Service Profiles and Templates

Service Profile Templates

Service profile templates enable you to quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools. There are two types of service profile templates:

- Initial—Service profiles created from this template inherit all the properties of the template, but will not be updated when this template is updated.
- Updating—Service profiles created from this template remain connected, and will be updated when this template is updated.

Creating or Editing a Service Profile Template

Service profile templates created in Cisco UCS Central can be used on any of your registered Cisco UCS domains.

Note When you edit an existing template, you should click **Evaluate** to estimate the impact of the changes, such as requiring a server reboot. Changes made to a service profile template affect all service profiles that are bound to that template.

Procedure

Step 1 In the **Actions** bar, type **Create Service Profile Template** and press Enter.

Step 2 In **Basic**, select the **Organization** where you want to create the service profile template.

You can configure an **Asset Tag** to uniquely identify a server. This tag can be 16 characters long. You can specify the asset tag on the **Creating or Editing a Service Profile** dialog box. The asset tag is displayed in the **Servers Details** page as a read only field, and in the **Service Profile Detail** after you reboot.

a) Enter a **Name** and optional **Description** and **User Label** to help identify the service profile template.
b) Select the **Template Instantiation Mode** to determine whether service profiles created from this template will be updated when this template is updated.
c) Set the **Desired Power State on Association** to **Power Off** if you want all servers to be powered down after being associated, otherwise, select **On**.
d) Select whether to enable **Compatability Check on Migration Using Server Pool**.

You must select a server pool on the **Servers** tab if you select **Enabled**.

Step 3 Click **Identifiers** to assign identifiers for this service profile.

Click each identifier that you want to use. On the right, click the drop-down to display available pools and choose the one you want to use for this service profile template.

Step 4 In **LAN**, click **Policy** to assign existing policies or click **Advanced** to create new vNICs or iSCSI vNICs for this service profile template.

To create a new vNIC, click on + and specify the vNIC name and select the following properties:

- **Basic**— Select the **Fabric Interconnect**, **Fabric Failover** option (Enabled or disabled), **MTU**, and the **CDN Source** (vNIC Name or User Defined Name for the CDN source.
- **MAC Address**— Select the MAC address from a pool.
- **VLANs**— Specify or search for the VLAN name. You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100. You cannot set multiple native VLANs for a vNIC in a Service Profile. When you click on **Set as Native**, a **Configuation Error** results.
- **VLAN Groups**— Specify the VLAN Group name that you have created to group the VLANs.

For more information on creating vNICs, see .

Note We recommend that you choose existing policies for your LAN settings. Individual settings are not efficient for a scale environment.

Note You can configure a Native VLAN on each VLAN Group, and also on the vNIC while selecting a specific VLAN. However, only one Native VLAN can be configured in the collective pool of individual VLANs and VLAN Groups selected for a particular vNIC. A configuration error results on the Service Profile upon association if more than one Native VLAN is configured .

Step 5 In **SAN**, click **Policy** to assign existing policies or click **Advanced** to create new vHBAs and assign WWPN pools for this service profile template.

For more information on creating vHBAs, see .

Note We recommend that you choose existing policies for your SAN settings. Individual settings are not efficient for a scale environment.

Step 6 Click **Servers** to assign an existing server pool or server pool qualification policy.

You can click on the policies, use the drop-down option on the right, and select the server-related policies that you want to assign to this template.

Step 7 Click **Storage** to assign an existing local disk configuration policy or storage profile.

You can click on the policies, use the drop-down option on the right, and select the storage-related policies that you want to assign to this template.

Step 8 Click **Policies** to assign existing policies to the service profile template.

You can click on all service profile related policies, use the drop-down option on the right, and assign policies to this template.

Step 9 Click **Create**.

After you create a Service Profile, you can check the status of the deployment in the **Configration Status** window from the **Service Profile Details** page.

Service Profile Template Detail View

The Service Profile Template page displays detailed information about a service profile template. From here, you can:

- View audit logs
- Delete, clone, or rename the service profile template
- Create a service profile from this service profile template
- Configure the host interface placement

Service Profiles

Service profiles in Cisco UCS Central define servers and their storage and networking characteristics.

