Network Configuration after Cluster Setup

Creating a QoS 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.

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.

You can configure the system classes shown in the following table:

Table 1: System Classes

System Class	Description
Platinum Gold Silver Bronze	Configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies.

System Class	Description
Best Effort	Sets the quality of service for the lane reserved for basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class.
Fibre Channel	Sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class. **Note** FCoE traffic has a reserved QoS system class that should not be used by any other type of traffic. If any other type of traffic has a CoS value that is used by FCoE, the value is remarked to 0.

To create a Qos Policy in UCS Manager, perform the following steps:

Step 1 Open a web browser and enter the IP address for Cisco UCS Manager. Enter the login credentials.

Step 2 In the **Navigation** pane, click **LAN**.

Step 3 In the **LAN** tab, expand **LAN** > **Policies**.

Step 4 Expand the **root** node > **Sub-org > hx-cluster**

Step 5 Right-click **QoS Policy** and select **Create QoS Policy**.

Step 6 In the **Create QoS Policy** dialog, complete the fields for your systems class as shown in the following table:

QoS Policy Name	QoS Class	Burst Size	Rate	Host Control
Platinum	Platinum	10240	Line-rate	none
Gold	Gold	10240	Line-rate	none
Silver	Silver	10240	Line-rate	none
Bronze	Bronze	10240	Line-rate	none
Best Effort	Best Effort	10240	Line-rate	none

Step 7 Click **OK**.

Creating MAC Address Pools

You can change the default MAC address blocks to avoid duplicate MAC addresses that may already exist. Each block contains 100 MAC addresses by default to allow for up to 100 HX servers for deployment per UCS system. We recommend that you use one MAC pool per vNIC for easier troubleshooting.

Note The 8th digit is set to either A or B. The *A* is set on vNICs pinned to Fabric Interconnect (FI) A. The *B* is set on vNICs pinned to FI B.

Step 1 Open a web browser and enter the IP address for Cisco UCS Manager. Enter the login credentials.

Step 2 In Cisco UCS Manager, navigate to **LAN tab** > **Pools** > **root** > **Sub-org** > **hx-cluster** > **MAC Pools**.

Step 3 Right-click **MAC Pools** and select **Create MAC Pool**.

Step 4 In the **Define Name and Description** page of the **Create MAC Pool** wizard, complete the required fields as shown in the following table:

MAC Pool Name	**Description**	**Assignment Order**	**MAC Address block**
hv-mgmt-a	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:01:01-64
hv-mgmt-b	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:02:01-64
storage-data-a	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:03:01-64
storage-data-b	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:04:01-64
vm-network-a	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:05:01-64
vm-network-b	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:06:01-64
hv-vmotion-a	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:07:01-64
hv-vmotion-b	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:08:01-64

Step 5 Click **Next**.

Step 6 In the **Add MAC Addresses** page of the **Create MAC Pool** wizard, click **Add**.

Step 7 In the **Create a Block of MAC Addresses** dialog box, complete the following fields:

Entry	**Description**
First MAC Address field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.

Step 8 Click **OK**.

Step 9 Click **Finish**.

After the MAC address change, the software reconfigures ESXi to how it was configured earlier. But, if management IP was DHCP assigned, then the IP changes.

Impact of Manufacturing process on MAC address change

- The MAC address will change between the manufacturing process and the customer site, especially if the customer orders HyperFlex serves without UCS Fabric Interconnects.
- A MAC address is configured during Service Profile association. It is un-configured during Service Profile disassociation.

- At the end of manufacturing process, the service profiles are disassociated, hence the MAC addresses are un-configured.
- When a HyperFlex server is deployed, configure the MAC address pools as described earlier.
- VMware supports consistent device naming, but issues have been reported since 5.5.SR has been opened.

Creating VLANs for HX Servers

Step 1 Open a web browser and enter the IP address for Cisco UCS Manager. Enter the login credentials.

Step 2 Navigate to **LAN tab** > **LAN** > **LAN Cloud** > **VLANS**.

