Network Policies

This chapter includes the following sections:

Global VLAN

Cisco UCS Central enables you to define global VLANs in LAN cloud at the domain group root or at the domain group level. You can create a single VLAN or multiple VLANs in one operation.

Global VLAN resolution takes place in Cisco UCS Central prior to global service profiles deployment. If a global service profile references a global VLAN, and that VLAN does not exist, the global service profile deployment fails in the Cisco UCS domain due to insufficient resources. All global VLANs created in Cisco UCS Central must be resolved before deploying that global service profile.

Global VLANs are pushed to Cisco UCS along with the global service profiles that reference them. Global VLAN information is visible to Cisco UCS Manager only if a global service profile with reference to a global VLAN is deployed in that UCS domain. When a global VLAN is deployed and becomes available in the UCS domain, locally-defined service profiles and policies can reference the global VLAN. A global VLAN is not deleted when a global service profile that references it is deleted.

Note Beginning with Cisco UCS Manager Release 1.3, you can push global VLANs to Cisco UCS Manager without deploying a service profile. For more information, see Enabling Global VLANs in a Cisco UCS Manager Instance, on page 4.

You cannot delete a global VLAN from Cisco UCS Manager. If you want to delete a global VLAN from Cisco UCS Manager, you have to localize the VLAN and then delete it.

VLAN Org Permission

All VLANs configured in Cisco UCS Central are common to the orgs in which they are created. You must assign organization permissions before the Cisco UCS Manager instances that are part of the organizations can consume the resources. When you assign org permission to a VLAN, the VLAN is visible to those

organizations, and available to be referenced in service profiles maintained by the Cisco UCS Manager instances that are part of the organization.

VLAN name resolution takes place within the hierarchy of each domain group. If a VLAN with the same name exists in multiple domain groups, the organization permissions are applied to all VLANs with the same name across the domain groups.

You can create, modify or delete VLAN org permission.

Note Make sure to delete the VLAN org permission from the same org you created it in. On Cisco UCS Central GUI you can view the org structure where this VLAN is associated. But at the sub org level on the Cisco UCS Central CLI, you cannot view the VLAN org permission association hierarchy, so if you try to delete the VLAN at the sub org level on the Cisco UCS Central CLI the delete operation will fail.

Creating a Single VLAN

This procedure describes how to create a single VLAN in the domain group root or in a specifc domain group.

Important

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-group** *domain-name*	Enters the UCS domain group root.
Step 3	UCSC(resource-mgr) # **scope eth-uplink**	Enters Ethernet uplink command mode.
Step 4	UCSC(resource-mgr) /domain-group/eth-uplink # **create vlan** *vlan-namevlan-id*	Creates a VLAN and assigns a VLAN ID. **Note** The VLAN name is case sensitive.
Step 5	UCSC(resource_mgr)/domain-group/eth-uplink/vlan # **set mcastpolicy** *{default | policy-name}*	(Optional) Assigns a specific multicast policy name. If you do not enter a multicast policy name, the name is resolved from the Cisco UCS Manager domain upon deployment.
Step 6	UCSC(resource-mgr) /domain-group/eth-uplink/vlan# **commit-buffer**	Commits the transaction to the system.

The following example shows how to create a VLAN named Administration in the domain group root, assign it VLAN ID 15, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-group /
```

```
UCSC(resource-mgr) /domain-group # scope eth-uplink
UCSC(resource-mgr) /domain-group/eth-uplink create vlan Administration 15
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # commit-buffer
UCSC(resource-mgr) /domain-group/eth-uplink/vlan #
```

The following example shows how to create a VLAN named Administration in domain group 12, assign it VLAN ID 15, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-group 12
UCSC(resource-mgr) /domain-group # scope eth-uplink
UCSC(resource-mgr) /domain-group/eth-uplink create vlan Administration 15
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # commit-buffer
UCSC(resource-mgr) /domain-group/eth-uplink/vlan #
```

Creating Multiple VLANs

This procedure describes how to create multiple VLANs.

