** On the **Add Entry to VLANs** screen, complete the following fields: • **Name** drop-down list—Choose the VLAN that you want to associate with the vNIC template. • **Set as Native VLAN** check box—Check the check box if you want this VLAN to be the native VLAN for the port. **c.** Click **Submit**.

Name	Description
MTU field	The MTU, or packet size, to be used by the vNICs created from this vNIC policy. Enter an integer between 1500 and 9216. **Note** If the vNIC template has an associated QoS policy, the MTU specified has to be equal to, or less than the MTU specified in the associated QoS System class. If this MTU value exceeds the MTU value in the QoS system class, packets are dropped during data transmission.
Pin Group drop-down list	This is a *display-only* field.
Adapter Policy field	This field is autopopulated with **Linux**.
Dynamic vNIC Connection Policy drop-down list	This is a *display-only* field.
QoS Policy drop-down list	Choose the quality of service policy that is used by the vNICs created from this vNIC policy.
Network Control Policy drop-down list	This is a *display-only* field.

Step 3 Click **Submit**.

Step 4 Click **Next**.

What to do next

Create a boot order policy.

Creating a Boot Order Policy

The Cisco UCS Manager boot policy overrides the boot order in the BIOS setup menu, and determines the following:

- Selection of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

Step 1 On the **Create Boot Order Policy** page of the **Create UCS SP Template for Big Data** wizard, set the boot order for the following devices:

- **CD-ROM**
- **Storage**
- **LAN**

If you do not want to boot from a specific device, choose the blank space at the bottom of the drop-down list.

Note If you are booting for the first time, choose **1** for the LAN drop-down list to set it as the first boot device.

Step 2 In the **Select vNIC Policy for LAN Ethernet** table, click **Add (+)**.

Step 3 On the **Add Entry to Select vNIC Policy for LAN Ethernet** screen, do the following:

a) From the **Select vNIC** drop-down list, choose the vNIC that you want to assign to the LAN.
b) If you want the VLAN shown in the **VLAN** field to be the primary VLAN, check the **Set as Primary** check box.
c) Click **Submit**.

Step 4 If you want to choose vNIC policies for other VLANs, repeat Steps 2 and 3 with a different vNIC from the **Select vNIC** drop-down list.

Step 5 Click **Next**.

What to do next

Create a BIOS policy.

Creating a BIOS Policy

The BIOS policy automates the configuration of certain BIOS settings for the servers in the cluster.

Note All the drop-down lists on the **Create UCS BIOS Policy** page are set to **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. For more information, see BIOS Parameters by Server Model.

Step 1 On the **Create UCS BIOS Policy** page of the **Create UCS SP Template for Big Data** wizard, complete the following fields:

Name	Description
Main	
Quiet Boot drop-down list	Determines what the BIOS displays during Power On Self-Test (POST).
POST Error Pause drop-down list	Determines what happens when the server encounters a critical error during POST.
Resume AC on Power Loss drop-down list	Determines the server behavior when the power is restored after an unexpected power loss.
From Panel Lockout drop-down list	Determines whether the server ignores the power and reset buttons on the front panel.
Processor	

Name	Description
Turbo Boost	Determines whether the processor uses Intel Turbo Boost Technology. This allows the processor to automatically increase its frequency if it is running below specifications for power, temperature, or voltage. Choose either **Enabled** or **Disabled**.
Enhanced Intel SpeedStep	Determines whether the processor uses Enhanced Intel SpeedStep Technology. This allows the system to dynamically adjust processor voltage and core frequency. Choose either **Enabled** or **Disabled**.
Hyper Threading	Determines whether the processor uses Intel Hyper-Threading Technology. This allows multithreaded software applications to execute threads in parallel within each processor. Choose either **Enabled** or **Disabled**.
Excute Disabled Bit	Classifies the memory areas on the server to specify where the application code can execute. Choose either **Enabled** or **Disabled**.
Virtualization Technology	Determines whether the processor uses Intel Virtualization Technology (VT). This allows a platform to run multiple operating systems and applications in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect. Choose either **Enabled** or **Disabled**.
Processor C State	Determines whether the system enters into the power savings mode during idle periods. Choose either **Enabled** or **Disabled**.
Processor C1E	Determines whether the CPU transitions to its minimum frequency when entering the C1 state. Choose either **Enabled** or **Disabled**.

