Handling Traffic Using VN−Link

Document ID: 112140

Contents

Introduction

Cisco VN−Link in hardware is a hardware−based method of handling traffic to and from a virtual machine on a server with a VIC adapter. This method is sometimes referred to as pass−through switching. This solution replaces software−based switching with ASIC−based hardware switching and improves performance.

The distributed virtual switch (DVS) framework delivers VN−Link in hardware features and capabilities for virtual machines on Cisco UCS servers with VIC adapters. This approach provides an end−to−end network solution to meet the new requirements created by server virtualization. With VN−link in hardware, Layer 2 traffic between two VMs on the same host is not locally switched on the DVS but it sent upstream to the UCs−6100 for the policy application and switching. Switching occurs in the fabric interconnect (hardware). As a result, network policies can be applied to traffic between virtual machines. This capability provides consistency between physical and virtual servers.

Note: VMotion is supported in the VN−Link Hardware.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Enterprise Plus License must be installed on the ESX hosts. This is **required** for DVS switching function.

Components Used

The information in this document is based on these software and hardware versions. All components in the chassis and blades have been upgraded to 1.3.1c.

- Cisco UCS 6120XP 2x N10−S6100
- 1 N20−C6508
- 2x N20−B6620−2
- Cisco UCS VIC M81KR Virtual Interface Card 2x N20−AC0002

These three main components must be connected for VN−Link in hardware to work:

- **VMware ESX Host**

  A server with the VMware ESX installed. It contains a datastore and the virtual machines. The ESX host must have a Cisco M81KR VIC installed, and it must have uplink data connectivity to the network for communication with VMware vCenter.
- **VMware vCenter**

  Windows−based software used to manage one or more ESX hosts. VMware vCenter must have connectivity to the UCS management port for management plane integration, and uplink data connectivity to the network for communication with the ESX Host. A vCenter extension key provided by Cisco UCS Manager must be registered with VMware vCenter before the Cisco UCS instance can be acknowledged.
- **Cisco UCS Manager**

  The Cisco UCS management software that integrates with VMware vCenter to handle some of the network−based management tasks.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Cisco UCS Manager must have management port connectivity to VMware vCenter for management plane integration. It also provides a vCenter extension key that represents the Cisco UCS identity. The extension key must be registered with VMware vCenter before the Cisco UCS instance can be acknowledged.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

Network Configuration VLAN and IP Ranges Used

- UCS Management VLAN 8¡72.21.60.64/26

- VC/ESX Management VLAN 103¡72.21.61.192/26
- Public VLAN 100¡0.21.60.0/24
- VLAN numbers used 8,100,103

vCenter IP

- − 172.21.61.222

Host IPs

- ESX Hosts

1. − pts−01 − 172.21.61.220
2. − pts−02 − 172.21.61.221

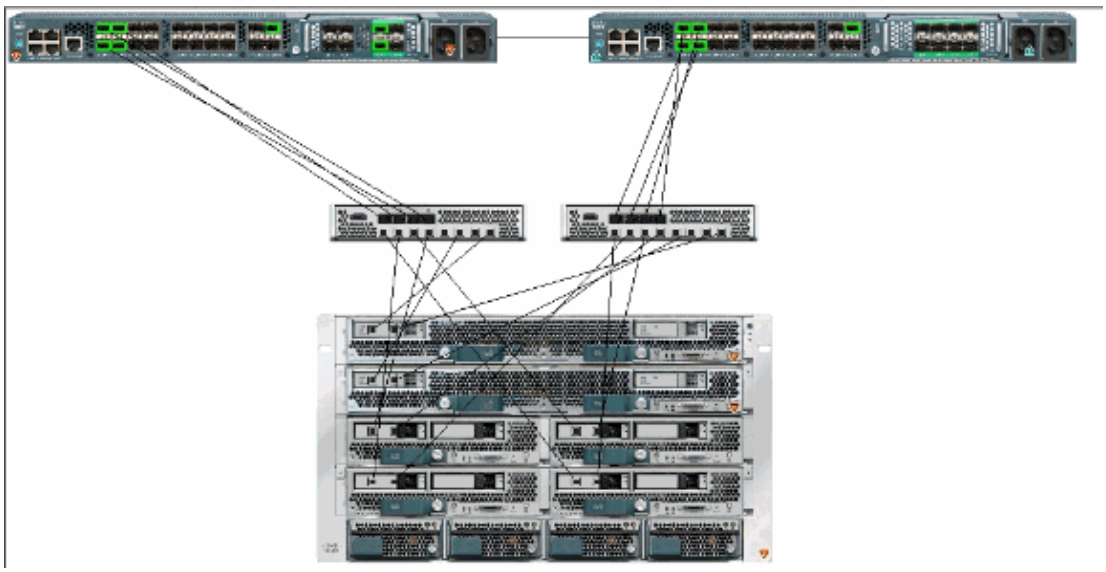
VM IPs

- RHEL5.5 VMs

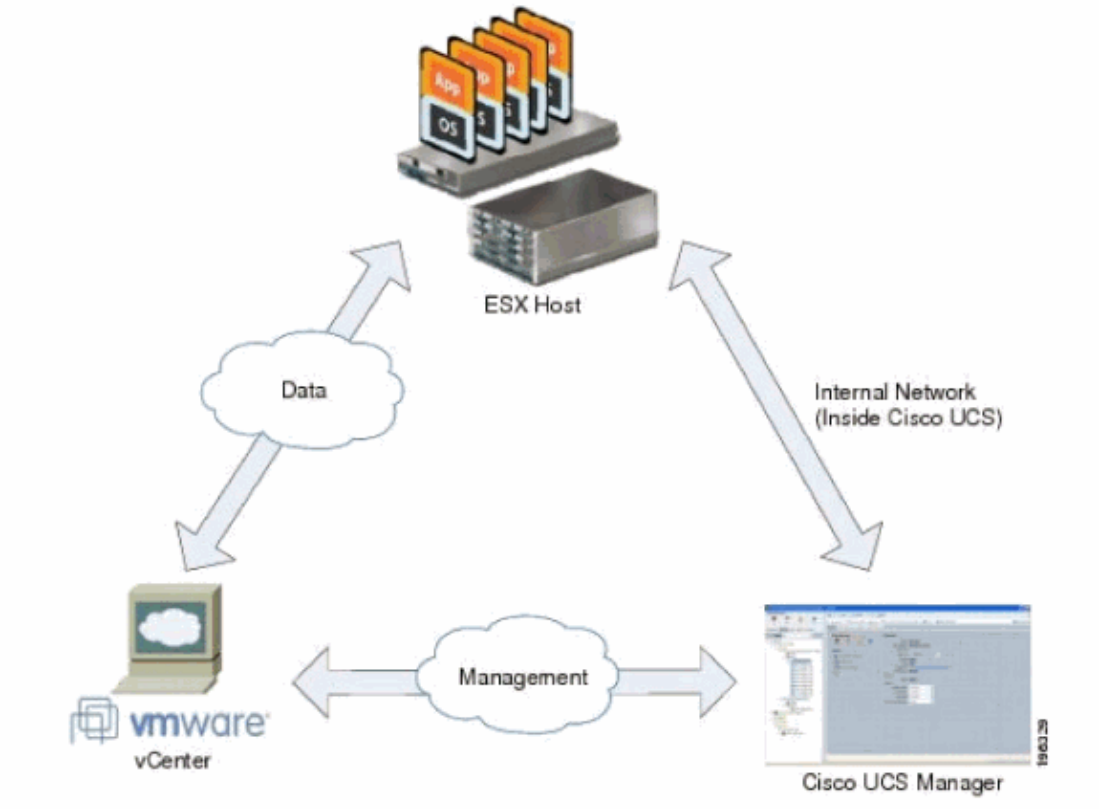
1. − rhel5x−1 − 172.21.61.225
2. − rhel5x−2 − 172.21.61.226
3. − rhel5x−2 − 172.21.61.227
4. − rhel5x−2 − 172.21.61.228
5. − rhel5x−2 − 172.21.61.229

- Ubuntu VMs

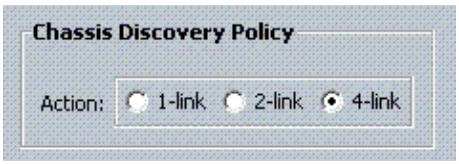
1. − ubuntu10x−1 − 10.21.60.152
2. − ubuntu10x−2 − 10.21.60.153



This figure shows the three main components of VN−Link in hardware and the methods by which they are connected:



Chassis Discovery Policy



Configurations

Complete these steps in order to create a Dynamic vNIC Connection Policy.

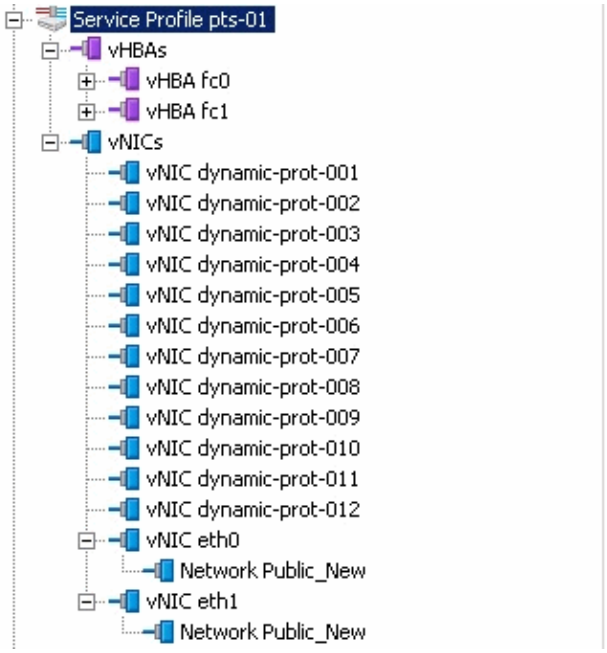
1. In the Navigation pane, click the **LAN** tab.
2. On the LAN tab, choose **LAN > Policies**.
3. Expand the node for the organization where you want to create the policy. If the system does not include multi−tenancy, expand the root node.
4. Right−click the Dynamic vNIC Connection Policies node and choose **Create Dynamic vNIC Connection Policy**.
5. In the Create Dynamic vNIC Connection Policy dialog box, complete these fields:

    - **The name of the policy** This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
    - **Description field** A description of the policy. Cisco recommends that you include information about where and when the policy should be used.
    - **Number of Dynamic vNICs field** The number of dynamic vNICs that this policy affects. The actual number of dynamic vNICs that can be used for VN−lInk in HW is less since you have to account for static vNICs and vHBAs. Typically you need to apply the formula **15 x No of uplinks − 6**. Hence it would be 54 for four uplinks, 24 for two uplinks.

- **Adapter Policy drop−down list** The adapter profile associated with this policy. The profile must already exist to be included in the drop−down list.
- **Protection field** This field is always set to *protected* because failover mode is always enabled for virtual NICs.

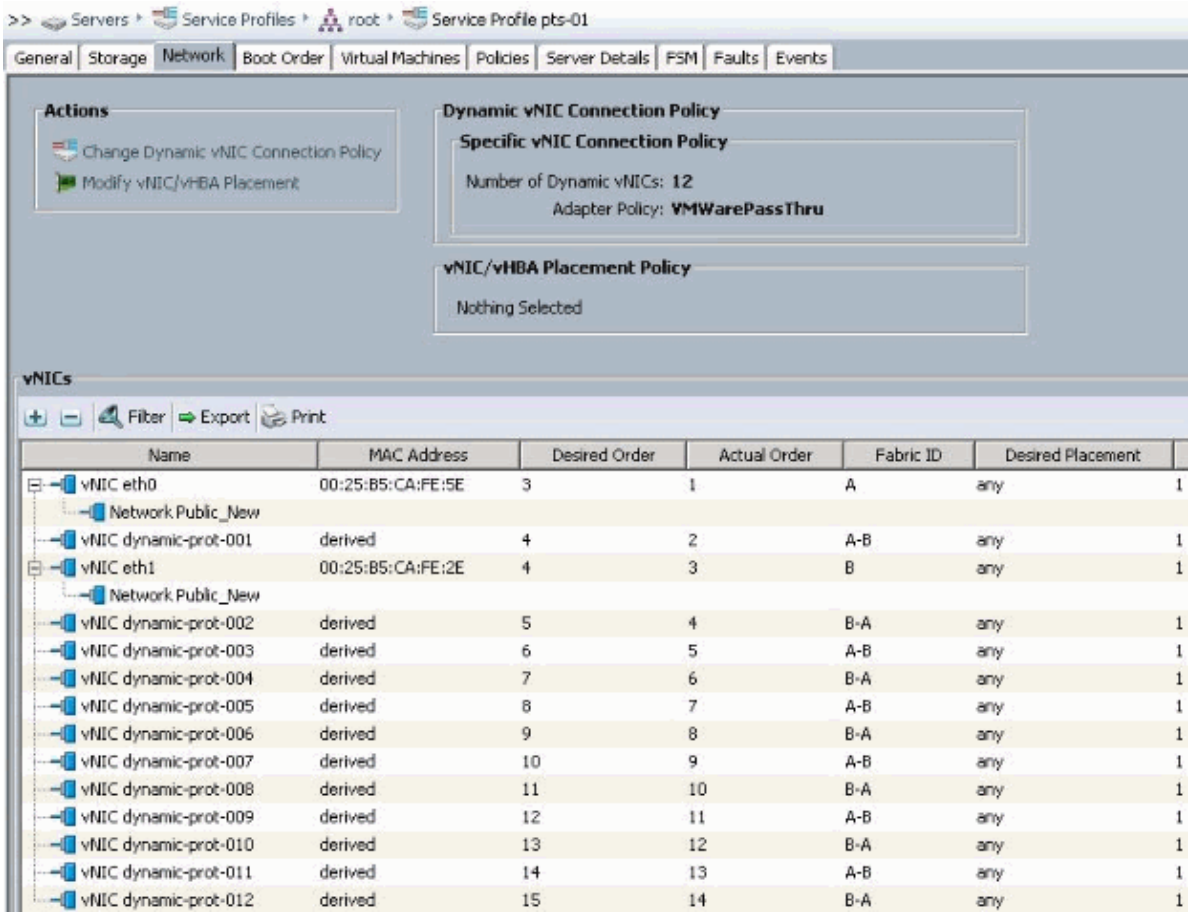
6. Click **OK.**
7. If Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Service Profile configured with Dynamic vNICs.