Important

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) #**scope domain-group** *domain-group*	Enters the UCS domain group root.
Step 3	UCSC(resource-mgr) #**scope eth-uplink**.	Enters Ethernet uplink command mode.
Step 4	UCSC(resource-mgr) /domain-group/eth-uplink #**create vlan** *vlan-name vlan-id*	Creates a VLAN and with the VLAN name and VLAN ID you enter. **Note** The VLAN name is case sensitive.
Step 5	UCSC (resource-mgr) /domain-group/eth-uplink/vlan # **set mcastpolicy** *{default | policy-name}*	(Optional) Assigns a particular multicast policy name. If you do not enter a multicast policy name, the name is resolved from the Cisco UCS Manager upon deployment.
Step 6	UCSC (resource-mgr) /domain-group/eth-uplink/vlan # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create two VLANs in domain group 12, assign multicast policies, and commit the transactions:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-group 12
UCSC(resource-mgr) /domain-group # scope eth-uplink
UCSC(resource-mgr) /domain-group/eth-uplink create vlan Administration 15
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # set mcastpolicy default
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # create vlan Finance 20
```

```
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # set mcastpolicy mpolicy
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # commit-buffer
UCSC(resource-mgr) /domain-group/eth-uplink/vlan
```

Enabling Global VLANs in a Cisco UCS Manager Instance

The **publish vlan** command allows you to use global VLANs that were created in Cisco UCS Central in a Cisco UCS Manager instance without deploying a service profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) #**scope domain-mgmt**	Enters the UCS domain management configuration mode.
Step 3	UCSC(resource-mgr) /domain-mgmt #**scope ucs-domain** *domain-ID*	Enters the UCS domain configuration mode for the specified domain ID. **Note** If you do not know the UCS domain ID, use the **show ucs-domain** command.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain #**publish vlan** *vlan_name* .	Pushes the selected global VLAN to the Cisco UCS Manager instance.

The following example shows how to enable global VLAN globVLAN in the local domain 1008:

```
UCSC# connect resource-mgr
UCSC(resource-mgr) # scope domain-mgmt
UCSC(resrouce-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resrouce-mgr) /domain-mgmt/ucs-domain # publish vlan globVLAN

Publish Vlan is a standalone operation. You may lose any uncommitted changes in this CLI
session.
Do you want to continue? (yes/no): yes
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Deleting a VLAN

This procedure describes how to delete a VLAN from a domain group.

Before You Begin

Consider the following points before deleting global VLANs in Cisco UCS Central:

- Before deleting global VLANs, ensure that any global service profiles that reference them are updated.
- Before deleting the last global VLAN from a domain group, you should remove its organization permissions.
- If you delete a global VLAN, it is also deleted from all registered Cisco UCS Manager instances that are associated with the domain groups in which the VLAN resides.

- Global service profiles that reference a global VLAN that is deleted in Cisco UCS Central will fail due to insufficient resources. Local service profiles that reference a global VLAN that is deleted will be set to virtual network ID 1.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-group** *{/ | domain-name}*	Enters the UCS domain group root or the domain group name you enter.
Step 3	UCSC(resource-mgr) # **scope eth-uplink**	Enters Ethernet uplink command mode.
Step 4	UCSC(resource-mgr) /domain-group/eth-uplink # **delete vlan***vlan-name*	Deletes the VLAN with the name you entered.
Step 5	UCSC(resource-mgr) /domain-group/eth-uplink # **commit-buffer**	Commits the transaction to the system.

The following example shows how to delete the VLAN named Finance from the domain group root and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-group /
UCSC(resource-mgr) /domain-group # scope eth-uplink
UCSC(resource-mgr) /domain-group/eth-uplink delete vlan Finance
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # commit-buffer
UCSC(resource-mgr) /domain-group/eth-uplink/vlan #
```

Creating VLAN Permissions for an Organization

This procedure describes how to assign a VLAN permission to organizations in Cisco UCS Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC# (resource-mgr) **scope org** *{org-name}*	Enters organization management mode for the organization name you enter.
Step 3	UCSC(resource-mgr) /org # **create vlan permit** *vlan-name*	Assigns the specified VLAN permission to the organization, and all of the suborganizations that belong to it. **Note** VLAN name is case sensitive.
Step 4	UCSC(resource-mgr) /org # **commit-buffer**	Commits the transaction to the system.

The follwing example shows how to assign the VLAN named Administration permission to Sub-Org1, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org Sub-Org1
UCSC(resource-mgr) /org #create vlan-permit Administration
UCSC(resource-mgr) /org* #commit-buffer
UCSC(resource-mgr) /org #
```