Name	Description
Processor C3 Report	Determines whether the BIOS sends the C3 report to the operating system. When the OS receives the report, it can transition the processor into the lower C3 power state to decrease energy usage while maintaining optimal processor performance. This option can be one of the following: • Disabled—The BIOS does not send the C3 report. • ACPI C2—The BIOS sends the C3 report using the ACPI C2 format, allowing the OS to transition the processor to the C3 low-power state. • ACPI C3—The BIOS sends the C3 report using the ACPI C3 format, allowing the OS to transition the processor to the C3 low-power state.
Processor C6 Report	Determines whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance. Choose either **Enabled** or **Disabled**.
RAS Memory (reliability, availability, and serviceability of the memory)	
NUMA(nonuniform memory access)	Determines the BIOS support for NUMA. Choose either **Enabled** or **Disabled**. • Disabled—The BIOS does not support NUMA. • Enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.

Step 2 Click **Next**.

What to do next

Create a Local Disk Configuration Policy.

Creating a Local Disk Configuration Policy

This policy defines disk configuration for disk partitions, and storage local to the server for the selected Hadoop and Splunk container types. It provides a flexible mechanism to define the RAID levels and JBOD configuration for name nodes and data nodes resident in a Hadoop cluster. This policy enables you to set a local disk configuration for all servers associated with a service profile.

Step 1 On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, review the following fields:

Name	Description
Configure RAID Policy for the Hadoop cluster table	RAID level configuration for Hadoop NameNode and DataNode (OS and data drives).
Configure Splunk RAID Policy table	RAID level configuration for Splunk Indexer, Search Heads, and Administrative nodes.
Use LVM For Disk Configuration check box	Create Logical Volume Manager (LVM) groups for disk partitions.
Partition Configuration table	Create partitions other than the /, /boot, swap, /tmp, /var/tmp, and /home partitions.

Step 2 Click **Submit**.

What to do next

- Create a Hadoop cluster profile template to deploy a Hadoop cluster.
- Create Cluster Deploy Templates for Hadoop and Splunk Enterprise clusters.

Editing RAID Policy for Hadoop

Use this procedure to edit the local disk drive configuration associated with the hardware RAID controller for C220 and C240 M3/M4/M5 servers, and for the standalone (PCH Controlled SSD disks) on C240 M4/M5 and C220 M5.

Before you begin

Create a Local Disk Configuration Policy.

Step 1 On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, choose the node type in the **Configure RAID Policy** table.

Step 2 In the **Configure RAID Policy** table, click the **Edit selected entry in the table below** icon.

Step 3 On the **Edit Configure RAID Policy Entry** screen, complete the following fields:

Name	Description
Node Type	The selected node type. **Note** The following are the supported nodes: • Cluster node is applicable only for MapR cluster • Master and Data Nodes are applicable only for Cloudera and Hortonworks clusters. • Kafka Node is applicable only for Cloudera and Hortonworks clusters. • Edge Node is applicable for all the Hadoop clusters.
OS Disks	
Use HDD drives on servers with insufficient standalone boot drives check box	Allows you to enable an alternate policy for Cisco UCS servers with insufficient standalone boot drives.
Use standalone boot drives check box	By default, this option is checked and disabled. Check this check box for Cisco UCS servers with sufficient standalone boot drives.
RAID Level [OS] drop-down list	Choose the RAID level for the OS (operating system) disks.
Disks Per Group field	Specifies the number of disks that can exist per group during RAID configuration.
Write Mode drop-down list	Choose either **Write through** to write data without the RAID controller cache, or **Write back** to write data with the cache.
Read Mode drop down-list	Choose the method to read data from the disks.
Use Cache check box	Check the **Use Cache** check box to use the RAID controller cache to read and write operations.
Use Cache if Bad BBU check box	Check the **Use Cache if Bad BBU** check box to ensure that if the Battery Backup Unit (BBU) is not available for any reason, **Write back** will be disabled and **Write Through** will be enabled.
Strip Size (KB) drop- down list	Allows specification, in KB, of the strip size for each disk within a stripe.
Data Disks	
Use JBOD mode [Data] check box	Check the **Use JBOD mode [Data]** check box to configure Hadoop data disks in JBOD mode.
RAID Level [Data] drop-down list	Choose the RAID level for the Hadoop data disks.