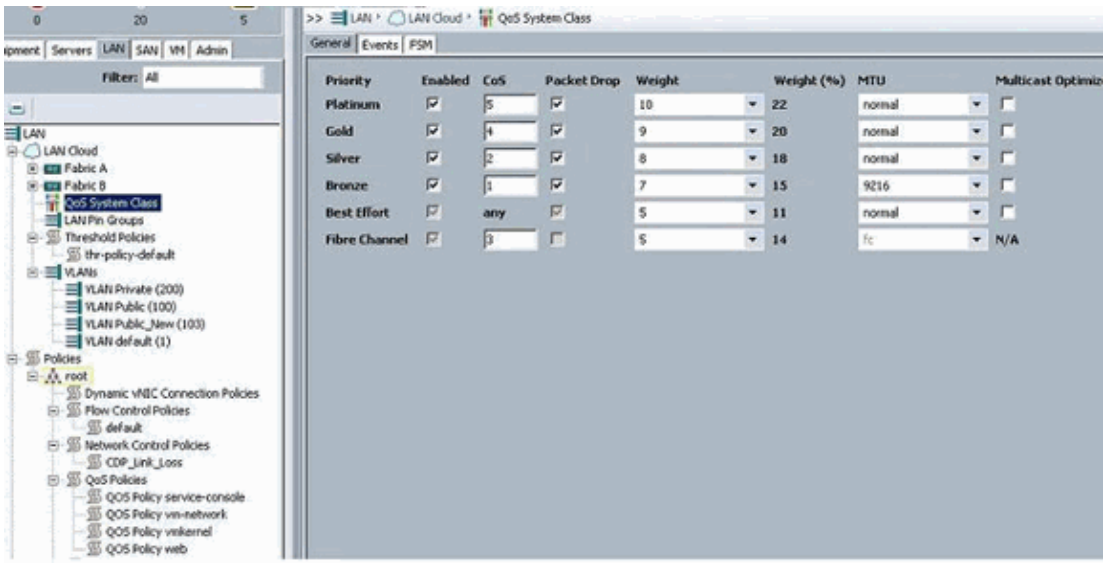
This document uses these configurations:

Dynamic vNICs defined in Service Profile



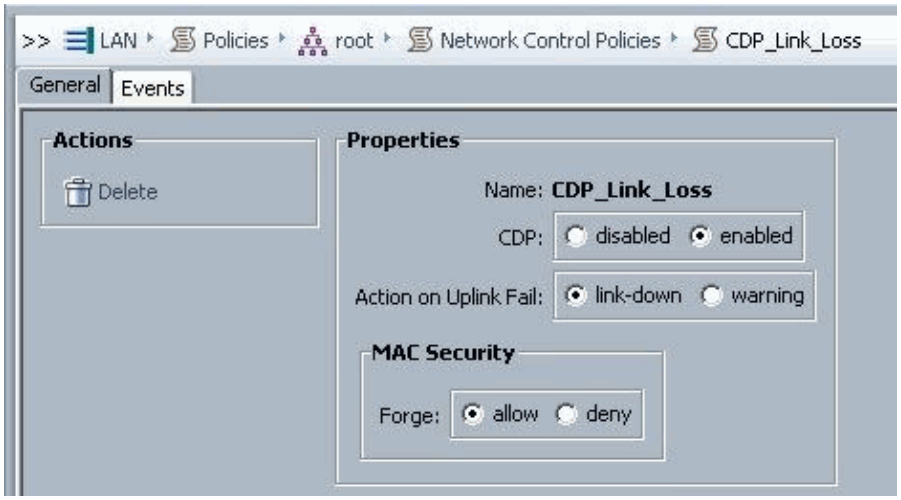
Name	MAC Address	Desired Order	Actual Order	Fabric ID	Desired Placement	
vNIC eth0	00:25:B5:CA:FE:5E	3	1	A	any	1
Network Public_New						
vNIC dynamic-prot-001	derived	4	2	A-B	any	1
vNIC eth1	00:25:B5:CA:FE:2E	4	3	B	any	1
Network Public_New						
vNIC dynamic-prot-002	derived	5	4	B-A	any	1
vNIC dynamic-prot-003	derived	6	5	A-B	any	1
vNIC dynamic-prot-004	derived	7	6	B-A	any	1
vNIC dynamic-prot-005	derived	8	7	A-B	any	1
vNIC dynamic-prot-006	derived	9	8	B-A	any	1
vNIC dynamic-prot-007	derived	10	9	A-B	any	1
vNIC dynamic-prot-008	derived	11	10	B-A	any	1
vNIC dynamic-prot-009	derived	12	11	A-B	any	1
vNIC dynamic-prot-010	derived	13	12	B-A	any	1
vNIC dynamic-prot-011	derived	14	13	A-B	any	1
vNIC dynamic-prot-012	derived	15	14	B-A	any	1

QOS Policy Definition

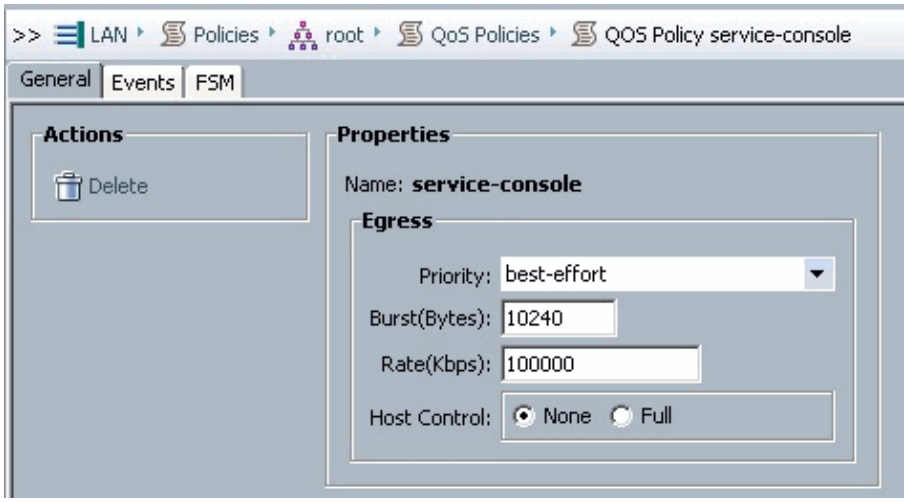


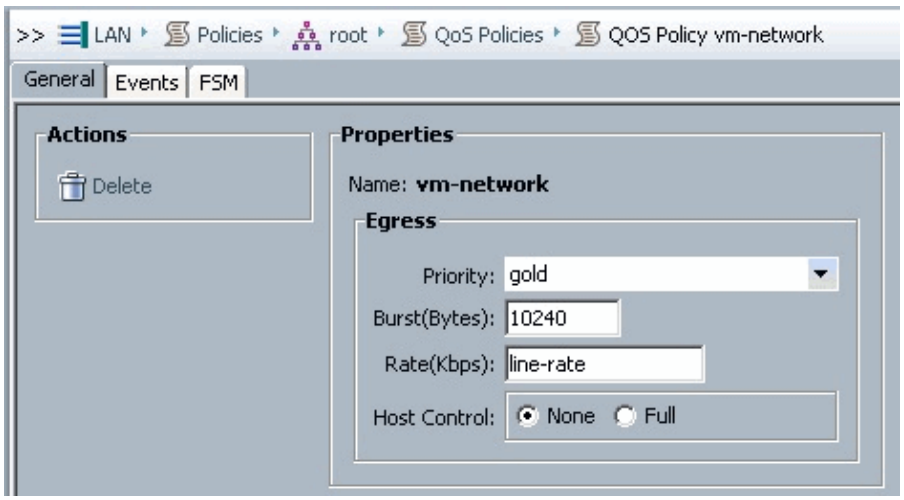
The Network Control and QOS policy has been configured accordingly. This comes into play later when you use iPerf from the VMs to show egress rate limiting.

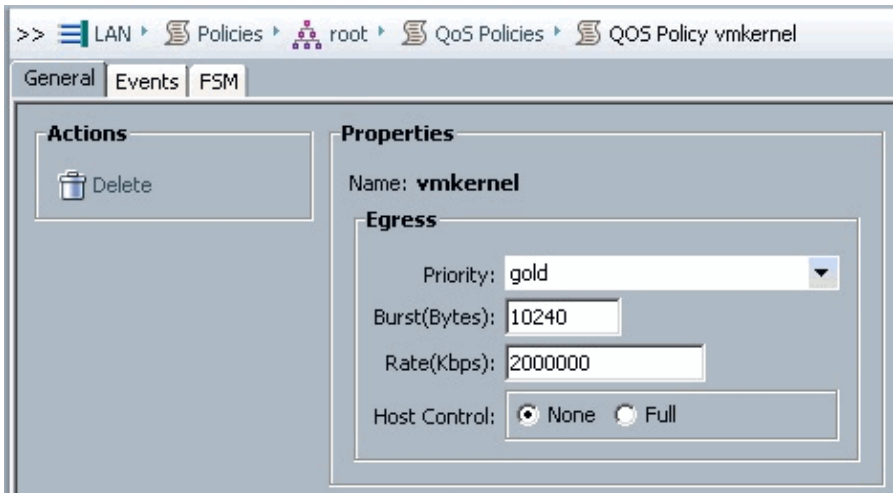
Network Control Policy is used in this example:

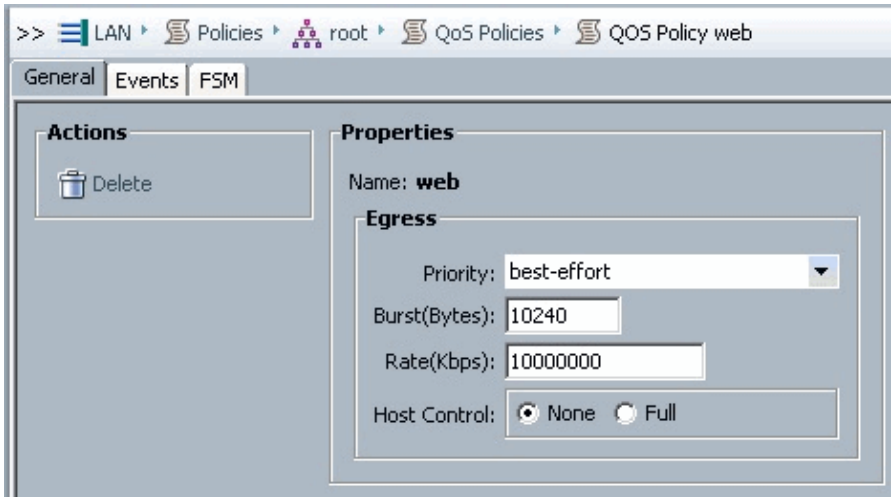


QOS Policy is used in the example:

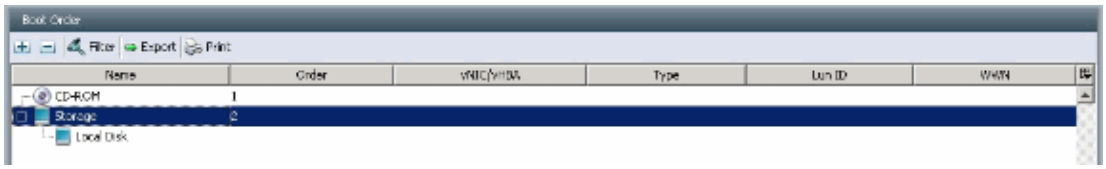








Boot Policy is used for this example. The VMFS shared volume is configured on the SAN, but the systems are local disk boot systems.



Click the **VM** tab.

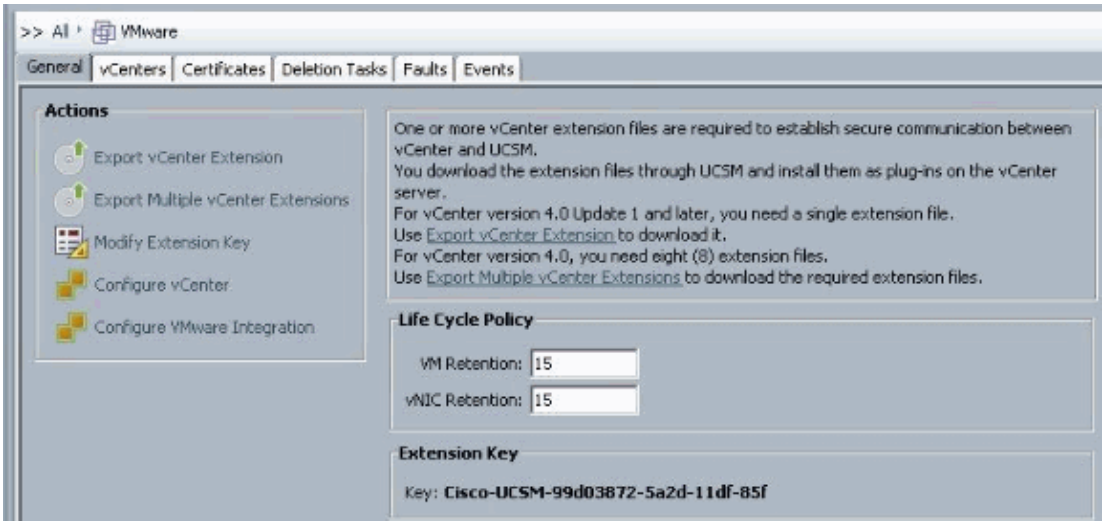
Export a vCenter Extension File from Cisco UCS Manager

You can either generate one extension file or a set of nine extension files, which depends on the version of VMware vCenter. Complete these steps:

1. In the Navigation pane, click the **VM** tab.
2. On the VM tab, expand the **All node.**
3. On the VM tab, click **VMWare.**
4. In the Work pane, click the **General** tab.
5. In the Actions area, click one of these links:

    - Export vCenter Extension For vCenter version 4.0 update 1 and later.
    - Export Multiple vCenter Extensions For vCenter version 4.0.

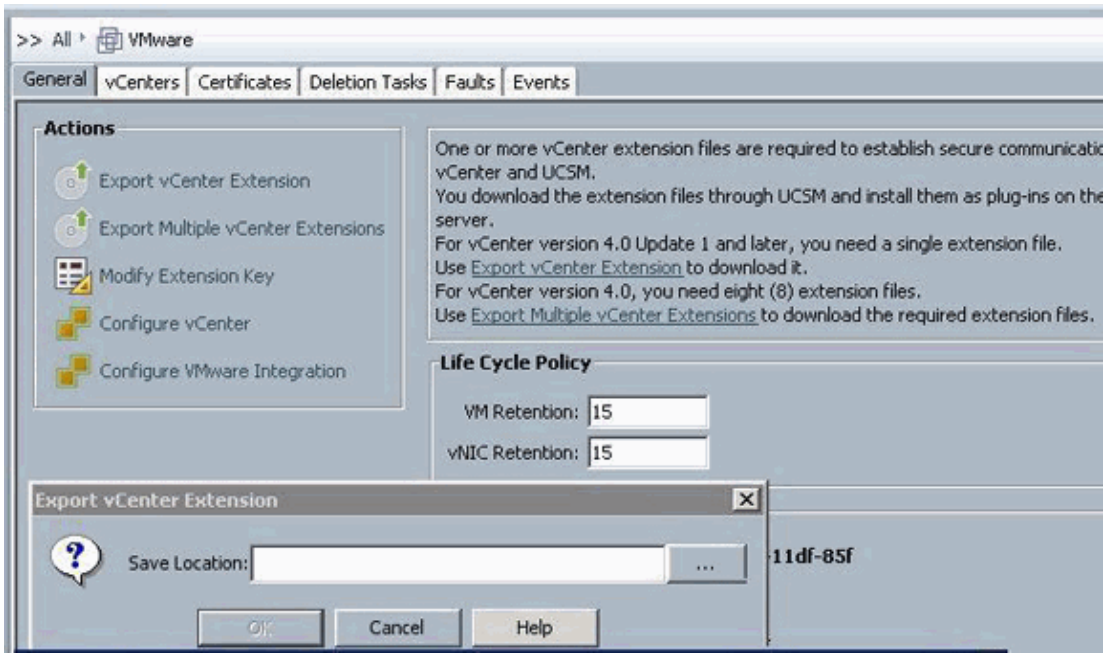
Export Extension Key

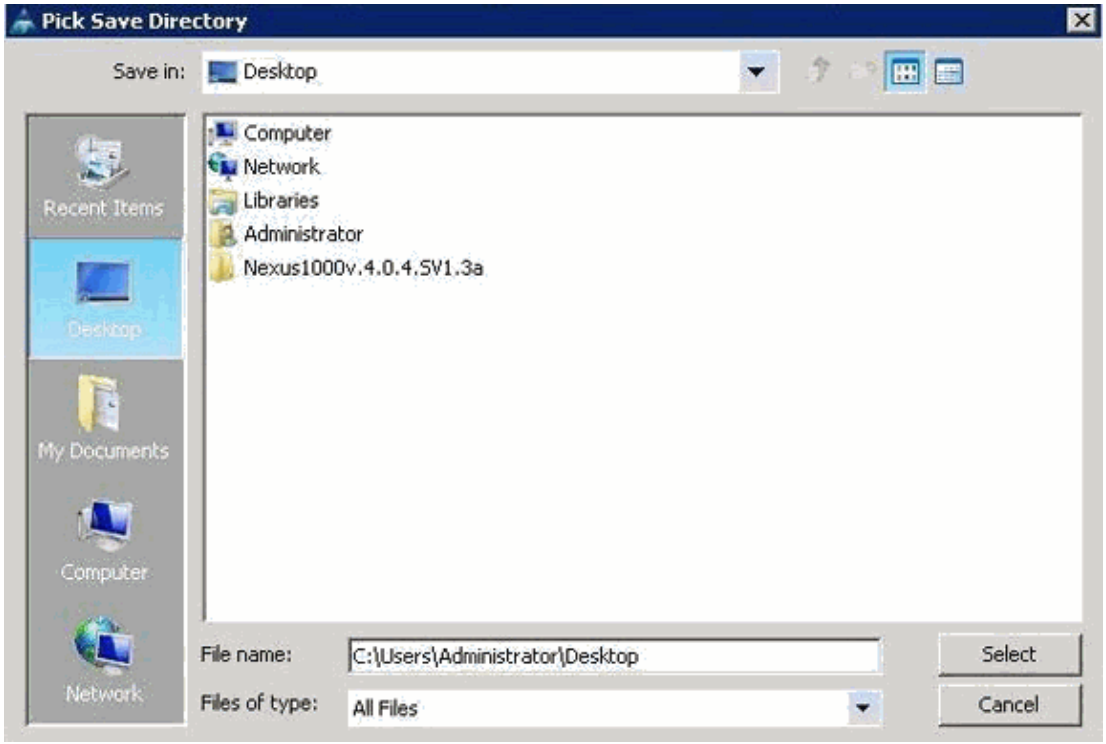


6. In the Export vCenter Extension dialog box, complete these steps::

   Cisco UCS Manager generates the extension file(s) and saves them to the specified location.

   a. In the Save Location field, enter the path to the directory where you want to save the extension file or files. If you do not know the path, click the **...** button and browse to the location.
   b. Click **OK**.





