Configuring a Service Profile with VM-FEX

This chapter includes the following sections:

Modifying the VMwarePassThrough Ethernet Adapter Policy

VM-FEX in high-performance mode has a system-provided VMwarePassThrough adapter policy. Most of the default settings are sufficient. However, you might need different settings than this policy provides to accommodate your particular implementation. If you need different settings, we recommend that you create another Ethernet adapter policy with your specific settings. In particular, you might want to check the following settings to make sure that they work with your particular implementation:

- Guest OS requirements
  - Transmit queue
  - Receive queue
  - Completion queues
  - Interrupts
- Maximum number of interfaces per host.
- Maximum number of interfaces in pass-through mode per host.

For more information about configuring an Ethernet adapter policy, see the *Cisco UCS Manager GUI Configuration Guide*.

Configuring Dynamic vNIC Connection Policies

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.

For VM-FEX that has all ports on a blade in standard mode, you need to use the VMware adapter policy.

For VM-FEX that has at least one port on a blade in high-performance mode, use the VMwarePassThrough adapter policy or create a custom policy. If you need to create a custom policy, the resources provisioned need to equal the resource requirements of the guest OS that needs the most resources and for which you will be using high-performance mode.

Static vNICs

Note In a VM-FEX deployment, a VM will attach to a dynamic vNIC only if the VIC adapter has two static vNICs, one for each fabric, attached to the DVS in vCenter. If a server contains more than one VIC adapter, each adapter must have two static vNICs configured.

Server Migration

Note If you migrate a server that is configured with dynamic vNICs using VMotion, the dynamic interface used by the vNICs fails and notifies you of that failure.

When the server comes back up, 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 Connection Policy

You can create a dynamic vNIC connection policy.

Procedure

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

Step 2 On the **LAN** tab, 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 **Dynamic vNIC Connection Policies** node and choose **Create Dynamic vNIC Connection Policy**.

Step 5 In the **Create Dynamic vNIC Connection Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of 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 has been saved. **Note** Do not specify "default" as the value for the dynamic vNIC connection policy name. Cisco UCS Manager automatically resolves any empty policy references to "default". Any service profiles or service profile templates with only static vNICS defined will automatically reference the policy "default" when it is present. If you specify “default” for the dynamic vNIC connection policy name, then unexpected dynamic vNICs might be created on those service profiles or service profile templates.
Description field	A description of the policy. We recommend that you include information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects. Enter an integer between 0 and 256. The default is 54. **Note** Components of your system might limit this number to fewer than 256 vNICs.
Adapter Policy drop-down list	The adapter profile associated with this policy. The profile must already exist to be included in the drop-down list.
Protection field	Dynamic vNICs are always protected in Cisco UCS, but this field allows you to select a preferred fabric, if any. You can choose one of the following: • **Protected Pref A—**Cisco UCS attempts to use fabric A but fails over to fabric B if necessary • **Protected Pref B—**Cisco UCS attempts to use fabric B but fails over to fabric A if necessary • **Protected—**Cisco UCS uses whichever fabric is available

Step 6 Click **OK**.

Step 7 If a confirmation dialog box appears, click **Yes.**

Changing a Dynamic vNIC Connection Policy

You can change a dynamic vNIC connection policy.

Procedure

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

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

Step 3 Expand the node for the organization that contains the policy that you want to change.
If the system does not include multitenancy, expand the **root** node.

Step 4 Expand the **Dynamic vNIC Connection Policies** node and click the policy that you want to change.

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

Step 6 Change one or more of the following fields:

Name	Description
Description field	A description of the policy. We recommend that you include information about where and when the policy should be used.
Number of Dynamic vNICs field	The number of dynamic vNICs that this policy affects.
Adapter Policy drop-down list	The adapter profile associated with this policy. The profile must already exist to be included in the drop-down list.

You cannot change the other properties of the policy, such as the **Name** field.

Step 7 Click **Save Changes**.

