Network Policies

This chapter includes the following sections:

vNIC Template

This policy defines how a vNIC on a server connects to the LAN. This policy is also referred to as a vNIC LAN connectivity policy.

Cisco UCS Central does not automatically create a VM-FEX port profile with the correct settings when you create a vNIC template. If you want to create a VM-FEX port profile, you must configure the target of the vNIC template as a VM.

You need to include this policy in a service profile for it to take effect.

Note If your server has two Emulex or QLogic NICs (Cisco UCS CNA M71KR-E or Cisco UCS CNA M71KR-Q), you must configure vNIC policies for both adapters in your service profile to get a user-defined MAC address for both NICs. If you do not configure policies for both NICs, Windows still detects both of them in the PCI bus. Then because the second eth is not part of your service profile, Windows assigns it a hardware MAC address. If you then move the service profile to a different server, Windows sees additional NICs because one NIC did not have a user-defined MAC address.

Creating a vNIC Template

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **vNIC Templates** and choose **Create vNIC Template**.

Step 4 In the **Create vNIC Template** dialog box, enter the **Name** and optional description.

Step 5 Choose the **Fabric ID** and **Template Type**, enter the **MTU**, and choose a **Type**.
You can also create a MAC pool from this area.

Step 6 In the **VLANs** table, select the VLANs that you want to use.

Step 7 In the **Policies** area, choose a **MAC Pool**, **QoS Policy**, **Network Control Policy**, and **Stats Threshold Policy** from the drop-down lists, and enter the **Pin Group Name**.
You can also create a MAC pool, a QoS policy, a network control policy, and a threshold policy from this area.

Step 8 Click **OK**.

Deleting a vNIC Template

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **vNIC Templates**.

Step 4 Right-click the vNIC template that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Default vNIC Behavior Policy

Default vNIC behavior policy allows you to configure how vNICs are created for a service profile. You can choose to create vNICS manually, or you can allow them to be created automatically

You can configure the default vNIC behavior policy to define how vNICs are created. This can be one of the following:

- **None**—Cisco UCS Central does not create default vNICs for a service profile. All vNICs must be explicitly created.
- **HW Inherit**—If a service profile requires vNICs and none have been explicitly defined, Cisco UCS Central creates the required vNICs based on the adapter installed in the server associated with the service profile.

Note If you do not specify a default behavior policy for vNICs, **HW Inherit** is used by default.

Configuring Default vNIC Behavior

If you do not specify a default behavior policy for vNICs, **HWInherit** is used by default.

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
You can only configure the default vNIC behavior policy in the root organization. You cannot configure the default vNIC behavior policy in a sub-organization.

Step 3 Right-click **Default vNIC Behavior** and choose **Properties**.

Step 4 In the **Properties (Default vNIC Behavior)** dialog box, choose the **Action** and the optional **vNIC Template**.

Step 5 Click **OK**.

LAN and SAN Connectivity Policies

Connectivity policies determine the connections and the network communication resources between the server and the LAN or SAN on the network. These policies use pools to assign MAC addresses, WWNs, and WWPNs to servers and to identify the vNICs and 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.

Privileges Required for LAN and SAN Connectivity Policies

Connectivity policies enable users without network or storage privileges to create and modify service profiles and service profile templates with network and storage connections. However, users must have the appropriate network and storage privileges to create connectivity policies.

Privileges Required to Create Connectivity Policies

Connectivity policies require the same privileges as other network and storage configurations. For example, you must have at least one of the following privileges to create connectivity policies:

- admin—Can create LAN and SAN connectivity policies
- ls-server—Can create LAN and SAN connectivity policies
- ls-network—Can create LAN connectivity policies
- ls-storage—Can create SAN connectivity policies

Privileges Required to Add Connectivity Policies to Service Profiles

After the connectivity policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create connectivity policies.

Creating a LAN Connectivity Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **LAN Connectivity Policies** and choose **Create LAN Connectivity Policy**.

Step 4 In the **Create LAN Connectivity Policy** dialog box, enter the **Name** and optional description.

Step 5 Click **Create vNIC** in the **vNICs** area to add vNICs to the LAN connectivity policy.
The vNICs you create will be added to the **vNIC** table.

Step 6 Click **Create iSCSI vNIC** in the **iSCSI vNICs** area to add iSCSI vNICs to the LAN connectivity policy.
The iSCSI vNICs you create will be added to the **iSCSI vNIC** table.

Step 7 Click **OK**.

Creating a vNIC for a LAN Connectivity Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the LAN connectivity policy for which you want to create a vNIC.

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

Step 6 In the **vNICs** area, click **Create vNIC**.

Step 7 In the **Create vNIC** dialog box, enter the name, select a **MAC Address Assignment**, and check the **Use vNIC Template** check box if you want to use an existing vNIC template.
You can also create a MAC pool from this area.

Step 8 In the **Details** area, choose the **Fabric ID**, select the VLANs you want to use, and enter the **MTU**.

Step 9 In the **Pin Group** area, choose a **Pin Group Name**.

Step 10 In the **Operational Parameters** area, choose a **Stats Threshold Policy**.
You can also create a threshold policy from this area.