Deleting VLAN Permissions from an Organization

This procedure describes how to delete a VLAN Org permission in Cisco UCS Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC# (resource-mgr) **scope org** *{org-name}*	Enters organization management mode for the organization name you enter.
Step 3	UCSC(resource-mgr) /org # **delete vlan-permit** *vlan-name*	Deletes permission for the specified VLAN from the organization and all sub organizations that belong to it. **Note** VLAN name is case sensitive.
Step 4	UCSC(resource-mgr) /org # **commit-buffer**	Commits the transaction to the system.

The follwing example shows how to deleted permission for the VLAN named Administration from Sub-Org1, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org Sub-Org1
UCSC(resouce-mgr) /org #delete vlan-permit Administration
UCSC(resouce-mgr) /org* #commit-buffer
UCSC(resouce-mgr) /org #
```

Configuring MAC Pools

MAC Pools

A MAC pool is a collection of network identities, or MAC addresses, that are unique in their layer 2 environment and are available to be assigned to vNICs on a server. MAC pools created in Cisco UCS Central can be shared between Cisco UCS domains. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multi-tenancy, you can use the organizational hierarchy to ensure that MAC pools can only be used by specific applications or business services. Cisco UCS Central uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

Creating a MAC Pool

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type **/** as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create mac-pool** *pool-name*	Creates a MAC pool with the specified name, and enters organization MAC pool mode.
Step 4	UCSC(policy-mgr) /org/mac-pool # **set descr** *description*	(Optional) Provides a description for the MAC pool. **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	UCSC(policy-mgr) /org/mac-pool # **create block** *first-mac-addr last-mac-addr*	Creates a block (range) of MAC addresses, and enters organization MAC pool block mode. You must specify the first and last MAC addresses in the address range using the form *nn*:*nn*:*nn*:*nn*:*nn*:*nn*, with the addresses separated by a space. **Note** A MAC pool can contain more than one MAC address block. To create multiple MAC address blocks, you must enter multiple **create block** commands from organization MAC pool mode.
Step 6	UCSC(policy-mgr) /org/mac-pool/block # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to create another pool, wait at least 5 seconds.

The following example shows how to create a MAC pool named GPool1, provide a description for the pool, specify a block of suffixes to be used for the pool, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create mac-pool GPool1
UCSC(policy-mgr) /org/mac-pool* # set descr "This is MAC pool GPool1"
```

```
UCSC(policy-mgr) /org/mac-pool* # create block 00:A0:D7:42:00:01 00:A0:D7:42:01:00
UCSC(policy-mgr) /org/mac-pool/block* # commit-buffer
UCSC(policy-mgr) /org/mac-pool/block #
```

What to Do Next

Include the MAC pool in a vNIC template.

Deleting a MAC Pool

If you delete a pool, Cisco UCS Central does not reallocate any addresses from that pool that have been assigned to vNICs or vHBAs in Cisco UCS Manager. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete mac-pool** *pool-name*	Deletes the specified MAC pool.
Step 4	UCSC(policy-mgr) /org/ # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to delete another pool, wait at least 5 seconds.

The following example shows how to delete the MAC pool named GPool1 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete mac-pool GPool1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring Network Related Policies

Configuring the Default vNIC Behavior Policy

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 a Default vNIC Behavior Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the root organization mode.
Step 3	UCSC(policy-mgr)/org # **scope vnic-beh-policy**	Enters default vNIC behavior policy mode.
Step 4	UCSC(policy-mgr)/org/vnic-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	Specifies the default vNIC behavior policy. This can be one of the following: • **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. If you specify **hw-inherit**, you can also specify a vNIC template to create the vNICs.

	Command or Action	Purpose
		• **none**—Cisco UCS Central does not create default vNICs for a service profile. All vNICs must be explicitly created.
Step 5	UCSC(policy-mgr)/org/vnic-beh-policy # **commit-buffer**	Commits the transaction to the system configuration.