Note You cannot create service profiles directly in Cisco UCS Central. You must create a service profile template first.

Creating a Service Profile from a Template

Procedure

Step 1 In the **Actions** bar, type **Create Service Profile from Template** and press Enter.

Step 2 In **Basic**, select the **Service Profile Template to Instantiate** , and select the **Organization** where you want to create the service profile.

Step 3 Determine the type of **Service Profile Naming Convention** that you want to use. This can be one of the following:

- **Simple**—Enter the number of service profiles that you want to create, and the naming prefix for each service profile.

The service profiles are created using the format prefixX. For example, three service profiles would be called prefix1, prefix2, and prefix3.

- **Advanced**—Enter the prefix, suffix, number of service profiles, the first number, and the number of digits.

  The service profiles are created using the format prefixXXsuffix. For example, three service profiles starting at 400 and using 4 digits would be called prefix0400suffix, prefix0401suffix, and prefix0402suffix.

- **Manual Entry**—Enter the service profile names as comma separated values. A service profile will be created for each value entered.

Note You can create up to 99 service profiles at one time from a single template.

Step 4 In **Servers**, select an existing server pool or server pool qualification policy.

Note If the service profiles are created from an updating template, then after the service profile instances are created, making changes to the server pool or service pool qualification policy in the template will update the values that you selected here. This may potentially change the associated server to a different server if the server is rebooted.

Step 5 Click **Create**.

Binding a Service Profile to a Template

Procedure

Step 1 From the **Service Profile** page, click the **Tools** icon and choose **Bind to Template**.

Step 2 In **Service Profile Template to Instantiate**, choose the service profile template from the available list.

Step 3 Click **Bind**.

Unbinding a Service Profile from a Template

Procedure

Step 1 From the **Service Profile** page, click the **Tools** icon and choose **Unbind from Template**.

Step 2 In the Unbind from Template confirmation dialog, click **Yes**.

Manually Assigning a Server to a Service Profile

To watch a video manually assigning a server, see Video: Assigning a Server to a Global Service Profile Manually.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Profiles**.

Step 2 On the **Profiles** page, choose the service profile that you want to modify.

Step 3 On the **Service Profile** page, click the **Tools** icon and choose **Assign Server Manually**.

Step 4 Choose whether to enable **Compatibility Check On Migration Using Manual Assignment**.

Step 5 Choose the server that you want to assign to the service profile.

Step 6 Click **Assign**.

Configuring Interface Placement on a Service Profile or Service Profile Template

Procedure

Step 1 Click the **Browse Tables** icon and choose **Profiles** or **Templates**.

Step 2 Choose the service profile or service profile template that you want to edit.

Step 3 Click the **Tools** icon and choose **Configure Interface Placement**.

Step 4 In the **Configure Host Interface Placement** dialog box, in the **Placement** tab, choose whether to enable **Manual Interface Placement**.

If you choose **Disabled**, the system automatically assigns interfaces based on their PCI order.

Step 5 If you choose **Enabled**, add vHBAs or vNICs.

You can associate each vNIC or vHBA with a vCON, and then choose how to assign the Admin Host Port:

- **Any**—Allows Cisco UCS Central to determine the host port to which the vNIC or vHBA is assigned.
- **1**—Explicitly assigns the vNIC or vHBA to host port 1.
- **2**—Explicitly assigns the vNIC or vHBA to host port 2.

Step 6 In **Preference**, choose the **Virtual Slot Selection Preference** for each virtual slot.

Note This field is only present on service profile templates.

This can be one of the following:

- **All**—All configured vNICs and vHBAs can be assigned. This is the default.
- **Assigned Only**—vNICs and vHBAs must be explicitly assigned.
- **Exclude Dynamic**—Dynamic vNICs and vHBAs cannot be assigned.
- **Exclude Unassigned**—Unassigned vNICs and vHBAs cannot be assigned.
- **Exclude usNIC**—usNIC vNICs cannot be assigned.