What to Do Next

◊ Register the vCenter extension file or files in VMware vCenter.
◊ Registering a vCenter Extension File in VMware vCenter

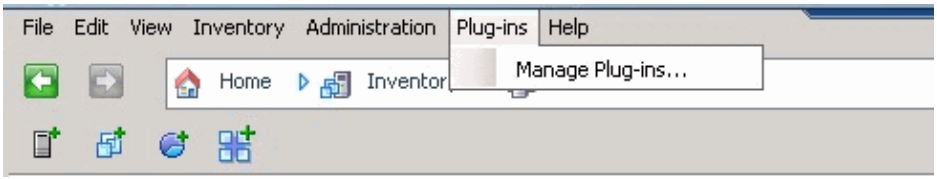
In VMware vCenter, the vCenter extension files are called plug−ins.

Export the vCenter extension file(s) from Cisco UCS Manager. Ensure that the exported vCenter extension files are saved to a location that can be reached by VMware vCenter.

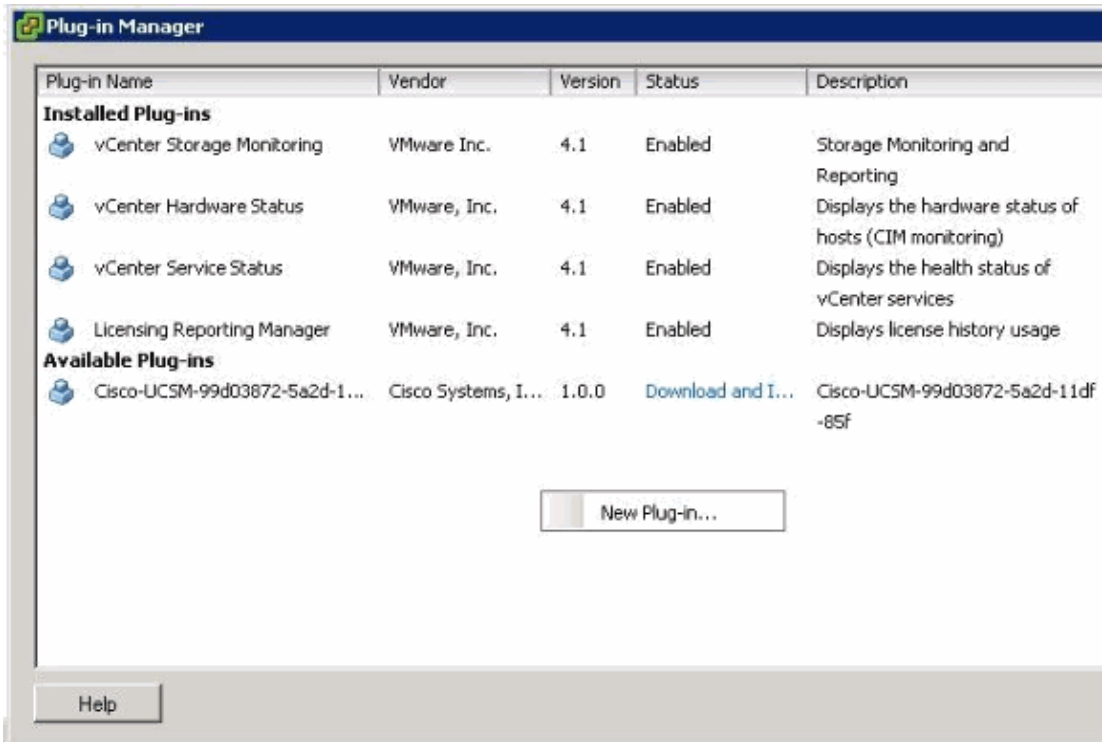
Complete these steps:

1. In VMware vCenter, choose **Plug−ins > Manage Plug−ins**.

   The vCenter extension file registers as an available VMware vCenter plug−in. You do not need to install the plug−in; leave it in the available state. If you are registering multiple vCenter extension files, repeat this procedure until all files are registered.

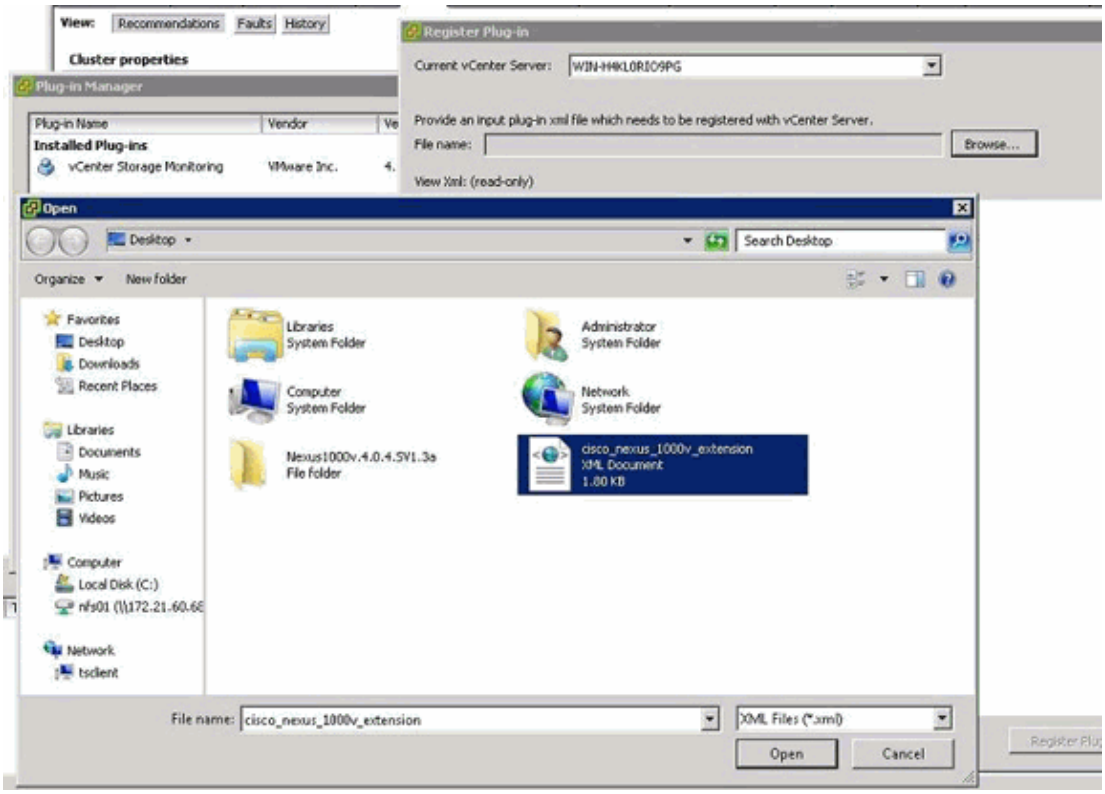


2. Right−click any empty space below the Available Plug−ins section of the Plug−in Manager dialog box and click **New Plug−in**.

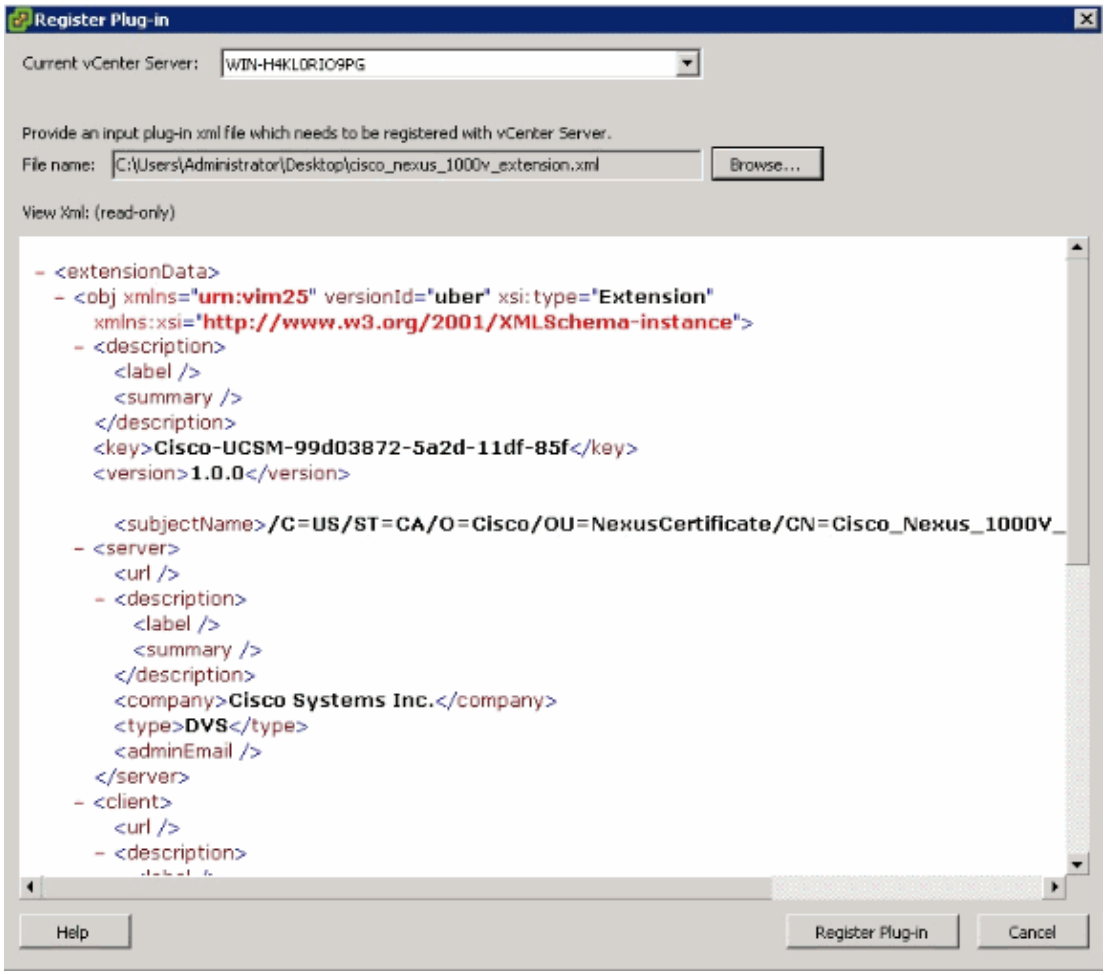


Import Extension Key previously saved from the desktop.

3. Click **Browse** and navigate to the location where the vCenter extension file(s) are saved.



4. Choose a vCenter extension file and click **Open.**
5. Click **Register Plug−in**.
6. If the Security Warning dialog box appears, click **Ignore**.
7. Click **OK**.



Now configure vCenter communication with UCSM.

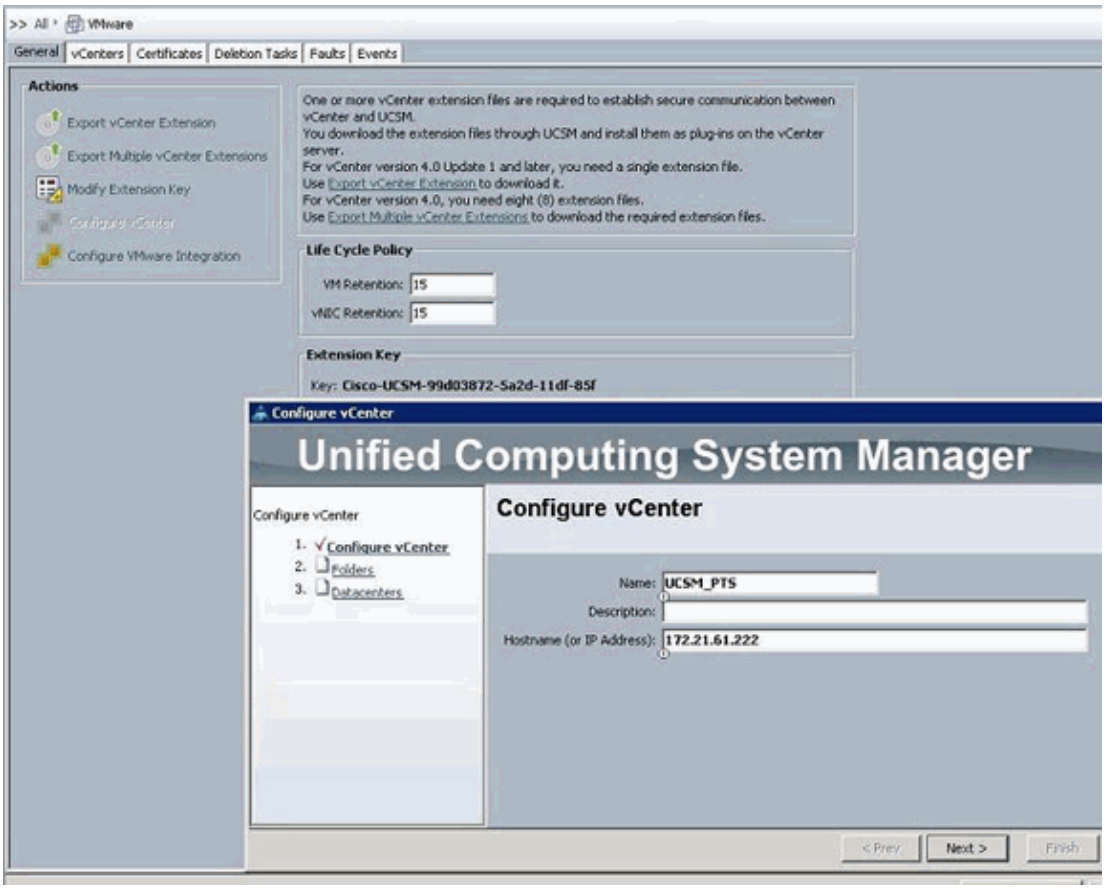
Define a VMware vCenter Distributed Virtual Switch

This procedure directly follows the steps in Page 1: Establishing the Connection to vCenter Server. It describes how to define the components of a distributed virtual switch in VMware vCenter through the Configure VMware Integration wizard.

