Appendix

This chapter contains the following sections:

About Virtual SAN UCS Service Profile Templates

Cisco UCS Director VMware Virtual SAN implementation with UCS servers requires a standard configuration of a UCS service profile template. Cisco UCS Director workflows use the template to create service profiles with Virtual SAN specific configurations. You must make sure that the template follows the guidelines listed below.

Note Cisco UCS with VMware Virtual SAN implementation requires initiating a UCS service profile template, and it does not support updating an existing UCS service profile template.

When creating a Virtual SAN UCS service profile template, the template should not be associated with any server pool. You can select the **Assign Later** option in the server pool template, to assign the server pool to the Virtual SAN service profile.

In addition to any guidelines or recommendations that are specific to policies and pools included in service profiles and UCS service profile templates, you need to be aware of the following requirements for creating a Virtual SAN UCS service profile template.

- BIOS policy requirements
- Network configuration requirements
- Boot policy requirements
- Local disk configuration policy requirements

For an overview of requirements for setting up a Virtual SAN UCS service profile template, see Prerequisites for Creating a Virtual SAN from a Bare Metal Server.

For more information on creating Cisco UCS Manager service profile templates, see the Cisco UCS Manager GUI Configuration Guide.

Creating Virtual SAN UCS Service Profile Templates

Summary of Steps for Setting Virtual SAN Cisco UCS Manager Service Profile Template, Network, and Policy requirements

This procedure provides a high-level summary of the steps involved to satisfy the network configuration requirements, LAN boot policy requirements, and scrub policy requirements for setting up a Virtual SAN UCS service profile template.

Note The following procedures explain only how to kick-start templates for a Virtual SAN configuration. The steps are generic and will vary depending on your Cisco UCS Manager configuration. If any option is unavailable, refer to the Cisco UCS Manager GUI for the specific Cisco UCS Manager version.

Step 1 Define UUID suffix pools as described in Creating a UUID Suffix Pool, on page 2.

Step 2 Define MAC address pools as described in Creating a MAC Pool, on page 3.

Step 3 Define a multicast policy as described in Creating a Multicast Policy, on page 3.

Step 4 Define VLANs as described in Creating a Named VLAN, on page 4.

Step 5 Create a vNIC template with the VLANs defined as described in Creating a vNIC Template, on page 5.

Step 6 Create a QoS policy as described in Creating a QoS Policy, on page 6.

Step 7 Create and define a vNIC from the template as described in Creating a vNIC for a LAN Connectivity Policy, on page 7.

Step 8 Create a boot policy as described in Creating a Boot Policy, on page 7.

Step 9 Create a local disk configuration policy as described in Creating a Local Disk Configuration Policy, on page 8.

Step 10 Create a BIOS policy as described in Creating a BIOS Policy, on page 9.

Creating a UUID Suffix Pool

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Pools**.

Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **UUID Suffix Pools** and select **Create UUID Suffix Pool**.
Step 5 In the **Define Name and Description** page of the **Create UUID Suffix Pool** wizard, complete the required fields.
Step 6 Click **Next**.
Step 7 In the **Add UUID Blocks** page of the **Create UUID Suffix Pool** wizard, click **Add**.
Step 8 In the **Create a Block of UUID Suffixes** dialog box, complete the required fields.
Step 9 Click **OK**.
Step 10 Click **Finish** to complete the wizard.

What to do next

Include the UUID suffix pool in a service profile and/or template.

Creating a MAC Pool

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Pools**.
Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **MAC Pools** and select **Create MAC Pool**.
Step 5 In the **Define Name and Description** page of the **Create MAC Pool** wizard, complete the required fields.
Step 6 Click **Next**.
Step 7 In the **Add MAC Addresses** page of the **Create MAC Pool** wizard, click **Add**.
Step 8 In the **Create a Block of MAC Addresses** dialog box, complete the required fields.
Step 9 Click **OK**.
Step 10 Click **Finish**.

What to do next

Include the MAC pool in a vNIC template.

Creating a Multicast Policy

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Policies**.
Step 3 Expand the **root** node.
Step 4 Right-click the **Multicast Policies** node and select **Create Multicast Policy**.
Step 5 In the **Create Multicast Policy** dialog box, specify the name and IGMP snooping information.