Step 7 In **PCI Order**, click the up and down arrows to arrange the order.

Note If **Manual Interface Placement** is enabled, the PCI order is read-only.

Step 8 Click **Configure**.

Viewing Service Profile Configuration Status

Procedure

Step 1 Click the **Browse Tables** icon and choose **Profiles**.

Step 2 Click on a service profile to select it.

Step 3 On the service profile page, click the **Alerts** icon on the far right and select **Configuration Status**.

The Configuration Status page for the selected service profile displays.

Step 4 Click **Close** to close the window.

UUID Synchronization Behavior

For Cisco UCS M3 and greater server models, the UUID that is configured in Cisco UCS Manager is not synchronized with the UUID that is seen by the operating systems running on those servers. UUID synchronization flips the prefix of the UUID in Cisco UCS Manager to match the UUID on the server operating system. By default, the UUIDs are unsynchronized.

Note Changing the UUID synchronization behavior may cause the server to reboot.

The following guidelines apply to UUID synchronization:

- UUID synchronization is supported only for global service profiles.
- UUID synchronization is supported only on the following Cisco UCS Manager releases:
  - Cisco UCS Manager release 2.2(7) and above
  - Cisco UCS Manager release 3.1(2) and above
- UUID synchronization is not applicable on Cisco UCS M1 and M2 server models.
- If UUID synchronization is enabled, you must disable UUID synchronization before downgrading or upgrading to a Cisco UCS Manager version that does not support UUID synchronization.
- When changing the service profile to which a server is associated:
  - Cisco UCS M1 and M2 server models are automatically synchronized at association.

- If synchronization is enabled, Cisco UCS M3 and greater server models are automatically synchronized at association
- If synchronization is not enabled, Cisco UCS M3 and greater server models are not synchronized at association.

Configuring UUID Synchronization Behavior

Procedure

Step 1 Click the **Browse Tables** icon and choose **Profiles**.

Step 2 Choose the service profile that you want to modify.

Step 3 On the service profile page, click the **Tools** icon and choose **UUID Synchronization Behavior**.

Step 4 Choose whether to enable or disable UUID synchronization.

Step 5 Click **Save**.

Using Static IDs

Cisco UCS Central centralizes ID sourcing with pools. Centralizing IDs makes it simple to move objects between Cisco UCS domains.

Previously, you could only set static IDs by using a script. Now, you can still use a script if you choose to, but the UI provides an easier method. You can now manually create and enter, or copy and paste, static IDs into the UI static ID fields. You can set static IDs for the following addresses:

- MAC
- IP, both IPv4 and IPv6
- IQN
- WWPN
- WWNN
- UUID
- iSCSI Initiator IP

Setting the Management VLAN

When using static IDs for In-Band IPv4 and IPv6 addresses, you must first set the management VLAN.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Profiles**.

Step 2 Choose the global service profile for which you want to add static IDs.

Step 3 From the **Service Profile** page, click the **Edit** icon.

Step 4 Click the **LAN** icon.

Step 5 Click **Connectivity** and choose **Management VLAN**.

Step 6 Click the Management VLAN drop-down and select a VLAN.

Step 7 Click **Save**.

Assigning Static IDs

Before you begin

- Unbind the global service profile from the service profile template, if using an updating template.
- If using static IDs for In-Band IPv4 and IPv6 addresses, you must first set the management VLAN.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Profiles**.

Step 2 Choose the global service profile for which you want to add static IDs.

Step 3 From the **Service Profile** page, click the **Tools** icon and choose **Configure Static IDs**.

Step 4 In the various **Identifier** fields, enter the static IDs.

Static ID for WWNN or WWPN must be in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF.

Note You can access the IQN from both the Identifier section and the Interface section. If you set the IQN through the identifier, and then set it through the interface, the last ID overwrites the first, so be careful to only enter the IQN once. Conversely, if you set it in the interface first, setting it again through the identifier overwrites it.

Step 5 Click **Check Utilization** to check if the ID is available or in use.

Check the utilization every time you enter a static ID.