1. In the vCenter Server area, complete these fields in order to define the connection to VMware vCenter:

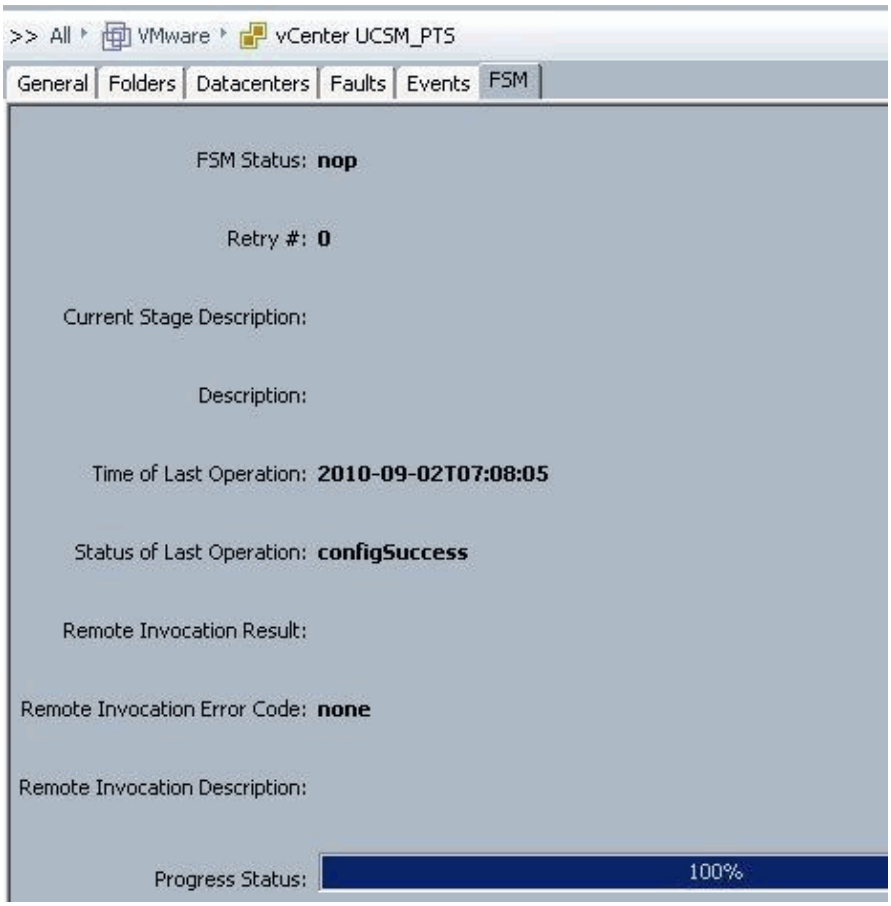
    - Name Field vCenter Server Name field. The user−defined name for the vCenter server. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
    - Description field The description of the vCenter server.
    - vCenter Server Hostname or IP Address field The hostname or IP address of the vCenter server.

    Note: If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.



Once this relevant information is provided, click **Next** for the UCSM to try to establish communication to vCenter. A good indication that communication is successful is to see the Key being generated.

Also check the FSM for a `configSuccess` and `nop` state.

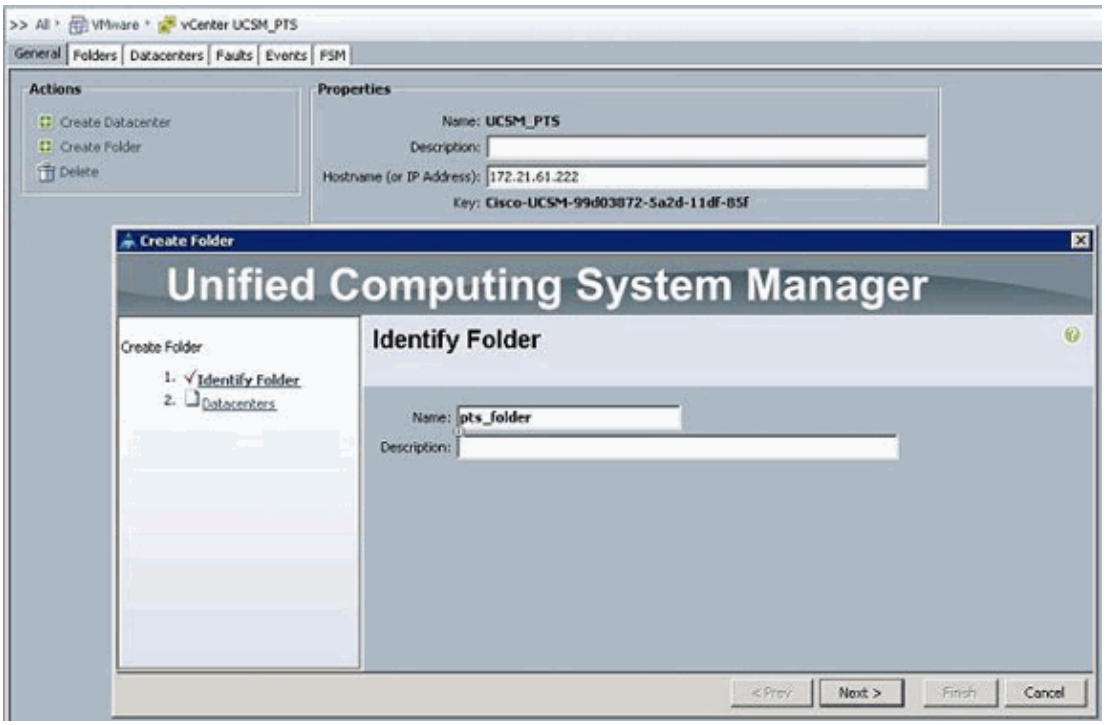


2. In the Datacenter area, complete these fields in order to create the datacenter in VMware vCenter:

    - Name Field vCenter Datacenter Name. The name of the vCenter Datacenter. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
    - Description field The user−defined description of the Datacenter.

   Note: In this document, a Datacenter is not created from UCSM, but you start by creating Folders.
3. In the DVS Folder area, complete these fields in order to create a folder to contain the distributed virtual switch in VMware vCenter:

    - Name Field Folder Name field. The name of the folder that contains the distributed virtual switch (DVS). This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
    - Description field The user−defined description of the folder.



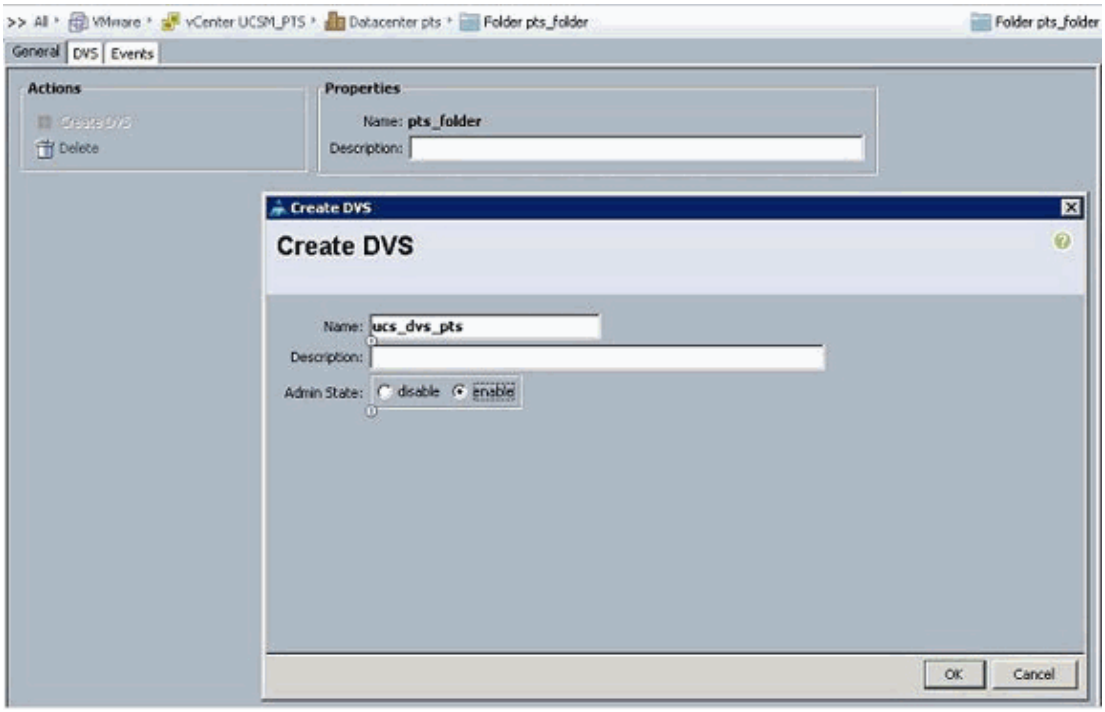
4. In the DVS area, complete these fields in order to create the distributed virtual switch in VMware vCenter:

    - Name Field DVS Name field. The name of the DVS. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
    - Description field The user−defined description of the DVS. DVS field
    - Admin state This can be:

      * disable

      * enable

      If you disable the DVS, Cisco UCS Manager does not push any configuration changes related to the DVS to VMware vCenter.



Port Profiles

Port profiles contain the properties and settings used to configure virtual interfaces in Cisco UCS for VN−Link in hardware. The port profiles are created and administered in Cisco UCS Manager.

Note: There is no clear visibility into the properties of a port profile from VMware vCenter.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile are visible in VMware vCenter.

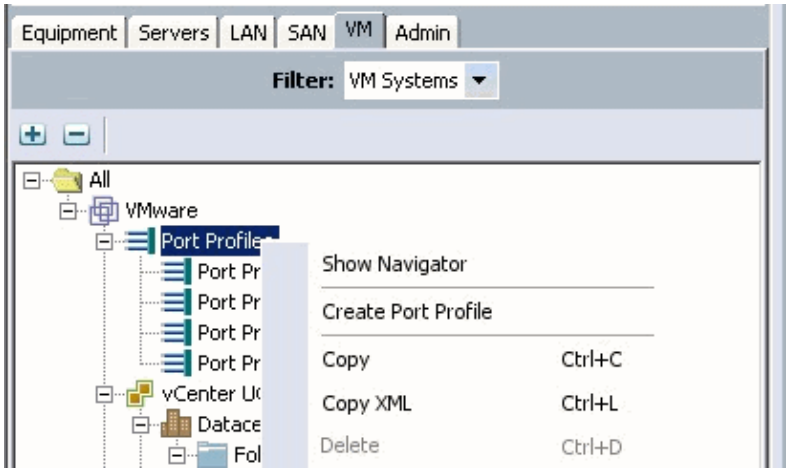
After a port profile is created, assigned to, and actively used by one or more DVSes, any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSes. You must configure at least one port profile client for a port profile, if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Port Profile Clients

The port profile client determines the DVSes to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSes in the vCenter. But, you can configure the client to apply the port profile to all DVSes in a specific datacenter or datacenter folder, or only to one DVS.

Complete these steps in order to create a Port Profile:

1. In the Navigation pane, click the **VM** tab.
2. On the VM tab, choose **All > VMWare**.
3. Right−click the Port Profiles node and choose **Create Port Profile**.
4. In the Create Port Profile dialog box, complete these fields:

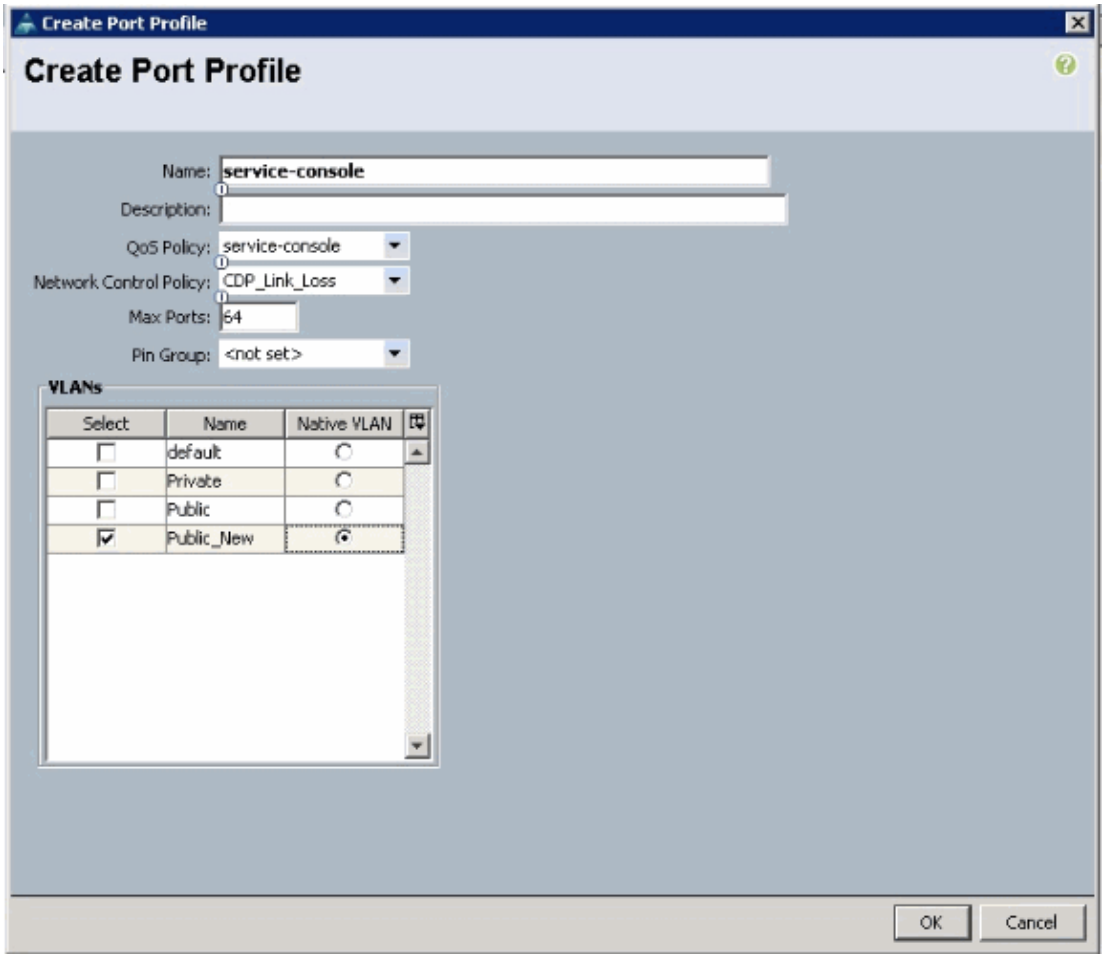


- Name field The user−defined name for the port profile.This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
- Description field The user−defined description of the Port Profile.
- QoS Policy drop−down list The quality of service policy associated with this port profile.
- Network Control Policy drop−down list The network control policy associated with this port profile.
- Max Ports field The maximum number of ports that can be associated with this port profile. The default is 64 ports. The maximum number of ports that can be associated with a single distributed virtual switch (DVS) is 4096. If the DVS has only one associated port profile, that port profile can be configured with up to 4096 ports. However, if the DVS has more than one associated port profile, the total number of ports associated with all of those port profiles combined cannot exceed 4096.
- Pin Group drop−down list The pin group associated with this port profile.

