Configuring VN-Link Components and Connectivity

This chapter includes the following sections:

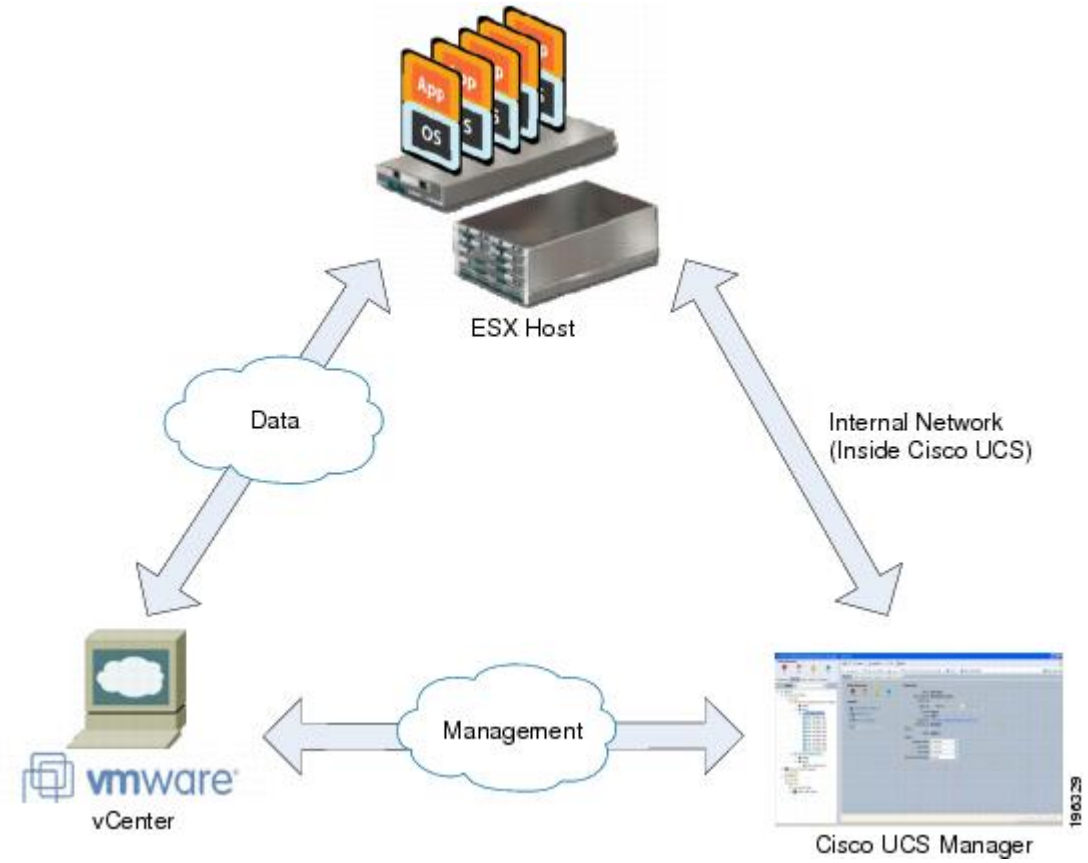
Components of VN-Link in Hardware

The following 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. 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.

The following figure shows the three main components of VN-Link in hardware and the methods by which they are connected:

Figure 1: Component Connectivity for VN-Link in Hardware



Configuring a VMware ESX Host for VN-Link

Before You Begin

Ensure that Virtualization Technology is enabled in BIOS of the UCS server if you intend to run 64-bit VMs on the ESX host. An ESX host will not run 64-bit VMs unless Virtualization Technology is enabled.

Procedure

Step 1 If not already present, install a Cisco M81KR VIC in the server you intend to use as the VMware ESX host. For more information about installing a Cisco M81KR VIC, see the *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.

Step 2 Configure and associate a service profile to the server. The service profile configuration must include the following:

- A Dynamic vNIC Connection policy that determines how the VN-link connectivity between VMs and dynamic vNICs is configured.
- Two static vNICs for each adapter on the ESX host. For ESX hosts with multiple adapters, your service profile must use either vCons or have an associated vNIC/vHBA placement profile that ensures the static vNICs are assigned to the appropriate adapters.

For more information, see the following chapter: Configuring Service Profiles.

Step 3 Install VMware ESX 4.0 or later on the blade server. No additional drivers are required during the installation.

Configuring a VMware vCenter Instance for VN-Link

Procedure

Step 1 Configure a Window-based machine to use a static IP address. Take note of the IP address. You will use it to connect to vCenter Server.
The Windows-based machine must have network connectivity to the the Cisco UCS management port and to the uplink Ethernet port(s) being used by the ESX host. The management port connectivity is used for management plane integration between VMware vCenter and Cisco UCS Manager; the uplink Ethernet port connectivity is used for communication between WMware vCenter and the ESX host.

Step 2 Install WMware vCenter (vCenter Server and vSphere Client 4.0 or later) on the Windows-based machine.

Step 3 Launch vSphere Client.

Step 4 On the vSphere Client launch page, enter the following information to connect to vCenter Server:

a) Static IP address of the Windows-based machine.

b) User name and password specified while installing vCenter Server. During the vCenter Server installation you chose to use the Windows logon credentials, then you can check the **Use Windows session credentials** check box.

Step 5 If a Security Warning dialog box appears, click **Ignore**.

What to Do Next

Do one of the following:

- (Optional) If you plan to use a custom certificate for VN-Link in hardware, configure the certificate for VN-Link in hardware.
- Connect Cisco UCS Manager to VMware vCenter using the extension key.