Name	Description
Disks Per Group field	Specifies the number of disks that can exist per group during RAID configuration.
Write Mode drop-down list	Choose either **Write through** to write data without the RAID controller cache, or **Write back** to write data with the cache.
Read Mode drop down-list	Choose the method to read data from the disks.
Use Cache check box	Check the **Use Cache** check box to use the RAID controller cache to read and write operations.
Use Cache if Bad BBU check box	Check the **Use Cache if Bad BBU** check box to ensure that if the Battery Backup Unit (BBU) is not available for any reason, **Write back** will be disabled and **Write Through** will be enabled.
Strip Size (KB) drop- down	Allows specification, in KB, of the strip size for each disk within a stripe.

Step 4 Click **Submit**.

Editing RAID Policy for Splunk

Use this procedure to edit the local disk drive configuration associated with the hardware RAID controller for C220 and C240 M4/M5 servers, and for the standalone (PCH Controlled SSD disks) on C240 M4/M5 and C220 M5 servers.

Before you begin

- Create a UCS Service Profile Policy for the Splunk cluster deployment.
- Create a Local Disk Configuration Policy.

Step 1 On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, go to the **Configure Splunk RAID Policy** table and choose the node type.

Step 2 Click the **Edit selected entry in the table below** icon.

Step 3 On the **Edit Configure Splunk RAID Policy Entry** screen, complete the following fields:

Name	Description
Node Type	The selected node type.
OS Disks	
Use standalone boot drives check box	By default, this option is checked for Cisco UCS servers with sufficient standalone boot drives.

Name	Description
Use HDD drives on servers with insufficient standalone boot drives check box	Allows you to enable an alternate policy for Cisco UCS servers with insufficient standalone boot drives.
RAID Level [OS] drop-down list	Choose the RAID level for the OS (operating system) disks.
Disks Per Groups field	Specifies the number of disks that can exist per group during RAID configuration.
Write Mode drop-down list	Choose either **Write through** to write data without the RAID controller cache, or **Write back** to write data with the cache.
Read Mode drop down-list	Choose the method to read data from the disks.
Use Cache check box	Check the **Use Cache** check box to use the RAID controller cache to read and write operations.
Use Cache if Bad BBU check box	Check the **Use Cache if Bad BBU** check box to ensure that if the Battery Backup Unit (BBU) is not available for any reason, **Write back** will be disabled and **Write Through** will be enabled.
Strip Size (KB) drop- down list	Allows specification, in KB, of the strip size for each disk within a stripe.
Data Disks for Hot Data	
Use only NVMe disks [Hot] check box	Check the **Use only NVMe disks [Hot]** check box to choose NVMe disks.
RAID Level [Hot Data] drop-down list	Choose the RAID level for the splunk data disks.
Disks Per Groups field	Specifies the number of disks that can exist per group during RAID configuration.
Write Mode drop-down list	Choose either **Write through** to write data without the RAID controller cache, or **Write back** to write data with the cache. This field is not displayed when **Use only NVMe disks [Hot]** is checked.
Read Mode drop down-list	Choose the method to read data from the disks. This field is not displayed when **Use only NVMe disks [Hot]** is checked.
Use Cache check box	Check the **Use Cache** check box to use the RAID controller cache to read and write operations. This field is not displayed when **Use only NVMe disks [Hot]** is checked.