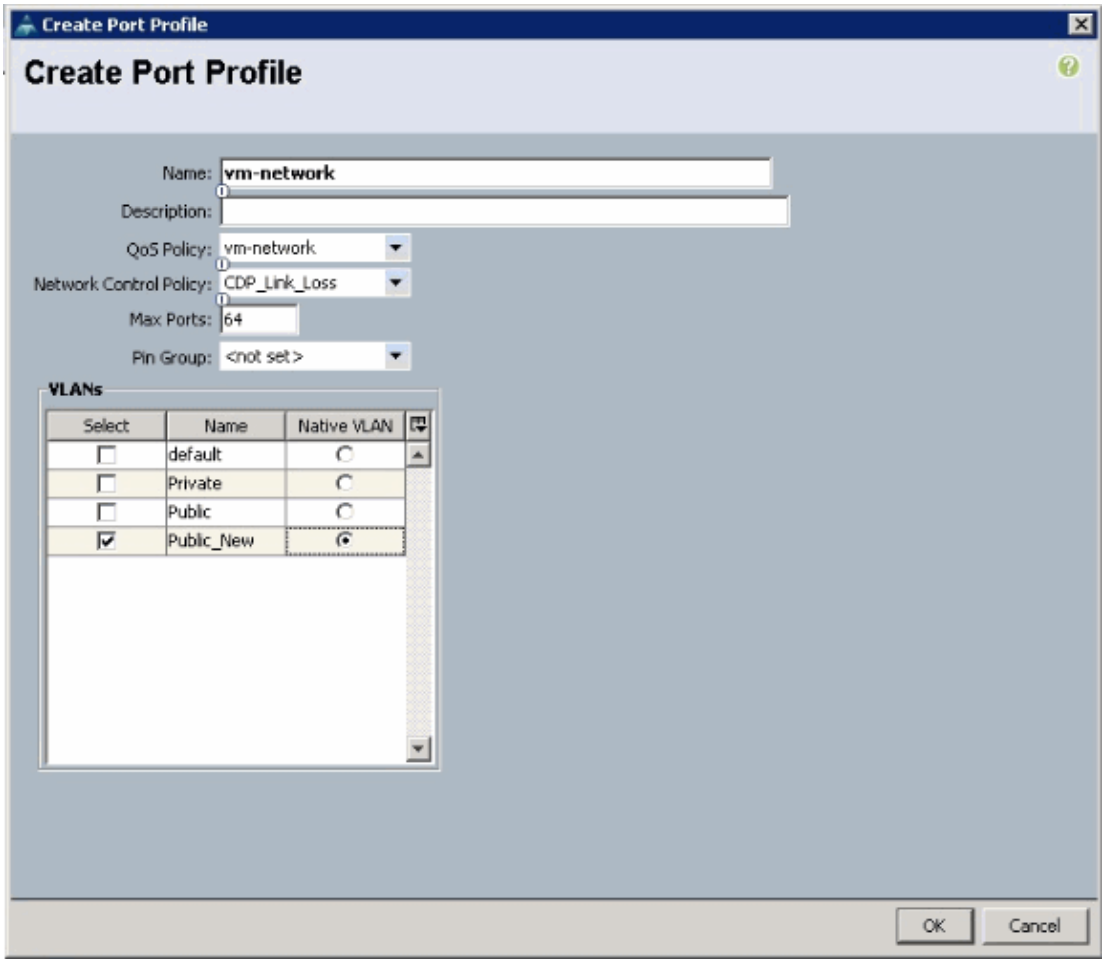
5. In the VLANs area, complete these fields:

- Select column Check the check box in this column for each VLAN you want to use.
- Name column The name of the VLAN
- Native VLAN column To designate one of the VLANs as the native VLAN, click the radio button in this column.

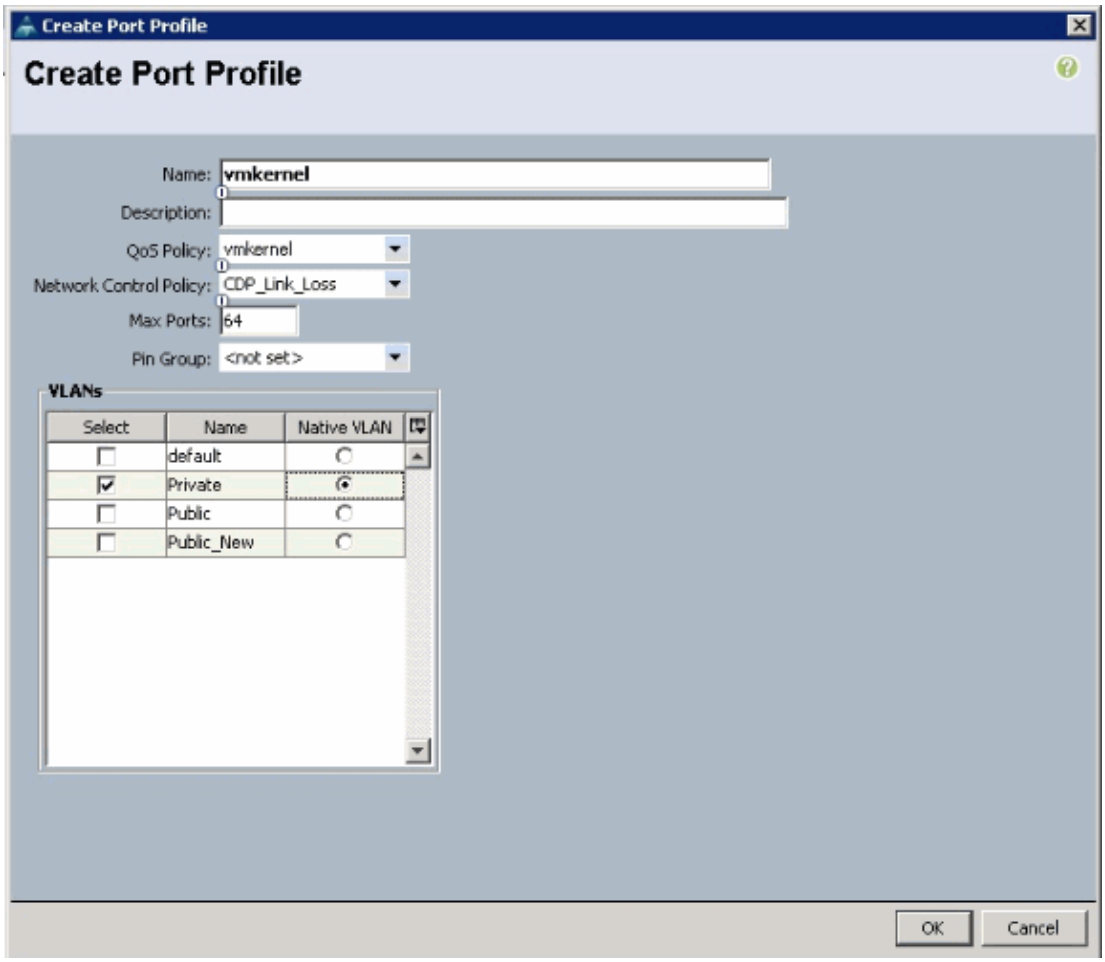
6. Click **Finish**.



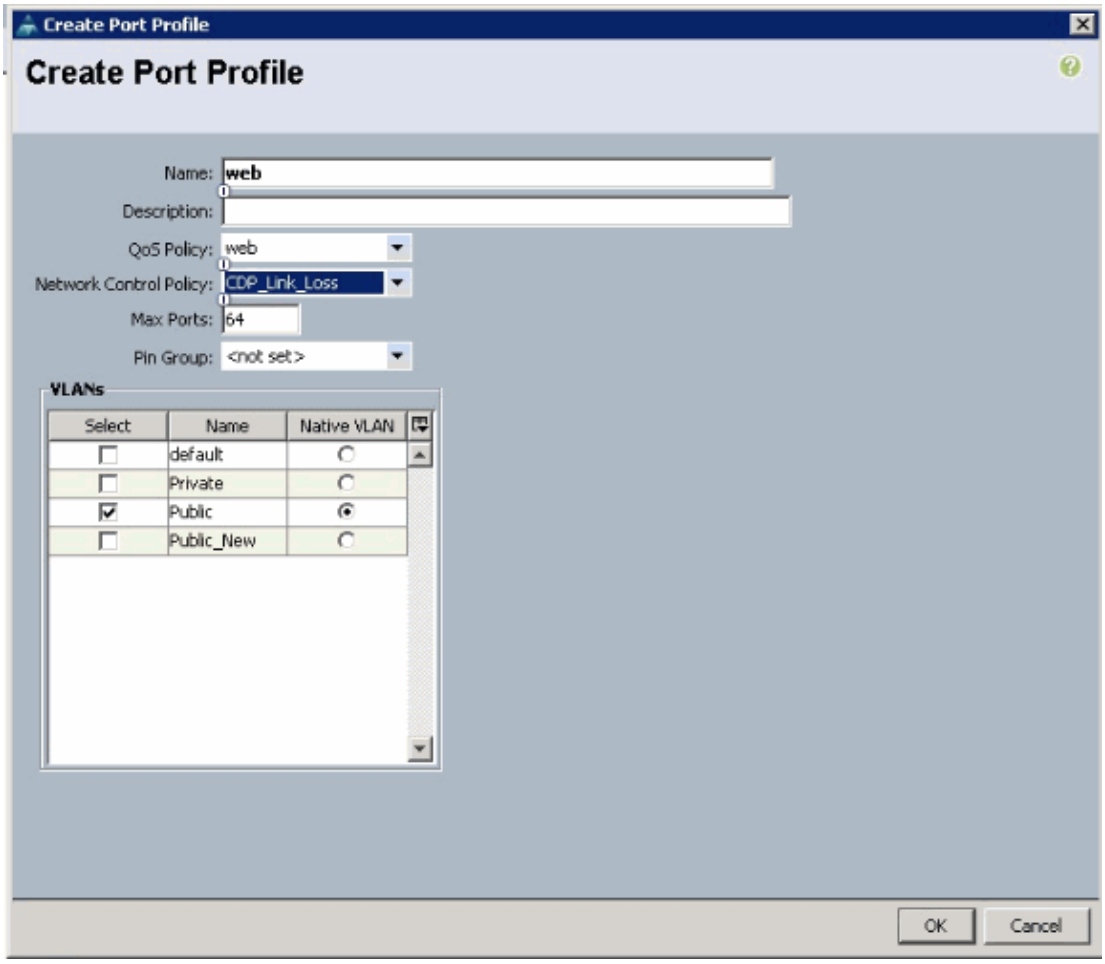
Do the previous steps for each Port Profile.



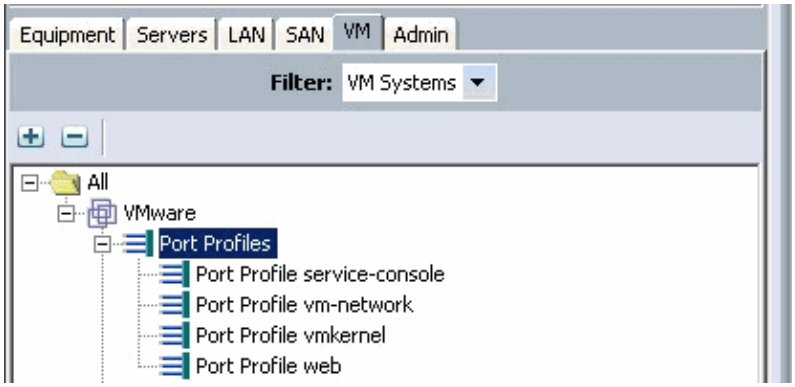
Do the previous steps for each Port Profile.

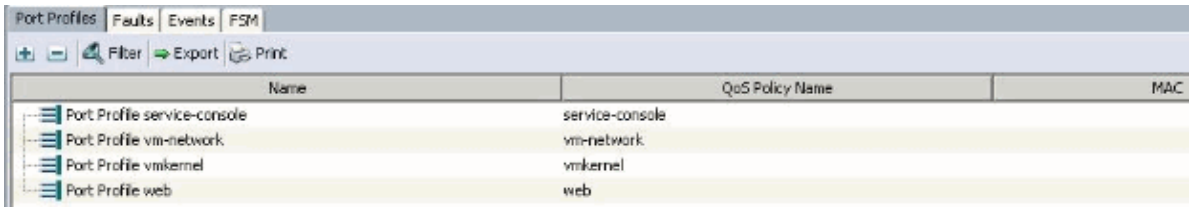


Do the previous steps for each Port Profile.

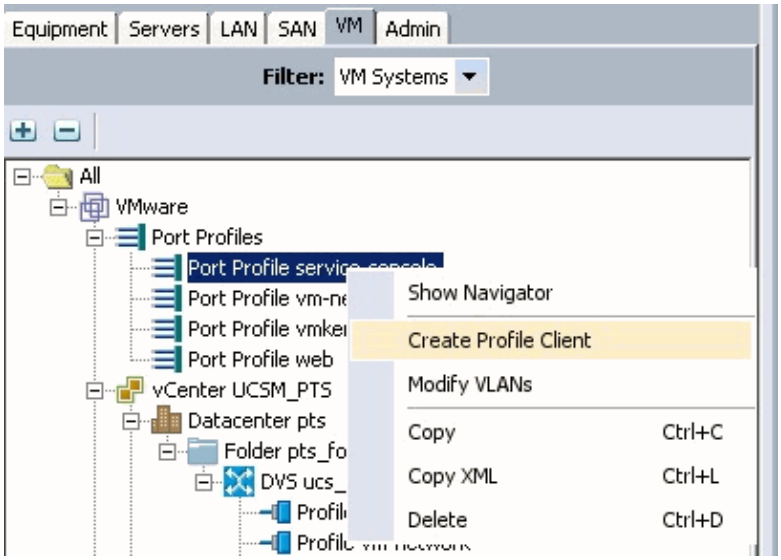


You see Port Profiles similar to these screen shots once you are done.