This example shows how to set the default vNIC behavior policy to **hw-inherit**:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr)/org # scope vnic-beh-policy
UCSC(policy-mgr)/org/vnic-beh-policy # set action hw-inherit
UCSC(policy-mgr)/org/vnic-beh-policy* # commit-buffer
UCSC(policy-mgr)/org/vnic-beh-policy #
```

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.

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.

Configuring a vNIC Template

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter **/** as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create vnic-templ** *vnic-templ-name* [**eth-if** *vlan-name*] [**fabric** {**a** | **b**}] [**target** [**adapter** | **vm**]]	Creates a vNIC template and enters organization vNIC template mode. The target you choose determines whether or not Cisco UCS Central automatically creates a VM-FEX port profile with the appropriate settings for the vNIC template. This can be one of the following: • **Adapter —**The vNICs apply to all adapters. No VM-FEX port profiles is created if you choose if you this option. • **VM —**The vNICs apply to all virtual machines. A VM-FEX port profiles is created if you choose this option.
Step 4	UCSC(policy-mgr) /org/vnic-templ # **set descr** *description*	(Optional) Provides a description for the vNIC template.
Step 5	UCSC(policy-mgr) /org/vnic-templ # **set fabric** {**a** | **a-b** | **b** | **b-a**}	(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. 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) . **Note** Do not enable fabric failover for the vNIC under the following circumstances: • 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 Central generates a configuration fault when you associate the service profile with the server.
Step 6	UCSC(policy-mgr) /org/vnic-templ # **set mac-pool** *mac-pool-name*	The MAC address pool that vNICs created from this vNIC template should use.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/vnic-templ # **set mtu** *mtu-value*	The maximum transmission unit, or packet size, that vNICs created from this vNIC template should use. Enter an integer between 1500 and 9216. **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.
Step 8	UCSC(policy-mgr) /org/vnic-templ # **set nw-control-policy** *policy-name*	The network control policy that vNICs created from this vNIC template should use.
Step 9	UCSC(policy-mgr) /org/vnic-templ # **set pin-group** *group-name*	The LAN pin group that vNICs created from this vNIC template should use.
Step 10	UCSC(policy-mgr) /org/vnic-templ # **set qos-policy** *policy-name*	The quality of service policy that vNICs created from this vNIC template should use.
Step 11	UCSC(policy-mgr) /org/vnic-templ # **set stats-policy** *policy-name*	The statistics collection policy that vNICs created from this vNIC template should use.
Step 12	UCSC(policy-mgr) /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 13	UCSC(policy-mgr) /org/vnic-templ # **commit-buffer**	Commits the transaction to the system configuration.

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

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

Deleting a vNIC Template

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete vnic-templ** *vnic-templ-name*	Deletes the specified vNIC template.
Step 4	UCSC(policy-mgr) /org* # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the vNIC template named VnicTemp42 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)UCS-A# scope org /
UCSC(policy-mgr) /org # delete vnic template VnicTemp42
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring LAN Connectivity Policies

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

You can create a LAN connectivity policy for LAN networks.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create lan-connectivity-policy** *policy-name*	Creates the specified LAN connectivity policy, and enters organization network control policy mode. 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.
Step 4	UCSC(policy-mgr) /org/lan-connectivity-policy # **set descr** *policy-name*	(Optional) Adds a description to the policy. We recommend that you include information about where and how 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).
Step 5	UCSC(policy-mgr) /org/lan-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows you how to create a LAN connectivity policy named Local_LAN:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
```

```
UCSC(policy-mgr) /org# create lan-connectivity-policy Local_LAN
UCSC(policy-mgr) /org/lan-connectivity-policy # set descr Local on site LAN policy
UCSC(policy-mgr) /org/lan-connectivity-policy # commit buffer
```