Name	Description
Use Cache if Bad BBU check box	Check the **Use Cache if Bad BBU** check box to ensure that if the Battery Backup Unit (BBU) is not available for any reason, **Write back** will be disabled and **Write Through** will be enabled. This field is not displayed when **Use only NVMe disks [Hot]** is checked.
Strip Size (KB) drop- down	Allows specification, in KB, of the strip size for each disk within a stripe. This field is not displayed when **Use only NVMe disks [Hot]** is checked.
Data Disks for Cold Data	
Same Disk As Hot Data check box	Check the check box to enable that the same disk is configured for Hot Data to also host Cold Data. **Note** By default, all RAID configurations are available in **Data Disks for Cold Data**. Checking this check box hides all RAID configuration for cold data.
Data Disks for Frozen Data	
Same Disk As Cold Data check box	Check the check box to enable that the same disk is configured for Cold Data to also host Frozen Data. **Note** By default, all RAID configurations are available in **Data Disks for Frozen Data**. Checking this check box hides all RAID configuration for frozen data.

Note
- The RAID configuration of Data disks for hot, cold, or frozen data is applicable only for Indexer nodes. The RAID configuration of OS disks applies to Search Head and Administrative nodes.
- One RAID group is created for each RAID configuration for hot, cold, or frozen data (for example, /data/disk1 for Hot, /data/disk2 for Cold, and /data/disk3 for Frozen).

Configuring Local Disk Partitions

Each partition in the disk has two attributes, mount point and size. You can create, edit, and delete partitions as per your requirements. The **Partition Configuration** table displays the /, /boot, swap, /tmp, /var/tmp, and /home partitions by default. You can update the size allocated for these partitions except for the root (/) and boot (/boot) partitions, but cannot delete the entries.

Table 1: Sample Partitions Table

Mount Point	Size	Editable
/	1 GB with grow	Not Editable
/boot	1024 MB	Not Editable
Swap	Any value	Editable
/tmp	5 GB	Editable
/var/tmp	5 GB	Editable
/home	5 GB	Editable

Step 1 On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, click **Add** in the **Partition Configuration** table.

Step 2 On the **Add Partition Configuration Entry** screen, enter the mount name in the **Mount Point** field.

Step 3 Enter the size in the **Size** field. The OS disk partition value can be greater than 50 GB. However, we recommend that you should allocate the OS disk partition value based on the available actual disk size.

Step 4 Click **Submit**.

Creating a Customized Service Profile Template

Step 1 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 **VLANs**.

Step 4 Click **Add (+)** to add three VLANs for creating three vNIC templates.

Step 5 In the right pane, click **Organizations**.

Step 6 Select the organization in which you want to create the service profile template and then click **View Details**.

Step 7 Click **vNIC Template** and click **Add (+)**.

Step 8 Create three vNIC templates using the created VLANs.

Step 9 Click **Boot Policy** and click **Add (+)** to create a Boot policy by adding a local disk.

Step 10 Click **QoS Policy** and click **Add (+)** to create a QoS policy.

Step 11 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 12 Click **Storage Policy** and specify the Cisco UCS connections for the storage policy.

Step 13 Click **Network Policy** and specify the required details.

Step 14 Click **vNIC** and create three vNICs by mapping the vNIC templates. The name of the vNIC should be eth0, eth1, and eth2 respectively. After the service profile template creation, vNIC name will be generated as eth0-1, eth1-2, and eth2-3 respectively.

Step 15 Click **Placement Policy** and specify the required details.

Step 16 Choose **Physical** > **Compute** > **Organizations**.

Step 17 Open the root and click **Service Profile Template**.

Step 18 Click **Add (+)** and choose the created policies and provide the required information.

Step 19 Click **Submit**.

Step 20 Log on to UCSM. Launch the created service profile template and update the desired placement as 1, 2, and 3 for the three vNIC templates respectively.

Step 21 Click **Save Changes**.

Note In the Storage module, select the **No vHBAs** option in the **How would you like to configure SAN connectivity?** field. This option 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.

Cloning a Cisco UCS Service Profile Template

Step 1 Choose **Solutions** > **Big Data** > **Containers**.

Step 2 Click **UCS SP Templates for Big Data**.

Step 3 Click the row for the template that you want to clone.

Step 4 Click **Clone**.

Step 5 In the **UCS SP Template Specification** page of the Clone UCS SP Template for Big Data wizard, do the following:

a) Enter a unique name and description for the new service profile template.
b) Choose the Template Type from the drop-down list.
c) Click **Next**, review the information on each page, and modify if necessary.
d) Click **Submit**.