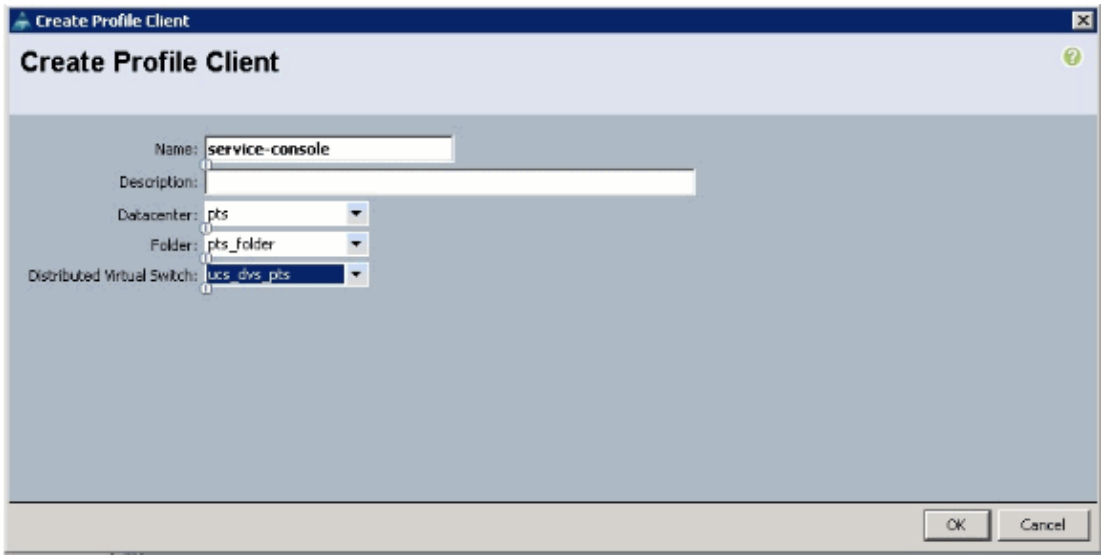




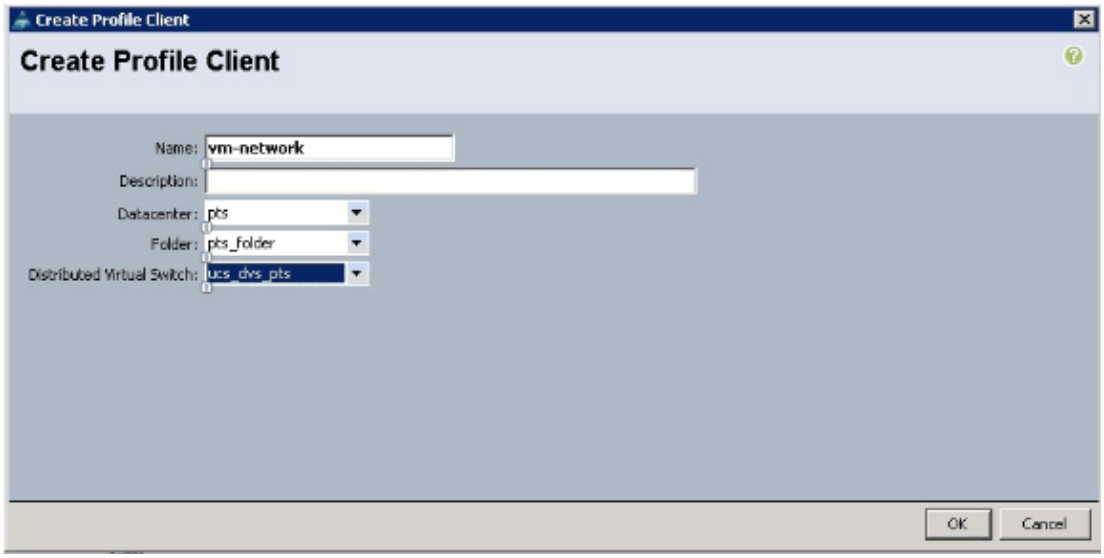
You can now go through and apply Port Profiles to the Port Profile Clients.



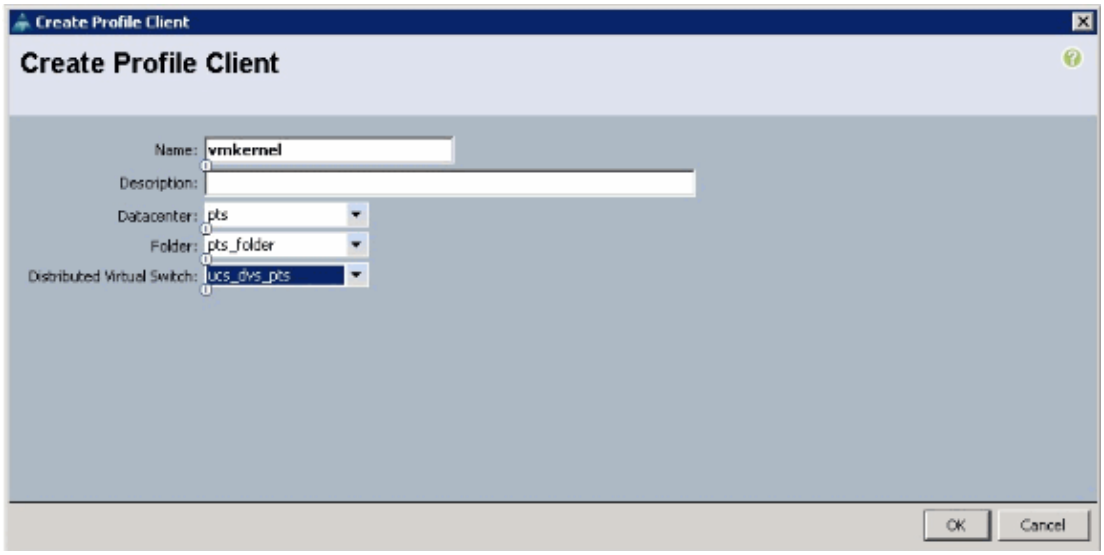
You can now go through and apply Port Profiles to the Port Profile Clients.

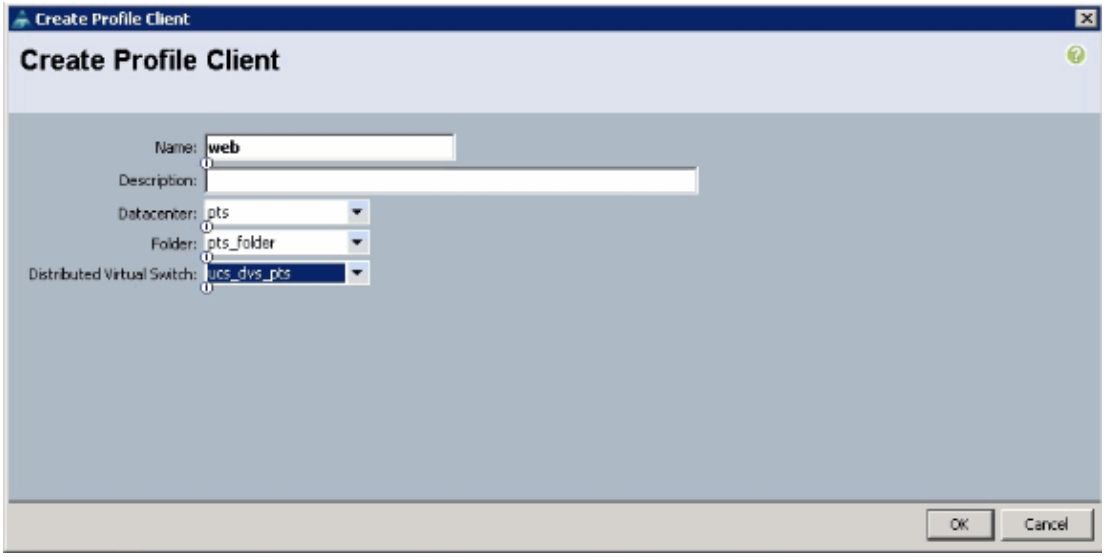


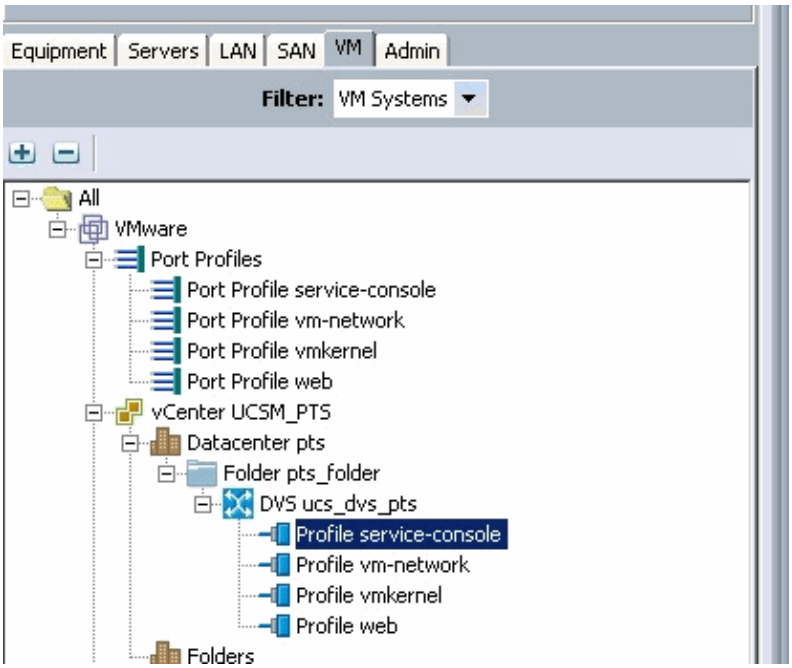
You can now go through and apply Port Profiles to the Port Profile Clients.



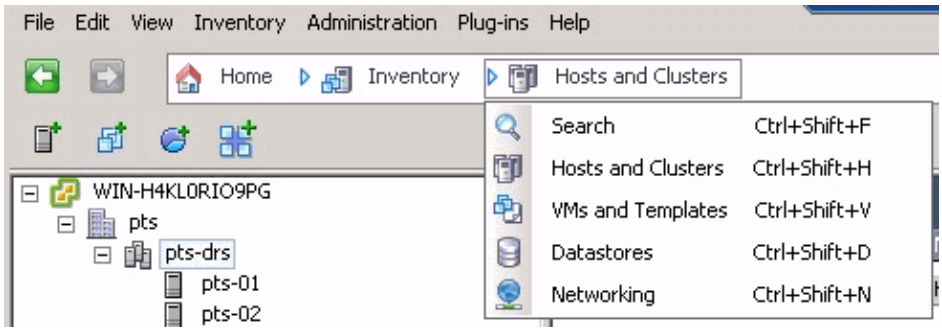
You can now go through and apply Port Profiles to the Port Profile Clients.



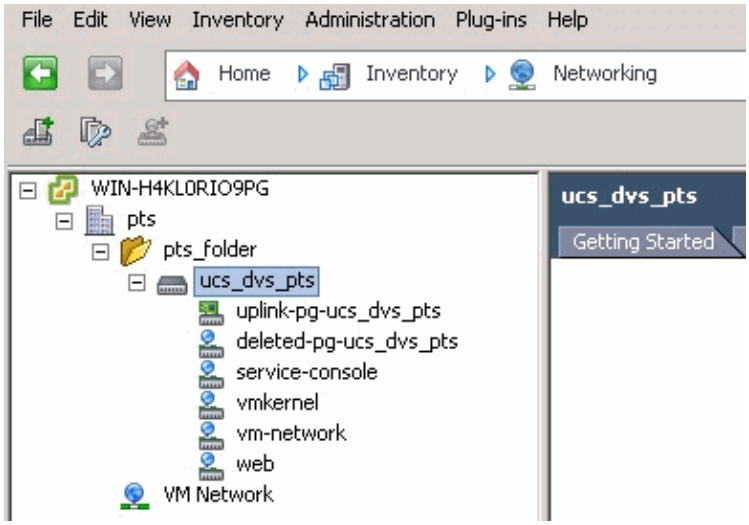




You can now confirm all the port profiles are created successfully on the vCenter. Click **Hosts and Clusters** and from the drop−down menu, choose **Networking.**

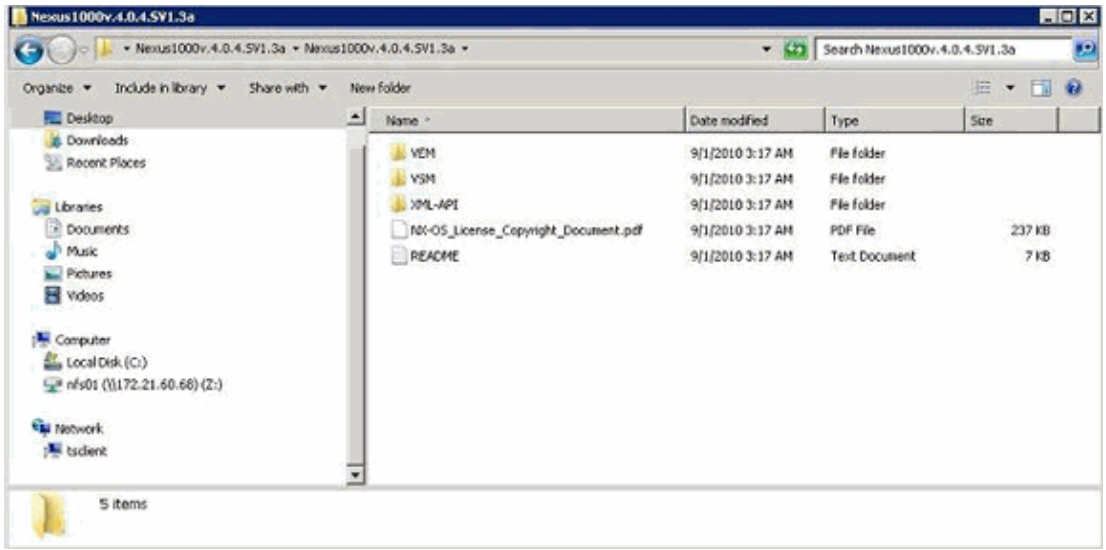


All the port profiles created from the UCSM VM tab are now reflected in the respective folder in vCenter.



At this stage you can now install the respective VEMs on the ESX hosts. Download the Nexus1K software package from Cisco Software Download (registered customers only) .

Unzip the file downloaded from CCO, and when unzipped the folder would contain these directories and files:



Make sure to read the README.TXT to match the version of VEM to use with respects to the ESX/ESXi version and build number being used.

As an example, the version of the ESX build being used in this document is :

So based on this previous build information, you see the respective version of VEM to use from the README.TXT file. For example:

```
11. VMware ESX410 (build 260247) and ESXi410 (build 260247) (4.1 GA) :
VEM410-201007311.zip                                (md5 c1d4542b34a90204b6968cd88d08f93b)
cross_cisco-vem-v121-4.0.4.1.3.1.0-2.0.3.vib (md5 f5bef9e6689bab29b2a7576b7199f5c3)
```

Use some file transfer mechanism in order to get the respective .vib file to the ESX hosts and use this command in order to install the VEM.

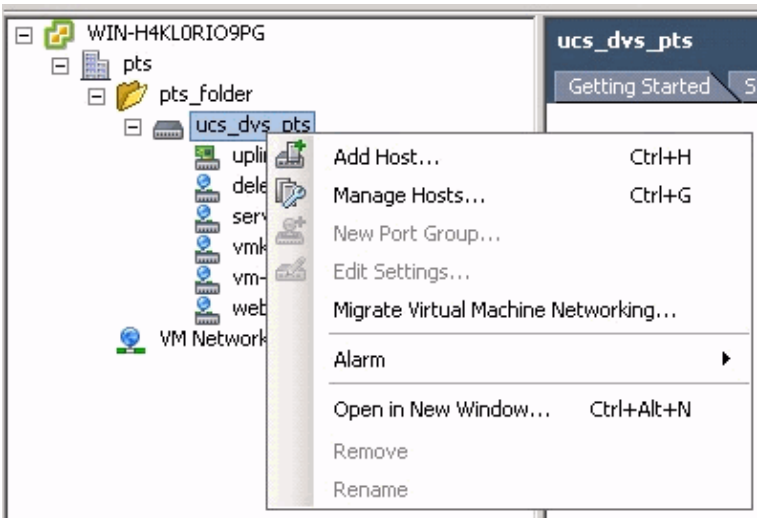
```
root@pts-01 tmp]# esxupdate -b cross_cisco-vem-v121-4.0.4.1.3.1.0-2.0.3.vib update
Unpacking cross_cisco-vem-v121-esx_4.0.4.1.3.1.0-2.0.3
########################################################################## [100%]
Installing cisco-vem-v121-esx
########################################################################## [100%]
Running [/usr/sbin/vmkmod-install.sh]...
ok.

Check status of the VEM to confirm the modules loaded successfully.
[root@pts-01 tmp]# vmkload_mod -l | grep vem
vem-v121-svs-mux         2    32
vem-v121-pts             0    92

root@pts-02 tmp]# esxupdate -b cross_cisco-vem-v121-4.0.4.1.3.1.0-2.0.3.vib update
Unpacking cross_cisco-vem-v121-esx_4.0.4.1.3.1.0-2.0.3
########################################################################## [100%]
Installing cisco-vem-v121-esx
########################################################################## [100%]
Running [/usr/sbin/vmkmod-install.sh]...
ok.

Check status of the VEM to confirm the modules loaded successfully.
[root@pts-02 tmp]# vmkload_mod -l | grep vem
vem-v121-svs-mux         2    32
vem-v121-pts             0    92
```

You can now advance to the next step to add the hosts to the DVS.