Step 11 In the **Adapter Performance Profile** area, choose an **Adapter Policy**, **QoS Policy**, and a **Network Control Policy**.
You can also create an ethernet adapter policy, a QoS policy, and a network control policy from this area.

Step 12 Click **OK**.

Creating an iSCSI vNIC for a LAN Connectivity Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the LAN connectivity policy for which you want to create an iSCSI vNIC.

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

Step 6 In the **iSCSI vNICs** area, click **Create iSCSI vNIC**.

Step 7 In the **Create iSCSI vNIC** dialog box, enter the name, choose the **Overlay vNIC**, **iSCSI Adapter Policy**, and **VLAN** from the drop-down lists, and select a **MAC Address Assignment**.
You can also create an iSCSI adapter policy and a MAC pool from this dialog box.

Step 8 Click **OK**.

Deleting a LAN Connectivity Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a vNIC from a LAN Connectivity Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the policy for which you want to delete the vNIC.

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

Step 6 In the **vNICs** table, click the vNIC you want to delete.

Step 7 On the **vNICs** table icon bar, click **Delete**.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting an iSCSI vNIC from a LAN Connectivity Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the policy for which you want to delete the iSCSI vNIC.

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

Step 6 In the **iSCSI vNICs** table, click the vNIC you want to delete.

Step 7 On the **iSCSI vNICs** table icon bar, click **Delete**.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Network Control Policy

This policy configures the network control settings for the Cisco UCS domain, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the virtual interface (VIF) behaves if no uplink port is available in end-host mode
- The action that Cisco UCS Central takes on the remote Ethernet interface, vEthernet interface , or vFibre Channel interface when the associated border port fails
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect
- Whether MAC registration occurs on a per-VNIC basis or for all VLANs

Action on Uplink Fail

By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. For adapters such as the Cisco UCS M81KR Virtual Interface Card, this default behavior directs Cisco UCS Central to bring the vEthernet or vFibre Channel interface down if the associated border port fails. For Cisco UCS systems using a non-VM-FEX capable converged network adapter that supports both Ethernet and FCoE traffic, such as Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, this default behavior directs Cisco UCS Central to bring the remote Ethernet interface down if the associated border port fails. In this scenario, any vFibre Channel interfaces that are bound to the remote Ethernet interface are brought down as well.

Note if your implementation includes those types of non-VM-FEX capable converged network adapters mentioned in this section and the adapter is expected to handle both Ethernet and FCoE traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Note that this configuration might result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

MAC Registration Mode

MAC addresses are installed only on the native VLAN by default, which maximizes the VLAN port count in most implementations.

Note If a trunking driver is being run on the host and the interface is in promiscuous mode, we recommend that you set the Mac Registration Mode to All VLANs.

Creating a Network Control Policy

MAC address-based port security for Emulex converged Network Adapters (N20-AE0102) is not supported. When MAC address-based port security is enabled, the fabric interconnect restricts traffic to packets that contain the MAC address that it first learns. This is either the source MAC address used in the FCoE Initialization Protocol packet, or the MAC address in an ethernet packet, whichever is sent first by the adaptor. This configuration can result in either FCoE or Ethernet packets being dropped.

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Network Control Policies** and choose **Create Network Control Policy**.

Step 4 In the **Create Network Control Policy** dialog box, enter the **Name** and optional description.

Step 5 Choose the **CDP**, **MAC Register Mode**, and **Action on Uplink Fail**.

Step 6 In the **MAC Security** area, choose whether to allow or deny forged MAC addresses.

Step 7 Click **OK**.

Deleting a Network Control Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Network Control Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Dynamic vNIC Connection Policy

The dynamic vNIC connection policy determines how the connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS domains that include servers with VIC adapters on which you have installed VMs and configured dynamic vNICs.

Ethernet Adapter Policy

Each dynamic vNIC connection policy includes an Ethernet adapter policy and designates the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

Server Migration

Note If you migrate a server that is configured with dynamic vNICs or another migration tool, the dynamic interface used by the vNICs fails and Cisco UCS Central notifies you of that failure.

When the server comes back up, Cisco UCS Central assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

Creating a Dynamic vNIC Connections Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Dynamic vNIC Connection Policies** and choose **Create Dynamic vNIC Connection Policy**.

Step 4 In the **Create Dynamic vNIC Connection Policy** dialog box, enter the **Name**, optional description, **Naming Prefix**, and **Number of Dynamic vNICs**.

Step 5 Choose the **Adapter Policy** from the drop-down list, and set the **Protection** level.

Step 6 Click **OK**.

Deleting a Dynamic vNIC Connections Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Dynamic vNIC Connections Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Quality of Service Policy

A 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 additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Creating a QoS Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **QoS Policies** and choose **Create QoS Policy**.

Step 4 In the **Create QoS Policy** dialog box, enter the **Name** and optional description.

Step 5 In the **Egress** area, choose a **Priority**, enter the **Burst(Bytes)** and **Rate(Kbps)**, and choose the **Host Control**.

Step 6 Click **OK**.

What to Do Next

Include the QoS policy in a vNIC or vHBA template.

Deleting a QoS Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **QoS Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.