Step 3 Right-click and select Create VLANs as shown in the table below:

VLAN Name	Description	Multicast Policy Name	
hx-inband-mgmt	Used for: • ESX management • SSH to storage controller VM • HX Cluster management IP - using multicast traffic. • vCenter connectivity to the HyperFlex VM for the HX Data Platform plug-in	HyperFlex	3091
hx-storage-data	Used for: • ESX NFS client (IOvisor) • HyperFlex replication/cluster • Cluster data VIP	HyperFlex	3092
hx-vmotion	Used for: • VM and storage vmotion, FT, iSCSI	HyperFlex	3093

VLAN Name	Description	Multicast Policy Name	
insert existing vlan name	Used for: • VM data traffic	HyperFlex	Any*

Note:

- Configuration option is Common/Global. It applies to both fabrics and uses the same configuration parameters in both cases.
- *There is no specific recommendation for VM data VLANs. You can create your own VLANs for the VM data traffic. By default, the HXDP installer will not create VLANs for the VM data traffic.

About Private VLANs

A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing you to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. A private VLAN domain has only one primary VLAN. Each port in a private VLAN domain is a member of the primary VLAN, and the primary VLAN is the entire private VLAN domain.

Understanding Private VLAN Ports

Table 2: Types of Private VLAN Ports

VLAN Port	Description
Promiscuous Primary VLAN	Belongs to the primary VLAN. Can communicate with all interfaces that belong to those secondary VLANs that are associated to the promiscuous port and associated with the primary VLAN. Those interfaces include the community and isolated host ports. All packets from the secondary VLANs go through this VLAN.
Isolated Secondary VLAN	Host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports.
Community Secondary VLAN	Host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.

Following HX deployment, a VM network uses a regular VLAN by default. To use a Private VLAN for the VM network, see the following sections:

- Configuring a Private VLAN on a VM Network without Existing VMs, on page 7.
- Configuring a Private VLAN on a VM Network with Existing VMs, on page 7.

Configure the vSwitches

In both VMware ESX and ESXi host, you can configure vSwitches from either the GUI or the command line.

The CLI configurations are very helpful when you are installing multiple ESX servers and planning to script the vSwitch configuration.

After the ESX installation, configure your vSwitches on the ESX host with the following steps:

Step 1 Log in to the command line of each ESX Server.

Step 2 Create three vSwitches on each ESX server using the listed names.

- **vswitch-hx-storage-data**

  Set the MTU to 9000 on this switch.

- **vmotion**

  Set the MTU to 9000 on this switch.

- **vswitch-hx-vm-network**

Step 3 Use the following CLI commands to create the three new vSwitches:

```
# esxcli network vswitch standard add -v vswitch-hx-storage-data

# esxcli network vswitch standard set -v vswitch-hx-storage-data -mtu= 9000

# esxcli network vswitch standard add -v vswitch-vmotion

# esxcli network vswitch standard set -v vswitch-vmotion -mtu=9000

# esxcli network vswitch standard add -v vswitch-hx-vm-network
```

Step 4 The default vSwitch **vSwitch0** created during installation of ESXi needs to be renamed to **vswitch-hx-inband-mgmt** for the Hx Data Platform node set up scripts to work properly. Use the following command to rename the switch and then reboot the host so that the vmkernel re-reads its configuration file to use the new name.

```
# sed -i 's/vSwitch0/vswitch-hx-inband-mgmt/g' /etc/vmware/esx.conf

# reboot
```

Step 5 You can verify the creation and renaming of the vSwitches after a host reboot with the following command:

```
# esxcli network vswitch standard list
```

Confirm that you see the four previously listed vSwitches in the command output. Only the switch-hx-inband-mgmt vSwitch will have Uplinks and Port groups listed. The HX Data Platform installer scripts perform the rest of the network configuration.

Configuring a Private VLAN on a VM Network without Existing VMs

Step 1 To configure a private VLAN on Cisco UCS Manager, see the Cisco UCS Manager Network Management Guide.

Step 2 To configure a private VLAN on the upstream switch, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide.

Step 3 To configure a private VLAN on ESX hosts, see Configuring Private VLAN on ESX Hosts, on page 7.

Configuring a Private VLAN on a VM Network with Existing VMs

Step 1 To configure a private VLAN on Cisco UCS Manager, see the Cisco UCS Manager Network Management Guide.

Step 2 To configure a private VLAN on the upstream switch, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide.

Step 3 To configure a private VLAN on ESX hosts, see Configuring Private VLAN on ESX Hosts, on page 7

Step 4 Migrate VMs from vSphere standard switch to the newly created vSphere distributed switch.

a) Right-click the vCenter Virtual Machine and click **Migrate Virtual Machine Networking**.
b) Choose **source network** and **destination network** from the drop-down list.
c) Click **Next**.
d) Select the **Virtual Machines** that you want to migrate.
e) Click **Finish**.