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

Deleting a Dynamic vNIC Connection Policy

You can delete a dynamic vNIC connection policy.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 On the **LAN** tab, expand **LAN** > **Policies** > *Organization_Name*.
Step 3 Expand the **Dynamic vNIC Connection Policies** node.
Step 4 Right-click the policy that you want to delete and choose **Delete**.
Step 5 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Viewing Dynamic vNIC Properties in a VM

You can view dynamic vNIC properties in a VM.

Before You Begin

The VM must be operational.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.
Step 2 On the VM tab, expand **All** > **VMware**.
Step 3 Expand **Virtual Machines**.
Step 4 Expand the virtual machine that contains the dynamic vNIC.
Step 5 Choose the dynamic vNIC.
Step 6 In the **Work** pane, click the **General** tab.
In the **Properties** area, the vNIC properties appear.

Configuring the VM Lifecycle Policy

VM Lifecycle Policy

The VM lifecycle policy determines how long Cisco UCS Manager retains offline VMs and offline dynamic vNICs in its database. If a VM or dynamic vNIC remains offline after that period, Cisco UCS Manager deletes the object from its database.

All virtual machines (VMs) on Cisco UCS servers are managed by vCenter. Cisco UCS Manager cannot determine whether an inactive VM is temporarily shut down, has been deleted, or is in some other state that renders it inaccessible. Therefore, Cisco UCS Manager considers all inactive VMs to be in an offline state.

Cisco UCS Manager considers a dynamic vNIC to be offline when the associated VM is shut down, or the link between the fabric interconnect and the I/O module fails. On rare occasions, an internal error can also cause Cisco UCS Manager to consider a dynamic vNIC to be offline.

The default VM and dynamic vNIC retention period is 15 minutes. You can configure a retention period of between 1 minute and 7200 minutes (2 days).

Note The VM database displayed by Cisco UCS Manager is for information and monitoring only. You cannot manage VMs through Cisco UCS Manager. If you delete a VM from the Cisco UCS Manager database, the VM is not deleted from the server or from vCenter.

Configuring the VM Lifecycle Policy

You can configure the VM lifecycle policy.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 On the **VM** tab, click **VMWare**.

Step 4 In the **Work** pane, click the **Life Cycle Policy** tab.

Step 5 In the **Life Cycle Policy** area, complete the following fields:

Name	Description
VM Retention field	The period of time that Cisco UCS Manager retains an offline VM in its database. If a VM remains offline after that period, Cisco UCS Manager deletes the VM from its database. This can be one of the following: • **1 Min** • **1 Hour** • **1 Day** • **other—**Cisco UCS Manager displays the **Minutes** field that allows you to specify a custom retention time.
Minutes field	Enter an integer between 1 and 7200 minutes (or 5 days).

Name	Description
vNIC Retention field	The period of time that Cisco UCS Manager retains an offline dynamic vNIC in its database. If a dynamic vNIC remains offline after that period, Cisco UCS Manager deletes the dynamic vNIC from its database. This can be one of the following: • **1 Min** • **1 Hour** • **1 Day** • **other—**Cisco UCS Manager displays the **Minutes** field that allows you to specify a custom retention time.
Minutes field	Enter an integer between 1 and 7200 minutes (or 5 days).

Step 6 Click **Save Changes**.

Creating a BIOS Policy for VM-FEX in High-Performance Mode

For VM-FEX in high performance mode, you must configure specific BIOS settings.

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 and Sparing Mode for RAS Memory, are not supported by all Cisco UCS servers.

We recommend that you name this BIOS policy as VMwarePassThru so that you can identify it as being used for VM-FEX in high-performance mode.

You must enable these specific parameters in the following BIOS settings:

- **Processor—**Enable Virtual Technology (VT) and Direct Cache Access.

  Note You must enable VT if you intend to run 64-bit VMs on the ESX/ESXi host. An ESX/ESXi host will not run 64-bit VMs unless VT is enabled.

- **Intel Directed IO—**Enable the following parameters:
  - VT for Directed IO
  - Interrupt Remap

- Coherency Support
- ATS Support
- Pass Through DMA Support

Configure the remaining BIOS settings, as appropriate.

For more information, see the *Cisco UCS Manager GUI Configuration Guide*.