Step 6 Click **Clear Static ID** to erase the ID, when necessary.

Step 7 Click **Interfaces**.

Step 8 Click on an interface to activate the static ID field.

Step 9 Enter the static IDs in the various interface fields.

Step 10 Click **Save**.
Changing the UUID, WWNN, IQN or interface IDs causes the server to reboot.

Pool IDs

After setting static IDs, if you decide that you want to return to obtaining IDs from an ID pool, you can do it through editing the global service profile.

Switching Back to Pool IDs

Procedure

Step 1 Click the **Browse Tables** icon and choose **Profiles**.

Step 2 Choose the relevant global service profile.

Step 3 From the **Service Profile** page, click the **Edit** icon.

Step 4 Click **LAN**, select the appropriate fields, and select the drop-down arrow to select a pool from which to obtain IDs.

Step 5 Click **SAN**,select the appropriate fields and select the drop-down arrow to select a pool from which to obtain IDs.

Step 6 Click **Save**.

Resetting IDs

Cisco UCS Central updates the following addresses immediately, when you switch them back to the obtaining IDs from a pool.

- In-Band Management IP
- Out-of-Band Management IP
- iSCSI Initiator

The following IDs are not updated immediately. Therefore, you must reset the IDs manually.

- UUID
- IQN
- MAC
- WWNN
- WWPN

Resetting IDs Manually to Resolve IDs to a Global Pool

Procedure

Step 1 Click the **Browse Tables** icon and choose **Profiles**.

Step 2 Choose the global service profile for which you want to resolve the IDs.

Step 3 From the **Service Profile** page, click the **Identifiers** icon.

Step 4 In the assigned ID column, click the **Reset** icon for each identity.

Step 5 In the Reset ID from pool dialog, click **Reset** to confirm resetting the ID and resolving the statically assigned ID to a pool.

This step can take up to 10 seconds.

Step 6 Repeat for all identities that you want to manually reset.

Step 7 Click the **Connectivity** icon.

Step 8 In the Interfaces column, select the interface to manually reset.

Step 9 In the details column, find the assigned ID and click the **Reset** icon.

Step 10 In the Reset ID from pool dialog, click **Reset** to confirm resetting the IDs.

Step 11 Repeat for all valid interfaces.

Service Profile Views

From the **Service Profiles** page you can view a list of all service profiles in Cisco UCS Central, and filter which service profiles are displayed.

Service Profile Detail View

The Service Profile page displays detailed information about a service profile. You can view the following information on the selected service profile and its components:

- **Basic**—Displays the overall status and an overview of all the components within the selected service profile. You can configure an **Asset Tag** such as a serial number, to uniquely identify a server. This tag can be 32 characters long. You can specify the asset tag on the **Creating or Editing a Service Profile** dialog box. The asset tag is displayed in the **Servers Details** page as a read only field, and in the **Service Profile Detail** after you reboot.

  Note Asset tags are configurable directly on a service profile, and only on the associated servers. Consider the following points when you configure the asset tags:

  - Because the new asset tag needs to be picked up by the BIOS, configuring the asset tag will require a host reboot. The new tag will not take effect on the host OS until the next reboot.
  - Cisco UCS Manager will not automatically reboot the host when the asset tag is changed if the service profile is already associated. You must manually reboot the host (either through Cisco UCS Manager or through the host) in order for the new asset tag to take effect in BIOS.
  - On a standalone service profile or on a service profile derived from a template without a pool, you can set the asset tag before the association so that the tag can be applied directly on the BIOS. But if a template has a server pool mentioned, the association process could already complete before you configure the asset tag. In such cases, you have to manually reboot the server to view the asset tag.

- **Identifiers**—Displays a list of entities used to identify the service profile.
- **Connectivity**—Displays a list of connectivity-related information. Shows the list of VLANs and Netwrok Groups associated with the Service Profile under **Interfaces**.

