



Configuring a Service Profile with VM-FEX

This chapter includes the following sections:

- [Modifying the VMwarePassThrough Ethernet Adapter Policy, page 1](#)
- [Configuring Dynamic vNIC Connection Policies, page 2](#)
- [Configuring the VM Lifecycle Policy, page 6](#)
- [Creating a BIOS Policy for VM-FEX in High-Performance Mode, page 8](#)

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.

**Note**

If you have VMs with two or more vCPUS and you have upgraded from earlier versions of VM-FEX for VMware to release 2.1, you need to manually modify the following parameters with the specified values:

- wq—Set this parameter to 4.
- comp-queues—Set this parameter to 8.
- interrupts—Set this parameter to 12.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A /org # scope eth-policy VMWarePassThru	Enters organization Ethernet policy mode for the system-provided adapter policy.
Step 3	Modify the Ethernet adapter policy settings.	(Optional) For more information about configuring an Ethernet adapter policy, see the <i>Cisco UCS Manager CLI Configuration Guide</i> .

The following example shows you how to modify a system-provided Ethernet adapter policy and commit the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope eth-policy VMWarePassThru
UCS-A /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

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.

**Note**

Do not configure dynamic vNICs in a non-VM-FEX environment. If you configure dynamic vNICs in a service profile in a non-VM-FEX environment, the ESX OS installation may lead to a purple screen of death (PSOD).

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 without any redundancy. 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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A /org # create dynamic-vnic-conn-policy <i>policy-name</i>	Creates the specified vNIC connection policy and enters organization vNIC connection policy mode. This name can be between 1 and 32 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.

	Command or Action	Purpose
		<p>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.</p>
Step 3	<pre>UCS-A /org/dynamic-vnic-conn-policy # set desc <i>description</i></pre>	<p>(Optional) Provides a description for the policy.</p> <p>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).</p> <p>If your description includes spaces or nonalphanumeric characters, you must begin and end your description with double quotation marks. The quotation marks do not appear in the description field of any show command output.</p>
Step 4	<pre>UCS-A /org/dynamic-vnic-conn-policy # set adapter-policy <i>policy-name</i></pre>	<p>Specifies the Ethernet adapter policy to use for this policy. The adapter policy must already exist.</p>
Step 5	<pre>UCS-A /org/dynamic-vnic-conn-policy # set dynamic-eth {<i>dynamic-eth-num</i> off}</pre>	<p>Specifies the number of dynamic vNICs to use for this policy.</p> <p>Enter an integer between 0 and 256. The default is 54.</p> <p>Note Components of your system may limit this number to fewer than 256 vNICs.</p>
Step 6	<pre>UCS-A /org/dynamic-vnic-conn-policy # set protection {protected protected-pref-a protected-pref-b}</pre>	<p>Dynamic vNICs are always protected in Cisco UCS, but this command allows you to select a preferred fabric, if any. You can choose one of the following options:</p> <ul style="list-style-type: none"> • protected—Cisco UCS uses whichever fabric is available. • 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.
Step 7	<pre>UCS-A /org/dynamic-vnic-conn-policy # commit-buffer</pre>	<p>Commits the transaction.</p>

The following example shows how to create a dynamic vNIC connection policy named MyDynVnicConnPolicy that uses the system-provided VMWarePassThru Ethernet adapter policy for 12 dynamic vNICs and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # create dynamic-vnic-conn-policy MyDynVnicConnPolicy
UCS-A /org/dynamic-vnic-conn-policy* # set adapter-policy VMWarePassThru
UCS-A /org/dynamic-vnic-conn-policy* # set desc "Dynamic vNIC for Eth policy"
UCS-A /org/dynamic-vnic-conn-policy* # set dynamic-eth 12
UCS-A /org/dynamic-vnic-conn-policy* # commit-buffer
UCS-A /org/dynamic-vnic-conn-policy #
```

Deleting a Dynamic vNIC Connection Policy

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope org <i>org-name</i>	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the <i>org-name</i> .
Step 2	UCS-A /org # delete dynamic-vnic-conn-policy <i>policy-name</i>	Deletes the specified vNIC connection policy.
Step 3	UCS-A /org # commit-buffer	Commits the transaction.

The following example shows how to delete the dynamic vNIC connection policy named MyDynVnicConnPolicy and commit the transaction:

```
UCS-A# scope org /
UCS-A /org # delete dynamic-vnic-conn-policy MyDynVnicConnPolicy
UCS-A /org* # commit-buffer
UCS-A /org #
```

Viewing Dynamic vNIC Properties in a VM

Before You Begin

The VM must be operational.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope system	Enters system mode.
Step 2	UCS-A /system # scope vm-mgmt	Enters VM management mode.
Step 3	UCS-A /system/vm-mgmt # scope vmware	Enters VMware mode.

	Command or Action	Purpose
Step 4	UCS-A /system/vm-mgmt/vmware # show virtual-machine	(Optional) Displays the running virtual machines.
Step 5	UCS-A /system/vm-mgmt/vmware # scope virtual-machine <i>uuid</i>	Enters command mode for the virtual machine that contains the dynamic vNIC.
Step 6	UCS-A /system/vm-mgmt/vmware/virtual-machine # show vnic [detail]	Displays the vNIC properties.

The following example shows how to display the properties of a dynamic vNIC in a VM:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # show virtual-machine
Virtual Machine:
  UUID: 420a00c8-934b-4ae3-6af5-2ce9b8bd0f44
  Service Profile: org-root/ls-PTS-ch6-7
  Server: sys/chassis-6/blade-7
  Status: Online
.
.
.
UCS-A /system/vm-mgmt/vmware # scope virtual-machine 420a08b0-cda7-9e0a-424f-01ec8653eea0
UCS-A /system/vm-mgmt/vmware/virtual-machine # show vnic detail

vNIC:
  Name: 4479
  Status: Online
  MAC Address: 00:50:56:8A:07:B5
  Profile Name: VM-mgmt
  Virtual Adapter: sys/chassis-1/blade-1/adapter-1/host-eth-9
  Vnic Dn: org-root/ls-PTS-ch1-1/ether-dynamic-prot-009
  Current Task:

UCS-A /system/vm-mgmt/vmware/virtual-machine #
```

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

Procedure

	Command or Action	Purpose
Step 1	Switch-A# scope system	Enters system mode.
Step 2	Switch-A /system # scope vm-mgmt	Enters VM management mode.
Step 3	Switch-A /system/vm-mgmt # scope vm-life-cycle-policy	Enters VM lifecycle policy mode.
Step 4	Switch-A /system/vm-mgmt/vm-life-cycle-policy # set vmretention {minutes 1-day 1-hour 5-days}	Specifies the period of time (minutes, one day, one hour, or five days) that an offline VM is retained in the database. If a VM remains offline after that period, it is deleted from the database. The <i>minutes</i> variable can be from 1 to 7200. The default is 15 minutes.
Step 5	Switch-A /system/vm-mgmt/vm-life-cycle-policy # set vnicretention {minutes 1-day 1-hour 5-days}	Specifies the period of time (minutes, one day, one hour, or five days) that an offline dynamic vNIC is retained in the database. If a dynamic vNIC remains offline after that period, it is deleted from the database. The <i>minutes</i> variable can be from 1 to 7200. The default is 15 minutes.
Step 6	Switch-A /system/vm-mgmt/vm-life-cycle-policy # commit-buffer	Commits the transaction to the system configuration.

The following example shows how to configure a one-day VM retention period and a one-hour vNIC retention period and commit the transaction:

```
Switch-A# scope system
Switch-A /system # scope vm-mgmt
Switch-A /system/vm-mgmt # scope vm-life-cycle-policy
Switch-A /system/vm-mgmt/vm-mgmt/vm-life-cycle-policy # set vmretention 1-day
Switch-A /system/vm-mgmt/vm-mgmt/vm-life-cycle-policy* # set vnicretention 1-hour
Switch-A /system/vm-mgmt/vm-mgmt/vm-life-cycle-policy* # commit-buffer
Switch-A /system/vm-mgmt/vm-mgmt/vm-life-cycle-policy #
```

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 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.