



Configuring Network-Related Policies

This chapter includes the following sections:

- [Configuring vNIC Templates, page 1](#)
- [Configuring Ethernet Adapter Policies, page 4](#)
- [Configuring Network Control Policies, page 7](#)

Configuring vNIC Templates

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.

Beginning in Cisco UCS, Release 2.0(2), Cisco UCS Manager 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.

Configuring a vNIC Template

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, type <i>/</i> as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create vnic-templ <i>vnic-templ-name</i> [eth-if <i>vlan-name</i>] [fabric { a b }] [target [adapter vm]] | <p>Creates a vNIC template and enters organization vNIC template mode.</p> <p>The target you choose determines whether or not Cisco UCS Manager automatically creates a VM-FEX port profile with the appropriate settings for the vNIC template. This can be one of the following:</p> <ul style="list-style-type: none"> • Adapter—The vNICs apply to all adapters. No VM-FEX port profile is created if you choose this option. • VM—The vNICs apply to all virtual machines. A VM-FEX port profile is created if you choose this option. |
| Step 3 | UCS-A /org/vnic-templ # set descr <i>description</i> | (Optional) Provides a description for the vNIC template. |
| Step 4 | UCS-A /org/vnic-templ # set fabric { a a-b b b-a } | <p>(Optional) Specifies the fabric to use for the vNIC. If you did not specify the fabric when creating the vNIC template in Step 2, you have the option to specify it with this command.</p> <p>If you want this vNIC to be able to access the second fabric interconnect if the default one is unavailable, choose a-b (A is the primary) or b-a (B is the primary).</p> <p>Note Do not enable fabric failover for the vNIC under the following circumstances:</p> <ul style="list-style-type: none"> • If the Cisco UCS domain is running in Ethernet Switch Mode. vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to the other. • if you plan to associate this vNIC with a server that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server. |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 5 | UCS-A /org/vnic-templ # set mac-pool <i>mac-pool-name</i> | The MAC address pool that vNICs created from this vNIC template should use. |
| Step 6 | UCS-A /org/vnic-templ # set mtu <i>mtu-value</i> | <p>The maximum transmission unit, or packet size, that vNICs created from this vNIC template should use.</p> <p>Enter an integer between 1500 and 9216.</p> <p>Note If the vNIC template has an associated QoS policy, the MTU specified here must be equal to or less than the MTU specified in the associated QoS system class. If this MTU value exceeds the MTU value in the QoS system class, packets may be dropped during data transmission.</p> |
| Step 7 | UCS-A /org/vnic-templ # set nw-control-policy <i>policy-name</i> | The network control policy that vNICs created from this vNIC template should use. |
| Step 8 | UCS-A /org/vnic-templ # set pin-group <i>group-name</i> | The LAN pin group that vNICs created from this vNIC template should use. |
| Step 9 | UCS-A /org/vnic-templ # set qos-policy <i>policy-name</i> | The quality of service policy that vNICs created from this vNIC template should use. |
| Step 10 | UCS-A /org/vnic-templ # set stats-policy <i>policy-name</i> | The statistics collection policy that vNICs created from this vNIC template should use. |
| Step 11 | UCS-A /org/vnic-templ # set type { initial-template updating-template } | Specifies the vNIC template update type. If you do not want vNIC instances created from this template to be automatically updated when the template is updated, use the initial-template keyword; otherwise, use the updating-template keyword to ensure that all vNIC instances are updated when the vNIC template is updated. |
| Step 12 | UCS-A /org/vnic-templ # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a vNIC template and commits the transaction:

```

UCS-A# scope org /
UCS-A /org* # create vnic template VnicTempFoo
UCS-A /org/vnic-templ* # set descr "This is a vNIC template example."
UCS-A /org/vnic-templ* # set fabric a
UCS-A /org/vnic-templ* # set mac-pool pool137
UCS-A /org/vnic-templ* # set mtu 8900
UCS-A /org/vnic-templ* # set nw-control-policy ncp5
UCS-A /org/vnic-templ* # set pin-group PinGroup54
UCS-A /org/vnic-templ* # set qos-policy QosPol5
UCS-A /org/vnic-templ* # set stats-policy ServStatsPolicy
UCS-A /org/vnic-templ* # set type updating-template
UCS-A /org/vnic-templ* # commit-buffer
UCS-A /org/vnic-templ #

```

Deleting a vNIC Template

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, type <i>/</i> as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete vnic-templ <i>vnic-templ-name</i> | Deletes the specified vNIC template. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the vNIC template named VnicTempFoo and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete vnic template VnicTempFoo
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Ethernet Adapter Policies

Ethernet and Fibre Channel Adapter Policies

These policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

**Note**

For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- **Max LUNs Per Target**—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs.
- **Link Down Timeout**—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- **Max Data Field Size**—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

**Important**

We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), you must use the following formulas to calculate values that work with Windows:

Completion Queues = Transmit Queues + Receive Queues

Interrupt Count = (Completion Queues + 2) rounded up to nearest power of 2

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

Completion Queues = 1 + 8 = 9

Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Configuring an Ethernet Adapter 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, type / as the <i>org-name</i> . |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 2 | UCS-A /org # create eth-policy <i>policy-name</i> | Creates the specified Ethernet adapter policy and enters organization Ethernet policy mode. |
| Step 3 | UCS-A /org/eth-policy # set comp-queue count <i>count</i> | (Optional) Configures the Ethernet completion queue. |
| Step 4 | UCS-A /org/eth-policy # set descr <i>description</i> | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 5 | UCS-A /org/eth-policy # set failover timeout <i>timeout-sec</i> | (Optional) Configures the Ethernet failover. |
| Step 6 | UCS-A /org/eth-policy # set interrupt { coalescing-time <i>sec</i> coalescing-type { idle min } count <i>count</i> mode { intx msi msi-x }} | (Optional) Configures the Ethernet interrupt. |
| Step 7 | UCS-A /org/eth-policy # set offload { large-receive tcp-rx-checksum tcp-segment tcp-tx-checksum } { disabled enabled } | (Optional) Configures the Ethernet offload. |
| Step 8 | UCS-A /org/eth-policy # set recv-queue { count <i>count</i> ring-size <i>size-num</i> } | (Optional) Configures the Ethernet receive queue. |
| Step 9 | UCS-A /org/eth-policy # set rss receivesidescaling { disabled enabled } | (Optional) Configures the RSS. |
| Step 10 | UCS-A /org/eth-policy # set trans-queue { count <i>count</i> ring-size <i>size-num</i> } | (Optional) Configures the Ethernet transmit queue. |
| Step 11 | UCS-A /org/eth-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example configures an Ethernet adapter policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create eth-policy EthPolicy19
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
UCS-A /org/eth-policy* # set failover timeout 300
UCS-A /org/eth-policy* # set interrupt count 64
UCS-A /org/eth-policy* # set offload large-receive disabled
UCS-A /org/eth-policy* # set recv-queue count 32
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

Deleting an Ethernet Adapter 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, type <i>/</i> as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete eth-policy <i>policy-name</i> | Deletes the specified Ethernet adapter policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the Ethernet adapter policy named EthPolicy19 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete eth-policy EthPolicy19
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Network Control Policies

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 VIF behaves if no uplink port is available in end-host mode
- The action that Cisco UCS Manager takes on the remote Ethernet interface, vEthernet interface, or vFibreChannel 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 Manager to bring the vEthernet or vFibreChannel 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 Manager to bring the remote Ethernet interface down if the associated border port fails. In this scenario, any vFibreChannel interfaces that are bound to the remote Ethernet interface are brought down as well.

**Note**

Cisco UCS Manager, release 1.4(2) and earlier did not enforce the **Action on Uplink Fail** property for those types of non-VM-FEX capable converged network adapters mentioned above. If the **Action on Uplink Fail** property was set to link-down, Cisco UCS Manager would ignore this setting and instead issue a warning. In the current version of Cisco UCS Manager this setting is enforced. Therefore, if your implementation includes one of those converged network adapters 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.

Please note that this configuration may result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

MAC Registration Mode

In Cisco UCS Manager, releases 1.4 and earlier, MAC addresses were installed on all of the VLANs belonging to an interface. Starting in release 2.0, MAC addresses are installed only on the native VLAN by default. In most implementations this maximizes the VLAN port count.

**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.

Configuring 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

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org / | Enters the root organization mode. |
| Step 2 | UCS-A /org # create nw-ctrl-policy <i>policy-name</i> | Creates the specified network control policy, and enters organization network control policy mode. |
| Step 3 | UCS-A /org/nw-ctrl-policy # {disable enable} cdp | Disables or enables Cisco Discovery Protocol (CDP). |
| Step 4 | UCS-A /org/nw-ctrl-policy # set uplink-fail-action {link-down warning} | Specifies the action to be taken when no uplink port is available in end-host mode. Use the link-down keyword to change the operational state of a vNIC to down when uplink connectivity is lost on the fabric interconnect, and facilitate fabric failover for vNICs. Use the warning keyword to maintain |

| | Command or Action | Purpose |
|---------------|---|--|
| | | server-to-server connectivity even when no uplink port is available, and disable fabric failover when uplink connectivity is lost on the fabric interconnect. The default uplink failure action is link-down. |
| Step 5 | UCS-A /org/nw-ctrl-policy # set mac-registration-mode {all-host-vlans only-native-vlan | Whether adapter-registered MAC addresses are added only to the native VLAN associated with the interface or added to all VLANs associated with the interface. This can be one of the following: <ul style="list-style-type: none"> • Only Native Vlan—MAC addresses are only added to the native VLAN. This option is the default, and it maximizes the port+VLAN count. • All Host Vlans—MAC addresses are added to all VLANs with which they are associated. Select this option if your VLANs are configured to use trunking but are <i>not</i> running in Promiscuous mode. |
| Step 6 | UCS-A /org/nw-ctrl-policy # create mac-security | Enters organization network control policy MAC security mode |
| Step 7 | UCS-A /org/nw-ctrl-policy/mac-security # set forged-transmit {allow deny} | Allows or denies the forging of MAC addresses when sending traffic. MAC security is disabled when forged MAC addresses are allowed, and MAC security is enabled when forged MAC addresses are denied. By default, forged MAC addresses are allowed (MAC security is disabled). |
| Step 8 | UCS-A /org/nw-ctrl-policy/mac-security # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a network control policy named ncp5, enables CDP, sets the uplink fail action to link-down, denies forged MAC addresses (enables MAC security), and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # create mac-security
UCS-A /org/nw-ctrl-policy/mac-security* # set forged-transmit deny
UCS-A /org/nw-ctrl-policy/mac-security* # commit-buffer
UCS-A /org/nw-ctrl-policy/mac-security #
```

Deleting a Network Control Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org / | Enters the root organization mode. |
| Step 2 | UCS-A /org # delete nwctrl-policy <i>policy-name</i> | Deletes the specified network control policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the network control policy named ncp5 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete nwctrl-policy ncp5
UCS-A /org* # commit-buffer
UCS-A /org #
```