Add a Host to a vNetwork Distributed Switch

Use the Add Host to vNetwork Distributed Switch wizard in order to associate a host with a vNetwork Distributed Switch. You can also add hosts to a vNetwork Distributed Switch with the use of Host Profiles.Complete these steps:

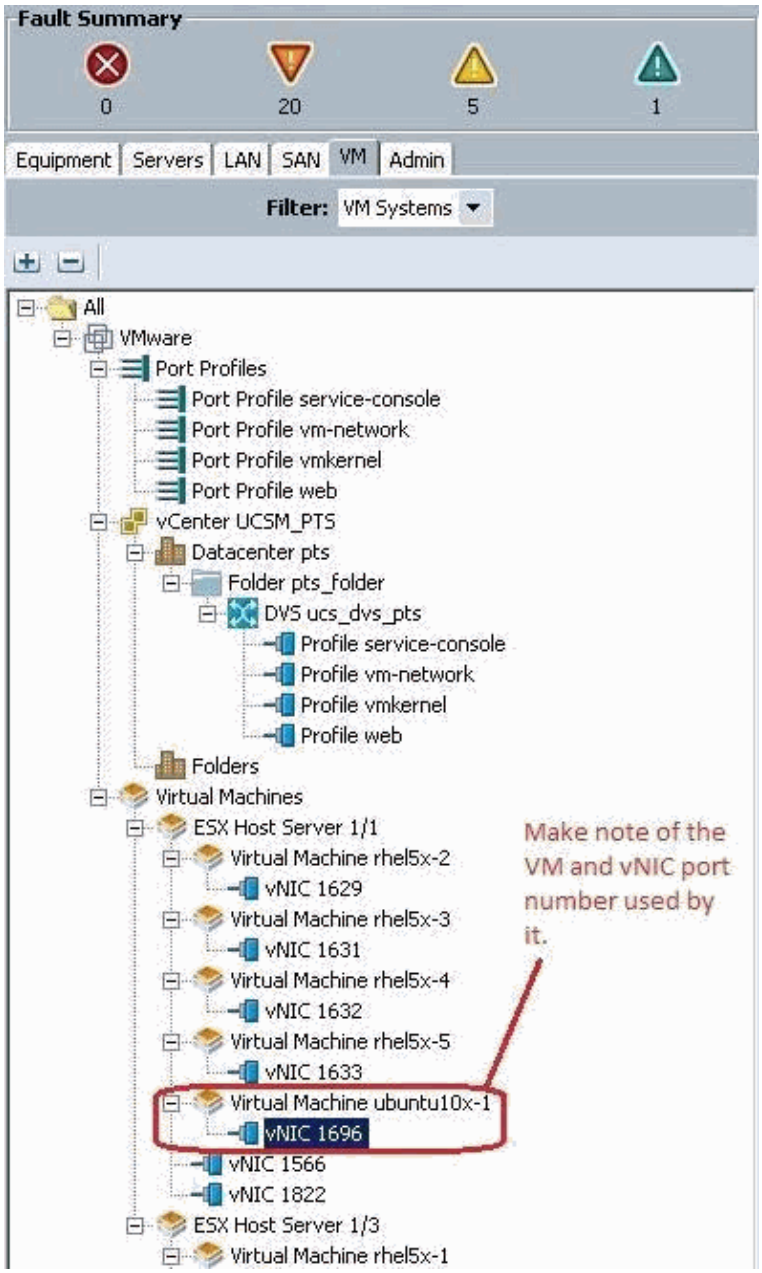
Note: Enterprise plus license is a requirement for DVS.

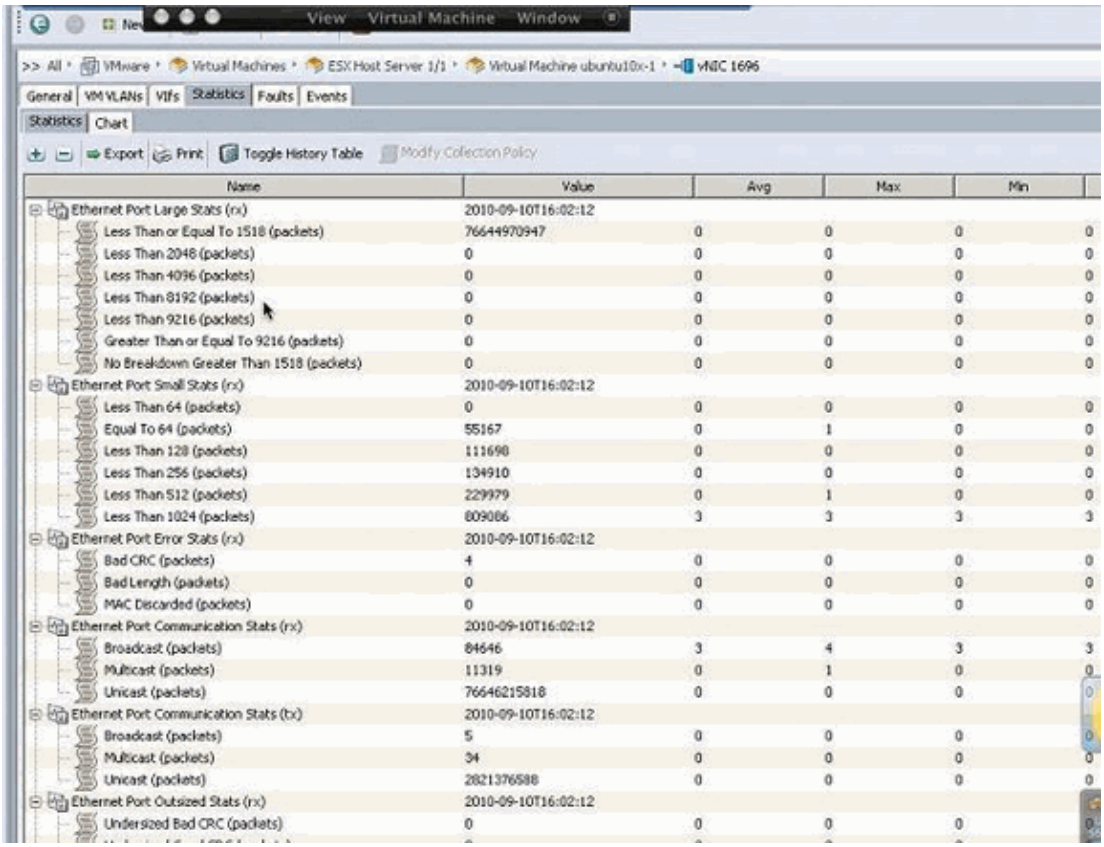
1. In the vSphere Client, display the Networking inventory view and choose **vNetwork Distributed Switch**.
2. From the Inventory menu, choose **Distributed Virtual Switch > Add Host**. The Add Host to vNetwork Distributed Switch wizard appears.
3. Choose the host to add.
4. Under the selected host, choose the physical adapters to add, and click **Next**.You can choose both free and in use physical adapters. If you choose an adapter that is currently in use by a host, choose whether to move the associated virtual adapters to the vNetwork Distributed Switch.

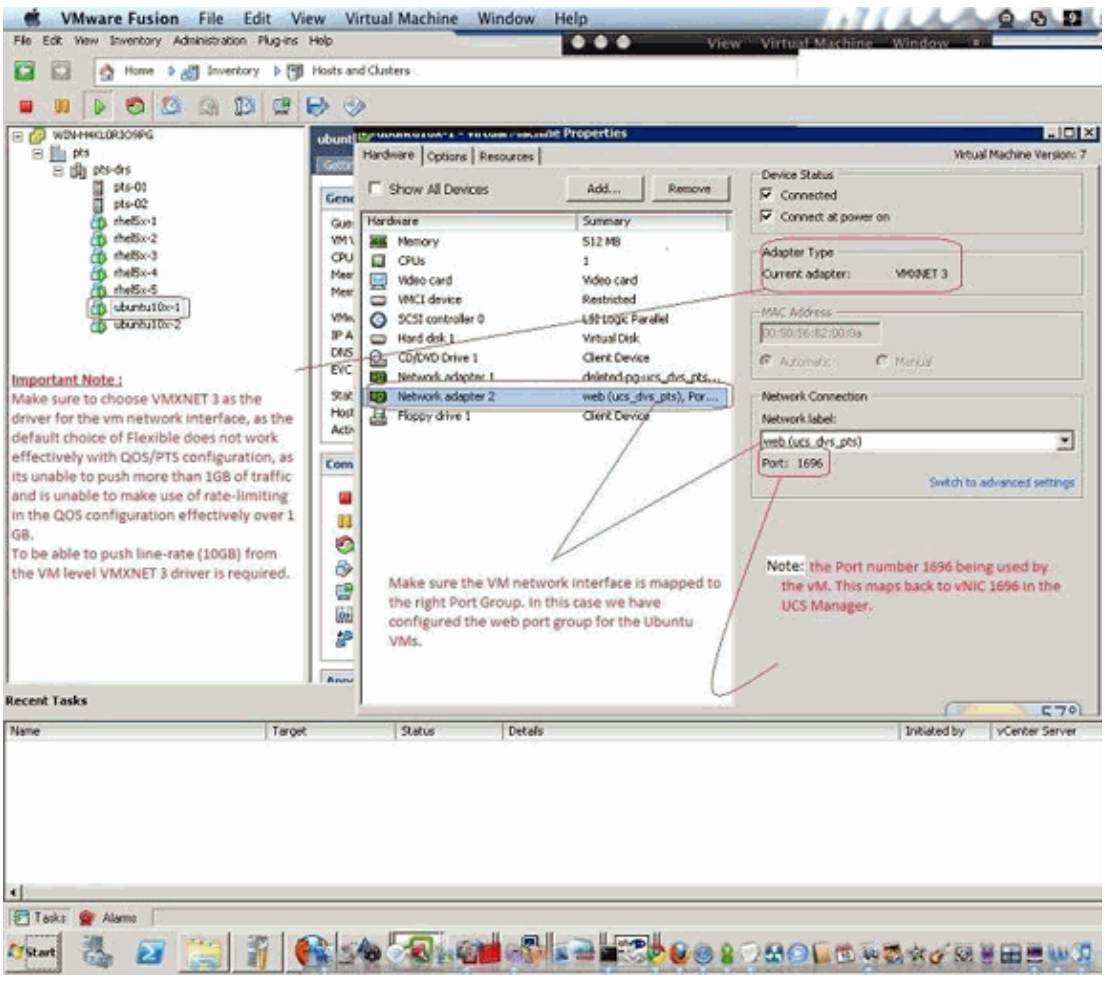
   Note: If you move a physical adapter to a vNetwork Distributed Switch without moving any associated virtual adapters, this causes those virtual adapters to lose network connectivity.
5. Click **Finish.**

Verify

Once the VMs are added into VC and the correct Port Groups are mapped respectively, you see these from both the UCS Manager/VM tab and VC interfaces.


Fault Summary
0
20
5
1
Equipment
Servers
LAN
SAN
VM
Admin
Filter: VM Systems
All
VMware
Port Profiles
Port Profile service-console
Port Profile vm-network
Port Profile vmkernel
Port Profile web
vCenter UCSM_PTS
Datacenter pts
Folder pts_folder
DVS ucs_dvs_pts
Profile service-console
Profile vm-network
Profile vmkernel
Profile web
Folders
Virtual Machines
ESX Host Server 1/1
Virtual Machine rhel5x-2
vNIC 1629
Virtual Machine rhel5x-3
vNIC 1631
Virtual Machine rhel5x-4
vNIC 1632
Virtual Machine rhel5x-5
vNIC 1633
Virtual Machine ubuntu10x-1
vNIC 1696
vNIC 1566
vNIC 1822
ESX Host Server 1/3
Virtual Machine rhel5x-1
Make note of the VM and vNIC port number used by it.

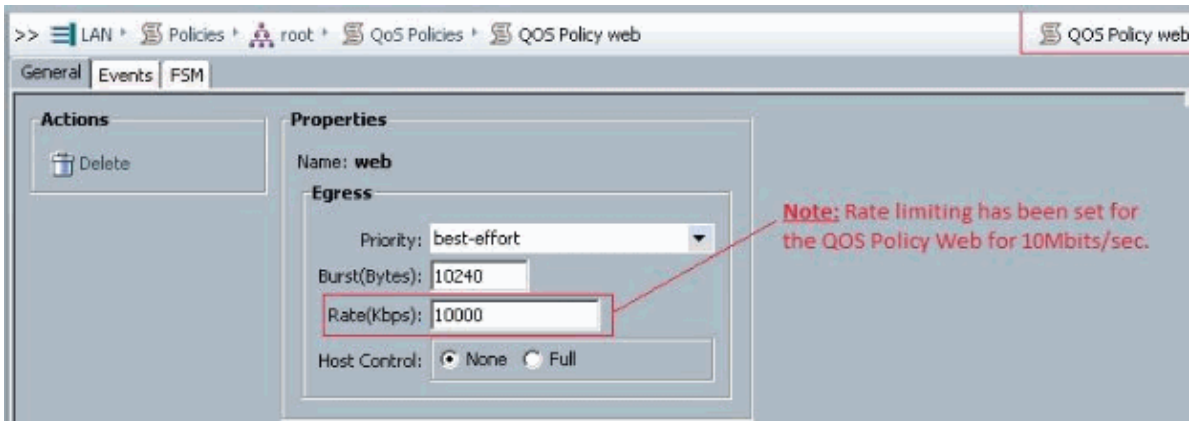

View Virtual Machine Window
>> All VMware Virtual Machines ESX Host Server 1/1 Virtual Machine ubuntu10x-1 vNIC 1696
General VM VLANs VIFs Statistics Faults Events
Statistics Chart
Export Print Toggle History Table Modify Collection Policy
Name Value Avg Max Min
Ethernet Port Large Stats (rx) 2010-09-10T16:02:12
Less Than or Equal To 1518 (packets) 76644970947 0 0 0 0
Less Than 2048 (packets) 0 0 0 0 0
Less Than 4096 (packets) 0 0 0 0 0
Less Than 8192 (packets) 0 0 0 0 0
Less Than 9216 (packets) 0 0 0 0 0
Greater Than or Equal To 9216 (packets) 0 0 0 0 0
No Breakdown Greater Than 1518 (packets) 0 0 0 0 0
Ethernet Port Small Stats (rx) 2010-09-10T16:02:12
Less Than 64 (packets) 0 0 0 0 0
Equal To 64 (packets) 55167 0 1 0 0
Less Than 128 (packets) 111690 0 0 0 0
Less Than 256 (packets) 134910 0 0 0 0
Less Than 512 (packets) 229979 0 1 0 0
Less Than 1024 (packets) 809086 3 3 3 3
Ethernet Port Error Stats (rx) 2010-09-10T16:02:12
Bad CRC (packets) 4 0 0 0 0
Bad Length (packets) 0 0 0 0 0
MAC Discarded (packets) 0 0 0 0 0
Ethernet Port Communication Stats (rx) 2010-09-10T16:02:12
Broadcast (packets) 84646 3 4 3 3
Multicast (packets) 11319 0 1 0 0
Unicast (packets) 76646215818 0 0 0 0
Ethernet Port Communication Stats (tx) 2010-09-10T16:02:12
Broadcast (packets) 5 0 0 0 0
Multicast (packets) 34 0 0 0 0
Unicast (packets) 2821376588 0 0 0 0
Ethernet Port Outsized Stats (rx) 2010-09-10T16:02:12
Undersized Bad CRC (packets) 0 0 0 0