For a Virtual SAN UCS service profile template, you must click the **Enabled** radio buttons in the **IGMP Snooping State** and **IGMP Snooping Querier State** fields. The **IGMP Snooping Querier IPv4 Address** must be the same subnet as the Cisco UCS Manager subnet.

Step 6 Click **OK**.

What to do next

Specify the multicast policy for the Virtual SAN VLAN.

Creating a Named VLAN

In a Cisco UCS domain that is configured for high availability, you can create a named VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Important VLANs with IDs from 4030 to 4047 and from 4094 to 4095 are reserved. You cannot create VLANs with IDs from this range. Until Cisco UCS Manager Release 4.0(1d), VLAN ID 4093 was in the list of reserved VLANs. VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration.

The VLAN IDs you specify must also be supported on the switch that you are using. For example, on Cisco Nexus 5000 Series switches, the VLAN ID range from 3968 to 4029 is reserved. Before you specify the VLAN IDs in Cisco UCS Manager, make sure that the same VLAN IDs are available on your switch.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN 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 In the **Navigation** pane, click **LAN**.

Step 2 On the **LAN** tab, click the **LAN** node.

Step 3 In the **Work** pane, click the **VLANs** tab.

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create VLANs** dialog box, complete the required fields.

Step 6 If you clicked the **Check Overlap** button, do the following:

a) Click the **Overlapping VLANs** tab and review the fields to verify that the VLAN ID does not overlap with any IDs assigned to existing VLANs.
b) Click the **Overlapping VSANs** tab and review the fields to verify that the VLAN ID does not overlap with any FCoE VLAN IDs assigned to existing VSANs.
c) Click **OK**.
d) If Cisco UCS Manager identified any overlapping VLAN IDs or FCoE VLAN IDs, change the VLAN ID to one that does not overlap with an existing VLAN.

Step 7 Click **OK**.

Cisco UCS Manager adds the VLAN to one of the following **VLANs** nodes:

- The **LAN Cloud** > **VLANs** node for a VLAN accessible to both fabric interconnects.
- The ***Fabric_Interconnect_Name*** > **VLANs** node for a VLAN accessible to only one fabric interconnect.

What to do next

Specify the previously created multicast policy name in the **Properties** area of the Virtual SAN VLAN **General** tab.

Creating a vNIC Template

Before you begin

This policy requires that one or more of the following resources already exist in the system:

- Named VLAN
- MAC pool
- QoS policy
- LAN pin group
- Statistics threshold policy

SUMMARY STEPS

1. In the **Navigation** pane, click **LAN**.
2. Expand **LAN** > **Policies**.
3. Expand the node for the organization where you want to create the policy.
4. Right-click the **vNIC Templates** node and choose **Create vNIC Template**.
5. In the **Create vNIC Template** dialog box, complete the required fields.
6. Check the **Enable Failover** checkbox.
7. In the **VLANs** area, use the table to select the VLANs to assign to vNICs created from this template.
8. In the **Policies** area, enter an integer between 1500 and 9000 for the **MTU** field.
9. Click **OK**.

DETAILED STEPS

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **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 **vNIC Templates** node and choose **Create vNIC Template**.

Step 5 In the **Create vNIC Template** dialog box, complete the required fields.

You must create two templates, specifying A and B fabrics, as your vNICs will be on separate fabrics for failover redundancy.

Step 6 Check the **Enable Failover** checkbox.

Step 7 In the **VLANs** area, use the table to select the VLANs to assign to vNICs created from this template.

Step 8 In the **Policies** area, enter an integer between 1500 and 9000 for the **MTU** field.

The MTU size must be set to 9000 for a jumbo frames network.

Step 9 Click **OK**.

What to do next

Include the vNIC template in a service profile.

Creating a QoS Policy

SUMMARY STEPS

1. In the **Navigation** pane, click **LAN**.
2. In the **LAN** tab, expand **LAN** > **Policies**.
3. Expand the node for the organization where you want to create the pool.
4. Right-click **QoS Policy** and select **Create QoS Policy**.
5. In the **Create QoS Policy** dialog box, complete the required fields.
6. Click **OK**.

DETAILED STEPS

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 In the **LAN** tab, expand **LAN** > **Policies**.

Step 3 Expand the node for the organization where you want to create the pool.

If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **QoS Policy** and select **Create QoS Policy**.

Step 5 In the **Create QoS Policy** dialog box, complete the required fields.

Step 6 Click **OK**.