Configuring a Certificate for VN-Link in Hardware

Certificate for VN-Link in Hardware

Cisco UCS Manager generates a default, self-signed SSL certificate to support communication with vCenter. You can also create your own custom certificate to communicate with multiple vCenter instances. When you create a custom certificate, Cisco UCS Manager recreates the extension files to include the new certificate. If you subsequently delete the custom certificate, Cisco UCS Manager recreates the extension files to include the default, self-signed SSL certificate.

To create a custom certificate, you must obtain and copy an external certificate into Cisco UCS, and then create a certificate for VN-Link in hardware that uses the certificate you copied into Cisco UCS.

Copying a Certificate to the Fabric Interconnect

Before You Begin

Obtain a certificate.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.
Step 2	UCS-A(local-mgmt)# **copy** *from-filesystem:*[*from-path*]*filename* *to-filesystem:*[*to-path*]*filename*	Copies the certificate from its source location to its destination location. For the *from-filesystem:* argument, use one of the following syntax: • **ftp:**//*server-ip-addr* • **scp:**//*username@server-ip-addr* • **sftp:**//*username@server-ip-addr* • **tftp:**//*server-ip-addr* **:***port-num* For the *to-filesystem:* argument, use one of the following syntax: • **Volatile:** • **Workspace:**

The following example uses FTP to copy a certificate (certificate.txt) to the temp folder in the workspace:

```
UCS-A # connect local-mgmt
Cisco UCS 6100 Series Fabric Interconnect

TAC support: http://www.cisco.com/tac

Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
```

```
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License. A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html

UCS-A(local-mgmt)# copy ftp://192.168.10.10/certs/certificate.txt
workspace:/temp/certificate.txt
UCS-A(local-mgmt)#
```

What to Do Next

Create a certificate for VN-Link in hardware.

Creating a Certificate for VN-Link in Hardware

Before You Begin

Copy a certificate to the fabric interconnect.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope vm-mgmt**	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # **scope vmware**	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt /vmware # **scope cert-store**	Enters system VM management VMware certificate store mode.
Step 5	UCS-A /system/vm-mgmt /vmware/cert-store # **create certificate** *certificate-name*	Creates the specified certificate for VN-Link in hardware and enters system VM management VMware certificate store certificate mode.
Step 6	UCS-A /system/vm-mgmt /vmware/cert-store/certificate # **set location** {**volatile** | **workspace**} **path** *path* **certfile** *file-name*	Specifies the location and filename of an existing certificate to use as the certificate for VN-Link in hardware.
Step 7	UCS-A /system/vm-mgmt /vmware/cert-store/certificate # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a certificate for VN-Link in hardware, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope cert-store
UCS-A /system/vm-mgmt/vmware/cert-store # create certificate VnLinkCertificate
UCS-A /system/vm-mgmt/vmware/cert-store/certificate* # set location workspace path /temp
certfile certificate.txt
UCS-A /system/vm-mgmt/vmware/cert-store/certificate* # commit-buffer
UCS-A /system/vm-mgmt/vmware/cert-store/certificate #
```

Deleting a Certificate for VN-Link in Hardware

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A /system # **scope vm-mgmt**	Enters system VM management mode.
Step 3	UCS-A /system/vm-mgmt # **scope vmware**	Enters system VM management VMware mode.
Step 4	UCS-A /system/vm-mgmt /vmware # **scope cert-store**	Enters system VM management VMware certificate store mode.
Step 5	UCS-A /system/vm-mgmt /vmware/cert-store # **delete certificate** *certificate-name*	Deletes the specified certificate for VN-Link in hardware.
Step 6	UCS-A /system/vm-mgmt /vmware/cert-store # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes a certificate for VN-Link in hardware, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope cert-store
UCS-A /system/vm-mgmt/vmware/cert-store # delete certificate VnLinkCertificate
UCS-A /system/vm-mgmt/vmware/cert-store* # commit-buffer
UCS-A /system/vm-mgmt/vmware/cert-store #
```

Connecting Cisco UCS Manager to VMware vCenter Using the Extension Key

(Optional) Modifying the vCenter Extension Key

You can modify the vCenter extension key for the following reasons:

- To provide better system identification, you can name the vCenter extension key something more meaningful than the default ID string.
- If two Cisco UCS instances want to connect to the same VMware vCenter instance, they must use the same extension key and certificate.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 On the **VM** tab, click **VMWare**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Modify Extension Key**.

Step 6 In the **Modify Extension Key** dialog box, do the following:

a) In the **Key** field, modify the key as needed.
A vCenter extension key can have a maximum length of 33 characters. These characters can be letters, numbers, or hyphens. No other characters or spaces are permitted in the extension key.

b) Click **OK**.

What to Do Next

Export the vCenter extension file or files from Cisco UCS Manager.

Exporting a vCenter Extension File from Cisco UCS Manager

Depending on the version of VMware vCenter you are using, you can either generate one extension file, or a set of nine extension files.

Procedure

Step 1 In the **Navigation** pane, click the **VM** tab.

Step 2 On the **VM** tab, expand the **All** node.

Step 3 On the **VM** tab, click **VMWare**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click one of the following links:

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

Step 6 In the dialog box, do the following:

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**.

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

What to Do Next

Register the vCenter extension file or files in VMware vCenter.

Registering a vCenter Extension File in WMware vCenter

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

Before You Begin

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

Procedure

Step 1 In WMware vCenter, choose **Plug-ins ➤ Manage Plug-ins**.

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

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

Step 4 Choose a vCenter extension file and click **Open**.

Step 5 Click **Register Plug-in**.

Step 6 If the **Security Warning** dialog box appears, click **Ignore**.

Step 7 Click **OK**.
The vCenter extension file registers as an available WMware 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.