Step 5 Change network connection of the network adapter on the VMs to private VLAN.

a) Right-click the vCenter Virtual Machine and click **Edit Settings**.
b) Under the **Hardware** tab, select the network adapter you want to modify.
c) Select the **Network Connection** you want to use from the **Network Label** drop-down list.
d) Click **OK**.

Configuring Private VLAN on ESX Hosts

To configure private VLANs on the ESX hosts do the following:

Step 1 Delete VMNICs on the vSphere Standard Switches from the VMware vSphere Client.

Step 2 Create new vSphere Distributed Switch with the VMNICs deleted from the previous step.

Step 3 Create promiscuous, isolated, and community VLAN.

Deleting VMNICs on the vSphere Standard Switch

Step 1 Log on to VMware vSphere Client.

Step 2 Select **Home** > **Hosts and Clusters**.

Step 3 Select the ESX host from which you want to delete the VMNIC.

Step 4 Open the **Configuration** tab.

Step 5 Click **Networking**.

Step 6 Select the **switch** you wish to remove a VMNIC from.

Step 7 Click the **Manage the physical adapters connected to the selected switch** button.

Step 8 Select the `vminc` you want to delete and click **Remove**.

Step 9 Confirm your selection by clicking **Yes**.

Step 10 Click **Close**.

Creating vSphere Distributed Switch

Step 1 Log on to the VMware vSphere Client.

Step 2 Select **Home** > **Networking**.

Step 3 Right click on the cluster **Distributed Switch** > **New Distributed Switch**.

Step 4 In the **Name and Location** dialog box, enter a name for the distributed switch.

Step 5 In the **Select Version** dialog box, select the distributed switch version that correlates to your version and configuration requirements.

Step 6 Click **Next**.

Step 7 In the **Edit Settings** dialog box, specify the following:

- Number of uplink ports
- **Enable** Network I/O Control.
- **Create a default port group** should be checked.
- Enter the default port group **name** in the **Port Group Name** box.

Step 8 Click **Next**.

Step 9 Review the settings in the **Ready to complete** dialog box.

Step 10 Click **Finish**.

Creating Private VLANs on vSphere Distributed Switch

Step 1 From the VMware vSphere Client, select **Inventory** > **Networking**.

Step 2 Right-click on the dvSwitch.

Step 3 Click **Edit Settings**.

Step 4 Select the **Private VLAN** tab.

Step 5 On the **Primary private VLAN ID** tab, enter a `private VLAN ID`.

Step 6 On the **Secondary private VLAN ID** tab, enter a `private VLAN ID`.

Step 7 Select the type of VLAN from the **Type** drop-down list. Valid values include:

- **Isolated**
- **Community**
- **Promiscuous** (Default)

Step 8 Click **OK**.

Set Private VLAN in Distributed Port Group

Before you begin

Create Private VLAN on the vSphere Distribute Switch.

Step 1 Right click **dvPortGroup** under **dvSwitch**, and click **Edit Settings**.

Step 2 Click **Policies** > **VLAN**.

Step 3 Select **Private VLAN**, from the **VLAN type** drop-down list.

Step 4 From the **Private VLAN Entry** drop-down list, select the type of private VLAN. It can be one of the following:

- **Isolated**
- **Community**

Note Community private VLAN is recommended.

Promiscuous ports are not supported

Step 5 Click **OK**.

Migrating vMotion Networks to Virtual Distributed Switches (VDS) or Cisco Nexus 1000v (N1Kv)

Note

- The HX Data Platform can be configured with VMware DVS or Cisco Nexus 1000v for specific non-HX dependent networks:

  vMotion networks

  and virtual machine networks

- For further details, see Cisco Nexus 1000v documentation.

To migrate non-HX dependent vSwitches and associated port groups to DVS or N1Kv networks, follow the listed steps:

Step 1 From vCenter, create DVS Switch and port groups.

a) Select **vCenter Inventory Lists** > **Datacenters** > **datacenter** > **Related Objects** > **Distributed Switches** . Click **Add Distributed Switch** icon.

b) Complete the New Distributed Switch wizard. Create each DVS switch with two uplinks.