VMware Fusion File Edit View Virtual Machine Window Help
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
pts
pts-drs
pts-01
pts-02
rhel5x-1
rhel5x-2
rhel5x-3
rhel5x-4
rhel5x-5
ubuntu10x-1
ubuntu10x-2
Important Note :
Make sure to choose VMXNET 3 as the driver for the vm network interface, as the default choice of Flexible does not work effectively with QOS/PTS configuration, as its unable to push more than 1GB of traffic and is unable to make use of rate-limiting in the QOS configuration effectively over 1 GB.
To be able to push line-rate (10GB) from the VM level VMXNET 3 driver is required.
Hardware Options Resources
Virtual Machine Version: 7
Show All Devices Add... Remove
Hardware Summary
Memory 512 MB
CPUs 1
Video card Video card
VMCI device Restricted
SCSI controller 0 LSI Logic Parallel
Hard disk 1 Virtual Disk
CD/DVD Drive 1 Client Device
Network adapter 1 deleted:pg:ucs_dvs_pts...
Network adapter 2 web (ucs_dvs_pts), Por...
Floppy drive 1 Client Device
Device Status
Connected
Connect at power on
Adapter Type
Current adapter: VMXNET 3
MAC Address
Automatic Manual
Network Connection
Network label:
web (ucs_dvs_pts)
Port: 1696
Switch to advanced settings
Make sure the VM network interface is mapped to the right Port Group. In this case we have configured the web port group for the Ubuntu VMs.
Note: the Port number 1696 being used by the vM. This maps back to vNIC 1696 in the UCS Manager.
Recent Tasks
Name Target Status Details Initiated by vCenter Server
Tasks Alarms
Start

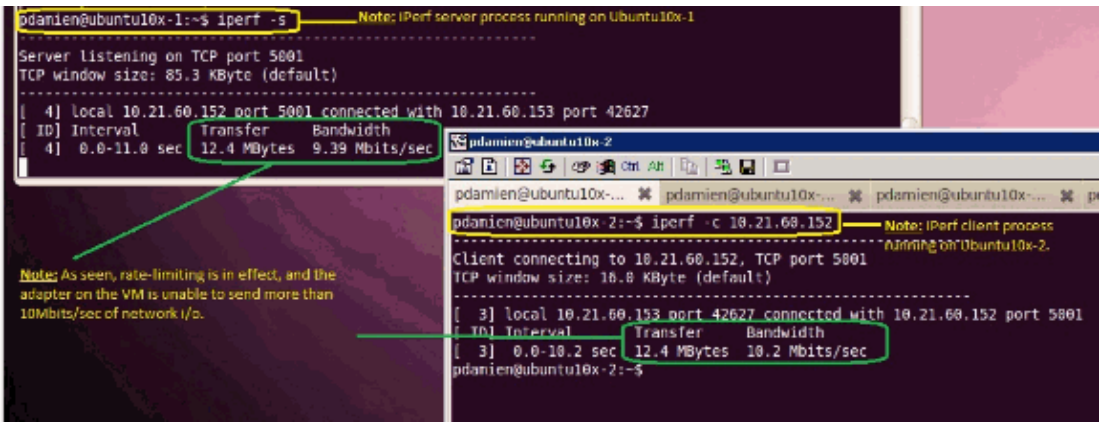
Testing QOS/Rate Limiting

Test Case 1 − Qos Policy web − rate limited at 10Mbits/sec

On the QOS policy "web" rate limiting has been configured so the port group "web" is throttled at 10Mbits/sec.

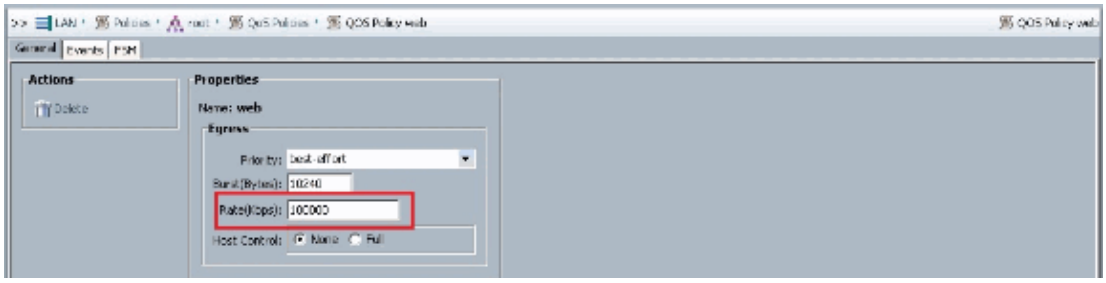


Hosts running iPerf

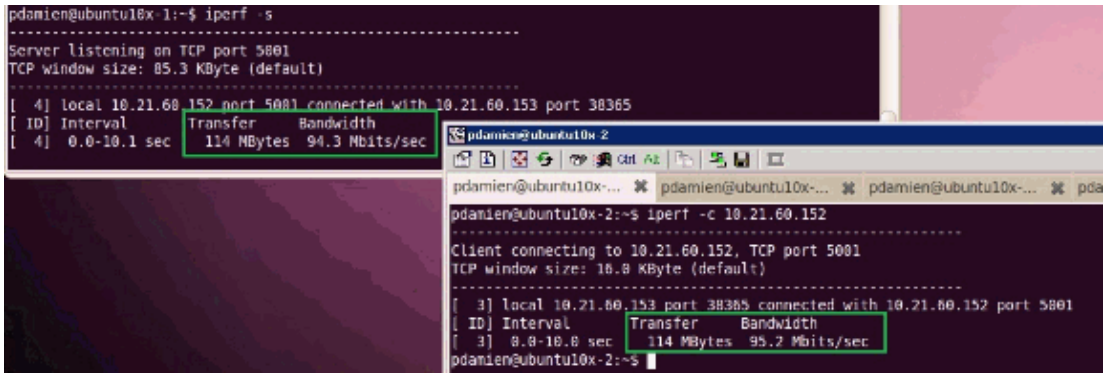


Test Case 2 − Qos Policy web − rate limited at 100Mbits/sec

On the QOS policy "web" rate limiting has been configured so the port group "web" is throttled at 100Mbits/sec.

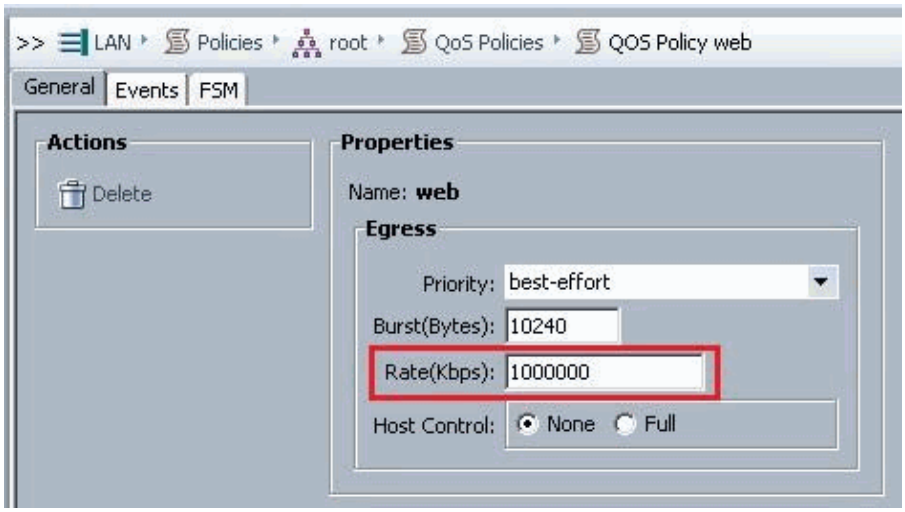


Hosts running iPerf

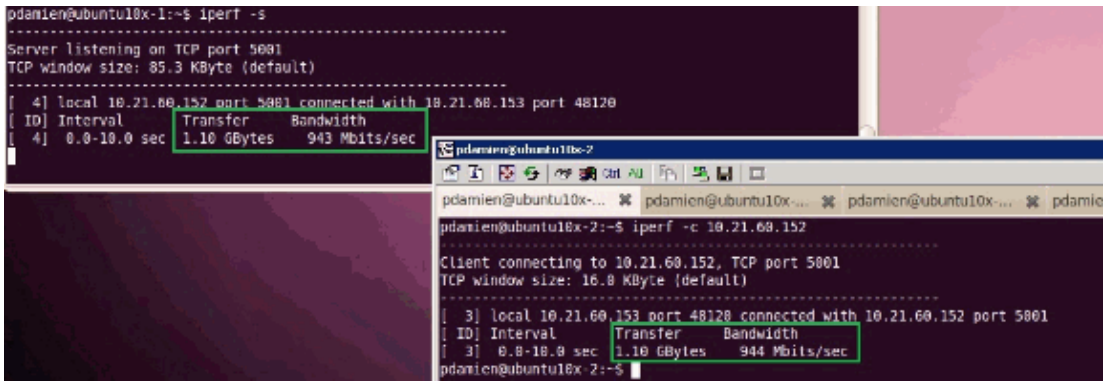


Test Case 3 − Qos Policy web − rate limited at 1000Mbits/sec

On the QOS policy "web" rate limiting has been configured so the port group "web" is throttled at 1000Mbits/sec.

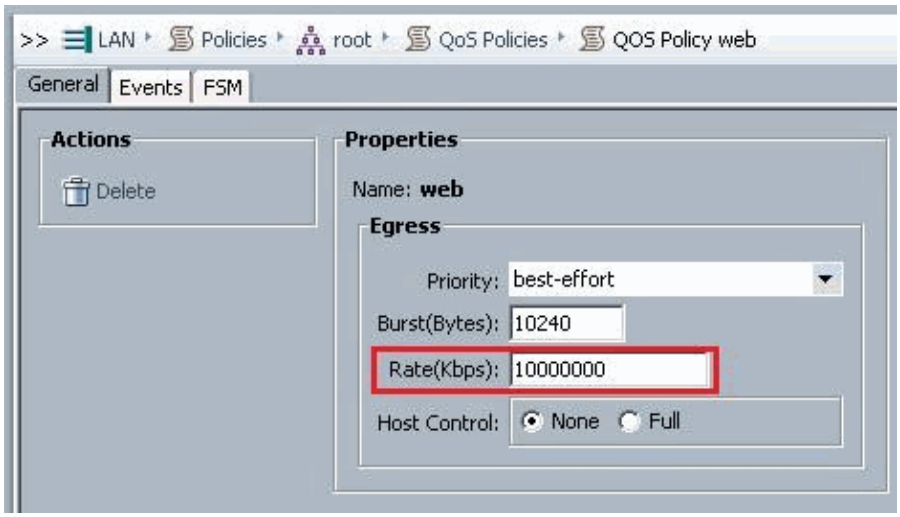


Hosts running iPerf

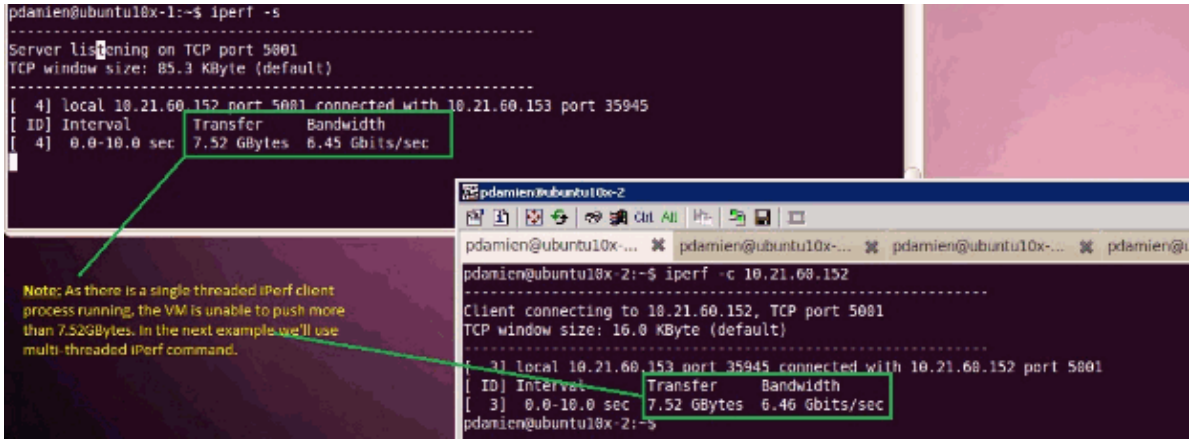


Test Case 4 − Qos Policy web − rate limited at 10000Mbits/sec

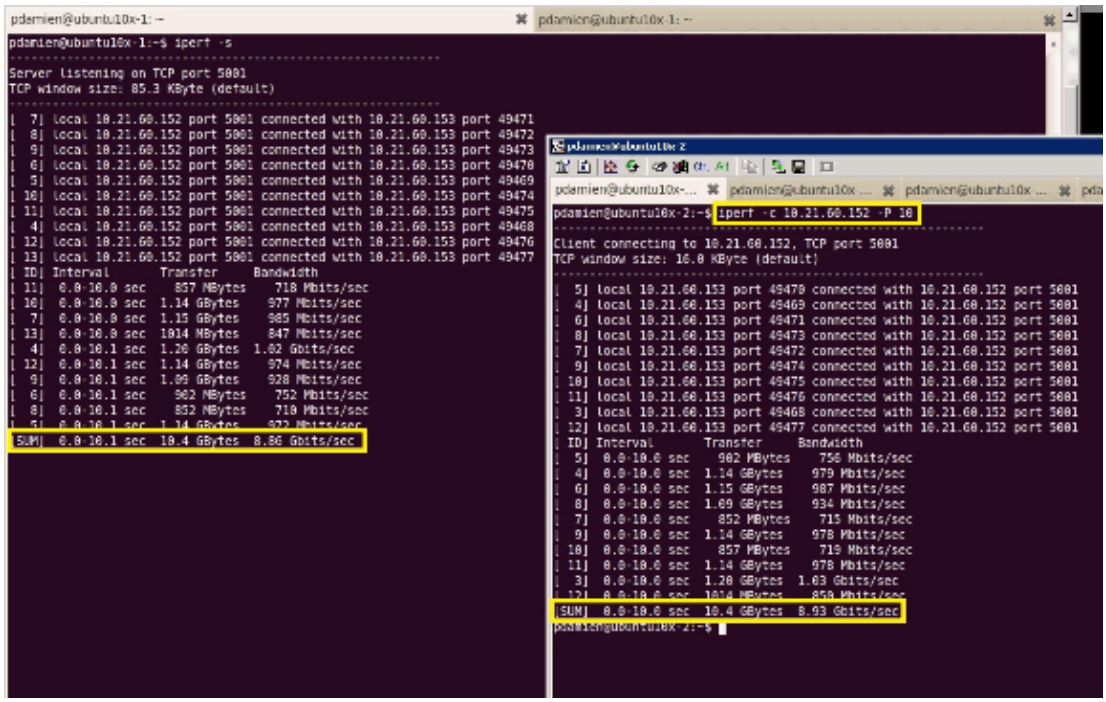
On the QOS policy "web" rate limiting has been configured so the port group "web" is throttled at 10000Mbits/sec.



Hosts running iPerf



iPerf runs with 8 parallel threads and you can see the VM now able to push close to 10GB of network I/O.



Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Introduction to UCS M81KR Virtual Interface Card**
- **Overview of VN Link in Hardware**
- **Cisco UCS M81KR Virtual Interface Card**
- **Cisco UCS M81KR Virtual Interface Card Video Data Sheet**
- **UCS M81KR Whitepaper − Simplify and Enhance Your Virtual Environment**
- **UCS M81KR − Cisco VIC Performance with VMDirectPath**
- **Technical Support & Documentation − Cisco Systems**

Updated: Dec 21, 2010 Document ID: 112140