What to do next

Include the QoS policy in a vNIC or vHBA template.

Creating a vNIC for a LAN Connectivity Policy

SUMMARY STEPS

1. In the **Navigation** pane, click **LAN**.
2. Expand **LAN** > **Policies** > *Organization_Name*.
3. Expand the **LAN Connectivity Policies** node.
4. Choose the policy to which you want to add a vNIC.
5. In the **Work** pane, click the **General** tab.
6. On the icon bar of the **vNICs** table, click **Add**.
7. In the **Create vNIC** dialog box, enter the name, select a **MAC Address Assignment**, and check the **Use vNIC Template** check box to use one the previously created vNIC templates.
8. In the Adapter Performance Profile area, choose **VMware** from the **Adapter Policy** drop-down menu.
9. Click **OK**.
10. Click **Save Changes**.

DETAILED STEPS

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **Policies** > *Organization_Name*.

Step 3 Expand the **LAN Connectivity Policies** node.

Step 4 Choose the policy to which you want to add a vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 On the icon bar of the **vNICs** table, click **Add**.

Step 7 In the **Create vNIC** dialog box, enter the name, select a **MAC Address Assignment**, and check the **Use vNIC Template** check box to use one the previously created vNIC templates.

Step 8 In the Adapter Performance Profile area, choose **VMware** from the **Adapter Policy** drop-down menu.

Step 9 Click **OK**.

Step 10 Click **Save Changes**.

What to do next

Create a total of three vNICs, two of which are on a separate fabric to provide failover redundancy.

Creating a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, Cisco recommends that you create a global boot policy that can be included in multiple service profiles or service profile templates.

Cisco UCS Director Virtual SAN workflows support installing ESXi with an SD card. You must define a boot policy with an SD card specified as the first boot device in the boot order.

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 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 **Boot Policies** and select **Create Boot Policy**.

The **Create Boot Policy** wizard displays.

Step 5 Enter a unique name and description for the policy.

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 is saved.

Step 6 (Optional) After you make changes to the boot order, check the **Reboot on Boot Order Change** check box to reboot all servers that use this boot policy.

For boot policies applied to a server with a non-Cisco VIC adapter, even if the **Reboot on Boot Order Change** check box is not checked, when SAN devices are added, deleted, or their order is changed, the server always reboots when boot policy changes are saved.

Step 7 (Optional) If desired, check the **Enforce vNIC/vHBA/iSCSI Name** check box.

- If checked, Cisco UCS Manager displays a configuration error and reports whether one or more of the vNICs, vHBAs, or iSCSI vNICs listed in the **Boot Order** table match the server configuration in the service profile.
- If not checked, Cisco UCS Manager uses the vNICs or vHBAs (as appropriate for the boot option) from the service profile.

Step 8 In the Boot Mode field, choose the **Legacy** or **UEFI** radio button.

Step 9 If you selected UEFI, check the **Boot Security** checkbox if you want to enable UEFI boot security.

Step 10 Click the down arrows to expand the **Local Devices** area.

Step 11 Click **Add SD Card** to add the device to the **Boot Order** table.

What to do next

Include the boot policy in a service profile and template.

After a server is associated with a service profile that includes this boot policy, you can verify the boot order in the **Boot Order Details** area on the **General** tab for the server.

Creating a Local Disk Configuration Policy

SUMMARY STEPS

1. In the **Navigation** pane, click **Servers**.
2. Expand **Servers** > **Policies**.
3. Expand the node for the organization where you want to create the policy.
4. Right-click **Local Disk Config Policies** and choose **Create Local Disk Configuration Policy**.
5. In the **Create Local Disk Configuration Policy** dialog box, specify the name and choose **No Raid** from the **Mode** drop-down menu.

6. Uncheck the **Protect Configuration** check box.
7. Click the **Enable** radio button in the **FlexFlash State** field.
8. If you are using two SD cards, click the **Enable** radio button in the **FlexFLash RAID Reporting State** field.
9. Click **OK**.

DETAILED STEPS

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 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 **Local Disk Config Policies** and choose **Create Local Disk Configuration Policy**.

Step 5 In the **Create Local Disk Configuration Policy** dialog box, specify the name and choose **No Raid** from the **Mode** drop-down menu.

Step 6 Uncheck the **Protect Configuration** check box.

Step 7 Click the **Enable** radio button in the **FlexFlash State** field.