- **FC Zones**—Displays a list of Fibre Channel zones included in the service profile. To create an FC Zone Profile, see Creating or Editing an FC Zone Profile, on page 12.
- **Server**—Displays a list of the storage-related policies and profiles included in the service profile.
- **Storage**—Displays a list of the storage-related policies and profiles included in the service profile.
- **Policies**—Displays a list of all the policies included in the service profile.

You can also perform the following tasks:

- View logs and configuration status.
- Create a service profile template from this service profile.
- Delete, clone, or rename the service profile.
- Assign or unassign a server.
- Reapply the configuration to the associated server.
- Configure the host interface placement.
- Configure zoning.
- Configure iSCSI targets.
- Configure Static IDs.
- Configure UUID synchronization behavior.
- Bind or unbind from the service profile template.
- Shut down or reset server.

  If you want to shutdown the server from a service profile, you can select one of the following **Graceful Shutdown** options to trigger a shutdown and reboot. If you choose **Enabled**, and if there is a maintenance policy assigned to the service profile, Cisco UCS Manager waits for the **Hard Shutdown Timer** value specified in Cisco UCS Central (Maintenance Policy) before it triggers a shutdown and reboot.

  > **Note** The **Hard Shutdown Timer** specifies time in seconds (150, 300, or 600) that Cisco UCS Manager waits before it triggers a shutdown and reboot. You can set this timer value in the global maintenance policy in the **Creating a Maintenance Policy** dialog box. If you choose **Enable** and there is no maintenance policy assigned, Cisco UCS Central waits for 150 seconds by default before triggering a shutdown. Otherwise, it will immediately shutdown and reboot. If you choose **Graceful Shutdown Disabled**, Cisco UCS Manager immediately triggers a shutdown and reboot.

- Launch Cisco UCS Manager for the specific Cisco UCS domain.

Note

- Your browser must have pop-ups enabled.
- For Cisco UCS Manager release 3.1(2) or later, this launches the HTML5 GUI. If the Cisco UCS Manager credentials match the credentials for your Cisco UCS Central login, then the system will automatically log in to the Cisco UCS Manager GUI without prompting for the login information.
- For Cisco UCS Manager release 3.1(1) or previous, this launches the Java-based GUI.

Creating or Editing an FC Zone Profile

FC Zone profile is a logical representation of all zoning needs for a VM, to represent a single data replication solution between a few storage arrays. An FC Zone Profile contains a collection of all member WWPNs along with their VSAN and FC Zoning enabled. You can create an FC Zone profile and directly deploy it. On Cisco UCS Manager, the **Admin State** appears as **Enabled**.

Before you begin

- FC Zone Active option must be enabled.
- The fabric interconnects on Cisco UCS Manager must have FC switching mode turned on.
- FC Zoning must be enabled on the VSANs. The FC Zone profiles will not deploy if FC Zoning is disabled.
- All FC Zones must have members associated with it and configured. They do not appear as deployed on the fabric interconnect, and their status is shown as inactive if no members are configured.

Procedure

Step 1 In the **Navigation** pane, expand **UCS Domains**.

Step 2 Click on a **Domain**, and then click the **Tools** icon and select **Create FC Zone Profile**.

Step 3 In the create **FC Zone Profile** dialog box, enter the **Name** and optional **Description** for the FC Zone Profile.

Step 4 In the **FC Zone Active** options, click **Enable** to create the zone set. This option is disabled by default.

Step 5 Click **Save**.

Step 6 In the **FC Zones** group, do the following:

a) Provide a name for the zone set you want to create, and select fabric interconnect **A** or **B** to make the zone set accessible.
b) Add the **VSAN** information for the zone set and ensure that it has FC zoning enabled.
c) Enter the **Member WWPN Address** for the zone set. You can add multiple WWPN addresses for a zone set.

Step 7 Click **Save** to create the zone profile. You can also edit to delete the zone profile you have created from the **Domain** dashboard.

Local Service Profile Detail View

The Local Service Profile page displays detailed information about a local service profile. Local service profiles are managed by Cisco UCS Manager.