Creating a vNIC for a LAN Connectivity Policy

You can create a vNIC for a LAN connectivity policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope lan-connectivity-policy** *policy-name*	Enters organization network control policy mode.
Step 4	UCSC(policy-mgr) /org/lan-connectivity-policy # **enter vnic** *vnic-name*	Creates a vNIC and enters configuration mode for the specified vNIC.
Step 5	UCSC(policy-mgr) /org/lan-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows you how to add a vNIC called vNIC1 to an existing LAN connectivity policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope lan-connectivity-policy Local_LAN
UCSC(policy-mgr) /org/lan-connectivity-policy # enter vnic vNIC1
UCSC(policy-mgr) /org/lan-connectivity-policy # commit buffer
```

Creating an iSCSI vNIC for a LAN Connectivity Policy

You can create an iscsi vNIC for a LAN connectivity policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope lan-connectivity-policy** *policy-name*	Enters organization network control policy mode.
Step 4	UCSC(policy-mgr) /org/lan-connectivity-policy # **enter vnic-iscsi** *iscsi-vnic-name*	Creates an iSCSI vNIC and enters configuration mode for the specified iSCSI vNIC.
Step 5	UCSC(policy-mgr) /org/lan-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows you how to add an iSCSI vNIC called iSCSI_vNIC1 to an existing LAN connectivity policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope lan-connectivity-policy Local_LAN
UCSC(policy-mgr) /org/lan-connectivity-policy # enter vnic-iscsi iSCSI_vNIC1
UCSC(policy-mgr) /org/lan-connectivity-policy # commit buffer
```

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 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.

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	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create nw-ctrl-policy** *policy-name*	Creates the specified network control policy, and enters organization network control policy mode.
Step 4	UCSC(policy-mgr) /org/nw-ctrl-policy # {**disable** | **enable**} **cdp**	Disables or enables Cisco Discovery Protocol (CDP).
Step 5	UCSC(policy-mgr) /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 server-to-server connectivity even when no uplink port is available, and disable fabric failover when uplink

	Command or Action	Purpose
		connectivity is lost on the fabric interconnect. The default uplink failure action is link-down.
Step 6	UCSC(policy-mgr) /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: • **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 Vlan—**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 *not* running in Promiscuous mode.
Step 7	UCSC(policy-mgr) /org/nw-ctrl-policy # **create mac-security**	Enters organization network control policy MAC security mode
Step 8	UCSC(policy-mgr) /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 9	UCSC(policy-mgr) /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:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create nw-ctrl-policy ncp5
UCSC(policy-mgr) /org/nw-ctrl-policy* # enable cdp
UCSC(policy-mgr) /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCSC(policy-mgr) /org/nw-ctrl-policy* # create mac-security
UCSC(policy-mgr) /org/nw-ctrl-policy/mac-security* # set forged-transmit deny
UCSC(policy-mgr) /org/nw-ctrl-policy/mac-security* # commit-buffer
UCSC(policy-mgr) /org/nw-ctrl-policy/mac-security #
```

Deleting a Network Control Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the root organization mode.
Step 3	UCSC(policy-mgr) /org # **delete nwctrl-policy** *policy-name*	Deletes the specified network control policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

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

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete nwctrl-policy ncp5
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring Dynamic vNIC Connections 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.

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

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create dynamic-vnic-conn-policy** *policy-name*	Creates a dynamic vNIC connectivity policy.
Step 4	UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # **set adapter-policy** *profile-name*	Associates the adapter profile to the policy.
Step 5	UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # **set dynamic-eth** *value*	(Optional) Displays 54, the default number. You can enter an integer between 0 to 256 for the number of dynamic vNICs this policy affects.
Step 6	UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # **set protection protected-pref-a**	(Optional) Protects dynamic vNIC connectivity policy. 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 A—** Cisco UCS attempts to use fabric B but fails over to fabric A if necessary • **Protected—**Cisco UCS uses whichever fabric is available
Step 7	UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # **commit-buffer**	Commits the transaction to the system configuration.

Following example creates a dynamic vNIC connectivity policy called g-DyVCONPol-1, sets adapter profile g-ethPol-1 to associate with the policy, and commits the transaction.

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr) /org # create dynamic-vnic-conn-policy g-DyVCONPol-1
UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # set adapter-policy g-ethPol-1
UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # commit-buffer
UCSC(policy-mgr) /org /dynamic-vnic-conn-policy #
```

Deleting a Dynamic vNIC Connection Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **delete dynamic-vnic-conn-policy** *policy-name*	Deletes the specified dynamic vNIC connection policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the dynamic vNIC connection policy named sample-1 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete dynamic-vnic-conn-policy sample-1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring Quality of Service Policies

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.