Step 8 If you are using two SD cards, click the **Enable** radio button in the **FlexFLash RAID Reporting State** field.

Step 9 Click **OK**.

What to do next

Specify the local disk configuration policy in the service profile template.

Creating a BIOS Policy

Note pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 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 **BIOS Policies** and select **Create BIOS Policy**.

Step 5 On the **Main** page of the **Create BIOS Policy** wizard, enter a name for the BIOS policy in the **Name** field.

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 is saved.

Step 6 In the **Create BIOS Policy** wizard, do the following to configure the BIOS settings:

a) If you want to change a BIOS setting, click the desired radio button or make the appropriate choice from the drop-down list.

For descriptions and information about the options for each BIOS setting, see the Cisco UCS Manager GUI Configuration Guide.

b) Click **Next** after each page.

Step 7 On the **USB** page, click the **enabled** radio button in the **USB PORT: SD Card** field.

Step 8 After you have configured all of the BIOS settings for the policy, click **Finish**.

Configuring a LAN Boot for a Boot Policy

You can add a LAN boot policy to use with Virtual SAN actions and workflows. the LAN boot policy is used to PXE boot for ESXi installations.

This procedure continues directly from Creating a Boot Policy, on page 7.

Step 1 Click the down arrows to expand the **vNICs** area.

Step 2 Click the **Add LAN Boot** link.

Step 3 In the **Add LAN Boot** dialog box, enter the name of the vNIC that you want to use for the LAN boot in the **vNIC** field, then click **OK**.

The vNIC name needs to match the defined vNIC name for the UCS service profile template.

Step 4 Check the **Enforce vNIC/vHBA/iSCSI Name** check box.

Step 5 Do one of the following:

- Add another boot device to the **Boot Order** table.
- Click **OK** to finish.

Creating a Scrub Policy

You can add a FlexFlash scrub policy for use with Virtual SAN actions and workflows.

SUMMARY STEPS

1. In the **Navigation** pane, click **Servers**.
2. Expand **Servers** > **Policies**.
3. Expand the node for the organization where you want to create the policy.
4. Right-click **Scrub Policies** and select **Create Scrub Policy**.

5. In the **Create Scrub Policy** wizard, enter the name of the policy, and in the **FlexFlash Scrub** field, click the **Yes** radio button.
6. Click **OK**.

DETAILED STEPS

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 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 **Scrub Policies** and select **Create Scrub Policy**.

Step 5 In the **Create Scrub Policy** wizard, enter the name of the policy, and in the **FlexFlash Scrub** field, click the **Yes** radio button.

Step 6 Click **OK**.

Creating a Template for VM Provisioning

You cannot provision a Windows 2016 VM or a Windows 10 VM using an ISO image. You must create a template to provision these VMs.

Step 1 Login to the vCenter and create a blank virtual machine.

Select **Windows** as the guest operating system, and select **Microsoft Windows Server 2016 (64-bit)** as the version.

LSI Logic SAS is automatically selected as the SCSI Controller.

Step 2 Convert the virtual machine into a template.

Step 3 Run an inventory process.

For information on how to initiate an inventory process, see Collecting ISO Inventory

Step 4 Create a standard catalog. For information on creating a standard catalog, see Creating Catalogs for ISO-Based VM Provisioning

Be sure to specifiy the following:

- Check the **Provision New VM for ISO Mounting** check box
- In the **Template** field, select the blank VM template you created.

Step 5 Create a service request. For more information, see Creating Service Requests for ISO-Based VM Provisioning.

Known Issues with the Collect VMware Object Level Inventory task

Following are the known issues with the **Collect VMware Object Level Inventory** task:

- If you run the **Collect VMware Object Level Inventory** task on a host and select a virtual switch as the entity, the task initiates an inventory collection for all virtual switches present in the vCenter rather than limiting the inventory collection to the host that you selected.
- Entities selected in the **Collect VMware Object Level Inventory** task are independent of each other.

  When you run this task by selecting multiple entities, and try to filter objects, the inventory process runs at the account level of the selected entity. To elaborate, let us assume that you created two new VMs (VM11 and VM21) in two separate hosts (H1 and H2). While running this inventory task, you select the following two entities:

  - A host—in this example H1.
  - A VM but do not select a specific VM

  When the inventory process completes, instead of showing only the selected host on VM11, the report displays both VMs from both hosts (H1 and H2).