You can perform the following tasks on the local service profile page:

- View fault logs.
- Shut down or reset server.
- Launch KVM.
- Launch Cisco UCS Manager Host Firmware Package tab to view the pack items. This option is available under **Policies** when there is an associated Service Profile.
- Launch Cisco UCS Manager for the specific Cisco UCS domain.

Note

- Your browser must have pop-ups enabled.
- For Cisco UCS Manager release 3.1(2) or later, this launches the HTML5 GUI. If the Cisco UCS Manager credentials match the credentials for your Cisco UCS Central login, then the system will automatically log in to the Cisco UCS Manager GUI without prompting for the login information.
- For Cisco UCS Manager release 3.1(1) or previous, this launches the Java-based GUI.

Templates Table

The **Templates** page allows you to view all templates in Cisco UCS Central. You can filter to view the following types of template:

- Chassis profile template
- Service profile template
- vHBA template
- vNIC template

From this page, you can:

- Add tags to one or more templates.
- Delete one or more templates.
- Click on a selected template to view the details page for that template.

Profiles Table

The **Profiles** page allows you to view all service profiles or all chassis profiles in Cisco UCS Central. Select either **Service Profiles** or **Chassis Profiles** from the top of the page.

From this page, you can:

- Filter which service profiles or chassis profiles are displayed.
- Add tags to one or more service profiles or chassis profiles.
- Delete one or more service profiles or chassis profiles.
- Click on a selected service profile or chassis profile to view the details page for that profile.

UCS Central Faults

Cisco UCS Central collects and displays all the Cisco UCS Central service profile and chassis profile faults on the **Fault Logs** page. To view these faults, click the **Faults** icon in the **Fault Summary** section of a service profile or chassis profile details page. The **Faults Logs** page displays information on the type and severity level of the fault and allows you to monitor and acknowledge the system faults.

The faults table includes the following information for each fault:

- **Code**—The ID associated with the fault
- **Timestamp**—Date and time at which the fault occurred
- **Type**—Origin of the fault
- **Cause**—Cause of the fault
- **Affected Object**—The component that is affected by this fault
- **Fault Details**—The details of the fault.
- **Severity**—The severity of the fault
- **Action**—Any action required by the fault

To manage the information that is collected, see .

Service Profile Server Faults

Cisco UCS Central collects and displays all the server faults associated with a service profile. To view server faults, click the **Faults** icon in the **Server Fault Summary** section of a **Service Profile** details page. The **Faults Logs** page displays information on the type and severity level of the fault and allows you to monitor and acknowledge the faults.

The faults table includes the following information for each fault:

- **Filters**—Filter the data in the table by severity, fault type, and timestamp.
- **Code**—The ID associated with the fault
- **Timestamp**—Date and time at which the fault occurred
- **Cause**—Cause of the fault
- **Affected Object**—The component that is affected by this fault
- **Fault Details**—The details of the fault.
- **Severity**—The severity of the fault
- **Action**—Any action required by the fault

Service Profile Faults

To view consolidated faults of both the service profile and associated servers, click the **Alerts** icon on the service profile page and choose **Faults**. The following information is displayed:

- **Filters**—Filter the data in the table by severity, fault type, and timestamp.
- **Code**—The ID associated with the fault
- **Timestamp**—Date and time at which the fault occurred
- **Cause**—Cause of the fault
- **Affected Object**—The component that is affected by this fault
- **Fault Details**—The details of the fault.
- **Severity**—The severity of the fault
- **Action**—Any action required by the fault

Service Profile Event Logs

Displays event logs for the selected service profile. This can include the following:

- **ID**—Unique identifier associated with the event that caused the fault
- **Timestamp**—Date and time at which the event occurred
- **Trig. By**—Type of user associated with the event
- **Affected Object**—The component that is affected by the event

Service Profile Audit Logs

Displays the audit logs for the selected service profile. This includes the following:

- Resources that were accessed
- Day and time at which the event occurred
- Unique identifier associated with the log message
- The user who triggered an action to generate the audit log. This can be an internal session or an external user who made a modification using the Cisco UCS Central GUI or the Cisco UCS Central CLI.
- The source that triggered the action
- The component that is affected