Configuring a QoS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters org mode for the specified organization. To enter the default org mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create qos-policy** *policy-name*	Creates the specified QoS policy, and enters org QoS policy mode.
Step 4	UCSC(policy-mgr) /org/qos-policy # **create egress-policy**	Creates the egress policy (for both vNICs and vHBAs) to be used by the QoS policy, and enters org QoS policy egress policy mode.
Step 5	UCSC(policy-mgr) /org/qos-policy/egress-policy # **set host-cos-control** {**full** | **none**}	(Optional) Specifies whether the host or Cisco UCS Central controls the class of service (CoS) for a vNIC. This setting has no effect on a vHBA. Use the **full** keyword to have the host control the CoS. If the packet has a valid CoS value, the host uses that value. Otherwise, it uses the CoS value associated with the specified class priority. Use the **none** keyword to have Cisco UCS Central use the CoS value associated with the specified priority.
Step 6	UCSC(policy-mgr) /org/qos-policy/egress-policy # **set prio** *sys-class-name*	Specifies the system class to be used for the egress policy. The *sys-class-name* argument can be one of the following class keywords: • **FC—**Use this priority for QoS policies that control vHBA traffic only. • **Platinum—**Use this priority for QoS policies that control vNIC traffic only. • **Gold—**Use this priority for QoS policies that control vNIC traffic only. • **Silver—**Use this priority for QoS policies that control vNIC traffic only. • **Bronze—**Use this priority for QoS policies that control vNIC traffic only. • **Best Effort—**Do not use this priority. It is reserved for the Basic Ethernet traffic lane. If you assign this priority to a QoS policy and configure another system class as CoS 0, Cisco UCS Central does not default to this system class. It defaults to the priority with CoS 0 for that traffic.
Step 7	UCSC(policy-mgr) /org/qos-policy/egress-policy # **set rate** {**line-rate** | *kbps*} **burst** *bytes*	Specifies the rate limit for egress traffic by defining the average traffic rate and burst size. The **line-rate** keyword sets the rate limit to the physical line rate. Rate limiting is supported only on vNICs on Cisco VIC 1240 and Cisco VIC 1280. M81KR supports rate limiting on both vNICs and vHBAs.

	Command or Action	Purpose
Step 8	UCSC(policy-mgr) /org/qos-policy/egress-policy # **committ-buffer**	Commits the transaction to the system configuration.

The following example creates a QoS policy for vNIC traffic, assigns the platinum system class and sets the rate limit (traffic rate and burst size) for the egress policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create qos-policy VnicPolicy34
UCSC(policy-mgr) /org/qos-policy* # create egress-policy
UCSC(policy-mgr) /org/qos-policy/egress-policy* # set prio platinum
UCSC(policy-mgr) /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
UCSC(policy-mgr) /org/qos-policy/egress-policy* # commit-buffer
UCSC(policy-mgr) /org/qos-policy/egress-policy #
```

The following example creates a QoS policy for vHBA traffic, assigns the fc (Fibre Channel) system class and sets the rate limit (traffic rate and burst size) for the egress policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create qos-policy VhbaPolicy12
UCSC(policy-mgr) /org/qos-policy* # create egress-policy
UCSC(policy-mgr) /org/qos-policy/egress-policy* # set prio fc
UCSC(policy-mgr) /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
UCSC(policy-mgr) /org/qos-policy/egress-policy* # commit-buffer
UCSC(policy-mgr) /org/qos-policy/egress-policy #
```

What to Do Next

Include the QoS policy in a vNIC or vHBA template.

Deleting a QoS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete qos-policy** *policy-name*	Deletes the specified QoS policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following deletes the QoS policy named QosPolicy34 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
```

```
UCSC(policy-mgr) /org # delete qos-policy QosPolicy34
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```