   For example: VM network and vmotion pg

   - DVSwitch-VMNetwork: DVPortGroup-VMNetwork
   - DVSwitch-Vmotion: DVPortGroup-Vmotion

Step 2 Migrate the vSwitch, VMNetwork. Perform the following steps to migrate VMNetwork from legacy vSwitch to DVS.

a) Select **vCenter Inventory Lists** > **Datacenters** > **datacenter** > **Related Objects** > **Distributed Switches**.

b) Select the **DVSwitch-VMNetwork** vSwitch. Click the **Add and Manage Hosts** icon. This starts the **Add and Manage Hosts** wizard.

c) On the Select task page, select **Add Hosts**. Click **Next**.

d) On the Select hosts page, click **Add New Hosts**. Select all hosts in the cluster. Click **Next**.

e) On the Select network adapter tasks page, select **Manage physical adapters** and **Migrate virtual machine** networking. Click **Next**.

f) On the Manage physical network adapters page, the physical adapters part of vswitch-hx-vm-network:VM Network are assigned to the DVSwitch-VMNetwork.

g) Under the **On other switches/unclaimed list**, select the vmnic corresponding to the **In Use by Switch**, vswitch-hx-vm-network.

h) Click **Assign** uplink.

i) Select Auto-assign.

j) Click **OK**. The page refreshes with the newly assigned vmnic listed under **On this switch**.

k) The **Analyze impact** page shows the impact of this migration. Verify the impact is all green. Click **Next**.

l) On the Migrate VM networking page, select the VMs to migrate to the new network, DVPortGroup-VMNetwork.

   Next

Select all the VMs, except the controller VMs, stCtlVM, from all the hosts. Select the DVPortGroup-VMNetwork. Click **Next**.

Note The list of VMs for each host includes all the VMs, including the controller VMs. DO NOT select any controller VMs. Migrating the controller VMs will break your storage cluster.

m) On the Ready to complete page, confirm the summary of the migration. Click Finish.

Note Post migration system generates several network related alarms. Verify and clear the alarms.

Step 3 Migrate the vSwitch to vmotion pg. Perform the following steps to migrate vmotion pg from legacy vSwitch to DVS.

a) Select **vCenter Inventory Lists** > **Datacenters > datacenter > Related Objects > Distributed Switches**.
b) Select the DVSwitch-Vmotion vSwitch. Click the **Add and Manage Hosts** icon. This starts the **Add and Manage Hosts** wizard.
c) On the Select task page, select **Add Hosts**. Click **Next**.
d) On the Select hosts page, click **Add New Hosts**. Select all hosts in the cluster. Click **Next**.
e) On the Select network adapter tasks page, select the tasks Manage physical adapters and Manage VMkernel adapters. Click **Next**.
f) On the **Manage physical network adapters** page, the physical adapters part of vmotion:vmotion pg are assigned to the DVSwitch-Vmotion.

   Under the **On other switches/unclaimed** list, select the vmnic corresponding to the In Use by Switch, vmotion. Click **Assign uplink**, select Auto-assign, and click OK. The page refreshes with the newly assigned vmnic listed under **On this switch**. Click **Next**.

g) On the **Manage VMkernel network adapters** page, migrate the VMkernel adapter to the port group, DVPortGroup-Vmotion.

   For each host, under the **On other switches** list, select the VMKernel adapter corresponding to the **In Use by Switch**, vmotion. Click **Assign port group**. Select the destination port group, DVPortGroup-Vmotion. Click **OK**. The page refreshes with the Reassigned VMkernel network adapters, listing the Source Port Group and Destination Port Group.

h) Select the hosts to migrate to the new network, DVPortGroup-Vmotion. Click **Next**.
i) On the Ready to complete page, confirm the summary of the migration, click **Finish**.

Step 4 Post migration step. Verify there is no impact on the VMs with respect to IO, Network connectivity and VM Migration.

Reset Stats Daemon

Description

A network daemon listens for statistics, like counters and timers, sent over UDP or TCP and sends aggregates to one or more pluggable backend services.

After manually re-installing ESX on your HX Data Platform servers, reset the stats daemon to ensure performance statistics display correctly.

Action: restart stats daemon

Step 1 Login to the command line of the controller VM of the ESX host.

Step 2 Run the restart command.

```
# /etc/init.d/statsd restart
```

Step 3 Repeat Step 1 and Step 2 on the controller VM of every ESX host in the storage cluster.